Зоран Гацовски

БЕЗБЕДНОСТ НА ИНФОРМАЦИОНИ СИСТЕМИ

Скопје, 2007

Гацовски, Зоран
Безбедност на информациони системи, 2007

СОДРЖИНА

ПРЕДГОВОР

Оваа книга е наменета да служи како учебно помагало по предметот Безбедност на информациони системи на Факултетот за информатика, при Европскиот Универзитет. Исто така, може да им послужи на поширок круг читатели, кои се заинтересирани за изучување на информатичката безбедност.

Потребата за криење на информациите датира од многу одамна - уште од пред нашата ера. Прочуен е Цезаровиот шифрер, кој пораките ги претворал во нечитлив текст со едноставно разместување - шифтирање на буквите. Исто така, прочуена е машината Енигма, која Германците масовно ја користеле за шифрирана комуникација во Втората светска војна и која работела на електро-механички принцип (со 3 ротори), но била и една од причините за поразот на Третиот рајх, откако била разбиена од Англичаните (тимот на Алан Тјуринг). Потребата за компјутерска и мрежна безбедност датира од неодамна (од осумдесетите години на минатиот век). Првите компјутерски мрежи биле локални и во академска средина, па постоела голема доверба помеѓу корисниците што биле поврзани со нив (немало безбедносни проблеми). Со наглиот развој на информатичката технологија и сè присутниот Internet, се јавиле и првите злоупотреби, па и потребата за заштита на приватните и корпорациските податоци. Секако - безбедноста е клучна и најмногу доаѓа до израз токму во електронската трговија и е-бизнисот. Ниеден клиент не би купувал online, ако не е сигурен дека "продавницата" не нуди сто-процентна заштита на личните податоци (пред сè - бројот на кредитната картичка).

Во оваа книга се опфатени многу области од компјутерската безбедност. Нивото на книгата е почетно кон средно. Се претпоставува дека читателот има основни познавања од компјутерските мрежи и оперативните системи. Секако дека во рамките на едносеместрален предмет - не може да се покрие целокупната компјутерска и мрежна безбедност. Затоа - во книгава не е навлезено во напредните опции за заштита што ги нудат оперативните системи Windows Server и UNIX/Linux. Нивните концепти и опции можеби ќе бидат предмет на изложување во следните изданија на книгава. Во ова издание најголем акцент е ставен на безбедносните концепти, криптографијата, автентикацијата, безбедноста на компјутерската мрежа, безбедноста на оперативниот систем, апликациите, електронската пошта, протоколите IPSec, SSL и безбедноста на безжичните комуникациски системи. Многу од темите се испреплетени меѓусебно, па криптографијата се споменува во повеќе поглавја, како и автентикацијата, а хакерските напади се застапени во скоро секоја глава, но од различен аспект.

Како и секоја литература од областа на информатичката технологија, и јас се сретнав со инвазијата од англиски поими; некои термини ги преведував (browser=пребарувач, e-mail=електронска пошта), некои термини ги прилагодував (router=рутер, backup=бекап, file=фајл, датотека), додека некои термини ги оставив во оригинал (gateway, firewall, proxy, spoofing, sniffers). За добивање на сеопфатни информации во врска со безбедноста на информатичките системи и симнување на бесплатна литература, можете да се послужите со многубројните ресурси на Internet (линкови се дадени во Користена литература). Би сакал да изразам благодарност на рецензентите на укажаните сугестии со цел за подобрување на ракописот. Во иднина ќе бидат земени во предвид сите забелешки и сугестии, како од страна на студентите, така и од надворешни систем-администратори.

1. БЕЗБЕДНОСНИ КОНЦЕПТИ

Современиот начин на живот, развојот на технологијата и модерните е-бизнис тенденции условуваат глобално поврзување на луѓе и компании од целиот свет. Без разлика дали станува збор за домашен персонален компјутер кој преку модем е поврзан на Интернет, или пак за корпорациска мрежна структура, мрежната комуникација и размената на информации претставуваат основно средство за работа и комуникација помеѓу индивидуи и ентитети. Како таква - комуникацијата е подложна на постојани напади, чија крајна цел е - неовластен пристап до информации и против-правно стекнување на туѓа сопственост.

1.1 ЗОШТО КОМПЈУТЕРСКА БЕЗБЕДНОСТ?

Можеби е апсурдно да се постави прашањето зошто е важна компјутерската и мрежната безбедност, но од пресудно значење е организациите да дефинираат зошто е потребна компјутерска безбедност и како ќе ја постигнат. Компјутерската и мрежната безбедност се важни од следните причини:

1) *Да се заштити компаниската сопственост*: една од примарните цели на компјутерската и мрежната безбедност е заштита на сопственоста. Под сопственост не мислиме само на хардверот и софтверот т.е. компјутерите и мрежата. Сопственоста се состои од информациите што се сместени во компјутерите. Информацијата е витална организациска сопственост и вредност. Компјутерската и мрежната безбедност е засегната пред сè со заштита, интегритет и достапност на информациите.

2) *Да се добие предност пред конкуренцијата*: развивањето и спроведувањето на ефективни сигурносни мерки може да и обезбеди на организацијата предност пред конкурентите. Мрежната безбедност е особено важна во доменот на Интернет финансиските сервиси и е–бизнисот. На пример, колку клиенти би одбрале Интернет банка за која е познато дека системот и е пробиен во минатото. Не многу. Тие би отишле кај конкуренцијата што нуди поголема сигурност.

3) *Да се одговори на потребната регулатива и да се одредат одговорности*: Information Security Officers (ISO) на секоја компанија имаат одговорност да обезбедат сигурност во работата на фирмата. Следствено, фирмите што користат компјутери во својот бизнис, мораат да развијат процедури што се однесуваат на безбедносните потреби. Дел од таа одговорност вклучува и непрекинато функционирање на мрежата. Постојат владини и меѓународни регулативи во поглед на безбедноста. Неуспех да се одговори на владините регулативи може да резултира со затворање на институцијата од страна на надлежните органи. Не ретко компаниските менаџери кои не успеале во имплементација на овие регулативи се сметаат за главни виновници.

4) *Да се задржи работата*: конечно, за да се зачува позицијата во организацијата и да се осигура идното напредување во кариерата, важно е да се спроведат мерки за заштита на сопственоста. Безбедноста треба да е дел од работата на секој системски и мрежен администратор. Неуспех да се одговори адекватно може да резултира со отпуштање. Отпуштањето не е автоматски резултат на безбедносен

крах, но ако по детална анализа се утврди дека неуспехот е резултат на неадекватни полиси и процедури, или неисполнување на процедурите, тогаш менаџментот мора да направи промени.

Битна работа која треба да се запомни е дека мрежната безбедност чини скапо. Скапо чини да се најми, обучи и задржи персонал; да се купи хардвер и софтвер за мрежна безбедност; да се плати за зголемената оптовареност и намалувањето на мрежните и системски перформанси итн. Како резултат на сето ова, мрежната безбедност не е евтина. Но многу е поевтина од загубите кои се јавуваат по евентуален упад во системот.

Потребата од мрежна безбедност е релативно нова. Пред 1980-те повеќето компјутери не биле во мрежа. Тоа не било поради недостаток од желба за умрежување, туку заради недостаток на технологија. Повеќето компјутери биле mainframe или midrange системи и биле централно контролирани и управувани. Терминалите имале ограничени можности. Тогашната поврзаност била потполно различна од сегашната ситуација, каде што илјадници врски однадвор доаѓаат до системот. Во 1980-те, развојот на персоналниот компјутер, развојот на стандардите на мрежниот протокол, падот на цената на хардверот и развојот на новите апликации, придонеле за мрежата да биде прифатена во пракса. Како резултат на тоа LAN, WAN и дистрибуираното компјутерство доживеале неверојатен раст за време на овој период. Кога првпат се појавиле, LAN биле релативно сигурни, бидејќи биле физички изолирани. Обично не биле приклучени на WAN така што нивната издвоеност ги заштитувала мрежните ресурси. Мрежите овозможиле многу системи да делат ресурси, т.е. многу луѓе и организации можеле да бидат поврзани во една мрежа. Повеќе не било потребно да се користи point-to-point конфигурацијата за поврзување. Ситуацијата со безбедноста е значително влошена со поврзување на релативно сигурните LAN со несигурните WAN. Пакетите на една организација се мешаат со пакетите на сите останати. Во оваа околина вниманието било свртено кон обезбедување на лесен пристап и поврзаност. Безбедноста не била толку битна, ако воопшто била и разгледувана. Како резултат на ова, многу системи биле потполно отворени и ранливи за закани кои претходно не ни постоеле.

Интернетот е најголема и најпозната мрежа од овој тип. Интернет користи TCP/IP и бил примарно дизајниран да поврзува компјутери, без оглед на нивните оперативни системи, на лесен и ефикасен начин. Безбедноста не била дел од првичниот дизајн на TCP/IP и имало голем број на јавни напади кои ги искористиле внатрешните слабости на дизајнот. Добро познат настан е Интернет црвот кој го доведе Интернет на колена во 1996 год. Денес, безбедноста е поважна од лесниот пристап.

1.2 БЕЗБЕДНОСНО ТРОЈСТВО: ПРЕВЕНЦИЈА, ДЕТЕКЦИЈА, ОДГОВОР

Трите крака на безбедносното тројство: превенција, детекција и одговор, ги претставуваат основите на мрежната безбедност. Безбедносното тројство би требало да биде почеток за сите безбедносни полиси и мерки што една организација треба да ги применува и развива.

Основа на безбедносното тројство е превенцијата. За да се обезбеди одредено ниво на безбедност, неопходно е да се спроведат мерки за превенција од ранливости. Во развојот на шемите за мрежна безбедност, организациите треба да посветат повеќе внимание на превенцијата отколку на детекција и одговор. Полесно е, поефикасно и многу поисплатливо да се спречи безбедносен упад, отколку да се детектира и одговори на истиот. Невозможно е да се направи безбедносна шема што ќе спречи било каков упад, но фирмите треба да се сигурни дека нивните превентивни мерки се доволно силни да ги обесхрабрат потенцијалните напаѓачи.

Кога ќе се спроведат превентивните мерки, мора да се активираат одредени процедури за детекција на потенцијалните проблеми и безбедносни упади, во случај превентивните мерки да не успеат. Што поскоро се открие проблемот, полесно е да се исправи штетата. Организациите треба да развијат план што ќе претставува соодветен одговор на безбедностниот упад. Планот треба да е во писмена форма и треба да содржи кој е одговорен за кои акции и за различните нивои на безбедност.

1.3 ИНФОРМАЦИОНА БЕЗБЕДНОСТ

Мрежната безбедност е засегната пред сè со заштита на компаниските информациски сопствености. Често го забораваме фактот дека всушност ние се обидуваме да ги заштитиме информациите и можноста за пристап до нив, а не компјутерите и мрежите. Постои едноставна дефиниција за информациона безбедност:

Информациона безбедност = Доверливост + Интегритет + Достапност + Автентификација

Многу важно да се запомни е дека информационата безбедност не е само заштита на информациите од надворешни хакери. Најчесто опасноста доаѓа внатре од организацијата: *"Го пронајдовме непријателот и тоа сме ние"*.

Информационата безбедност се однесува и за процедури и полиси што ги заштитуваат информациониите од несреќи, некомпетентност и природни непогоди. Овие полиси и процедури мораат да се однесуваат на следното:

- Бекапи, конфигурациски контроли и медиски контроли,
- Опоравување од непогоди и планирање во континуитет,
- Интегритет на податоците.

Исто така е важно дека мрежната безбедност не е апсолутна. Секоја безбедност е релативна. Нивото на безбедност за систем или мрежа зависи од тоа каде се наоѓа во спектарот во однос на другите системи. Или е посигурен или е понесигурен во однос на другите системи. Не постои апсолутно сигурна мрежа или систем.

Концептот на проценка на ризикот е решавачки во развојот на пропорционалната одбрана. Да се изведе анализа на ризикот, организациите мора да разберат кои се

можните закани и ранливости. Ризикот е можноста дека ранливоста ќе биде искористена. Основните чекори за проценка на ризикот се:

- Идентификација на ранливости
- Идентификација на закани и нивна возможност
- Идентификација на контрамерки
- Развој на безбедносни полиси и процедури

1.4 БЕЗБЕДНОСНИ МОДЕЛИ

Има три основни приоди користени за развој на мрежниот модел на безбедност. Најчесто, организациите користат комбинација од овие три пристапи за да достигнат одредено ниво на безбедност. Овие три пристапи се: безбедност со прикривање, модел на периметарска одбрана и модел на длабинска одбрана.

Моделот на *одбрана со прикривање* се потпира на тајноста на заштитата. Концептот на овој модел е - ако никој не знае дека мрежата постои, истата нема да биде нападната. Основната надеж е дека криењето на мрежата и не-рекламирањето на нејзиното постоење ќе биде добра заштита. Проблемот е што тајноста не издржува во подолг период, и штом е забележана мрежата - станува потполно ранлива.

Моделот со *периметарска заштита* е аналоген на замок опкружен со вода. Кога се користи овој модел во мрежната безбедност, организациите ги зајакнуваат периметарските системи и гранични рутери, или ја кријат мрежата зад firewall кој ја одделува заштитената мрежа од недоверливата мрежа. Многу не се обрнува внимание на останатите системи во мрежата. Претпоставката е дека периметарската одбрана е доволна да ги стопира сите натрапници така што внатрешните системи ќе бидат сигурни. Има неколку дупки во овој концепт. Прво, овој модел не презема ништо да ги заштити системите од внатрешен напад, а знаеме дека најголемиот број на напади доаѓаат од внатре во организацијата. Второ, периметарската одбрана скоро секогаш попушта. Штом тоа ќе се случи, внатрешните системи се широко отворени за напад.

Најробусниот пристап е да се користи моделот на *длабинска одбрана*. Овој пристап тежи кон безбедност со зајакнување и мониторинг на секој систем, т.е. секој систем е остров кој се брани самиот себеси. Сеуште постојат периметарските системи, но безбедноста на внатрешната мрежа не се потпира само на нив. Овој пристап е потежок да се постигне и бара сите системски и мрежни администратори да го сработат нивниот дел. Дури и ако постои несугурен модем во мрежата, системот со модем ќе биде компромитиран, но другите системи во мрежата ќе можат да се одбранат. Тие исто така ќе можат да откријат обид за упад од компромитираниот систем. Овој пристап исто така обезбедува повеќе заштита против внатрешен натрапник.

1.5 ЗАКАНИ, РАНЛИВОСТИ И ОДБРАНА

Закана е сè што може да го прекине функционирањето, интрегритетот, и достапноста на мрежата или системот. Има различни типови на закани. Има

природни закани, појави како поплави, земјотреси или невреме. Има ненамерни закани кои се резултат на случајни несреќи или глупост. Конечно, има и намерни закани кои се резултат на задни намери. Секој од овие типови на закани може да биде погубен за мрежата.

Ранливоста е составна слабост на дизајнот, конфигурацијата или имплементацијата на мрежата или системот, што ја ослабува заштитата. Повеќето ранливости можат да се пронајдат во еден од овие извори:

- *Лош дизајн*: Хардвер и софтвер системи кои содржат дупки во дизајнот што можат бидат злоупотребени. Во основа, системите се создадени со безбедносни дупки. Пример за ова е sendmail пропустот во првите верзии на Unix. Тој овозможи хакерите да добијаат root пристап до Unix системите. Исто така видливи се многу пропусти во Windows оперативниот систем, кои потоа се надоградуваат со service pack исл.
- *Лоша имплементација*: Системите што се неточно конфигурирани се подложни на напади. Овој тип на ранливост обично резултира од неискуство, недоволна обученост или неодговорна работа. Пример за овој тип на ранливост би бил систем што нема привилегии за ограничен пристап на критичните извршни фајлови и со тоа им се дозволува пристап до фајловите на неовластени корисници
- *Лош менаџмент*: Неадекватни процедури и недоволни проверки. Безбедносните мерки не можат да делуваат во вакум, тие мораат да бидат документирани и надгледувани. Дури и наједноставни работи како дневен backup на системот мораат да бидат верификувани. Постои потреба за распределба на одговорност за некои работи, и поделба на одговорност за други. За ова прашање, организацијата може да се осигура дека се следат процедурите и дека ниедна личност нема тотална контрола на системот.

Иако постојат само три типа на ранливост, тие можат да се манифестираат на повеќе начини. Првото правило за безбедност е физичка заштита на системите и мрежите. Централните хостови и сервери треба да се чуваат во посебни простории во кои можат да влезат само овластени лица. Рутерите и комуникационата опрема исто така треба да се чуваат на сигурни локации со ограничен пристап. Во тој контекст, и важните преносни медиуми како што се backup-ите, треба да се чуваат на безбедносни места со ограничен пристап. Како дел на овој процес, организациите мора да ја земат во предвид физичката и природната околина во која работат. Треба да се земе во предвид можноста од земјотрес, пожар, поплава и други непредвидени несреќи и да се планира соодветно.

Дисковите, лентите и другите медиуми можат да бидат украдени, изгубени или оштетени. Информациите можат да се ископираат и тргнат од организациските сефови незабележано. Соодветно, компаниите мора да ја осигураат безбедноста на сите медиуми што содржат витални информации и да прават редовни бекапи на податоците.

Емисиите на сигнали од антена, можат да бидат далечински пресретнати и надгледувани со користење на софистицирани направи. Организациите исто така треба да се загрижат и за пресретнувањето на повеќето форми на комуникација.

Комуникација е делењето на информација на медиум. Како таква, таа е неизбежно ранлива на пресретнување, мониторинг, провали итн. Секој медиум употребен за пренос на информации може да биде сниман. Мрежните и пакетните прислушкувачи се чести алатки кои можат да читаат проток низ мрежата.

Човечката глупост, невнимание, мрзливост, алчност и бес претставуваат најголема закана за мрежите и системите и ќе направат повеќе штета отколку сите други комбинирано. Уште повеќе, човечката ранливост и ризикот поврзан со нив се најтешки за одбрана. Важно е да се напомене дека секоја мрежа и систем имаат ранливост. Не постои тотално безбедна мрежа или систем. ***Не постои!***

1.6 ДЕФАНЗИВНИ ИНФОРМАЦИОНИ ОПЕРАЦИИ

Дефанзивните информациони мерки често се нарекуваат и информационо осигурување. Информационите операции ги заштитуваат и бранат информациите и информационите системи со обезбедување на нивната достапност, интегритет, автентикација и доверливост. Оваа дефиниција ја дефинира заштитата на инфраструктурата со спречување на неавторизиран пристап или напад (проактивни мерки) и одбрана на инфраструктурата со детектирање, преживување или одговор на нападите (реактивни мерки). Ова осигурување ги вклучува следните компоненти и можности (колективно познати како CIA):

- Достапност (Availability) – сигурност дека информацијата, сервисите и ресурсите ќе бидат достапни и употребливи кога корисникот ќе го побара тоа.
- Автентикација (Authentication) – само авторизираните корисници имаат пристап до податоците и сервисите врз база на следните контроли: авторизација (давање и одземање на правата на пристап), делегација (пренесување на дел од правата на еден ентитет на друг) и автентикација на корисници (доверлива поддршка од корисникот).
- Доверливост (Confidentiality) – го заштитува постоењето на врската, текот на сообраќајот и содржината на информациите од разоткривање пред неавторизирани корисници.
- Реставрација – сигурност дека информациите и системите ќе преживеат напад и дека достапноста може да продолжи по самиот напад.

Информациското осигурување ги содржи традиционалните функции на информациска безбедност (INFOSEC) што е дефинирана на две нивоа. На нивото на полиси, INFOSEC е систем на полиси, процедури и услови неопходни за заштита на информацијата која, ако се подложи на неавторизирано разоткривање, би можела да стори значителна штета. На техничко ниво, INFOSEC вклучува мерки и контроли кои ја заштитуваат информационата инфраструктура од:

- Откажување на услугите (Denial of service, DoS).
- Неавторизирано (случајно или намерно) разоткривање.
- Модификација или деструкција на компоненти на информационата инфраструктура или податоци.

INFOSEC вклучува хардверски и софтверски функции, карактеристики, можности, операциони процедури, контрола на пристап кај централниот компјутер, оддалечени компјутери, физички структури и уреди, персонал и комуникациски контроли потребни за обезбедување на прифатливо ниво на ризик за инфраструктурата и податоците како и за податоците содржани во самата инфраструктура. INFOSEC вклучува четири компоненти во склоп на комуникацискатa сигурност (COMSEC):

- Еманациска сигурност (Emanations security, EMSEC) – контрола на еманацијата која може да ги загрози внатрешните информации.
- Електронска сигурност - заштита која произлегува од мерките дизајнирани да ги заштитат информациите од неавторизиран пристап реализиран со пресретнување и проучување на електромагнетни зрачења (радар, на пример).
- Трансмисиона сигурност (TRANSEC) – заштита на преносот од сигнали, пречки и имитациски измами.
- Криптографска сигурност (COMSEC) – употреба на енкрипција за заштита на комуникациските содржини.

Во последно време, аспектот на набљудливост (способност да се издржат напади и да се одржи функционалноста на одредено ниво на перформанси) е признат за клучна компонента на заштитата која ја пружа INFOSEC и информацискоto осигурување.

1.7 ДЕФИНИРАЊЕ НА БЕЗБЕДНОСНИТЕ КОНЦЕПТИ

Оперативните системи, апликациите и мрежните производи со кои се среќавате обично се сигурни кога се имплементирани на начин што го прецизира произведувачот. Во ова поглавје се опишуваат процесите за да бидете сигурни дека производите што ги користите се максимално безбедни.

Зацврстувањето се однесува на процесот со кој се намалуваат или елиминираат слабостите, се заштитуваат сервисите, и се прави работната околина - имуна на напади. Во ова поглавје, ќе ги изложиме генералните процеси инволвирани за заштита или зацврстување на системите, мрежите и апликациите кои се типични во секојдневната работа. Ова поглавје исто така ги обработува и темите врзани за опасностите кон вашата мрежа како и концептот за развивање на сигурносна основа. Многу од овие теми се тука за ваше запознавање и разбирање, тие не се дел од испитот.

1.7.1 Преглед на заканите за мрежна безбедност

Мрежните закани инволвираат многу аспекти од мрежата и самата организација. Самите знаете дека сите системи и информации се подложни на напади базирани на интерни, екстерни и дизајн фактори на системите кои се одржуваат. Знаејќи дека сите системи и апликации се надградуваат, строгото спроведување и почитување на безбедносните процедури - може да ги намали значително можностите за овие закани. Повеќето од нападите кои се појавуваат кај

програмите како што се Outlook, Outlook Express и Exchange се поправаат штом се откријат.

Како администратор вие морате да ги аплицирате поправките и закрпите веднаш по нивното темелно тестирање во лабораториски услови. Со самото тоа веќе е потешко за напаѓачите да дознаат повеќе за вашите системи и да ги искористат вашите слабости. Една од организациите која ги следи и пријавува безбедносните проблеми е CERT Coordination Center (CERT/CC). CERT/CC е дел од Software Engineering Institute (SEI) стационирана на Универзитетот Carnegie-Mellon. SEI е федерално финансирана истражувачка институција која става силен акцент на истражувањата врзани со безбедноста на компјутерските системи. CERT/CC изложува интересен преглед за развојот на инцидентите поврзани со компјутерите. Табелата 1.1 ја покажува бројката на инциденти поврзани со компјутерски напади пријавени во CERT во периодот 1990 – 2003.

Забелешка: CERT/CC овозможува преглед на голем дел од сегашните анализи на закани и идни анализи во областа на компјутерска безбедност. Интернет страницата на CERT/CC е www.cert.org.

Табела 1.1 – Пријавени CERT инциденти.

Година	**Пријавени инциденти**
1990	252
1991	406
1992	773
1993	1334
1994	2304
1995	2412
1996	2573
1997	2130
1998	3734
1999	9859
2000	21756
2001	52658
2002	82094
2003	137529

Овие бројки вклучуваат инциденти во кои можеби се зафатени еден или стотина сајтови. Иако бројките сами по себе не се големи, растот кој тие го покажуваат е голем. Кога правите евалуација на овие бројки, земете во предвид колку напади и инциденти не се пријавени.

Според CERT, од 1995-та, скоро 13000 безбедносни пропусти се пријавени. Голем дел од тие пропусти се пријавени по 2000-та. Според Интернет страницата на CERT/CC, CERT обработил повеќе од 1.100.000 електронски пораки кои на некој начин биле поврзани со безбедносни теми и закани. Во минатото компјутерската индустрија не ја земаше темата за компјутерска сигурност сериозно колку што требаше. Овој став е причина за големи фрустрации кај дел од корисниците и администраторите кои се трудат да ги заштитат своите добра. Brian Valentine кој е

под-претседател на Microsoft's Corporation Windows Development Team ја опиша ситуацијата во индустријата во говорот кој го оддржа на 5-ти септември 2002-ра на Windows .NET Server Development конференцијата: „Секој оперативен систем кој се наоѓа на пазарот има еднаков број на пропусти", а потоа продолжи „Сите сме за никаде". Важно е да се запомни дека до скоро, многу од производителите на софтвер плаќаа многу малку за проблемите кои оперативните системи и апликациите ги имаа со сигурносните пропусти.

1.7.2 Дефинирање на основите на безбедност

Еден од првите чекори во развивањето на безбедна околина е развивањето на основите на минимална безбедност кои се потребни во вашата организација. Основата го дефинира нивото на безбедност кое ќе биде имплементирано и одржувано. Можете да изберете да поставите *ниска основа* со тоа што ќе имплементирате скоро никакви безбедносни мерки, или *висока основа* која нема да им дозволи на корисниците да прават било какви промени во мрежата или во нивните системи. Во пракса повеќето имплементации спаѓаат помеѓу овие два екстреми. Мора да одредите што е најдобро за вашата организација.

Основата ви овозможува сè што е потребно за дизајнирање, имплементација и одржување на безбедна мрежа. Развивањето на основата вклучува собирање на податоци за специфичните безбедносни имплементации на системите со кои вие ќе работите. Најновиот стандард за безбедност е Common Criteria (CC). Овој документ е плод на заеднички напор на: Канада, Франција, Германија, Холандија, Велика Британија, и САД. Верзијата 2.1 се одликува со опсежни критериуми за евалуација, кои се подделени во 7 нивоа (Evaluation Assurance Levels – EAL). EAL1 – EAL7 сертификатите се опишани подолу.

Забелешка: Информациите во врска со Common Criteria – CC можат да се најдат на CC Интернет страницата: www.commoncriteria.nl. На оваа Интернет страница постои и регистар на продукти кои се CC-сертифицирани.

EAL1
EAL1 примарно се употребува таму каде што корисникот сака да се осигура дека системот ќе работи точно, но заканите за безбедност не се земаат сериозно.

EAL2
EAL2 бара од луѓето задолжени за развој на продуктите, користење на добри дизајнерски практики. Безбедноста не се смета за висок приоритет во EAL2 сертификатот.

EAL3
EAL3 бара совесни напори за развој, за да може да овозможи умерена безбедност.

EAL4
EAL4 бара позитивно безбедносно инженерство базирано на добри комерцијални развојни практики. Се предвидува дека EAL4 ќе биде заедничка референтна точка за комерцијалните системи.

EAL5
EAL5 е со намена да осигура безбедносна имплементација на производите уште во раните дизајнерски фази. Наменет е за високи нивоа на безбедносна гаранција. EAL документацијата покажува дека ќе бидат потребни специјални дизајнерски размислувања за да се постигне ова ниво на сертификација.

EAL6
EAL6 овозможува високо ниво на сигурност и специјализирано сигурносно инженерство. Ова сефтифицирање индицира високи нивоа на заштита против големи ризици. Овие системи ќе бидат со голема сигурност против пенетрирачки напади.

EAL7
EAL7 се користи за екстермно високо ниво на безбедност. Ова сертифицирање бара многу тестирање, мерење и комплетно независно тестирање на секоја компонента.

EAL сертификацијата го замени TCSEC (Trusted Computer Systems Evaluation Criteria) системот за сертификација. Препорачаното ниво на сертификација за комерцијалните системи е EAL4.

Сценарио од вистинскиот живот - имплементација на безбедна серверска околина

Назначени сте во тим кој ќе донесува решенија кои се однесуваат на купување на нов сервер за вашата организација. Новиот сервер треба да биде релативно безбеден и способен за чување на осетливи информации. Исто така ќе биде дел од е-комерц околината. Како можете да му помогнете на тимот?

Вашата помош може да биде во тоа што ќе помогнете во одредувањето на оперативните системи кои се сертифицирани според заедничките критериуми. Можете да ги посетите Интернет страните www.commoncriteria.com, или сестринската страна www.commoncriteria.nl, за да идентификувате кои оперативни системи и продукти се EAL4 сертифицирани. Охрабрете го вашиот ИТ тим своите решенија да ги донесува врз база на податоците за сигурност спротивни од оние на производителите. Повеќето производители тврдат дека имаат сигурни околини иако фактите го покажуваат спротивното. CC-сертификацијата покажува дека трета независна страна подобро ја прави проверката.

Во моментов, само неколку оперативни системи имаат EAL4 ниво. Sun Microsystems, од септември 2002-ра, понуди два EAL4 оперативни системи: Sun Solaris 8 Operating Environment и Sun Trusted Solaris верзија 8.4/01. Оперативниот систем Microsoft Windows 2000 е сертифициран со EAL4+ нивото, но тоа не значи дека вашата индивидуална имплементација на тој систем ќе функционира на тоа ниво. Доколку вашата имплементација не ги користи сите овозможени безбедносни мерки, таа ќе оперира под тоа ниво. Како администратор, вие треба да знаете дека самиот оперативниот систем кој го имате и кој носи одредено

безбедносно ниво со себе не значи дека вашата имплементација е со истото безбедносно ниво. Подолу ќе видите што сè треба да се направи како администратор на Windows 2000 за да постигнете слично EAL ниво.

1.8 МОДЕЛОТ BUSINESS CONTINUITY PLANNING

Business Continuity Planning (BCP) е процес на имплементирање на политики, контроли и процедури кои ќе ги надминат ефектите од загубите, проблемите, и престанувањето на критичните бизнис процеси. BCP е примарно алатка за контролирање, која осигурува критичните бизнис функции (CBF) да се извршуваат кога нормалните бизнис операции се стопирани.

Забелешка: Овој материјал е наменет да овозможи преглед на Business Continuity Planning процес, и е покриен со многу детали. Со други зборови, ако овој материјал го читате само за да го положите испитот, а не за да ви помогне вистински, тогаш овде можете да престанете да читате.

Критичните бизнис функции се однесуваат на процедурите или системите кои мораат да бидат оперативни веднаш штом се појави проблемот. Бизнисот не може да функционира без овие клучни критични безбедносни функции, многу од нив зависат од информациите и бараат пристап и кон технологијата и кон податоците.

Две од клучните компоненти на BCP се Business Impact Analysis (BIA) и пресметка на ризикот. BIA се занимава со проценка на процесите, додека пресметката на ризикот се занимава со проценување на ризикот односно загубата. Потребна е проценка на сите процеси во една организација или претпријатие за BCP да биде ефективна.

1.8.1 Спроведување на Анализата за удар врз бизнисот

Business Impact Analysis (BIA) е процес за проверка на сите критични системи во организацијата за да се одреди ударот и плановите за обнова доколку дојде до загуба. BIA не се грижи за надворешните закани или ранливости, оваа анализа се фокусира на самиот удар и каков би бил тој врз самата организација. Клучните компоненти на BIA ги вклучуваат следниве:

Идентификување на Критичните Функции
За да се идентификуваат критичните функции, компанијата мора сама да се запраша, "Кои функции се потребни за да компанијата продолжи да работи сè до моментот кога комплетниот сервис се врати?" Овој процес на идентификација ќе ви помогне да процените кои системи мораат да се вратат во работен модус за бизнисот да продолжи. Во извршувањето на оваа идентификација, вие можете да откриете дека мала или занемарена апликација може да биде критична за оперативноста. Многу организации ги занемаруваат навидум неважните чекори, процеси или системи кои всушност ја стопираат ефективноста на BCP. Треба да се процени секој оддел за да се осигура дека нема превид кај критичните процеси.

Поставување на приоритети кај критичните бизнис функции
Кога го продолжувате бизнисот после еден таков случај, операциите мора да се подредат според приоритети на есенцијални и не-есенцијални функции. Ако организацијата овозможи ресурси за процесот на опоравување, овие ресурси можат да бидат лимитирани. Понатаму, доколку проблемот бил навистина голем, можеби нема да може да се повратат сите операции подолго време. Што би се случило доколку, на пример вашите сервиси за комуникација паднат? Вие можете да поставите привремени сервиси, но најверојатно нема да можете да ги вратите комплетните опции на мрежата. Морате точно да знаете кои апликации и процеси имаат приоритет поради ресурсите кои ви се на располагање. Вашата компанија можеби ќе треба да го врати системот за електронска пошта пред самиот веб сајт.

Пресметка на временската рамка за загубата на критичните системи
Колку долго може вашата компанија да преживее без критичните функции? Некои функции во компанијата не бараат инстантна акција, некои други бараат. Кои функции треба да се повратат, и во која временска рамка? Ако вашиот бизнис целосно зависи од неговото присуство на Интернет и е ориентиран кон електронската комерција, колку долго вашиот веб сајт може да остане недостапен? Вашата организација треба да процени и да проба да го идентификува максималното време потребно за одредена функција да биде недостапна. Ова го диктира контингентот на процеси кој треба да биде спроведен, за загубите да не го пробијат дозволениот период.

Проценка на директните и индиректните удари врз организацијата
Вашата организација ќе претрпи загуби во нападот. Овие загуби ќе бидат од директна природа, како на пример загуба во продукцијата и загуба во продажбата. Но и индиректната загуба ќе биде фактор. На пример, дали вашите клиенти ќе загубат доверба во вас и во вашите услуги? Вашите откритија на овие ефекти можат во голем дел да ја зголемат свеста на компанијата за тоа - колку навистина загубата на овие сервиси ќе чини.

Темелна BIA ќе постигне неколку работи во вашата компанија. Прво, вистинскиот удар и штета кои ќе бидат предизвикани од нападот ќе бидат видливи. Второ, како заштита, откривањето на вистинските загуби може да ви помогне да барате поголем буџет. Трето и можеби најважно, е процесот кој ќе документира кои бизнис процеси се користени, каков удар имаат тие врз организацијата, и како брзо да ги поврати. BIA ќе има моќ во организацијата кога цената на нападот ќе биде позната. Луѓето купуваат осигурување не затоа што тие планираат да имаат несреќа, туку ако се случи да имаат покритие. BIA ќе ви помогне да откриете какво осигурување е потребно за организацијата да се чувствува безбедно.

1.8.2 Проценка на ризикот

Проценатa на ризикот (исто се вика и анализа на ризикот) примарно ги обработува заканите, ранливостите, и ударите во однос на губењето на информациите или можностите за процесирање на информациите. Секој ризик кој може да се идентификува - треба да се потенцира, опише, и евалуира поради можноста да се појави повторно.

Забелешка: Проценката на ризикот беше спомната погоре.

Главните компоненти на проценатa на ризикот се потенцирани овде:

Ризик на кој организацијата е изложена
Овој чекор дозволува да развиете сценарија кои ќе ви помогнат да процените како ќе ги решавате овие ризици, ако се појават. Оперативниот систем, серверот или апликацијата може да имаат познати ризици во некои околини. Како вашата организација ќе ги решава овие ризици, и како најдобро да се одговори?

Ризик на кој треба да му се посветиме
Проценатa на ризик како процес дозволува организацијата да спроведе реална проверка во која ризиците се реални. Овој процес помага организацијата да ги фокусира своите ресурси кон ризиците кои имаат најголема шанса да се појават. На пример индустриската шпионажа и кражбата се реални и големи ризици, но ризикот група кучиња да го украде платниот список е многу низок. Затоа, ресурсите треба да се лоцираат кон оневозможување на шпионажа или кражба.

Координација со BIA
Проценатa на ризикот во конјункција со BIA, и овозможува на организацијата точна слика за ситуацијата во која се наоѓа. И дозволува на организацијата да донесува интелигентни решенија за тоа како да одговори на различни сценарија.

Сценарио од вистинскиот живот - извршување на проценка на ризик

Од вас е побарано да извршите брза проценка на ризиците со кои вашата компанија се соочува од безбедносна гледна точка. Кои чекори можеби ќе треба да ги спроведете за да развиете преглед на проблемите во вашата компанија?

Треба да ги интервјуирате сите шефови на оддели и вработените за да одредите кои информации според нив имаат потреба од додатна безбедност и кои постоечки ранливости според нив постојат во компанијата. Исто така треба да ги процените серверите за да ги одредите нивните ранливости и како да ги намалите. Додатно, вие треба да бидете сигурни дека ќе извршите физичка проценка на ризиците. Наоружани со овие информации, имате од каде да почнете, и исто така можете да одредите кои мерки би биле потребни за компанијата од гледна точка на проценка на ризик.

Кога правите проценка на ризик, една од најважните работи е поставувањето на приоритети. Не се може да се вага еднакво, поради тоа што некои настани имаат поголема шанса да се случат; исто така, компанијата може да живее со некои ризици, но некои други би биле катастрофални. Еден метод за мерење е annualized rate of occurrence (ARO). Ова често се добива од историските податоци, од настани кои се случуваат во текот на годината. Оваа мерка може да се користи во конјункција со монетарната вредност дадена на податоците за да се пресмета единствениот трошок single loss expectancy (SLE) и годишниот трошок annual loss expectancy (ALE). Кога ќе го пресметувате ризикот, запамтете ја формулата:

SLE x ARO = ALE

Исто така реално можете да очекувате секој SLE да е еднаков на 1000$ и ако има седум појавувања во годината (ARO), тогаш ALE е 7000 $. Ако постои само 10 проценти шанса за настанот да се појави во годината (ARO =0.1), тогаш ALE паѓа на 100 $. Како професионалец за безбедност, вие треба да знаете како да ги пресметате SLE, ALE, и ARO. За дадени било кои од двата броја, можно е да се пресмета третиот. Подолу ќе ги пресметаме ARO, SLE, и ALE во едноставна ситуација.

1.8.3 Равенки за пресметки на ризик

Пример како се пресметува ризикот:

1. Вие сте администратор на веб сервер кој генерира 25.000$ на саат. Веројатноста на веб серверот да падне е пресметана на 25 проценти, и падот би водел кон три саати недостапност и чинење 5000$ во компоненти кои треба да се поправат. Колку е ALE?

SLE е 80.000$ (25.000$ x 3 саати + 5000$) и ARO е .25, па од таму ALE е 20.000$

2. Вие сте администратор во компанија која се занимава со развој, компанијата работи само еден проект во единица време, собирањето на податоците се одвива преку веб на еден сервер. Вредноста на секој развоен проект е обично 100.000$. Во било кое време, натрапник може да гледа не повеќе од 90 проценти на податоците. Просекот на ARO во индустријата е 0.33. Колку е ALE?

SLE = 90.000$ (100.000$ x o.9), ARO = 0.33, па следи ALE = 29.000$

3. Вие работите во одделот за помош на мала компанија. Едно од најчестите барања на кое треба да одговорите е да помогнете да се врати датотека која не-сакајќи била избришана од корисник. Во просек тоа се случува еднаш неделно. Ако корисникот креира, па потоа избрише датотека на серверот (60 проценти од инцидентите), тогаш може да се поврати за најкратко можно време од shadow copy сервисот, па со тоа ретко доаѓа до губење на податоци. Ако корисникот ја користи својата работна станица и тогаш дојде до бришењето (40 проценти од инцидентите), датотеката не може да се поврати, па на корисникот му треба околу два саати да ја рекреира датотеката, а секој саат му се проценува на 12$. Колку е ALE?

SLE = 24$ (12$ x 2), и ARO = 20.8 (52 недели x 0.4) Па така ALE = 499.20 $ (24 $ x 20.8)

1.9 РАЗВИВАЊЕ НА ПОЛИТИКИ, СТАНДАРДИ И ВОДИЧИ

Процесот на имплементација и одржување на безбедна мрежа прво мора да биде поставен од страна на политики, стандарди, водичи. Ова го поставува тонот, авторитетот, и им дава заби на вашите напори. Политиките и водичите поставуваат стандарди за заштита на организацијата. Процесот на развој на овие политики ќе помогне секој во организацијата да биде инволвиран во правењето на успешни планови. Можете да ги замислите политиките како креатори на големата слика на самите теми. Стандардите им кажуваат на луѓето што да очекуваат, а водачите овозможуваат специфични совети за тоа како да се постигне одредена задача или активност. Трите следни секции ги дискутираат политиките, стандардите и водачите кои ви требаат за да ги постигнете вашите безбедносни напори.

1.9.1 Имплементација на политики

Политиките им овозможуваат на луѓето во организацијата водач кон нивното очекувано однесување. Добро напишаните политики се чисти и концизни, тие ги отцртуваат последиците кога тие не се следат. Добрата политика содржи неколку клучни области покрај политиката:

Поента
Добра политика има поента која ги потенцира намерите на политиката и покажува што сака да постигне и кои документи, закони и практики се однесуваат на политиката. Поентата овозможува позадина која ќе помогне читателот да ја разбере политиката и како таа се однесува кон него.

Забелешка: Поентата е секогаш кратка – обично не поголема од една реченица.

Преглед на политиката
Прегледот ја овозможува целта на политиката, зошто е таа важна, и како да се однесува со политиката. Идеално, еден параграф е сè што ви треба за да им дадете на читателите смисол за политиката.

Изјави на политиката
Штом читателот на политиката ќе ја разбере важноста на самата политика, тој треба да е информиран што значи таа политика. Изјавата треба да е чиста и разбирлива колку што е можно повеќе. Политиката може да се презентира во форма на параграф, како листа на точки, или чек листа. Презентацијата ќе зависи од целната група на политиката како и од нејзината природа. Ако политиката е намената да им помогне на луѓето да одредат како да се заклучи зградата на крај од работниот ден, би било од помош да се даде и специфична листа за проверка на чекорите кои треба да се преземат.

Изјава за одговорност

Политиката треба да покажува кој е одговорен за нејзино извршување. Оваа изјава овозможува додатна информација до читателот за тоа - кого да контактира ако се открие проблем. Исто така треба да укажува на последиците кои произлегуваат од не извршување на политиката.

Забелешка: Изјавата за одговорност треба да е напишана со зборови разбирливи за читателот. Ако изјавата за одговорност се прочита пред корисниците, таа треба да е напишана на таков начин да никој не ја напушти собата со различно разбирање за политиката.

Изјава за изземање
Понекогаш, дури и најдобрите политики не ги предвидуваат сите можности. Изјавата за изземање овозможува специфични правила за процедурите или процесите кои мораат да се следат. Ова може да вклучува контакт за ескалација, така што лицето кое е задолжено за ситуацијата - да знае кого да контактира.

Процесот на развивање на политики понекогаш одзема многу време. Предноста на овој процес е дека овие решенија можат да бидат донесени однапред и можат да им се пратат на сите инволвирани страни. Со тоа се избегнува рекреирање на политиките одново и одново. Всушност, формалното развивање на политиките штеди време и овозможува структура: вработените, наместо да пробуваат да откријат што да направат, тие ќе знаат што да прават.

1.9.2 Обединување на стандардите

Стандардите се однесуваат на специфични теми или аспекти на бизнисот. Стандардите се извлекуваат од политиките. Стандардот треба да овозможи доволно детали кои ќе се проверат па со тоа се оценува дали стандардот е исполнет или не. Стандардите како и политиките, имаат одредени заеднички структурни аспекти. Следниве неколку точки се клучни аспекти кај стандардите:

Област и цел
Стандардот треба да ја објасни својата намера. Ако стандардот е развиен за техничка имплементација, областа може да вклучува софтвер, надградба, додаток и друга битна информација која помага имплементаторот да ја изврши својата задача.

Улога и одговорности
Оваа секција покажува кој е одговорен за имплементација, мониторирање и одржување на стандардот. Во системската конфигурација, оваа секција покажува *што* клиентот треба да постигне, а *што* инсталаторот. Ова не значи дека едниот или другиот треба да ги надминат своите улоги, тоа значи дека во случај на забуна, јасно е кој е одговорен за извршување на кои задачи.

Референтни документи
Оваа секција објаснува како стандардот се поврзува со различните организациски политики, па така стандардот поврзува линии со политиките кои се поставени на свое место. Доколку дојде до забуна или несигурност, им дозволува на луѓето да се вратат кон изворот и да откријат што значи самиот стандард. Ќе се сретнете со

многу ситуации низ вашата кариера каде што дадените стандарди немаат смисол. Фреквентно, со враќање кон полисите, вие можете да откриете зошто се стандардите напишани како што се напишани. Правењето на тоа само ви помага да ги извршите стандардите или да ги информирате луѓето одговорни за стандардот, за промената или проблемот.

Критериуми за перформанси
Овој дел од документот оцртува што или како да се постигне некоја задача. Треба да вклучува релевантни основи и технолошки стандарди. Основите овозможуваат минимум или стартна точка за самиот стандард. Технолошките стандарди овозможуваат информации за платформите и технологиите. Основните стандарди ги покажуваат високите нивоа за стандардот или технологијата.

Забелешка: Важна мерка за перформансите е бенчмаркот. Треба да дефинирате што ќе биде мерено и метриката која ќе биде употребена.

Ако сте одговорни за инсталација на сервер на надворешна локација, стандардите кажуваат каков компјутер ќе се користи, кој оперативен систем ќе се постави, и сите други битни спецификации.

Барања за одржување и администрација
Овие стандарди потцртуваат што е потребно за да се одржува и администрира системот или мрежата. Во случај ако е потребно физичко обезбедување - фреквенција на промена на брави или промена на комбинации.

Како што можете да видите - документираните стандарди овозможуваат постоење на механизам за новите и постоечките стандарди да бидат проверени за комплементарност. Процесот на проверка се вика аудит - следење; од организациите сè повеќе се бара да извршуваат редовно аудит - и на нивните стандарди и политики.

1.9.3 Следење на водичи

Водичите се нешто поразлични од политиките и стандардите. Тие помагаат во имплементација и одржување на стандардите со овозможување на информација како да се постигнат политиките и како да се одржат стандардите. Водичите можат да бидат помалку формални од политиките и стандардите, поради тоа што природата на овие документи е да овозможи помош на корисниците во работа со политиките и стандардите. Пример, можеби, е објаснувањето како да се инсталира сервисен пакет и кои чекори да се преземат пред самата инсталација. Водичите не се тврди и брзи правила. Тие кажуваат како чекор по чекор да се постигне задачата. Водичите, како стандардите и политиките треба да содржат позадинска информација која треба да помогне задачата да се изврши. Следните четири теми се минимум содржини за добар документ-водич:

Област и цел
Областа и целта овозможуваат преглед и изјава за намерата на водичот.

Улоги и одговорности
Оваа секција покажува која индивидуа или оддел се одговорни за постигнување на специфична задача. Ова може да вклучи имплементација, поддршка, и администрација на системот или сервисот. Во голема организација, веројатно единките инволвирани во процесот ќе имаат различни нивоа на тренинг и искуство. Од безбедносна перспектива, може да биде уништувачко, ако неквалификуван техничар го инсталира системот без водич.

Водички изјави
Овие изјави овозможуваат чекор по чекор инструкции за тоа како да се постигне специфична задача во специфичен дух. Повторно, ова се водичи - тие не мора да бидат тешки и брзи правила.

Оперативни замисли
Оперативните замисли кај водичите ги специфицираат и идентификуваат должностите кои се бараат и во кој интервал се бараат истите. Оваа листа може да содржи дневни, неделни и месечни задачи. Водичите за системски бекап може да овозможат водич за тоа - кои датотеки и директориуми мораат да се бекапираат и колку фреквентно.

Водичите помагаат во организацијата на неколку различни начини. Прво, ако процесот или сетот од чекори не се преземат рутинирано, искусните специјалисти за поддршка и безбедност ќе забораваат како да ги направат. Водичите ќе ја освежат нивната меморија. Второ, кога пробувате да тренирате некого за да направи нешто ново, напишаните водичи можат да ја подобрат линијата на учење. Трето, ако се појави стресна или кризна ситуација - водичите можат да помогнат да не дојде до паника.

1.9.4 Работење со Безбедносните стандарди и ISO 17799

Многу компании ги усвојуваат компликуваните безбедносни стандарди за нивните организации. Ако вашата организација е инволвирана во работа со владата, стандардот е најверојатно веќе постигнат и вие треба само да го следите. Последиците можат да бидат опасни ако не се следат политиките.

Потребата за безбедносни стандарди е препознаена на светско ниво. Еден од безбедносните стандарди кој добива на прифатеност е ISO 17799. Во продолжение накратко е опишан овој стандард. Интернационалната Организација за Стандардизација (ISO) го публикуваше ISO 17799 стандардот кој се нарекува и како "Код на практики за менаџментот со информации". Последната верзија на стандардот беше публикувана во август 2000-та. ISO 17799 ги идентификува главните чекори потребни за безбедна IT околина.

Забелешка: Овој материјал ви е овозможен само како позадина. Нема да бидете тестирани за ISO 17799 стандардот. Информацијата за ISO 17799 е достапна во пишана форма и на интернет. Добро место за да добиете повеќе информации е www.securityauditor.net/iso17799/.

Стандардниот документ потцртува 6 области. Организација која успешно ќе го комплетира сето таму напишано - може да се пријави за сертификација. Се повикуваат аудитори да ги верификуваат покриените области, секој аудит (следење) е темелен и бара напредни подготовки.

Еве ги 6-те области:

Безбедносна политика
Безбедносната политика вклучува процес на евалуација на очекувања, и го демонстрира менаџментот, поддршката и посветеноста на безбедноста. Безбедносните политики се дискутираа погоре.

Безбедносна Организација
Организацијата има структура која е одговорна за безбедност. Ова ги вклучува безбедносните координати, потребното делегирање на менаџмент и процесите за одговор на инциденти.

Класификација на сопственост и контрола
Оваа област се однесува на инвентарот на компанијата кој е дел од компјутерската инфраструктура и одредување на потребната безбедност на самите уреди.

Развој на системите и одржување
Оваа област ги проверува мерките превземени во делот на системскиот развој и одржувањето на софтверот, вклучувајќи ги тука поставувањето на мрежата и нејзиниот развој.

Business Continuity Management (BCM)
Оваа област ја испитува моќта на организациските планови за справување со природни катастрофи и со катастрофи предизвикани од човекот. Фокусот овдека е на опоравувањето и како ќе се дојде до него - ако се случи такво нешто.

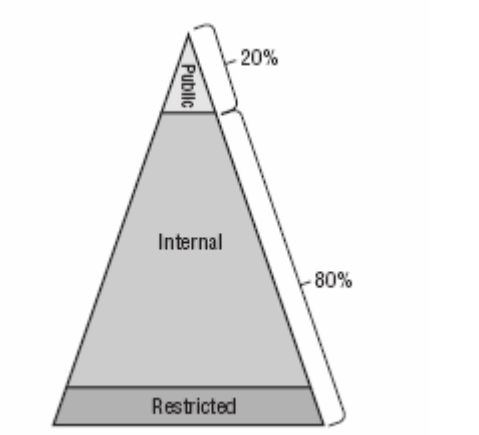
Одговарање
Оваа област испитува колку добро организацијата одговара на регулаторните и легалните барања. Ова исто ја проверува и соодветноста со интерните политики за приватност.

Кога ISO 17799 стандардот беше претставен во 1995-та, тој не го доби првобитното прифаќање; многу во индустријата не чувствуваа дека е доволно темелен за да биде сериозен стандард. Критиките на стандардот одеа на страна дека оваа сертификација е ориентирана кон давање на совети, а не кон овозможување на точен процес на сертификација. Оваа тема е една од главните на која и е пристапено во подоцнежните ревизии на самиот стандард. Верзијата од август 2000-та е прифатена секаде низ светот. Дури и ако вашата организација сака да се стандардизира според овој стандард, ова е корисно место за почеток на развојот на документите за самостојна акредитација.

1.10 КЛАЦИФИЦИРАЊЕ НА ИНФОРМАЦИЈАТА

Класифицирањето на информацијата е клучен аспект на сигурна мрежа. Повторно, процесот на развој на шема за класификација е како техничка, така и човечка тема. Технологиите кои ги користите мораат да ги поддржуваат потребите за приватност на вашата компанија. Луѓето и процесите мораат да се на точно определено место и да работат ефективно за да спречат неавторизиран пристап до битните информации.

Ако мислите на сите информации што ги чува вашата организација, најверојатно ќе откриете дека можете да ги поделите во три примарни категории: јавно користени, внатрешно користени и рестриктивно користени. Сликата 1.1 покажува типичен сооднос на поделбата на информациите. Ќе забележите дека 80 проценти од информациите во вашата организација се за интерна или приватна примена. Овие информации можат да вклучат меморандуми, работни хартии, финансиски податоци и информациони записи, покрај другото.



Сл. 1.1: Категории на информации

Во следните секции ќе дискутираме за разните модели на квалификација на информациите, улогите во безбедносниот процес и контролите за пристап до податоците.

Забелешка: Нема да ве испрашуваме за податоците од овој дел. Но од практична гледна точка треба да ви се познати овие теми.

1.10.1 Јавна информација

Јавната информација е примарна информација која е достапна до поголемите јавни или посебни индивидуи кои имаат потреба од истата. Финансиските изјави на приватните организации можат да бидат јавно достапна информација, но само ако одредени индивидуи или организации имаат потреба за тоа. Важна работа која не смее да се заборави е дека организацијата треба да развие политики за тоа - која информација е достапна и за која улога таа ќе биде достапна. Исто така, помага да се запознаат членовите на организацијата, кој има авторизација да донесува вакви одлуки. Постојат организации кои собираат битни

информации за надоместок, тие често го користат пристапот социјално инженерство за да добијат информации за бизнисот. Добрите политики ќе спречат несреќи од губењето на осетливи податоци. Следните секции ги објаснуваат разликите помеѓу лимитираните и комплетните дистрибуции.

1.10.2 Лимитирани дистрибуции

Лимитираната дистрибуција на информацијата не е наменета за објавување во јавноста. Оваа категорија на информација не е тајна, туку е приватна. Ако компанијата бара кредит, информацијата е приватна. Оваа информација ако се даде на конкуренцијата може да им даде внатрешни информации за плановите на организацијата. Оваа информација ако им стане достапна на клиентите, таа може да ги исплаши и да ги натера да прејдат кај конкуренцијата.

Забелешка: Некои договори со крајните корисници (EULA) ја ограничуваат информацијата која корисниците можат да ја добијат за проблемите со нивниот софтвер. Овие нови изјави уште не се потврдени на суд. Пробајте да избегнете да бидете тест случај за овој нов елемент кај некои нови софтверски лиценци. Прочитајте ги EULA договорите пред да се согласите на нив.

Овие типови на откривање обично се чуваат во тајност од страна на банките и финансиските институции. Овие институции типично имаат правила за приватност, како и политики кои треба да се следат од вработените на институцијата.

Производителите на софтвер типично пуштаат рани верзии на нивните продукти на своите клиенти кои сакаат да помогнат во евалуацијата на функционалноста. Овие рани верзии на софтвер не секогаш работат исправно и некогаш ги немаат сите функции кои се вклучени во финалната верзија. Овие верзии на софтверот се викаат beta test. Пред бета тестерите да добијат дозвола за користење на софтверот, тие треба да потпишат договор за неоткривање на информации (NDA). Овој договор му кажува на тестерот кои потреби за приватност постојат кај овој продукт. Продуктот кој се развива ќе се менува, и проблемите од бета верзиите најверојатно нема да бидат голема тајна. Но сепак, NDA останува како одговорност.

Забелешка: NDA е позната во технолошката арена. Прочитајте ги NDA договорите темелно пред да ги потпишете. Не морате да ги потпишете NDA договорите за да бидете обврзани со нив, ако прифатите дека ќе ја третирате информацијата како приватна и тогаш кога ја примате информацијата, во суштина сте ја прифатиле NDA. Во повеќето случаи - овој тип на NDA е валиден една година.

Изјавите кои индицираат приватност се документи со лимитиран пристап. Овие изјави треба да покажат дека оддавање на овие информации без дозвола е кршење на доверливоста. Ова може да помогне - некој да се сети што е, а што не е информација за јавно делење.

1.10.3 Целосна дистрибуција

Маркетинг материјалите се пример за информација која има целосна можност за дистрибуција до секого кој ја бара. Годишните извештаи на акционерите и другите информации од јавен карактер се исто така примери на материјал за целосна дистрибуција. Клучниот елемент на целосната дистрибуција инволвира донесување на решенија и одговорност. Кој ги носи решенијата за целосна дистрибуција? Поголемите организации имаат корпоративен оддел за комуникација кој е одговорен за процесот. Ако не сте сигурни, добро е да прашате за делењето на информацијата. Не претпоставувајте дека знаете. Ова е и целта на политиката за класификација на информации.

1.10.4 Приватни информации

Приватните информации се наменети само за интерна употреба во организацијата. Овој тип на информација може да ја засрами компанијата, да открие тајни договори или да влијае на самиот персонал. Приватните информации исто така се нарекуваат и работни документи или работен продукт. Многу е важно приватната информација да не биде покажана, поради тоа што потенцијално тоа може да инволвира судски спор (ако покажувањето на информацијата не било според закон). Можете повеќе да научите за разликата помеѓу интерните и рестриктивните информации во секциите кои следат.

1.10.5 Интерна информација

Интерните информации вклучуваат персонални информации, финансиски документи, листи на клиенти и било кои други информации кои се потребни за водење на бизнис. Овие информации се вредни и мораат да бидат заштитени. Во случај лични и медицински информации да бидат покажани на неавторизиран персонал, доаѓа до повик на одговорност. Многу организации не сакаат да направат нешто повеќе од самата верификација на вработените, па поради тоа се плашат од неавторизиран пристап. Школите гледаат на студентските информации како на интерни информации. Школите не можат да дадат информации за студентите без специфична дозвола од студентот.

1.10.6 Рестриктивна информација

Рестриктивните информации можат сериозно да ја оштетат организацијата ако се објават. Тоа ги вклучува сопствените процеси, тајни на трговијата, стратегиски информации и маркетинг планови. Овие информации никогаш не треба да се објават на надворешен субјект, освен ако менаџментот не даде специјална дозвола. Во многу случаи - овој тип на информација поставен е исто како моделот на ’потребно знаење’ - односно ако не треба да го знаете тоа, нема да бидете информирани.

Воени и владини класификации

Американската влада и војската имаат нешто различен збир на термини во врска со класификацијата на информацијата. Владините агенции се многу загрижени за приватноста и националната безбедност. Поради ова, единствен систем на класификација и контрола на пристап е имплементиран за заштита на информациите. Следи листата на некои типови на владини класификации:

Некласифицирани
Оваа класификација се користи да прикаже дека информацијата нема ризик за потенцијална загуба при обелоденување. Секој може да има пристап кон информациите од оваа категорија. Многу упатства за тренирање и правила се некласифицирани.

Осетливи, но некласификувани
Оваа класификација се користи кај ниското ниво на безбедност. Значи дека обелоденување на оваа информација може да донесе зло, но нема да им наштети на напорите за национална безбедност. Количеството на тоалетна хартија што се користи во воена база може да се смета за сензитивно, поради тоа што оваа информација може да помогне агенција за разузнавање да погоди колку луѓе работат во базата.

Доверливо
Оваа класификација се користи за да ги идентификува тајните од ниско ниво, ова генерално претставува најниско ниво на класификација кое се користи од страна на војската. Се користи често - за да оневозможи пристап до осетливите информации. Информациите кои се на пониско ниво од Доверливо - генерално се сметаат за некласифицирани. Доверливо, дозволува оваа информација да биде со рестриктивен пристап под Актот за Слобода на Информацијата. Потребите за одржување на пушка може да биде класифицирана како Доверливо. Оваа информација има цртежи, процедури и спецификации како оружјето работи.

Тајна
Тајните информации, ако се обелоденети можат да донесат сериозни и непоправливи штети на одбранбените напори. Информацијата која се квалификува како Тајна бара специјално тренирање и чување. Информацијата се смета за чувана тајна на војската и владата. Движењето на трупите, можностите и другите планови - минимално се класификуваат како Тајна. Воените правила го сметаат неавторизирано обелоденување на Тајните информации за криминален акт и потенцијално предавство.

ТОП Тајна (Top secret)
Оваа класификација е највисоко ниво на класификација. Постојат озборувања дека постојат и повисоки нивоа на класификација, но имињата на тие класификации се исто така класифицирани како ТОП Тајна. Овој дел на податоци не смее да биде компромитиран. Информациите како активности на агенцијата на разузнавање, нуклеарни воени планови, и системи за оружје и развој на истите - нормално се класификува како ТОП Тајна.

Владата исто така развива процес за преглед и намалување на класификациските нивоа на регуларни нивоа. Овој процес генерално ги деградира информациите врз база на старост, сензитивност и корисноста. Постојат методи за пребришување на овој процес, кој превентивно би делувал информациите да не бидат декласифицирани. Некои тајни е најдобро да останат тајни.

Војската исто користи додатни методи за класифицирање на информацијата и пристапот, кој има ефект на ставање на информацијата во кутии. На пример, ако развивате оружје, нема да ви треба информација од шпиунските сателити. Значи ви се дава пристап само до информацијата која ви е потребна за посебниот проект на кој работите. Кога овие проекти ќе завршат - пристапот кон овие информации ви се забранува. Овој процес дозволува информацијата да биде заштитена и пристапот да биде лимитиран на need to know база.

Процесот на добивање на безбедносна дозвола за воен или владин партнер - може да биде доста долг и обемен. Нормално тие ве истражуваат вас, фамилијата и потенцијално било кој, кој може да ве стави во компромитирачка позиција. Процесот може да трае со месеци, и тој инволвира агенти кои на терен ќе ја завршат истрагата.

1.10.7 Улоги во безбедносниот процес

Ефективниот безбедносен менаџмент бара поставување на чисти улоги и одговорности за секој кој е инволвиран во процесот. Во продолжени се опишани улогите во безбедносниот процес:

Сопственик
Сопственикот на податоците е примарно одговорен за поставувањето на заштитата и користењето на податоците. Сопственикот во повеќето ситуации, е постар менаџер или друг донесувач на одлуки во организацијата. Сопственикот е одговорен за поставувањето на системот - за секој да може да ги следи сите релевантни и потребни закони и правила. На крај, сопственикот обично делегира некоја или сите ролји поврзани со податоците и со другите индивидуи во организацијата.

Чувар
Чуварот на податоците е одговорен за одржување и чување на податоците. Во компјутеризирана околина, чуварот е обично IT одделот. Мрежните администратори, бекап операторите и другите, ги спроведуваат чуварските функции врз податоците. Безбедносните политики, стандардите, и водичите треба да ги дистрибуираат одговорностите и да ги дадат механизмите за нивна работа.

Корисник
Корисникот е личност или оддел кој ги користи податоците. Корисниците на податоците можат да прават влез, излез, едитирање и други функции, што се дозволуваат од страна на улогите кои ги имаат во процесот.

Постојат две додатни улоги, кои тука само ќе ги објасниме во кратки црти, поради тоа што можете да се сретнете во пракса:

Професионалец за безбедност
Безбедносните професионалци се запознаени со еден или повеќе аспекти од процесот. Тие можат да бидат истражувачи, имплементатори, тестери, или развивачи на политики. Истражувачите стануваат инволвирани во процесот кога безбедносниот проблем ќе се идентификува. Тестерите, од друга страна - можат да се повикаат да ги проверат искористувањата, или да ги тестираат безбедносните процеси или слабости. Развивачите на политиките му помагаат на менаџментот да развие и имплементира политики за организацијата.

Забелешка: Безбедносните професионалци често налетуваат на информации кои тие нормално не треба да ги знаат. Дискрецијата е критична вештина за безбедносните професионалци. На пример, може да ве прашаат да негирате постоење на одредена информација во организацијата. Ова имплицира релација на доверба која не треба да се земе здраво за готово.

Аудитор
Аудиторите се инволвирани во процесите на осигурување на практиките, политиките, механизмите и водичите кои постојат во самата организација. Оваа функција може да инволвира прегледување на документацијата, прегледување на дневниците на активностите, вршење на интервјуа, и вршење на голем број други задачи кои се потребни за да се осигура следењето на организациските безбедносни политики. Улогата на аудиторот не е таа како на полицаецот, но е повеќе консултантска. Аудиторот може да помогне - организацијата да ги идентификува и поправи проблемите со безбедноста.

Секоја од овие улоги презентира специјален предизвик и ве изложува на информации и процеси, на кои повеќето индивидуи во организацијата не би налетале. Многу е важно да ги сфатите овие одговорности сериозно, не треба да ја користите информацијата или процесите за да откриете неавторизирани индивидуи. Морате да се држите на повисоко ниво од тие кои ве опкружуваат.

1.11 КОНТРОЛИ ЗА ПРИСТАП НА ИНФОРМАЦИИТЕ

Контролите за пристап ги дефинираат методите кои се користат за да се осигурате дека - корисниците на вашата мрежа можат само да пристапат таму каде што се авторизирани. Овој процес на контрола на пристап треба да биде поставен во организациските безбедносни политики и стандарди. Неколку модели постојат за постигнување на тоа. Оваа секција накратко ќе ги објасни следниве модели:

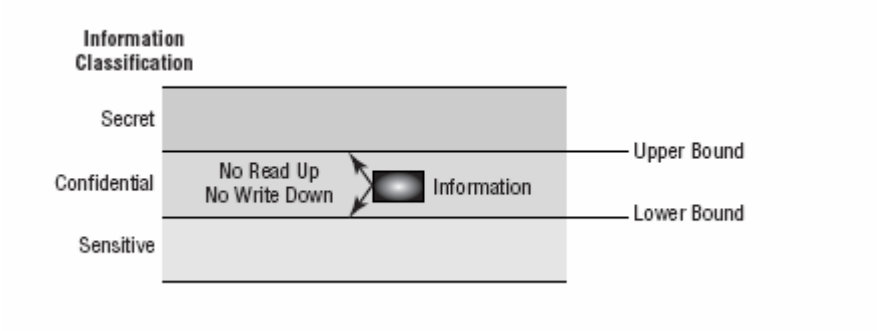
- Bell La-Padula
- Biba
- Clark – Wilson
- Information Flow Model
- Noninheritance

1.11.1 Bell La-Padula

Овој модел е дизајниран за војската, и навлегува во чувањето на податоците и заштитата на класифицирана информација. Моделот е специјално дизајниран да забрани неавторизиран пристап до класифицирана информација. Овој модел му забранува на корисникот да пристапи до информацијата која има повисок безбедносен рејтинг. Моделот исто така забранува запишување на информацијата на пониско ниво на безбедност. На пример, ако сте авторизирани да пристапувате кон *тајните* информации, вие не се авторизирани да пристапувате до ТОП тајните информации; исто така не ви е дозволено да запишувате во системот со ниво пониско од нивото *тајна*. Овој процес е прикажан на сликата 1.2. Забележете дека на сликата не можете да читате горе и да запишувате доле. Ова значи дека корисник не може да чита информација од повисоко ниво од авторизираното. Лицето кое запишува датотека не може да запише доле, кон пониското ниво на безбедност, од она што го поседува во моментот.

Процесот на забрана на пишување на пониско ниво од авторизираното, го спречува корисникот да направи дупка во безбедноста со запишување на тајна информација во следното пониско ниво, *доверливо*. Во вашиот пример можете да читате доверливи информации, но штом ви е дозволено нивото Тајна вие не можете да пишувате на нивото Доверливо. Овој модел нема ништо со интегритетот на податоците, туку само со доверливоста. За да видите како овој модел работи, мислете на корпоративните финансиски информации. Главниот финансиски офицер (CFO) има финансиски информации за компанијата што треба да ги заштити. Bell La-Padula моделот ќе го заштити од несакано постирање на информацијата на ниво на пристап помало од неговото и со тоа ќе оневозможи неавторизиран пристап и разоткривање на осетливи информации. Вработените кои имаат пониско ниво на пристап нема да можат да пристапат до овие информации поради тоа што не можат да читаат на исто ниво како и CFO.

Забелешка: Главната работа кај Bell La-Padula моделот е дека тој се поврзува со секој пристап, дозволувајќи го или недозволувајќи го.



Сл. 1.2: Моделот Bell La – Padula

1.11.2 Biba модел

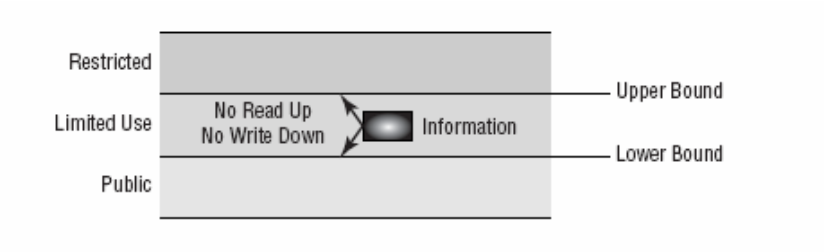
Овој модел е дизајниран после Bell La-Padula моделот. Biba моделот концептуално е сличен со Bell La-Padula моделот, но повеќе се занимава со интегритетот на информациите, област која во Bell La-Padula моделот воопшто не се споменува. Во овој модел нема пишување горе или читање долу. Накратко ако ви е доделен пристап до ТОП Тајна информациите - не можете да читате од *тајна* информациите или да пишувате на било кое ниво повисоко од нивото за кое сте авторизирани. Ова ги чува информациите од повисоките нивоа чисти - со спречување помалку битните информации да се замешаат со нив. Сликата 1.3 го покажува концептот подетално. Овој модел првенствено е развиен за индустриско користење, каде што доверливоста е помалку важна од интегритетот на податоците.

Помислете за податоците кои се генерирани од некој истражувач за научен проект. Истражувачот е одговорен за менаџирање на резултатите од истражувањето кое се одвива на пониско ниво на пристап, а тој треба да ги внесе податоците во своето истражување. Ако лоши податоци влезат во неговиот проект - целото истражување ќе биде уништено. Со овој модел такво нешто не може да се случи. Истражувачот нема да има пристап кон информациите од пониските нивоа. Таа информација прво треба да биде промовирана на ниво на истражувачот. Овој систем ќе ја чува информацијата на истражувачот недопрена и ќе спречи случајни грешки.

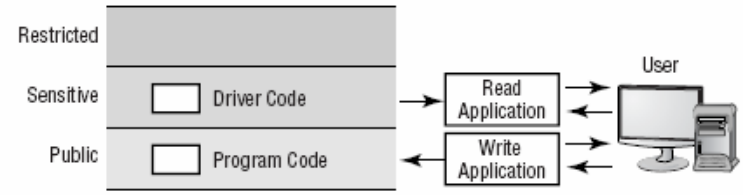
Забелешка: Biba Моделот се разикува од Bell La-Padula моделот во имплементацијата на нивоата на интегритет кое дозволува информациите да одат надолу, а не нагоре.

1.11.3 Clark – Wilson Модел

Овој модел е развиен по Biba моделот. Пристапот е малку различен од оној на двата претходни. Во овој модел, на податоците не може да им се пристапи директно: Мора да им се пристапи преку апликации кои имаат предефинирани можности. Овој процес спречува појавување на неавторизирани модификации, грешки и измама. Ако корисникот има потреба да пристапи до одредена информација која е на одредено ниво на безбедност, специфична програма се користи. Оваа програма може да дозволи право само на читање на информацијата. Ако корисникот има потреба од менување на податоците, треба да се користи друга апликација. Ова дозволува поделба на задолженијата, со тоа што на единките им се дозволува пристап само на алатките кои им се потребни. Сите трансакции имаат асоцирани аудит датотеки и механизми кои пријавуваат модификации. Сликата 1.4 го покажува процесот. Пристапот до информациите се добива со користење на програма која се специјализира за менаџмент на пристап. Ова може да биде единствена програма која го контролира целосниот пристап, или сет од програми кои го контролираат пристапот. Многу софтвер менаџмент програми работат користејќи го овој метод на безбедност.



Сл. 1.3: Моделот Biba



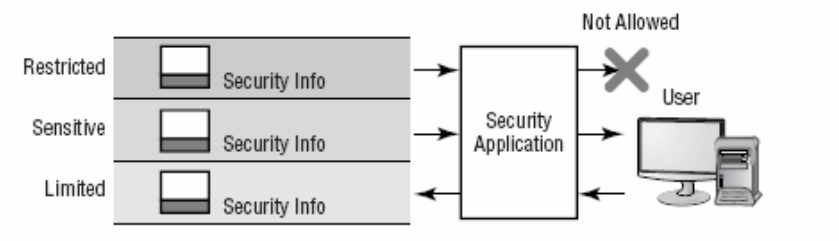
Сл. 1.4: Моделот Clark - Wilson

Да кажеме дека работите на некој софтверски продукт како дел од тим. Ви треба да пристапите до одреден код за да го вклучите во вашата програма. Вие не сте авторизирани да го модификувате овој код. Ќе користите програм кој ќе ве провери дали можете да го добиете кодот од библиотеката на кодови. Секоја проба да се модификува кодот ќе биде спречена. Развивачите на кодот во библиотеката се авторизирани да прават промени. Со овој процес вие сте сигурни дека само авторизираните луѓе имаат право да менуваат и само тие можат да ја комплетираат задачата.

Забелешка: Clark – Wilson моделот се фокусира на бизнис апликациите и на конзистентноста.

1.11.4 Модел на течење на информации

Овој модел има за задача да се концентрира на протокот на информации, не само на насоката на протокот. Моделите Bell La-Padula и Biba ги засега протокот на информации на однапред дефиниран начин. Но овој модел работи со сите насоки на проток на информации. Овој модел бара секое делче од информацијата да има единствени карактеристики, вклучувајќи ги и оперативните можности. Ако некој проба да запише информација со пониско ниво на пристап на повисоко, моделот ќе направи проценка на основа на карактеристиките на информацијата и ќе одреди дали операцијата е легална. Ако операцијата е нелегална - моделот ќе ја спречи. Сликата 1.5 го илустрира концептот.



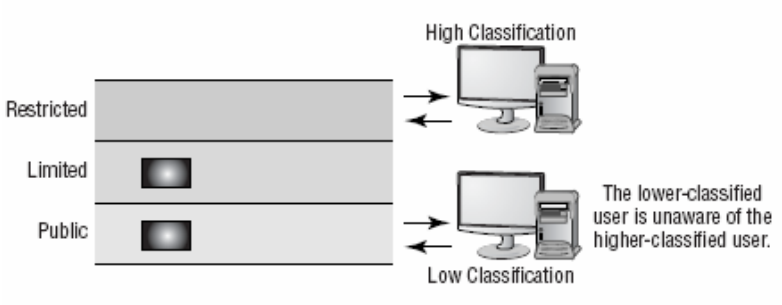
Сл. 1.5: Моделот на течење на информации

Да го искористиме претходниот проект со софтверот како пример. Развивачот може да работи со верзија на софтверот, за да ја подобри функционалноста. Кога програмерот направил подобрувања на кодот, тој ќе сака да го врати кодот назад во библиотеката. Ако обидот за запишување на кодот е успешен, тогаш овој код ќе го замени постоечкиот. Но ако се појави баг во новиот код, стариот код исто така ќе биде сменет. Решение би било да се креира нова верзија на кодот, но да се зачува и старата. Секоја промена во кодот ќе бара креирање на нова верзија и зачувување на старата. Овој процес можеби одзема дисковен простор, но спречува губење на работите, и креира механизам за следење на развојот на кодот.

1.11.5 Модел на немешање

Овој модел е наменет да обезбеди немешање на безбедносните функции со функциите од пониските нивоа. Во суштина, ако корисник со повисоки права менува некои информации, корисникот со пониски права нема да знае дека е зафатен со промената. Овој пристап оневозможува корисникот со пониски права да заклучи кои промени се направени во системот. Сликата 1.6 го илустрира концептот. Забележете дека корисникот со помали права не е свесен дека некои промени се случиле над него.

Да го разгледаме за последен пат примерот со проектот за развој на софтвер. Ако системскиот развивач правел промени во библиотеката која била користена од страна на програмер со пониски привилегии, промените ќе се направат во библиотеката без програмерот со пониски привилегии да е свесен за нив. Ова ќе му дозволи на развивачот со поголеми привилегии да работи на прототипови без да влијае врз развојните напори на програмерот со пониски привилегии. Кога развивачот ќе го заврши својот код, тој може да го публикува на програмерите со пониско ниво на пристап. Од тој момент сите корисници ќе имаат пристап кон промените и можат да ги користат во своите програми.



Сл. 1.6: Моделот на немешање

1.12 РЕЗИМЕ

Во ова поглавје ги покривме клучните елементи на физичката безбедност, социјалното инженерство и околината. Ова поглавје исто така покажа како работат бизнис континуитетот, безбедноста на информацијата и моделите на пристап. Мерките за физичка безбедност вклучуваат контроли на пристап, физички бариери, и системи на околината. Влијанието на околината вклучува електрични, противпожарни, и други типови на пречки. Технологијата на безжичните ќелии рапидно расте во светски рамки. Најновата GSM технологија дозволува променливите картички (SIM) да се користат интернационално. Американските и Европските стандарди не се еднакви во овој момент. Многу производители на мобилни телефони прават продукти кои можат да работат во двете околини подеднакво добро.

Безбедносните модели мора да се однесуваат на физичка безбедност, безбедносни зони, партиционирање, и комуникациска инфраструктура. Треба да го земете пристапот преку повеќе нивоа кога имплементирате безбедносен модел. Business Continuity Planning е процес на донесување на решенија за тоа како се решаваат загубите, проблемите и паѓањата во организацијата. Клучните аспекти на BCP се:

- Business Impact Analysis (BIA)
- Проценка на ризикот

BIA вклучува проценка на критичните функции во организацијата. Оваа информација се користи за креирање на решенија за тоа како да се справиме со снемување на струја, ако до тоа дојде. Процената на ризикот е процес на евалуирање и каталогизација на заканите, ранливостите и слабостите кои постојат во системот што се користи. Процената на ризикот треба да е во врска со BCP за да не убеди дека сите бази се покриени. Безбедносните модели започнуваат со разбирање на бизнис темите кои постојат во организацијата. Бизнис темите кои мораат да се дефинираат, содржат:

- Политики
- Стандарди
- Водичи

Добар дизајн на политика содржи поенти, изјави за политиката, изземање. Секој од овие аспекти на добро изработена политика помага за да се постават очекувањата за секого во компанијата. За политиката да биде ефективна, таа треба да има безрезервна поддршка од постариот менаџмент или од донесувачите на одлуки во компанијата. Многу стандарди се развиваат, за да се имплементираат безбедносните стандарди во организациите. Еден од поновите стандарди кој добива светска поддршка е ISO 17799; овој стандард ги идентификува 6-те клучни области кои безбедносната политика или модел мора да ги содржи. Сертификацијата со овој стандард е содржана низ функции на следење, направени од трета страна или акредитирана агенција.

Класифицирање на информацијата е процес на одредување на тоа - која информација е достапна до која страна и за која цел. Класификацијата во индустријата обично се темели на каталогизирање на информациите како јавни или приватни. Јавните информации можат да се класификуваат како информации за лимитирана дистрибуција и информации за целосна дистрибуција. Приватните информации обично се класифицираат како информации за интерна употреба и информации од рестриктивен карактер. Примарните улоги во безбедносен процес ги вклучуваат сопственикот, чуварот и корисникот. Сопственикот на податоците е одговорен за одредување на правилата за пристап и употреба. Чуварот е одговорен за одржување и заштита на податоците, а корисникот ги користи податоците за да си ја работи својата работа. Улогите за поддршка во класификацијата на информациите ги вклучуваат безбедносните професионалци и аудиторите. Безбедносен професионалец е личност која има пристап до информациите и процесите за да обезбеди заштита. Аудиторот примарно се грижи да се следат процесите и процедурите, за да се заштитат информациите.

Моделите за контрола на пристап постојат за да се категоризира користењето на осетливите информации. Трите најпознати модели се Bell La-Padula, Biba и Clark – Wilson моделот. Помалку познати се - моделот на течење на информацијата и моделот на немешање.

Bell La-Padula моделот работи според филозофијата во која вие не можете да читате преку вашето ниво на класификација и исто така не можете да пишувате во пониската класификација. Кај овој модел најбитна е безбедноста на информацијата.

Biba моделот е дизајниран да спречи корисникот да запишува на погорно ниво и не може да чита на пониско ниво. Biba моделот е дизајниран да овозможи интегритет на податоците, како спротивност на безбедноста на податоците.

Clark – Wilson моделот бара целиот пристап до податоците да се одвива преку контролирани програми за пристап. Програмите диктираат која информација може да биде користена и како може да и се пристапи. Овој модел е многу чест во системите за развој на софтвер.

Моделот *течење на информации* се базира не само на правецот на течење на информациите, туку и на карактеристиките на самото течење на информациите.

Овој модел бара секое парче информација да има единствени карактеристики и оперативни можности.

Моделот на *немешање* е со намена да осигура немешање на функциите со повисоки права со оние со пониски права на пристап. Во суштина ако некој со повисоко ниво на пристап менува некои информации, корисникот со пониско ниво на пристап нема да почувствува никакви промени. Овој пристап не дозволува корисниците со понизок пристап да знаат какви промени се случуваат во системот.

□

2. МРЕЖНА БЕЗБЕДНОСТ

2.1 ОПШТИ ПОИМИ ЗА КОМПЈУТЕРСКИ МРЕЖИ

Секој од последните 3 века бил доминиран од една технологија; во 18-тиот век тоа биле механичките системи кои ја придружувале Индустриската револуција, во 19-тиот тоа била парната машина, додека во 20-тиот век клучната технологија станало прибирањето, процесирањето и дистрибуцијата на информации. Помеѓу другото се развил глобален телефонски систем, се појавиле радиото и телевизијата, раѓањето и експанзијата на компјутерската индустрија и користењето на комуникациските сателити. Како резултат на брзиот технолошки развиток овие области брзо конвергираат една кон друга и се губат разликите помеѓу прибирањето, пренесувањето, чувањето и процесирањето на информациите.

Организациите со стотици оддалечени локации преку поширок географски области, очекуваат да бидат во можност да пристапуваат и ја испитуваат состојбата на било кое нивно оддалечено одделение на најлесен начин. Како што се зголемува способноста за прибирање, процесирање и дистрибуција на информациите, уште побрзо се зголемуваат барањата за пософистицирано процесирање на информациите. Мешањето на компјутерите и телекомуникациите имало големо влијание на начинот на кој се организирани компјутерските системи. Концептот на „компјутерски центар“ како просторија со голем компјутер каде што корисниците би ги носеле своите програми за извршување станал комплетно застарен. Стариот принцип на единствен компјутер кој ги опслужува потребите на целата организација се заменува со модел каде што голем број на одделени но поврзани компјутери ја извршуваат сета работа. Овие системи се наречени компјутерски мрежи.

Мрежа преставува систем кој овозможува комуникација помеѓу два корисници или машини. Во светот на компјутерските мрежи, потребно е детално дефинирање на правилата за комуникација; компјутерите кои меѓусебно комуницираат мора да ги познаваат овие правила, како и луѓето кои зборуваат на ист јазик за да комуницираат без проблеми. Ако компјутерите не се разбираат меѓусебно, не може да се оствари нивно поврзување и мрежните сервиси, како што се пристапот кон Интернет, делењето на датотеки и фолдери или печатењето, не се возможни.

Поимот „компјутерска мрежа“ означува множество на автономни компјутери поврзани со посредство на иста технологија. За два компјутери се вели дека се поврзани ако се во можност да разменуваат информации. Поврзувањето може да се оствари на многу начини, не само преку бакарни жици, туку и преку оптички влакна, микробранови и инфрацрвени бранови и комуникациски сателити. Постојат компјутерски мрежи со различни големини, форми и облици како што ќе биде прикажано понатаму. (Иако звучи чудно, но ниту Internet ниту WWW не се компјутерски мрежи, а причината за тоа е што: Интернет не е единична мрежа - туку мрежа од мрежи, а WWW преставува дистрибуиран мултимедиски систем кој го користи Internet-от како подлога).

Постои значајна конфузија во литературата околу поимите за компјутерска мрежа и дистрибуиран систем. Клучната разлика се состои во тоа што, кај дистрибуираниот систем - множеството од самостојни компјутери се преставуваат на корисникот како еден кохерентен систем. Обично, тоа е единичен модел (парадигма) кој се презентира на корисниците, и обично софтверски слој над оперативниот систем наречен „middleware“ е одговорен за неговата имплементација. Познат пример за дистрибуиран систем би бил World Wide Web, каде што сѐ преставува документ (Web страница).

Во компјутерската мрежа, не постои таков кохерентен модел или софтвер. На корисниците им се презентира актуелната машина, без обид за преставување дека машините изгледаат и се однесуваат како една машина. Ако машините имаат различен хардвер и различни оперативни системи, тоа е потполно видливо за корисниците. Ако корисникот сака да извршува програма на оддалечена машина, треба да се најави на машината и да го изврши на неа. Во суштина дистрибуираниот систем е софтвер изграден над мрежата. Софтверот овозможува висок степен на кохерентност и транспарентност. Така, разликата помеѓу мрежата и дистрибуираниот систем лежи во самиот софтвер (особено оперативниот систем), а не во хардверот.

2.1.1 Основи на умрежување

Мрежите се користат за поефикасна работа и комуникација. Мрежата може да поврзува компјутери, печатари, оптички уреди, скенери и друга опрема. Предноста на поврзувањето на компјутерите и опремата се состои во поефикасно пренесување на податоците. Пред појавата на мрежите, корисниците за делење на информациите користеле магнетни дискови, а пред тоа и печатен материјал. Друга предност при користењето на мрежите е овозможеното делење на ресурсите; печатарите, тврдите дискови и апликациите може да се делат и со тоа да се намалат трошоците со што ќе се овозможи пристап на секој корисник во организацијата.

Компјутерската мрежа е изградена околу концептот на испраќач – извор (sender - Source), кој врши испраќање на податоци кон примател, односно одредишен компјутер (receiver – destination computer). Компјутерите не се единствени машини кои можат да комуницираат на мрежата - и другите уреди имаат способност да бидат и извор и одредиште. Печатачот, компјутерот или било која друга машина која е способна за комуникација преку мрежата се нарекува *мрежен уред* или *јазол.*

Кога уредите учествуваат во комуникацијата на мрежата, треба да постои начин за пренесување на информациите помеѓу себе. Во повеќето мрежи, се користат кабли за поврзување на уредите. Можат да бидат поврзани со единствен кабел кој ги поврзува сите или пак каблите да го поврзуваат секој уред со централна локација. Каблите кои обично се користат се направени од бакарни жици слични на телефонските, но со значително повисок квалитет. Покрај бакарните кабли, се користат и други видови на медиуми како што се кабли направени од стакло или пластика, а од неодамна се користат радио бранови и микробранов пренос.

Поврзувањето на две или повеќе мрежи кои се способни да комуницираат меѓусебно се нарекува умрежување (*internetwork)*. Умрежувањето е способност различни мрежи да комуницираат со користење на специјален хардвер или софтвер.

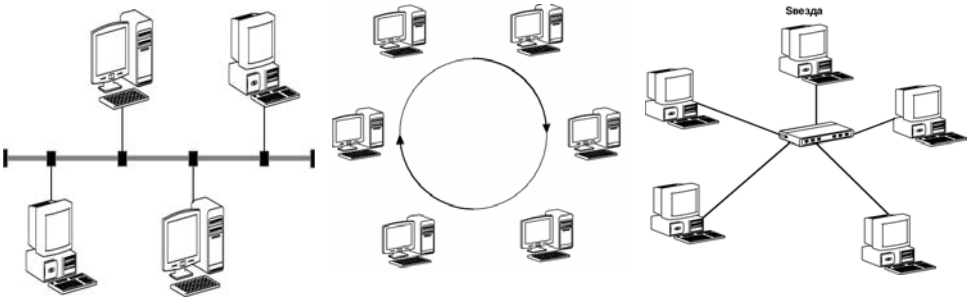
2.1.2 Видови на мрежи

Компјутерските мрежи може да се поделат на три главни категории:

- Локална мрежа (Local Area Network - LAN) е мала мрежа составена од компјутери и уреди во склоп на една зграда или кат.
- Метрополитен мрежа (Metropolitan Area Network - MAN) е умрежување на повеќе LAN мрежи со брзи врски преку област на еден град.
- Глобална мрежа (Wide Area Network - WAN) поврзува локални мрежи со користење на јавна телефонска мрежа.

Локалните, метрополитен и WAN мрежите се меѓусебно различни. Покрај тоа што покриваат различни географски области, тие имаат и различни типови на инсталации и користат различни уреди како и различен начин на одржување. Уредите во состав на една локална мрежа може да бидат релативно евтини и лесни за одржување и обично доволно е едно лице за нивно одржување. Во помалите мрежи, доволно е еден корисник да преземе, покрај своите работни обврски - и одговорност за одржување на мрежата, додека во средните и поголемите организации, постои потреба од администратори за обезбедување на техничка поддршка и одржување.

Според топологијата - локалните мрежи се имплементираат во облика на магистрала, прстен или ѕвезда (сл. 2.1).



Сл. 2.1: Топологии на локална мрежа (магистрала, прстен, ѕвезда).

Во поголемите мрежи како што се MAN и WAN, постои пософистицирана мрежна опрема за одржување и во цената на инвестицијата на овие мрежи влегуваат и трошоците за долговремено одржување и администрација, а постои потреба и од барем еден професионален мрежен администратор. Во денешно време, заради едноставниот пристап на Интернет, компаниите може да се поврзуваат со оддалечените локации без поголеми трошоци. Корисниците може да делат

документи и да пристапуваат кон сервери од оддалечени локации, овозможувајќи им секаков вид на поврзување без високи трошоци за поставување и одржување на приватните WAN мрежи.

Многу од корисниците инсталираат и домашни компјутерски мрежи *„Home Area Networks - HAN“*, кои им овозможуваат поврзување на различни електронски уреди како што се компјутери и нивни периферии, телефони, видео игри, домашни безбедносни системи и интелигентна техника.

2.1.3 Седум-слоен мрежен модел според ОСИ

Комуникацискиот систем се состои од многу компоненти, а се однесува на најмалку две “страни“ што сакаат да комуницираат. Компјутерската мрежа се состои од два или повеќе јазли (компјутери), поврзани преку одреден комуникациски канал. Треба да се истакне дека поврзувањето во мрежа овозможува зголемена функционалност, делење на ресурси итн., и дека Интернет претставува всушност мрежа од многу поврзани мрежи.

Мрежите вообичаено претставуваат сложени структури. Следејќи го принципот раздели-па владеј, модерните мрежи се дизајнираат, конструираат и опишуваат како повеќе-слојна архитектура, т.е. дефинирани се мрежни стандарди и протоколи за поврзување на различните слоеви (нивои) од мрежата. Во основа, повеќе-слојните протоколи се развиени заради следните цели:

- Ја редуцираат сложеноста на мрежата, т.е. нејзиниот дизајн и имплементација.
- Овозможуваат peer-to-peer комуникација помеѓу соодветните нивои во мрежата.
- Овозможуваат да се прават модификации на одредено ниво, кои не би ги засегнале останатите нивои.

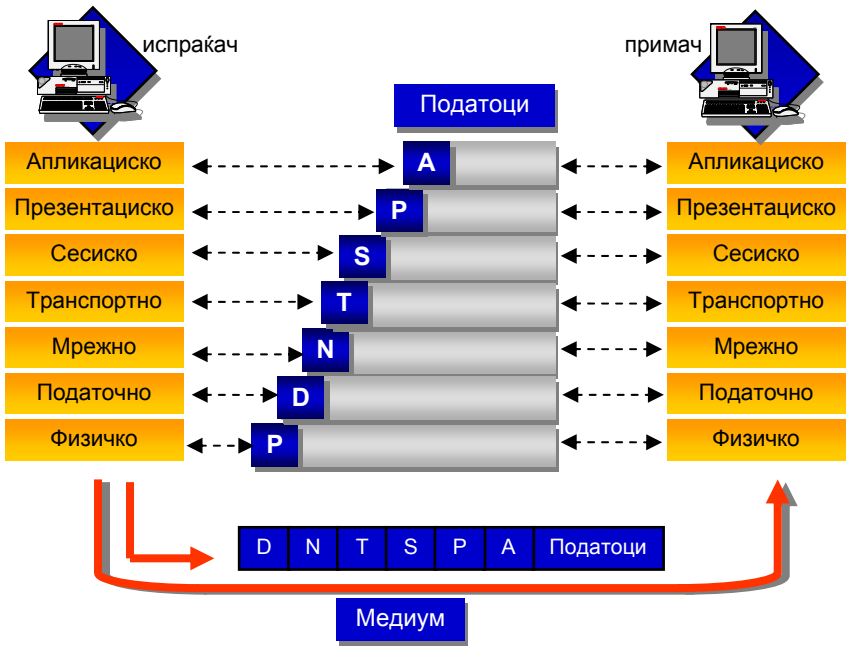
Кај повеќе-нивоовската архитектура, сложениот мрежен модел се дели на повеќе модули, кои припаѓаат на различни нивоа. Промените во дизајнот и конструкцијата на едно ниво, немаат значително влијание врз функционирањето на другите нивоа. На пр. промената на алгоритмот за корекција на грешка кај пониските нивои, не влијае на рутирачкиот алгоритам од повисоките нивои. Од друга страна, енкрипцискиот алгоритам на презентациското ниво кај испраќачот, е во тесна корелација со декрипцисиот алгоритам кај презентациското ниво на примачот. Компонентите од секое ниво кај испраќачот, комуницираат виртуелно со соодветното ниво кај примачот. Сепак, податоците реално се движат од највисокото ниво кај испраќачот кон пониските нивоа, па преку медиумот пристигнуваат кај примачот, и таму патуваат од најниското кон највисокото ниво (слика 2.2). Секое ниво кај испраќачот додава свое заглавје (header) кон податоците, а кај примачот заглавјата се анулираат и на крај остануваат чисти податоци.

Протоколите се подредени во нивои со цел да извршуваат точно одредени мрежни функции. Секое ниво користи услуги од нивото што е под него, а пружа услуги на нивото над него. Во 1983г. ISO го дефинирал седум-нивоовскиот отворен систем за интер-конекција (ОСИ), со цел да воспостави стандард што ќе опише

комплетното множество од протоколи, наменети за хетерогени мрежни околини. Мрежната архитектура според ОСИ е поделена во седум нивои, почнувајќи од најдолното – физичко, па до најгорното – апликативно ниво:

1. Физичко ниво – го опфаќа медиумот за пренос и форматот на сигналите кои се пренесуваат во бинарен облик. Ова ниво се грижи за механичките и електричните компоненти на мрежата, т.е. води сметка да битовите испратени на едната страна, бидат примени на другата страна.
2. Податочно (data link) ниво – служи за пристап и контрола на медиумот за трансмисија. Ова ниво се справува со регулацијата на протокот, форматирање на пакетите во рамки (frames) и детекција и корекција на грешки.
3. Мрежно ниво – ги форматира индивидуалните податочни пакети. Одговорно е за рутирање на пакетите низ мрежата; се справува и со адресирањето и испораката на податоците. Рутерите и IP-протоколот припаѓаат на мрежното ниво.
4. Транспортно ниво – се грижи за точен редослед на достава на пакетите. Главна задача на ова ниво е интегритетот на податоците - преносот на податоци помеѓу јазлите да биде сигурен и навремен. Два главни транспортни протоколи се TCP и UDP.
5. Сесиско ниво – ја воспоставува конекцијата помеѓу програмите кај испраќачот и примачот. Ова ниво управува со дијалогот, а исто така го синхронизира и мрежното време.
6. Презентациско ниво – служи за конверзија и приказ на податоците во соодветен формат. Примарната функција на ова ниво се синтаксата и семантиката на податочната трансмисија. ASCII и EBCDIC-конверзиите и крипто-заштитата се имплементирани во ова ниво.
7. Апликациско ниво – опфаќа апликациско-специфични информации за податоците што се пренесуваат. Ова ниво претставува интерфејс кон корисникот и дел од него се програмите: Telnet, FTP, E-mail client, Web browser.

Кај типичните мрежи, највисоките нивои – апликациското и презентациското, обично се реализирани преку апликативни програми (web browser, e-mail client исл.). Средните нивоа се често дел од оперативниот систем (драјвери, TCP/IP протокол), додека најниските нивои го претставуваат мрежниот хардвер (switches, кабли итн.). Иако денес има тврдења дека ОСИ моделот не е доследно имплементиран кај ниедна мрежа, и се предлагаат нови, скратени модели (како на пр. 4-слојниот TCP/IP-модел), може да се смета дека ОСИ претставува костур за сите постоечки и идни мрежни концепти.



Сл. 2.2: Седум-нивоовски ОСИ модел – peer to peer комуникацијата помеѓу нивоата е виртуелна, додека вистинскиот тек на податоци е од горе-надолу, па од доле-нагоре. Секое ниво кај испраќачот додава свој header (заглавје) кон податоците, а кај примачот, заглавјата се анулираат.

2.2 ФИЗИЧКА БЕЗБЕДНОСТ

Чувањето на компјутерите и мрежите во безбедна состојба бара повеќе од само технички аспекти на системите и мрежите. Морате да мислите за физичката околина и за бизнисот како таков. Тоа ги инволвира проценувањето на физичката безбедност, теми од социјалното инженерство и самата околина; некои од овие теми ќе бидат споменати во наредните поглавја, но сите овие работи се тесно поврзани. Сите овие теми бараат балансиран одговор и од техничка, но и од бизнис перспективата.

Ова поглавје ќе ви помогне да ја разберете важноста на физичките мерки за безбедност, како што се контроли на пристап, физички бариери и биометриски системи. Исто така го покрива социјалното инженерство и околината која им е потребна на вашите системи за да бидат безбедни и оперативни. Ова поглавје исто така дискутира за безбедноста на мрежите и за креирањето на безбедните зони и партиционирањето. На крај, исто така ќе се осврнеме на бизнис темите кои вклучуваат планирање, политики, стандарди, упатства, стандарди за безбедност и класификација на информации.

2.2.1 Разбирање на физичката и мрежна безбедност

Физичките безбедносни мерки ги чуваат вашите системи од неавторизиран пристап, примарно со превенција на неавторизиран корисник

физички да го допре системот или некој уред. Повеќето мрежни системи имаат развиено високи нивоа на софистицираност и безбедност од надворешни натрапници. Но овие системи генерално се ранливи на внатрешни напади, саботажа или погрешна употреба. Ако натрапникот има физички пристап до вашите системи, не можете да ги сметате за сигурни.

Следнава секција ги дискутира аспектите на физичката безбедност и ефектот што таа го има врз вашата околина, вклучувајќи ги контролите за пристап, социјалното инженерство и самата околина.

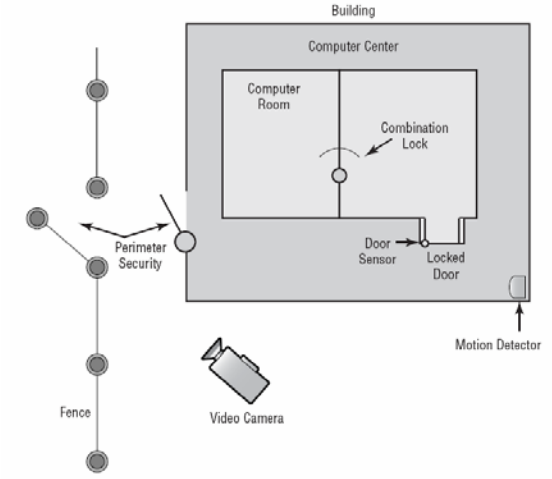
Имплементација на контрола на пристап

Контролата на пристап е критичен дел од физичката безбедност. Системите мораат да работат во контролирана околина за да бидат безбедни. Овие околини мораат да бидат, колку што е можно повеќе безбедни од упади. Конзолите на компјутерските системи можат да бидат главна точка на ранливост, поради тоа што многу административни функции можат да бидат постигнати преку системската конзола. Овие конзоли, како и системите мора да бидат заштитени од физички пристап. Две полиња кои можат да помогнат да се направи системот побезбеден се: физичките бариери и биометријата; и двете ќе бидат опишани во следните делови.

Физички бариери

Клучен аспект на контролата на пристап се физичките бариери. Целта на физичката бариера е да го оневозможи пристапот до компјутерите и мрежните системи. Најефективната имплементација на физичка бариера бара повеќе од една физичка бариера да биде помината, за да се добие пристап. Овој приод е наречен *систем на повеќе бариери.*

Идеално, вашиот систем треба да има минимум три физички бариери. Првата бариера е надворешниот влез во зградата, кој уште се вика и периметар, кој е заштитен со аларми против крадци, надворешни ѕидови, камери и друго. Втората бариера е влезот во компјутерскиот центар кој е позади заклучена врата. Третата бариера е влезот во самата компјутерска соба. Секој од овие влезови може да биде индивидуално обезбеден, мониториран, и заштитен со алармни системи. Сликата 2.3 го илустрира концептот. Иако овие три бариери нема секогаш да го застанат натрапникот, тие потенцијално ќе ги забават доволно - за да полицијата одговори пред да провалата комплетно се изврши.



Сл. 2.3: Безбедносен модел составен од три нивоа

Забелешка: Не е важно што мислите дека е безбеден вашиот систем; никогаш нема да можете да ги стопирате сите натрапници. Но нашата цел е да ги стопираме тие кои се помалку фанатични и да ги забавиме тие што се. Како аналогија, предната врата од вашиот дом може да има брава и резе. Доволно за да ги убедите повеќето крадци да пробаат некаде каде што е помалку безбедно. Фанатик кој намислил да влезе кај вас, може да земе клешта или слична алатка и - да влезе кај вас.

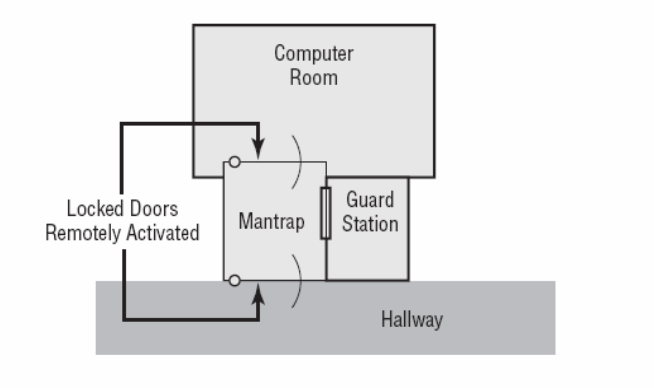
Високо-безбедните инсталации користат тип на контрола на пристап наречена стапица. Овие контроли на пристап бараат визуелна идентификација, како и автентикација за да се добие пристап. Стапицата е проблем за самата зграда поради тоа што дозволува само еден или двајца да влезат во исто време. Обично е дизајнирана физички да го задржи оној кој неавторизирано сака да влезе, додека не стигнат властите. Сликата 2.4 покажува како изгледа стапицата. Во овој случај визуелната верификација се прави со чувар. Комплетно развиена стапица вклучува стакло отпорно на куршуми, силни врати, и брави. Во места со голема безбедност или во војската, чувар со оружје, но и видео надзор се присутни кај стапицата. Штом ќе влезете, додатна безбедност и автентикација може да биде потребна за понатамошно влегување. Следнава секција дискутира за безбедноста на периметарот, поставувањето на безбедносните зони и партиционирањето.

Безбедност на периметарот

Дали физичка или технолошка - оваа безбедносна граница претставува прва линија на одбраната во вашиот безбедносен модел. Во случај на физичката безбедност, намерата е да се спречи неавторизиран пристап до ресурсите внатре во зградата.

Мрежниот еквивалент на физичкиот периметар е наменет да го постигне истото она што безбедносниот периметар значи за зградата. Како да ги спречите

неавторизираните натрапници да пристапат до системите и информациите во мрежата, низ самата мрежа?



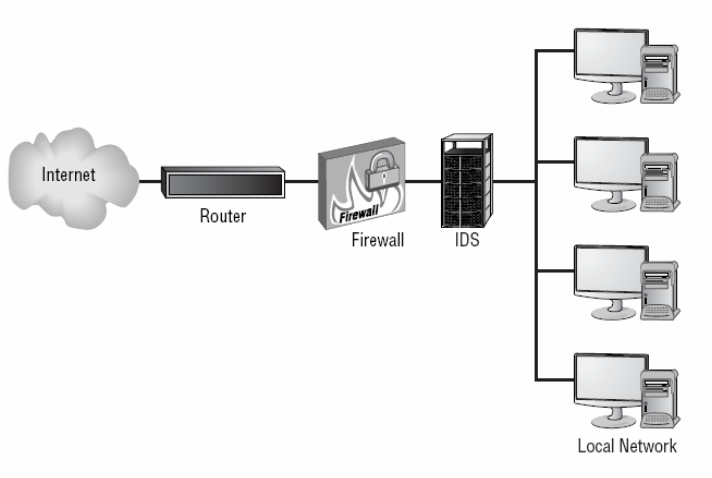
Сл. 2.4 : Стапица во акција

Во физичката околина, безбедносниот периметар се постигнува со користење на брави, врати, системи за надгледување и алармни системи. Ова од функционална гледна точка не е различно од мрежата која користи рутери, системи за детекција на неавторизирани влезови, и заштитни ѕидови за да се оневозможи неавторизиран пристап. Сликата 2.5 го прикажува системот кој се користи за да се стопира мрежниот напад. Малку безбедносни системи можат да се имплементираат, а да немаат слабости или ранливости. Цврсто решен натрапник, трпеливо може да ги надмине повеќето безбедносни системи. Задачата можеби и не е лесна, и можеби бара внимателно планирање, но сепак ако некој решил - може да најде начин да влезе. Ако сакате да ги набркате натрапниците да не влегуваат во вашата зграда, вие можете да инсталирате подобрени брави на вратите, да ставите кодирани алармни системи, магнетни контакти на вратите и прозорците. Запаметете дека не можете да ги спречите натрапниците да влезат во вашата зграда, но сепак можете да го направите нивниот потфат прискантен и полесен за откривање.

Забелешка: Не го заборавајте очигледното. Додавајќи чувар на предната врата многу ќе помогне во чувањето на натрапникот надвор.

2.2.2 Безбедносни зони

Безбедносна зона е област во самата зграда каде пристапот е индивидуално мониториран и контролиран. Голема мрежа, како на пример во голема нуклеарна централа, може да има многу области кои бараат рестриктивен пристап. Во зградата, катот, сектори на катовите, па дури и канцелариите, можат да бидат поделени во помали области. Овие помали области се викаат безбедносни зони. Во физичка околина, секој кат се дели на посебни зони. Алармните системи кои ја идентификуваат зоната на напад - можат да ја информираат чуварската служба за тоа каде се наоѓа натрапникот во зградата.



Сл. 2.5: Мрежна одбрана на периметарот

Сценарио од вистинскиот живот

Во последно време забележан е зголемен мрежен сообраќај доцна навечер и рано наутро. Не беше можно да се пронајде техничка причина за тоа што се случуваше. По истрагата утврдено е дека работник кој работел во трета смена - поставил сервер со игри за повеќе корисници во неговата канцеларија. Овој сервер бил подесен да се пали по 22.00 и да се гаси во 05.30, бил сокриен под бирото на работникот, и поддржувал околу 30 локални играчи. Овој работник немал клуч од зградата, па истрага е спроведена за тоа како тој го внесол серверот внатре. Зградата има електронски брави на надворешните влезови, и за да се влезе потребна е картичка.
Истрагата откри дека вработениот заедно со негов пријател откриле како да бутнат парче картон под една од вратите. Со тоа се активирал механизмот за отворање на вратата. Вратите се дизајнирани така да тие автоматски се отклучуваат кога некој ја напушта зградата. Натрапниците ја искористиле оваа слабост за да влезат во зградата по работното време.

Концептот на безбедносни зони е стар колку и самата безбедност. Повеќето аларми дозволуваат креирање на индивидуални зони во зградата или во куќата; овие зони се третираат различно. Кога одите да спиете - алармот не треба да ја мониторира спалната за движење поради тоа што движењето е најнормално таму. Подолу ќе ги погледнете безбедносните зони од различни агли.

Безбедносни зони во физичка околина

Треба да го процените вашето работно место и да размислувате за физичките зони кои би требало да постојат во поглед на различни типови на индивидуи кои можеби ќе бидат присутни. Доколку вашето работно место е веќе поделено на зони, заборавете дека тоа е така - и почнете одново. Одговорете ги следниве прашања:

1. Кои области ги претставуваат физичките димензии на вашето работно место (згради, катови, канцеларии, итн.)?
2. Кои области се пристапни од сите (од администратори до посетители)? Може ли посетителот да ја напушти рецепцијата без придружба, и ако може, тој може да оди каде (тоалет, кујна итн.)?
3. Во кои области корисниците смеат да се движат слободно? Дали сте сигурни дека посетителите не можат да влезат во тие области?
4. Кои области се дозволени за влез само на администраторот? Серверска соба? Плакари со жици? Како ги идентификувате корисниците кој може да влезе, а кој не?
5. Дали некои други области треба да се обезбедат за влез и покрај поделбата корисник/администратор?

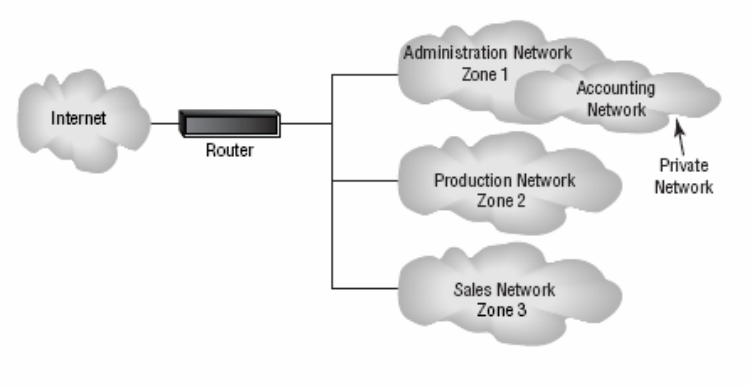
Треба да ја проверите вашата околина рутински, за да бидете сигурни дека зоните кои постојат во вашите безбедносни зони се сеуште валидни. Секогаш почнете од ништо и преправајте се дека зоната не постои; тогаш потврдете дека зоните постојат и дека тие се исти како тие што ги креиравте во вежбава.

Мрежниот еквивалент на безбедносна зона е мрежна безбедносна зона. Тие ја имаат истата функција. Ако креирате помала секција на мрежата, секоја зона може да има сопствени безбедносни поставки и мерки – исто како кај физичка безбедносна зона. Сликата 2.6 покажува голема мрежа разделена на три помали зони. Забележете дека првата зона исто така содржи помала зона, во која се чува информацијата со високо значење. Ова дозволува - нивоата на безбедност да бидат аплицирани околу чувствителните информации. Поделбата на мрежата е постигната со имплементација на VLAN-ови и поставување на DMZ зони; и за двете ќе дискутираме подолу.

Партиционирање

Да партиционираме мрежа е исто како да партиционираме зграда. Во зградата, ѕидовите постојат за да ги насочуваат луѓето, за да овозможат контрола на пристап и да ги разделат околините по функционалност. Овој процес дозволува информацијата и сопственоста да бидат чувани под физичка брава и клуч.

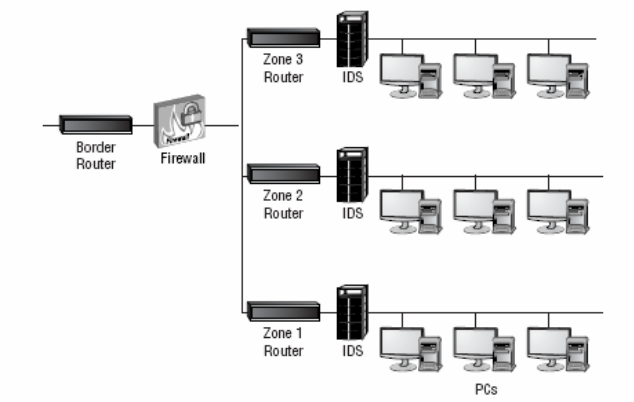
Забелешка: Партициите можат да бидат привремени или перманентни структури.



Сл. 2.6: Мрежна безбедносни зони

Ходниците во зградата се градат различно од внатрешниот канцелариски простор. Тие се обично поотпорни на пожари, и се нарекуваат огнени коридори. Овие коридори им дозволуваат на луѓето во зградите да избегаат доколку дојде до пожар. Ѕидовите кај коридорите одат од катот кон покривот, додека внатрешните ѕидови можат да застанат пред да дојдат до кровот (повеќето канцеларии имаат лажни кровови во кои држат светло и кабли). Мрежното партиционирање ја постигнува истата функција за мрежата, како што физичкото партиционирање за зградата. Зградите имаат ѕидови, а мрежата тоа го прави со креирање на приватни мрежи во поголемите мрежи. Овие партиции можат да бидат изолирани со рутери и сигурносни ѕидови. Затоа, додека мрежните системи се поврзани преку жица, функционалниот поглед е тој што е сочинет од многу мали мрежи. Сликата 2.7 покажува партиционирана мрежа. Важно е да се разбере дека доколку физичкиот уред (рутер) не ги раздели овие партиционирани мрежи, сите сигнали се делат преку жицата. Овој уред ја постигнува истата функција како ходник или заклучена врата – гледано од физичка перспектива.

Забелешка: Партиционирањето и безбедносните зони се вразни заедно. Типично партиционирањето е потесно фокусирано од зоните, но тоа не мора секогаш да е така. Во типична инсталација, зоната се однесува на кат, а партиционирањето на соба.



Сл. 2.7: Мрежно партиционирање и делење на мрежите една од друга

Проценка на вашиот безбедносен систем

Од вас е побарано да го процените безбедносниот систем во вашата зграда. Директорот ве одбрал вас поради тоа што ги разбирате компјутерите, а новиот алармен систем е компјутеризиран. Во проценката на околината, вие забележувате дека постои еден контролен панел за целата зграда. Неколку детектори на движење се лоцирани во главниот ходник. Никакви други безбедносни компоненти не се инсталирани.
Оваа ситуација тешко да е нормална за мала зграда. Би можеле да препорачате подобрување на системот со додавање на детектори за движење во секој главен ходник. Исто така можете да инсталирате видео надзор на сите влезови. Можете да ја зајакнете и безбедноста на периметарот со додавање на сензори на вратите и прозорците на приземјето. Проценете ја зградата од страна на повеќе - столбен пристап. Спојте ги безбедноста на периметарот, безбедносните зони и видео надзорот таму каде што е потребно.

2.2.3 Биометрија

Биометриските системи користат некаков единствен биолошки пристап за да идентификуваат личност. Некои од овие идентификатори користат отисоци на прсти, модели на ретина, и отисоци на рака. Некои од уредите кои се користат вклучуваат рачни скенери, скенери на ретина, и можеби DNA скенери кои се користат како дел од механизмите за контрола на пристап. Овие уреди треба да се вметнат во безбедносно-ориентираните компјутерски системи кои ги снимаат сите обиди за пристап. Исто така и тие треба да се под надзор за да се спречат неовластени лица да ги поминат. Овие технолошки достигнувања стануваат сè подостапни и сè пошироко користени. Некои компании користат паметни картички како примарен метод за контрола на пристап, но многу имплементации се лимитирани, поради високите цени кои се врзуваат со овие технологии.

Забелешка: Како генерално правило, моменталните цени за имплементација на било која форма на биометриска автентикација, е висока.

2.2.4 Разбирање на социјалното инженерство

Социјалното инженерство е процес во кој натрапниците добиваат пристап во вашите простории, мрежа, па дури и до вашите вработени со искористување на човековата природа да верува. Како што ќе кажеме понатаму, напад со социјалното инженерство може да дојде од некој кој се претставува како продавач или од електронска порака која доаѓа (можеби) од висок службеник кој е на пат - и вели дека заборавил како да се најави на мрежата, или како да влезе во зградата за време на викенд. Тешко е да се определи дали единката има легитимни или лоши намери.

Сценарио од вистинскиот живот - биометриски уреди

Од вас е побарано да го решите проблемот на луѓето кои ги забораваат паметните

картички кои им овозможуваат пристап во компјутерскиот центар. Едвај да помине ден во кој некој вработен не заборави да ја донесе својата картичка. Ова предизвикува голем проблем во работата поради тоа што некој мора цело време да издава нови картички. Компанијата пробала сè што може, па дури и отпуштање на луѓето кои многу пати забораваат картички. Што ќе препорачате? Пробајте со биометриски уреди (рачни скенери) или брави со нумерички пристап кои можат да работат заедно со паметните картички. Овие уреди ќе им дозволат на работниците да ги забораваат картичките, но сепак ќе можат да влезат таму каде што треба.

Нападите преку социјалното инженерство можат да се развијат многу суптилно. Исто така тие многу тешко се откриваат. Еве да погледнеме неколку такви напади:

- Некој влегува во вашата зграда носејќи бела јакна со лого на нејзе. Има исто така и алат. Доаѓа на рецепција и се претставува како поправач на фотокопир машини. Вели дека е тука заради превентивен сервис на фотокопирот. Во повеќето случаи рецепционистот ќе го пушти да помине и ќе му каже каде е копирот. Штом "техничарот" тргне рецепционерот најверојатно ќе заборави за него. Вашата компанија тукушто беше жртва на напад со социјално инженерство. Напаѓачот сега ја пробил вашата прва, а можеби и втора линија на одбрана. Во многу канцеларии, вклучувајќи ги и оние безбедносно ориентираните, единката ќе има пристап до целата организација и ќе може да оди каде што ќе посака. За овој напад не беа потребни никакви посебни таленти или вештини, освен способноста да се изгледа како поправач на копири.
- Следниот пример е вистинска ситуација; се случил во една високо безбедна владина институција. Пристапот кон просторијата бара проаѓање низ неколку места за проверка на кои се поставени тренирани и компетентни луѓе. Вработен решава да си поигра со одделот задолжен за безбедност. Земал стар бељ, ја исекол својата слика и на тоа место ставил слика ма Мики Маус. Влегувал две недели во просторијата пред да биде фатен.

Нападите преку социјалното инженерство како овие, се лесно изводливи во повеќето организации. Дури и ако организацијата користи биометриски уреди, магнетни картички или други електронски мерки, нападите преку социјалното инженерство се релативно едноставни. Омилена метода на добивање на пристап во електронски обезбеден систем е да се следи некој низ вратата која што туку ја отклучил, процес наречен фаќање опашка. Многу луѓе не мислат двапати, се случува цело време.

Како администратор, една од вашите одговорности е да ги едуцирате корисниците да не бидат лесни жртви на нападите преку социјалното инженерство. Тие треба да ги знаат безбедносните процедури и да ги следат истите. Треба да имате високо ниво на доверба во системите кои се имплементирани; еден начин за здобивање на таа доверба е редовно проверување на корисниците. Со следната вежба ќе процените дали е можно да дојде до напад со социјалното инженерство кај вас.

Тестирање на социјално инженерство

Со оваа вежба, може да ги тестирате корисниците за да одредите дали постои можност за напад преку социјално инженерство. Следново е предлог за тест; можеби ќе треба малку да ги модификувате за да бидат веродостојни за вашето работно место. Пред да ги спроведете осигурете се дека вашиот директор знае дека го правите овој тест и го одобрува:

1. Јавете се на рецепција од надворешна линија. Кажете дека сте новиот продавач, и дека не сте го запишале корисничкото име и лозинка кои ви ги дал менаџерот минатата недела, и дека морате да повлечете датотека од системот за електронска пошта за утрешната презентација. Дали таа ќе ве упати кон одговорната личност?
2. Јавете се во одделот за работа со човечки ресурси од надворешна линија. Не го давајте вистинското име, туку претставете се како продавач кој соработува со компанијата со години. Би сакале копија на телефонската листа на вработените да ви се испрати по електронска пошта - ако е можно. Дали се согласуваат да ви ја пратат листата, која ќе содржи информации кои можат да бидат употребени за погодување на кориснички имиња и лозинки?
3. Изберете случаен корисник. Јавете се и претставете се како некој кој работи во компанијата. Кажете им дека имате некој нов софтвер спремен за нив до крајот на следната недела и дека ви треба нивната лозинка за финално конфигурирање. Дали ќе ја сторат вистинската работа?

Најдобра одбрана против социјалното инженерство е едукацијата. Објаснете им на вработените како да реагираат при вакви барања. Превенцијата на нападите преку социјалното инженерство бара повеќе од само тренирање за тоа - како да ги детектирате и спречите нападите. Исто така бара осигурување дека луѓето секогаш остануваат внимателни. Социјалното инженерство е лесно да се направи, и покрај денешната технологија.

2.2.5 Скенирање на околината

Околината во која работи вашиот бизнис е поголема од физичките мерки на објектот во кој се вашите компјутери и работници. Исто така ги вклучува безжичните ќелии, физичките локации, заштитата од електрично зрачење, од поплави и заштитата од пожари. Следниве делови дискутираат за овие четири области за да ви помогнат да се заштитите подобро.

Безжични ќелии

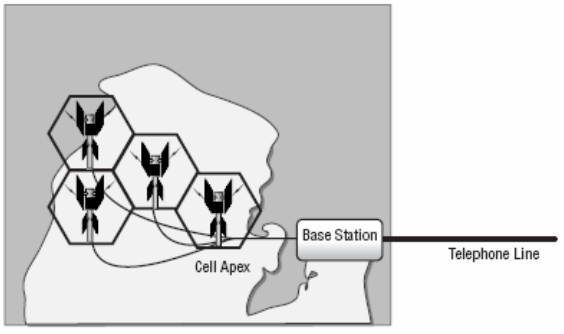
Ширењето на безжичната технологија креираше еден куп решенија и проблеми за професионалците за безбедност. Можноста за користење на мали уреди кои немаат потреба од многу струја, како што се мобилните телефони ја прави оваа технологија атрактивна за мобилните работници. Производителите сега прават паметни телефони, кои исто така се користат како PDA уреди. Адаптери се достапни за повеќето компјутерски системи и дозволуваат конекција за мобилните

телефони. Сега се поставуваат антени интернационално, и околината која ја покриват мобилните телефони се зголемува експоненцијално. Технологијата се базира на мали предаватели поставени стратегиски низ околината која ја поврзуваат. На провајдерите им се дадени отприлика 800 различни фреквенции да ги користат во околината која ја покриваат. Фреквенциите се поделени во 56 канали по ќелија. Сликата 2.8 ја покажува шемата на покривање.

Едноставните ќелии имаат високо ниво на компјутерска интелигенција, и тие ги предаваат разговорите една на друга автоматски. Мобилните телефони во USA работат во опсег од 824 MHz до 894 MHz – и Federal Communications Commission (FCC) бара полициските скенери да не ги следат тие фреквенции во USA. Повеќето други земји не бараат блокирање на овие фреквенции во комуникациската опрема.

Забелешка: Федерален криминал е мониторирањето на фреквенциите на мобилните телефони.

Мобилните телефони користат аналогни и дигитални можности за пренос. Аналогните системи дозволуваат отприлика 60 симултани разговори по ќелија. Дигиталната технологија тоа го проширува на 180 симултани разговори. Новите апликации, кои овозможуваат банкарство и други трансакции да се вршат преку ќелиите - се додаваат секојдневно. Global System for Mobile Communications (GSM) е најновиот стандард во овој ќелиски систем, и нуди енкрипција. GSM работи заедно со Subscriber Identification Module (SIM), дозволувајќи им на корисниците да менуваат мобилни телефони. SIM е картичка која може да се вади од еден и да се стави во друг мобилен телефон. За жал U.S. и Европските стандарди не се компатибилни, иако многу производители продаваат дуал-мод телефони. Многу луѓе веруваат дека мобилните телефони не можат да се следат, дека не можете да ја одредите локацијата на корисник на мобилен телефон. Ова не е така. Кога мобилен телефон ќе се вклучи, веднаш се идентификува ќелијата на која е најблиску. Системите можат да направат триаголник и да ја одредат позицијата на корисникот. Ова може да се направи, иако телефонот не се користи туку е само вклучен. Точката на пристап може да биде одредена само неколку моменти од вклучувањето поради целосната компјутеризација на системот.



Сл. 2.8: Систем на келии во градско подрачје

Сценарио од вистинскиот живот - обезбедување на безжичните уреди:

Загрижени сте за безбеден пристап кон вашата мрежа со користење безжични уреди. Многу менаџери и други вработени користат безжични PDA уреди за да комуницираат кога се надвор од канцеларија. Што можете да направите за да ги заштитите овие уреди?

Можеби ќе сакате да имплементирате безжичен безбедносен протокол (како што е Wirelss Transport Layer Security (WTLS) или Elliptic Curve Cryptography (ECC)) во тие уреди и во вашата мрежа. Со тоа вие ќе дозволите комуникација помеѓу безжичните корисници во вашата мрежа. ECC стана стандард во безбедноста на безжичната комуникација WTLS.

2.2.6 Локација

Локацијата на вашиот објект е критичен за неговата безбедност. Компјутерскиот објект мора да е на локација која од физички аспект може да се осигура. Додатно, локацијата мора да има правилни можности да одржува температура, влажност, и други фактори кои се битни за здравјето на вашиот компјутерски систем. Следната секција ја следи околината и системите на климатизација.

Системи за климатизација

Многу компјутерски системи бараат контрола на температурата и влажноста. Големите сервери, комуникациска опрема, и други уреди генерираат голема количина на топлина, ова е посебно нагласено кај мејнфрејмовите и постарите компјутери. Добриот систем кој го држи ова под контрола е релативно скап, и е како додаток на компјутерскиот систем. За жал поновите системи, оперираат со поголем распон на температурата. Повеќето нови системи се дизајнирани да работат во канцелариска околина. Ако компјутерските системи за кои сте одговорни бараат специјални потреби за климатизација, вие ќе треба да воспоставите контрола на влажноста и ладењето. Идеално, системите се лоцирани во средина на зградата, и тие се напојуваат посебно. Практика е, модерните згради да користат заедничка климатизација, која дозволува централно гаснење на системите кога зградата не се користи. Но компјутерската соба има потреба од контрола на климата цело време.

Забелешка: Системите за контрола на климата треба да се мониторираат за да не се случи нивото на влажност да падне под 50 %. Електростатски оштетувања можат да настанат, ако нивото на влажноста падне многу ниско.

Контролата на климата исто така се грижи за водата и опасностите од поплава, исто како и од опасноста од пожар. Компјутерските соби треба да имаат детектори за влага и пожар. Повеќето компаниски згради имаат водни пумпи и други системи во кровот. Ако пукне цевка (што е нормално во мали земјотреси), компјутерската соба може да се поплави. Водата и електриката не се мешаат.

Мониторите за влажност веднаш ја гаснат струјата во компјутерската соба, ако се детектира влажност поголема од нормалната.

Оган, не е битно колку мал, може да нанесе штета на компјутерските системи. Настрана големата топлина која може да стопи пластика и метал, чадот од огнот може да ги уништи компјутерите. Честичките од чадот се доволно големи да влезат во самиот хард диск, со тоа податоците се уништени. Како додаток - системите за гаснење на огнот се состојат од вода која е под притисок; водата која ќе се истури да изгасне дури и мал оган, може да уништи цел центар на податоци.

Забелешка: Трите критични компоненти на секој оган се топлина, гориво и кислород. Ако некоја од овие три работи се тргне, нема оган. Повеќето системи за стопирање на оган работат на овој принцип.

Сценарио од вистинскиот живот - обичните работи можат да имаат големи последици:

Водата може да дојде од било каде, вие само треба да сте спремни кога ќе дојде. Во компанија каде работев пред неколку години имаше најдобра можна серверска соба на последниот кат на самата зграда. Собата беше климатизирана и навистина убава. Директно над серверската соба беше покривот, а на кровот беа климатизерите за целата зграда. Преку еден екстремно топол викенд, кондензирало премногу вода и водата почнала да паѓа од кровот во самата соба над серверите. За многу кратко време сè беше уништено.
Колку и да звучи едноставно, вакви работи се случуваат цело време. Кога ќе се случат - бидете спремни со резервни копии, резервни сервери и резервни монитори.

2.2.7 Системи за струја

Компјутерските системи се подложни на проблеми со струјните напојувања. Компјутерот има потреба од рамномерна AC струја за да продуцира стандардна DC волтажа за електронските системи. Системите за струја се дизајнирани да работат со широк распон на струјни карактеристики, тие помагаат во одржување на електричниот сервис константен, и го осигуруваат нормалното течење на операциите.

Забелешка: Големите флуктуирања во AC струјата можат да доведат до состојба која се нарекува chip creep. Со ова слабо затегнатите чипови полека излегуваат од своите лежишта со тек на време.

Продуктите кои се достапни на пазарот, а ги решаваат повеќето проблеми се:

Штитници од струен удар - Овие уреди ги штитат електронските уреди од моментален пораст на напон (наречен шилец) во електричните линии. Повеќето штитници работат на тој начин што го испраќаат напонот кон заземјувањето преку уредите наречени *Metal Oxide Varistors (MOV).* Големи вакви штитници обично се стават во напојувањата на зградите или кај катните разделници во зградите. Малечки штитници можат да се купат како делови од продолжните кабли. Ако се

појават повеќе шилци еден по друг, овие штитници можеби нема да успеат да ги заштитат уредите. Штитниците се пасивни уреди, кои не се активираат превентивно.

Одржувачи на напон - Ова се активни уреди кои ефективно го изолираат и регулираат напонот во зградата. Овие уреди ја мониторираат струјата во зградата и ја чистат. Одржувачите на напон имаат филтри, штитници од струен удар, и привремени волт регулатори. Исто така тие можат да ги активираат резервните струјни уреди. Одржувачите на напон можат да бидат дел од целосната струјна мрежа на самата зграда. Но исто така може да ги забележите присутни само во компјутерските соби.

Резервна струја - Резервната струја генерално се користи во ситуации каде не смее да дојде до губење на струјата. Овој тип на системи обично се дизајнирани како краткотрајни замени, слични како батериски резервни системи, или за подолги користења како кај Uninterrruptible Power Supply (UPS). Овие системи генерално користат батерии за да обезбедат струја за краток временски интервал. За подолг временски интервал се користат струјни генератори. Овие генератори се вклучуваат штом детектираат снемување на струја. На генераторите им е потребно малку време пред да почнат да генерираат струја, тоа време им го обезбедуваат малите батериски системи. Повеќето генератори не се исклучуваат автоматски кога струјата ќе се врати во зградата, потребно е нивно мануелно исклучување. Ова е поради тоа што во голем број на случаи се случува лажно враќање на струја, пред комплетно да се врати струјата во струјната мрежа.

Повеќето генератори работат или на гас или на дизел, и тие исто така бараат редовно превентивно одржување. Овие системи воопшто не ни се потребни, доколку тие не стартуваат кога ни се потребни, или ако откажат поради тоа што нема масло во моторот. Понови системи се појавуваат на пазарот и користат сончева технологија, овие системи најверојатно ќе бидат сигурни и ќе имаат потреба од помалку одржување.

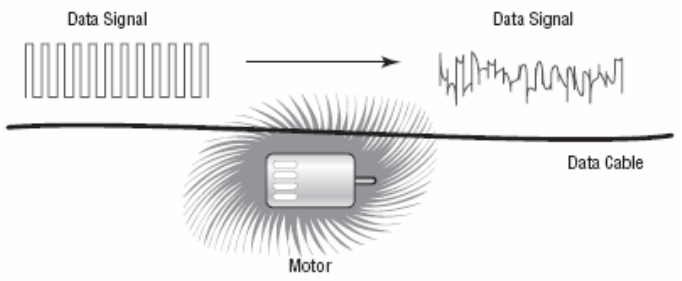
Користење на штитници

Користењето на штитниците се однесува на процесот на заштита случаите кога електричното зрачење од вашите компјутерски системи може да биде користено за прибирање на податоци, како и за заштита од надворешни електрични влијанија кои можат да ги прекинат вашите информатички процеси. Во фиксна канцеларија, како компјутерски центар на пример, добро е да се постави фарадеев кафез околу собата за да овозможи заштита. Фарадеевиот кафез обично се состои од жици кои ја опкружуваат собата во форма на кафез кој ја обиколува собата. Целата таа конструкција потоа се заземјува. Поради овој кафез, електро-магнетните сигнали ниту можат да влезат во собата ниту пак да ја напуштат. За да се потврди функционалноста на кафезот, радио бранови се пуштаат од собата и се тестираат со посебни уреди за мерење. Овој дел ги дискутира проблемите на радио и електромагнетните пречки.

Електромагнетни пречки и радио-фреквенциски пречки

Electromagnetic interference (EMI) и Radio Frequency interference (RFI) се две додатни работи за кои треба да се размислува при поставувањето на канцелариите. Мотори, светла и други типови на електро механички објекти причинуваат EMI, кои можат да доведат до преоптоварување на електричните кола, шилци, или уништување на електронските компоненти. Сите сигнални линии треба да се правилно заштитени и заземјени за да се минимизира EMI. Уредите кои генерираат EMI треба физички да се оддалечат од каблите поради тоа што овој тип на енергија слабее со зголемувањето на далечината.

Сликата 2.9 покажува мотор кој генерира EMI. Во овој пример кабелот кој се наоѓа до моторот прима EMI. Ова придонесува сигналот да деградира, што може да доведе до онеспособување на линијата. Сивата зона на сликата ги претставува пречките кои ги генерира моторот. RFI е нус - производ на електронскиот процес, и е сличен со EMI. Основната разлика е во тоа што RFI се шири низ радио спектарот. Моторите со расипани четкици генерираат RFI. Доколку нивото на RFI стане превисоко, може да ги онеспособи рисиверите во безжичните единици, (овој процес е наречен desensitizing, и се појавува поради големината на енергијата во RF). Ова може да се појави дури и ако сигналите се на различни фреквенции.



Сл. 2.9: EMI интерференци во каблите

Проектот TEMPEST

TEMPEST е името на проектот започнат од страна на USA во доцните 1950-ти. TEMPEST е проект кој имал за задача да доведе до намалување на електронските шумови кои можат да доведат до откривање на податоци кај системите и информациите. Овој програм стана стандард за компјутерските системи и нивна сертификација. TEMPEST заштитата значи дека компјутерскиот систем не произведува значајни количества на EMI и RFI. За уредот да биде одобрен како TEMPEST уред, тој мора да издржи големи тестирања, според строго пропишани стандарди. TEMPEST уредите чинат двапати повеќе од тие кои не се TEMPEST сертифицирани.

Сликата 2.10 го покажува процесот на нечувствителност кој се појавува кај WAP (Wireless Access Portal). Единствено решение во оваа ситуација е да се оддалечат уредите или да се изгаси RFI генераторот.

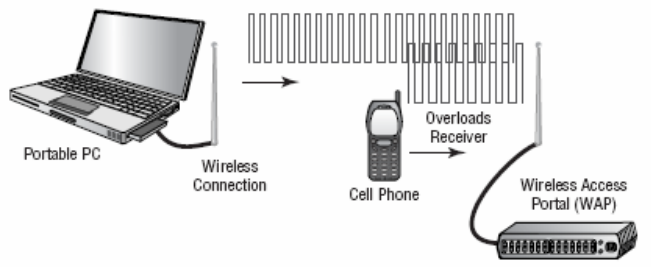
2.2.8 Гаснење на пожари

Гаснењето на пожарите е клучен момент во дизајнирањето на компјутерскиот центар. Тука станува збор за гаснење на пожарот и исто така превенцијата од пожари. Два типа на превенција од пожари се користи: противпожарни апарати и фиксни системи.

Противпожарни апарати

Противпожарните апарати се мали системи. Изборот и користењето на противпожарните апарати е критичен момент. Постојат четири типови на противпожарни апарати, класифицирани според типот на пожарот кој го гаснат: A, B, C и D. Табелата 2.1 ги опишува типовите на пожар и можностите на различните против-пожарни апарати.

Неколку мулти-функционални типови на противпожарни апарати ги комбинираат различните типови на гаснење во една боца. Попознати типови на противпожарни апарати се A-B, B-C и ABC. Препорачана процедура за користење на противпожарните апарати се нарекува PASS метода: Pull, Aim, Squeeze и Sweep. Противпожарните апарати работат само неколку секунди – ако користите таков апарат, немојте да се фиксирате само на една точка. Повеќето противпожарни апарати имаат лимитиран ефект на средна далечина.



Сл. 2.10: RFI нечувствителност која се појавува како резултат на мобилен телефон

Табела 2.1 Рангирање на противпожарните апарати

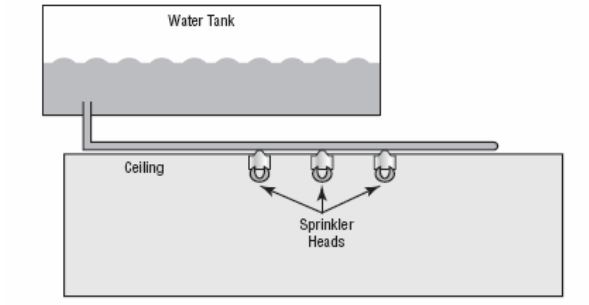
Тип	Користење	Состав
A	Дрво и хартија	Вода или хемикалија
B	Запалливи течности	Противпожарни хемикалии
C	Електрика	Хемикалии кои не пренесуваат струја
D	Запалливи метали	Различни, специфични типови

Забелешка: Голема опасност кај електричните пожари е тоа што тие се обновуваат многу брзо ако напонот не е тргнат. Значи прво изгасете го напонот ако дојде до пожар кај вашите системи.

Повеќето противпожарни апарати бараат редовна проверка. Ова е омилена поента на противпожарните инспектори. Постојат сервиси кои треба да го работат тоа редовно. Тие ќе ги прегледаат или ќе ги заменат противпожарните апарати според предвидениот план специфициран во договорот.

Фиксирани системи

Фиксираните системи обично се дел од системите на самата зграда. Најчестите фиксирани системи се комбинација од противпожарни детектори со системи за гаснење на пожари, каде детекторите обично стартуваат поради брзо зголемување на температурата или поради нагло појавување на чад. Противпожарните системи користат прскалки за вода или гас. Системите на вода работат со прскалки поставени на плафонот, како на сликата 2.11. Овие системи се најчести во модерните згради. Системите на вода се релативно евтини, сигурни и бараат малку одржување.



Сл. 2.11: Против пожарен систем базиран на вода

Единствениот недостаток кај противпожарните системи е тоа што водата екстремно ги оштетува односно уништува електронските системи и компјутерите. Овие системи можат да бидат поврзани со системите за електрична енергија, па така струјата може да се изгаси пред да се пушти вода во зградата. Системите базирани на гас оригинално биле дизајнирани да користат јаглерод диоксид, или подоцна гас наречен Halon. Halon – от не се користи повеќе поради тоа што ја оштетува озонската обвивка, сега постојат попријателски гасови за самата околина. Принципот на работа кај системите кои користат гас е да се истисне кислородот од самата соба, а со тоа се истиснува една од компонентите потребни за да има пожар.

Забелешка: Евакуирајте ја собата веднаш ако дојде до пожар. Системите базирани на гас работат на принцип на истиснување на кислородот од огинот, самото ова може да загуши секого во собата.

Главниот недостаток кај системите базирани на гас е тоа што тие, за да бидат ефективни, бараат затворена околина. Специјални системи за вентилација обично

се инсталираат во системите на гас за да ја ограничат циркулацијата на воздухот кога се испушта гасот. Системите на гас се исто така многу скапи и обично се имплементираат во компјутерските соби или во областите каде водата може да направи многу штета врз технологијата која е во тие простории.

2.3 НАПАДИ НА ОДРЕДЕНИ OSI-НИВОА

2.3.1 Хакерски напади

Потребно е да го познаваме непријателот. Хакерите се причина за имплементација на безбедносни мерки и длабинска одбрана. Познавајќи ги мотивите на хакерите, можете да го предвидите нивото на ризик и да се прилагодите на типот на опасност која ја очекувате, истовремено обезбедувајќи доволна достапност за овластените корисници. Хакирање е обид да се добие пристап до компјутерски систем без овластување. Оригинално, изразот хакер се однесувал на напреден PC корисник, и PC гурута сеуште го користат овој израз за да се нарекуваат себеси така. Но, кога провалувањето во компјутерските системи станало популарно, изразот хакер е искористен за обележување само на компјутерските криминалци, и со тоа изразот е доведен во негативна конотација. Хакерството е илегално. Според меѓународните закони, провалникот свесно го извршува криминалот и за да се гони - потребно е барем еден доказ дека неовластениот пристап е илегален.

Постојат неколку типа на хакерски напади на различните нивоа од ОСИ моделот: sniffers (прислушкувачи), spoofing attacks (лажно претставување), denial of service (поплава со пакети), вируси, spam и spyware. Во табела 2.2 е даден преглед на потенцијалните напади со кои може да се соочи мрежата.

Табела 2.2 – Напади врз мрежата (методи).

Закана	OSI ниво	Дефиниција	Типични симптоми
Измама (Spoofing)	- Мрежно - Data Link	Убедување на компјутер од мрежата да се претстави како друг компјутер, обично со специјални привилегии за пристап добивајќи така пристап до другите компјутери од мрежата.	Конкретниот компјутер најчесто нема пристап до user-level команди, па се обидува да пристапи до e-mail и handler на пораки
Маскирање (Masquerade)	- Мрежно	Пристап до компјутер преправајќи се дека има авторизиран идентитет.	Корисникот кој се маскира често користи мрежа или администраторски командни функции за уште поконкретен влез во системот –

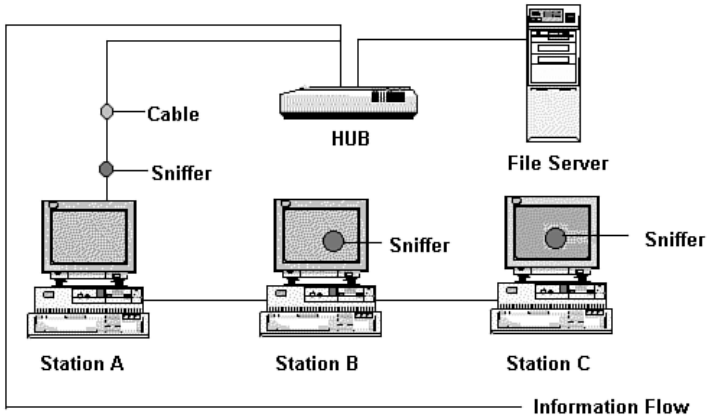
			симнување лозинка или рутирачки табели.
Секвенцијално скенирање	-Транспортно - Мрежно	Секвенцијално тестирање на лозинки се додека една не се покаже валидна.	Повеќе корисници се обидуваат да извршат администраторски командни функции, индицирајќи повеќекратно маскирање.
Скенирање на речници	-Апликациско	Скенирање низ речник од најчесто користени лозинки додека не се дојде до валидна лозинка.	Повеќе корисници се обидуваат да извршат администраторски командни функции, индицирајќи повеќекратно маскирање.
Дигитално трагање (Digital snooping)	- Мрежно	Електронско следење на дигитални мрежи со цел откривање на лозинки и други податоци.	Корисници или дури и администратори се on-line надвор од работно време. Линковите се поподложни на snooping од јазлите.
Spamming	-Апликациско - Мрежно	Преоптоварување на системот со пораки или друг сообраќај за да се предизвика пад.	Постојани падови на системот
Tunneling	- Мрежно	Било кој дигитален напад кој се обидува да навлезе “под” сигурносниот систем пристапувајќи до многу ниски системски функции – драјвери за уреди или OS тунели.	Бизарно однесување на системот, неочекувани пристапи до дискот, необјаснво откажување на уредите, стопиран сигурносен софтвер итн.
Browsing	-Апликациско - Мрежно	Најчесто автоматизирано скенирање на големо количество незаштитени податоци во обид да се добие идеја за пристап.	Авторизиран корисник on-line во невообичаено или надвор од работно време индицирајќи потенцијално маскирање.

2.3.2 Sniffers

Sniffer (прислушкувач), претставува (и вообичаено е) комбинација од хардвер и софтвер. Софтверот може да биде обичен мрежен анализер со додадени опции за дебагирање, а може да биде и вистински прислушкувач на сообраќај.

Sniffer-от мора да е лоциран внатре, во рамките на мрежата која е цел на прислушкувањето. Освен неколку исклучоци, sniffer-от може да се смести било каде во мрежата (слика 2.12). Sniffer-те претставуваат голема закана, бидејќи:

- Можат да ги слушнат лозинките (passwords).
- Можат да ги слушнат довелрливите информации.
- Можат да ја нарушат безбедноста и на соседните мрежи.



Сл. 2.12: Sniffer - прислушкување во мрежата

2.3.3 Spoofing attacks

Под spoofing attack се подразбира лажно претставување. Овој напад може да се изврши на две нивоа од ОСИ-моделот: на податочно ниво (ниво на преклопник - switch), т.н. ARP spoofing, и на мрежно ниво (ниво на рутер), т.н. IP spoofing. При ARP spoofing, напаѓачот неовластено се приклучува на некоја локација од мрежата и при тоа користи MAC-адреса од некој веќе постоечки хост. Кај IP spoofing нападите, хакерот се обидува да го искористи автоматскиот дијалог помеѓу хостовите. Затоа, нападот IP spoofing е многу опасен, бидејќи хакерот никогаш не користи username или password. За да нападне, хакерот прво лоцира која машина е ранлива, т.е. има отворени порти за влез. После тоа, може да ги пресретне, модифицира и избрише IP пакетите. Ефикасна заштита од spoofing, претставуваат методите за автентикација (докажување на идентитетот), кои се опишани во Поглавје 4.

2.3.4 Denial of service

***D**enial-**o**f-**s**ervice нападот,* претставува тип на мрежен напад што ја преплавува мрежата со бескорисен сообраќај. Многу DoS напади, како *Ping of Death* и *Teardrop* нападите, ги користат ограничувањата на TCP/IP протоколите. За сите познати DoS напади, постојат софтверски закрпи што администраторите можат да ги инсталираат за да ја намалат штетата која е предизвикана од нападот. Но, како и вирусите, нови DoS напади постојано се креираат од хакерите. DoS нападот може да предизвика откажување на мрежните сервиси, загуба на конекција и намален bandwidth, како и намалени перформанси на машината-жртва.

2.3.5 Вируси, spam, spyware

Вирусите, spam-от и spyware-от претставуваат напади на апликативното ниво (повеќе за нив ќе кажеме во Поглавје 9 - Безбедност на email). Компјутерските вируси се програми направени од социопатски програмери кои сакаат да причинат штета на вашиот компјутер. Некои вируси се само мали досадни работи, како вирусот амбуланта кој прикажува мала амбулантна кола како вози по вашиот екран. За несреќа, повеќето вируси се многу подеструктивни. Некои вируси бришат податоци од вашиот компјутер, или се обидуваат да го форматираат хард дискот, причинувајќи губење на сите податоци и програми.

Има многу различни типови на вируси. Вирусите на "boot sector" го напаѓаат вашиот master boot запис на дискот, кој му е потребен на компјутерот за да стартува. "Тројански коњ" е програма што се преправа дека е корисна, како игра. Скришно ги оштетува или брише вашите датотеки кога ги користите. Дали некогаш сте креирале "macro" документ додека сте работеле текст во Word. Ако примите пишан документ прикачен за вашиот mail, тој може да содржи macro кој може да е деструктивен. Денеска има повеќе од 8000 типови вируси. Дури и некој софтвер излезен од комерцијална фабрика за софтвер, може да е испорачан со вирус.

Исто така, како штетни компоненти што редовно ги примате на вашиот диск претставуваат spam и spyware. Скоро 80% од целокупната e-mail комуникација денес отпаѓа на spam. Spam претставува несакана порака, т.е. нешто што го добивате без да сте го побарале. Најголеми генератори на спам се САД и Кина. Најчесто spam-от се праќа со маркетиншки цели (рекламирање на одредени продукти), но често има и елементи на измама (лотарија, награди исл.). Spyware исто така претставува штетен програм, што се пренесува преку т.н. cookies, или преку peer-to-peer програми (Kazaa, E-mule исл.). Се користи или за рекламни цели, или со шпионски намери - го контролира вашиот софтвер дали е лиценциран, без вие да знаете.

Има неколку добри антивирус и anti-spyware програми на пазарот. Тие го проверуваат критичниот boot sector на вашиот компјутер секогаш кога тој стартува, но ова не е комплетна инспекција. Изложени сте на ризик од вирус (или spyware), секогаш кога некој од овие настани се случил:

1. Скенирајте ги сите непознати дискети за вируси, пред да ги употребите. Ако компјутерот веќе го прочитал дискот, скенирајте го хард дискот.

2. Сте се логирале на Mirc, или сте симнале датотека од Интернет.

3. Сте примиле e-mail attachment и сте го отвориле.

4. Еднаш неделно имајте регуларно-одредено време за одржување на компјутерот.

Тогаш, треба да направите комплетно скенирање со антивирусен (anti-spyware) програм. Кога за првпат ќе инсталирате програма за проверка од вируси, таа ќе ги сними информациите за сите важни системски датотеки на вашиот компјутер. Ова

се вика “inoculation”. Кога програмата проверува од вируси, ги споредува вашите системски датотеки со снимената информација. Ако го надградите вашиот оперативен систем, на пример од Windows 95 на 98, проверувачот на вируси ќе ве извести дека системските датотеки се промениле. Бидејќи ова е очекувано, ќе му дадете инструкции на програмот да инокулира повторно.

Најпопуларен антивирус е Norton Antivirus од Symantec. Друг популарен програм е Virusscan од McAfee. Популарен anti-spyware е Spyware Doctor. Антивирусната програма ги бара системските фајлови што се смениле и скенира за дигитални потписи од познати вируси. Како и да е, над 200 нови вируси се откриваат секој месец, така што треба да го надградувате вашиот антивирус редовно. Најновите Norton и McAfee програми ви дозволуваат да ги ажурирате вирусните дефиниции преку модем и Интернет конекција. Norton ажурирањето е бесплатно една година. Откако ќе ги симнете ажурирањата на вирусните потписи, треба да ги дистрибуирате на работните станици. Во табела 2.3 е даден преглед на методите кои се користат при напад со вируси.

Табела 2.3 – Напади врз мрежата (вируси)

Закана	**OSI ниво**	**Дефиниција**	**Типични симптоми**
Вирус (Virus)	Апликациско	Малициозен софтвер кој се прикачува себеси на постоечкиот софтвер. На пример, софтверска апликација со patch при што алгоритмот на patch-от е дизајниран така да се употреби себеси и на други апликации значи да се размножува	Се размножува во компјутерскиот систем закачувајќи се на секоја софтверска апликација. Повеќе категории: од шеговит до катастрофален.
Црв (Worm)	-Апликациско - Мрежно	Малициозен софтвер кој постои самостојно.	Најчесто се пропагира преку мрежа.
Тројански Коњ (Trojan Horse)	Апликациско	Црв кој се преправа дека е корисна програма или вирус кој е намерно прикачен на корисна програма пред дистрибуција.	Исто како кај Црвот и Вирусот; понекогаш праќа информации или ги прави достапни за натрапникот.
Временска Бомба (Time Bomb)	Апликациско	Вирус или Црв дизајниран да се активира во одредено време.	Исто како Црвот и Вирусот но се пропагира после програмираното време. Најчесто ги пронаоѓаат предвреме.
Логичка Бомба (Logic	Апликациско	Вирус или Црв дизајниран да се активира под одредени	Исто како Вирус и Црв.

Bomb)		околности.	
Зајак (Rabbit)	-Апликациско - Мрежно	Црв програмиран да се реплицира додека не ги исцрпи ресурсите на компјутерот.	Зајакот ги конзумира сите процесорски ресурси, цел хард диск, мрежни ресурси итн.
Бактерија (Bacterium)	Апликациско	Вирус дизајниран да се вметне себеси во OS и да ги исцрпи сите компјутерски ресурси, особено CPU циклусите.	Оперативниот систем троши се повеќе процесорско време што на крај резултира со осетно намалување на брзината на трансакциите.

2.4 FIREWALL

2.4.1 Општо за технологијата Firewall

Мрежните firewall-и претставуваат уреди или системи што го контролираат текот на мрежниот сообраќај помеѓу мрежите, применувајќи разни безбедносни процедури. Во денешни услови, firewall-от и неговата околина спаѓаат во областа на Internet безбедноста и TCP/IP протоколите. Сепак, firewall-от може да се примени и во мрежа која воопшто не е поврзана на Internet. На пример, многу корпорациски мрежи користат firewall за да го ограничат поврзувањето до и од внатрешните мрежи кои имаат специфична функција, како на пример Секторите за финансии или за кадровски работи. Со примена на firewall за контрола на конективноста, организацијата се заштитува од неавторизиран пристап до одредени системи и ресурси. Постојат неколку типови на firewall-платформи кои се достапни на пазарот. Еден начин за споредба на перформансите на firewall-те е преку нивоата на мрежниот OSI модел што даден firewall ги користи во своето функционирање. Основните firewall-и работат на мал број на нивоа; понапредните firewall-и покриваат поголем број на нивоа. Во термини на функционалност, firewall-те што можат да испитуваат поголем број на нивоа, се поефикасни.

2.4.2 Пакетни филтри

Најосновен, фундаментален тип на firewall е т.н. пакетен филтер. Пакетниот филтер претставува неопходен рутирачки уред што содржи функции за контрола на пристап до системските адреси и комуникациските сесии. Функциите за контрола на пристап на пакетниот филтер се прават со помош на множество од директиви, т.н. множество правила - ruleset. Едноставно множество правила на еден пакетен филтер е дадено во Табела 2.4.

Во најосновна форма, пакетните филтри работат на ниво 3 (мрежно) од OSI моделот. Основната функционалност е дизајнирана да овозможи мрежен пристап врз база на информациите кои се содржани во мрежниот пакет:

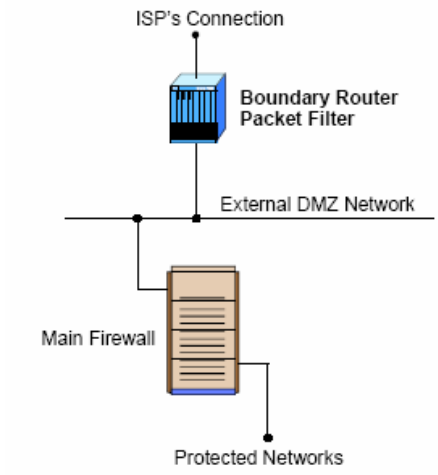
- *Изворна адреса* на пакетот, т.е., ниво 3 адреса на компјутерот од каде што доаѓа пакетот (IP адреса, на пр. 192.168.1.1).
- *Дестинациска адреса* на пакетот, т.е., ниво 3 адреса на компјутерот каде што треба да стигне мрежниот пакет (пр., 192.168.1.2).
- *Тип на сообраќај*, т.е., специфичен мрежен протокол што се користи за комуникација помеѓу изворните и дестинациските системи (најчесто Ethernet - Layer 2 и IP - Layer 3).
- Некои *карактеристики на Ниво 4 - комуникациските сесии*, како што се изворна и дестинациска порта на сесијата (пр., TCP:80 за дестинациската порта на web server, TCP:1320 за изворна порта на персонален компјутер што пристапува на серверот).
- Понекогаш, додатни информации за тоа *на кој интерфејс на рутерот доаѓа пакетот,* и од кој интерфејс на рутерот излегува пакетот; ова е корисно за рутери со 3 или повеќе мрежни интерфејси.

Табела 2.4. Множество правила на еден пакетен филтер.

Изворна адреса	**Извор. порта**	**Дестинацис. адреса**	**Дестинац. порта**	**Акција**	**Опис**
Any	Any	192.168.1.0	> 1023	Дозволи	Дозволува повратни TCP конекции до внатрешната подмрежа
192.168.1.1	Any	Any	Any	Забрани	Спречи го Firewall-от сам директно да се конектира било каде
Any	Any	192.168.1.1	Any	Забрани	Спречи ги надворешните корисници директно да пристапат до Firewall-от.
192.168.1.0	Any	Any	Any	Дозволи	Внатрешните корисници можат да пристапат до надворешните сервери
Any	Any	192.168.1.2	SMTP	Дозволи	Дозволи на надворешни корисници да ни пратат email

Any	Any	192.168.1.3	HTTP	Дозволи	Дозволи пристап на надворешни корисници до WWW серверот
Any	Any	Any	Any	Забрани	"Catch-All" правило - Сè што не е дозволено - е забрането

Пакетниот филтер има две главни предности: брзина и флексибилност. Бидејќи пакетниот филтер обично не ги третира нивоата што се над третото во OSI моделот, тој работи многу брзо. Исто така, бидејќи модерните мрежни протоколи се имплементираат на ниво 3 и подолните нивои, пакетните филтри можат да ги обезбедуваат скоро сите мрежни комуникации и протоколи. Оваа едноставност му овозможува на пакетниот филтер да биде применет во скоро секоја мрежна инфраструктура. Важна поента е што неговата брзина и флексибилност, како и способноста да блокира denial-of-service и слични напади, го прават погоден за сместување на најдалечната граница на една необезбедена мрежа. Пакетниот филтер, познат како *граничен рутер*, може да блокира одредени напади, да ги филтрира несаканите протоколи, да врши едноставна контрола на пристап, а потоа да го проследува сообраќајот кон други firewall-и што ги испитуваат повисоките нивоа од OSI моделот.



Сл. 2.13: Пакетен филтер применет како граничен рутер.

Пакетниот филтер поседува и некои слабости:

- Бидејќи пакетниот филтер не ги испитува горните нивоа, тој не може да пружа заштита од напади што користат апликациско-специфични ранливости. На пример, пакетниот филтер не може да блокира специфични апликативни

наредби; ако пакетниот филтер дозволува одредена апликација, сите функции од таа апликација ќе бидат дозволени.

- Заради ограничените информации што ги има firewall-от, можноста за евиденција на сообраќајот - кај пакетниот филтер е лимитирана. Пакетниот филтер ги евидентира само информациите што се битни за контролата на пристап (изворна адреса, дестинациска адреса, и тип на сообраќај).
- Повеќето пакетни филтри не поддржуваат напредни методи за автентикација на корисниците. Уште еднаш, ова ограничување се должи на недостатокот за испитување на погорните нивоа од ОСИ моделот.
- Тие се ранливи на напади и имаат слабости во врска со TCP/IP протоколот, како што е *spoofing на адреси на мрежното ниво*. Повеќето пакетни филтри не можат да детектираат мрежен пакет во кој била сменета OSI Layer 3 - адресната информација. Spoofing нападите претежно се корстат за да се премостат сигурносните контроли имплементирани во firewall-от.
- Конечно, заради малиот број на варијабли кои се користат за контрола на пристапот, пакетните филтри се подложни и на несоодветно конфигурирање. Со други зборови, лесно е да се згреши конфигурирањето на пакетен филтер, при што ќе биде дозволен оној сообраќај што би требало да биде забранет според сигурносната политика на организацијата.

Според тоа, пакетно-филтерските firewall-и се многу погодни за брзи мрежи каде што евиденцијата на сообраќај и автентикацијата на корисниците не се многу важни.

Бидејќи денешната firewall технологија содржи многу особини и функции, тешко е да се идентификува единствен firewall што содржи само особини на пакетен филтер. Најблизок пример е мрежниот рутер што користи кодирана листа за контрола на пристап за да управува со мрежниот сообраќај. Едноставноста на пакетните филтри овозможува имплементација на решенија кои пружат голема достапност и сигурност; некои производители нудат хардверски и софтверски решенија што пружат голема достапност и сигурност. Повеќето SOHO (Small Office Home Office) -домашни firewall-и и firewall-и на оперативниот систем се претежно пакетни филтри.

2.4.3 Состојбено-инспекциски firewall

Состојбено-инспекциските firewall-и претставуваат пакетни филтри што вклучуваат испитување на нивото 4 од OSI, (транспортно ниво). Состојбената инспекција е креирана од потребата да се вклучат некои особини на TCP/IP протоколот што го отежнуваат поставувањето на firewall. Кога TCP (конекциски-ориентиран транспорт) апликацијата креира сесија со далечински хост, се креира порта на изворниот компјутер која служи за примање на мрежниот сообраќај од дестинацискиот компјутер. Според TCP спецификацијата, оваа клиентска *изворна порта* ќе биде поголема од 1023 и помала од 16384. Согласно со конвенциите, дестинацискатa порта на оддалечениот хост ќе биде со помал број, т.е. помал од 1024. Таа изнесува 25 за SMTP, на пример. Во суштина, состојбено-инспекциските

firewall-и додаваат функционалност од нивото 4 кон стандардната архитектура на пакетен филтер. Состојбено-инспекциските firewall-и ги содржат добрите и лошите страни на пакетните филтри, но заради состојбената табела, состојбено-инспекциските firewall-и во општ случај се посигурни од пакетните филтри. Табела 2.5 дава пример на состојбена табела на состојбено-инспекциски firewall.

Табела 2.5. Состојбена табела на состојбено-инспекциски firewall.

Изворна адреса	**Изворна порта**	**Дестинациска адреса**	**Дестинац. порта**	**Конекциска состојба**
192.168.1.100	1030	210.9.88.29	80	воспоставена
192.168.1.102	1031	216.32.42.123	80	воспоставена
192.168.1.101	1033	173.66.32.122	25	воспоставена
192.168.1.106	1035	177.231.32.12	79	воспоставена

Состојбено-инспекцискиот firewall се разликува од пакетниот филтер со тоа што инспекцијата на состојбата е применлива само кај TCP/IP мрежите. Состојбено-инспекцискиот firewall може да се имплементира и за друг мрежен протокол (како и пакетниот филтер), но вистинската состојбена инспекција е можна само кај TCP/IP. Заради ова, многу автори ги класифицираат состојбено-инспекциските firewall-и како над-множество на пакетните филтри.

2.4.4 Апликациско-proxy-gateway firewall

Апликациско-proxy-gateway firewall е напреден firewall што ги комбинира пониските нивоа на пристап со функционалноста на горните нивои (ниво 7 - апликациско). Апликациско-proxy-gateway firewall-от не бара ниво 3 (мрежно) рутирање помеѓу внатрешниот и надворешниот интерфејс на firewall-от; софтверот на firewall-от го прави рутирањето. Ако апликациско-proxy-gateway софтверот откаже, firewall-от нема да биде во состојба да го проследува сообраќајот низ мрежата. Сите мрежни пакети што транзитираат низ firewall-от го прават тоа под софтверска (апликациско-proxy) контрола. Апликациско-proxy-gateway firewall-те имаат повеќе предности над пакетните филтри и состојбено-инспекциските firewall-и. Прво, апликациско-proxy-gateway firewall-те содржат повеќе опции за евиденција на сообраќајот, бидејќи firewall-от тука го испитува цел мрежен пакет, а не само адресата и портите. На пример, апликациско-proxy-gateway дневникот може да содржи апликациско-специфични команди за мрежниот сообраќај. Друга предност е што апликациско-proxy-gateway firewall-те им овозможуваат на систем-администраторите да ги принудат корисниците да се автентицираат соодветно со важноста на мрежната инфраструктура. Апликациско-proxy-gateway-те се способни за директна автентикација на корисниците, за разлика од пакетните филтри и состојбено-инспекциските firewall-и кои обично ги автентицираат корисниците врз база на адресата на мрежното ниво на нивниот компјутер. Знаејќи дека адресите на мрежното ниво лесно можат да бидат spoof-ирани, автентикациските можности на апликациско-proxy gateway-те се супериорни во споредба со пакетните филтри или состојбено-инспекциските firewall-и. Конечно, знаејќи дека апликациско-proxy-gateway firewall-те не се само Layer 3 уреди, тие се понеранливи на spoofing нападите. Напредната функционалност на апликациско-proxy-gateway firewall-те донесува и некои слабости во споредба со пакетниот

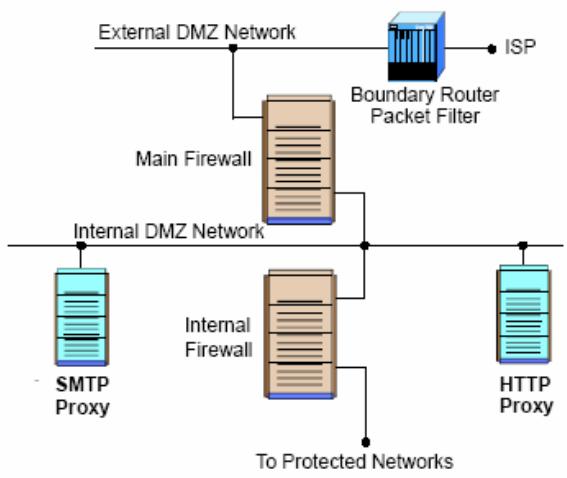
филтер или состојбено-инспекцискиот firewall. Прво, заради 'целосната свесност во поглед на пакетите' кај апликациско-proxy gateway-те, firewall-от е принуден да помине одредено време за читање и интерпретирање на секој пакет. Заради ова, апликациско-proxy-gateway firewall-те не се многу погодни за многу брзи реално-временски апликации. За да се редуцира оптоварувањето на firewall-от, може да се користи посветен proxy server (види подолу), кој ќе ги обезбедува побавните сервиси, на пр. email и поголемиот web сообраќај. Друга слабост е што апликациско-proxy-gateway firewall-от е ограничен во поддршката на новите мрежни апликации и протоколи. За секој тип на мрежен сообраќај што треба да транзитира низ firewall-от, се бара индивидуален апликациско-специфичен proxy агент.

2.4.5 Посветени Proxy сервери

Посветените proxy сервери се разликуваат од апликациски-proxy-gateway firewall со тоа што тие ја задржуваат proxy контролата на сообраќајот, но немаат особини на firewall. Заради тоа, тие типично се сместуваат позади класичните firewall-и. Во повеќето случаи, главниот firewall може да прифати влезен сообраќај, да одреди која апликација е потребна, и потоа да го насочи сообраќајот кон соодветниот proxy сервер, на пр., email proxy сервер. Proxy серверот типично прави филтрирање и евиденција на сообраќајот, а потоа го проследува кон внатрешните компјутери. Proxy серверот може да прифати и излезен сообраќај директно од внатрешните компјутери, да го филтрира и евидентира сообраќајот, а потоа да го проследи кон firewall-от за надворешна достава. Пример за ова е HTTP proxy сместен позади firewall; корисниците се конектираат на овој proxy на пат кон надворешниот web server. Типично, посветените proxy сервери се користат да го намалат оптоварувањето на firewall-от и да направат поспецијализирано филтрирање и евиденција, што би било тешко да го направи самиот firewall.

Како додаток на функциите автентикација и евиденција, посветените proxy сервери се погодни и за скенирање на web и email содржини, вклучително и:
- Филтрирање на Java . applet-и или апликации,
- Филтрирање на ActiveX,
- Филтрирање на JavaScript,
- Блокирање на специфични типови attachment-и (MIME), на пример, .application/ msword (Microsoft Word документи),
- Скенирање и бричење на вируси,
- Скенирање, филтрирање, и бришење на макро вируси,
- Апликациско-специфични, на пример, блокирање на HTTP "delete" наредбата,
- Корисничко-специфични контроли, вклучително блокирање на одредени содржини за определени корисници.

Сл. 2.14 прикажува едноставна мрежа што применува посветени proxy сервери за HTTP и email, сместени позади друг firewall. Во овој случај, email proxy може да биде организацискиот SMTP gateway за излезна пошта. Главниот firewall ќе ја проследи влезната пошта на proxy за да се скенира содржината, а потоа пораката ќе пристигне кај внатрешните корисници, на пр., со POP или IMAP.



Сл. 2.14: Конфигурација со апликациски proxy

2.4.6 Хост-базирани firewall-и

Firewall софтвери се достапни за некои оперативни системи како Linux исл.; тие можат да се користат само за заштита на хостот. Ова може да биде корисно за внатрешните сервери; на пример, внатрешниот web сервер може да се смести на компјутер што има host-базиран firewall. Ова носи одредени предности, вклучително и:

- Серверската апликација се заштитува подобро отколку stand-alone; внатрешните сервери треба посебно да се заштитат и не треба да мислиме дека се безбедни, бидејќи се наоѓаат позади главниот firewall.
- Посебен firewall и подмрежа не се доволни за обезбедување на серверот; хост-базираниот firewall ги врши овие функции.

Хост-базираниот firewall типично овозможува контрола на пристап и рестрикција на сообраќајот од и до серверите што се сместени на хостот, а исто така и лимитирање на логирањата. Додека хост-базираниот firewall е непожелен во околини со интензивен сообраќај, во внатрешните мрежи и регионалните канцеларии тој нуди голема сигурност за мала цена. Слабост на хост-базираните firewall-и е што тие мора да се администрираат одвоено, и после извесен период станува поедноставно и поевтино да се сместат сите сервери позади наменски (посветен) firewall.

2.4.7 Лични firewall-и

Обезбедувањето на домашните компјутери денес е важно како и безбедноста на работа; многу луѓе работат од дома при што користат службени податоци. Домашните корисници пристапуваат преку Internet Service Provider (ISP), и имаат слаба firewall заштита, бидејќи ISP не можат да обезбедат потенцијално многу различни безбедносни политики. Затоа, развиени се лични personal firewall-и кои обезбедуваат заштита на домашните компјутери, а извршуваат скоро исти функции како и големите firewall-и.

Овие продукти типично се имплементираат во една или две конфигурации. Една од конфигурациите е т.н. *личен Firewall*, кој се инсталира на компјутерот што треба да се заштити; личните firewall-и обично не нудат заштита на други компјутери и ресурси. Исто така, личните firewall-и не обезбедуваат контрола на мрежниот сообраќај што се движи низ компјутерскиот систем - тие само го штитат компјутерот на кој се инсталирани.

2.4.8 Firewall околина

Firewall околина е поим што опишува множество од системи и компоненти што овозможуваат целосна firewall функционалност во дадена точка од мрежата. Едноставна firewall околина може да се состои од еден пакетен филтер и ништо повеќе. Во посложена и посигурна околина, таа може да се состои од неколку firewall-и, proxi-ја, и специфични топологии за поддршка на системите и безбедноста. Во продолжение ќе опишеме системи и мрежни топологии кои се користат во популарните firewall околини. Постојат 4 принципи што треба да се напомнат:

Направете го едноставно - овој принцип треба да го имате прво на ум кога дизајнирате firewall околина. Навистина, колку е поедноставно firewall решението, ќе биде и побезбедно и полесно за одржување. Сложеноста во дизајнот честопати доведува до грешки во конфигурацијата.

Користете уреди што се наменети за тоа - користењето на мрежни уреди за она за што тие се наменети значи да не правите firewall од нешто што не може да служи како firewall. На пример, рутерите се за рутирање; нивната можност за филтрирање пакети не е нивна примарна цел, и ова треба да го има на ум секој што прави имплементација на firewall. Користењето само на рутер во улога на firewall е опасно; може да биде конфигуриран погрешно. Мрежните преклопници (switch) се друг пример; кога се користат за насочување на сообраќајот *надвор* од firewall околината, тие се подложни на напади однадвор при што можат целосно да откажат. Во многу случаи, хибридните firewall-и и софтверските firewall-и се подобро решение, бидејќи тие се оптимизирани да бидат firewall и ништо друго.

Креирајте длабинска заштита - длабинската одбрана опфаќа креирање на безбедносни нивои (не едно туку неколку). Познатата Maginot линија, е пример за тоа што не треба да се прави во firewall околината: да ја сместите цела заштита во еден firewall. Ако се потребни повеќе firewall -и, тогаш навистина треба да се применат сите. Ако рутерот овозможува некаква контрола на пристап или филтрирање, тоа треба да се искористи. Ако оперативниот систем на серверот обезбедува некакви firewall можности, искористете го и него.

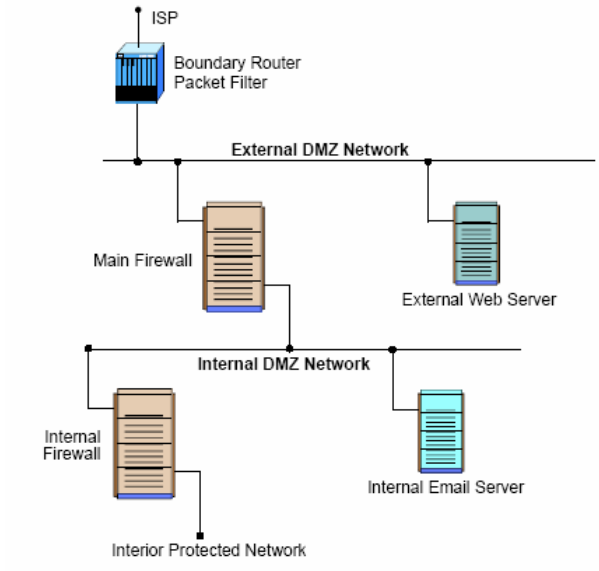
Внимавајте на внатрешните закани - конечно, внимавањето само на надворешните закани - ја остава мрежата широко отворена за напади одвнатре. Ако не ви се верува дека вашите колеги се потенцијална закана, сметајте на тоа дека ако некој натрапник успее да го пробие firewall-от - ќе има слободен пристап до внатрешните сервери. Затоа, важните сервери (на пр. email server или финансиски податочен сервер) треба да се сместат позади внатрешни firewall-и или т.н. DMZ околини.

Како заклучок од оваа дискусија, треба да се сфати дека изреката “сите правила постојат за да се прекршат” целосно се однесува на правењето firewall околини.

Дизајнерите на firewall треба да се придржуваат до правилата кога градат околини, но секоја мрежа и организација има уникатни барања и потреби, па според тоа бара и уникатни решенија.

2.4.9 DMZ мрежи

Најопшта околина со firewall имплементација е т.н. DMZ, или демилитаризирана зона. DMZ мрежата се креира како мрежна конекција на два firewall-и; т.е., кога два или повеќе firewall-и постојат во околината, мрежите што ги поврзуваат firewall-те може да бидат DMZ мрежи.



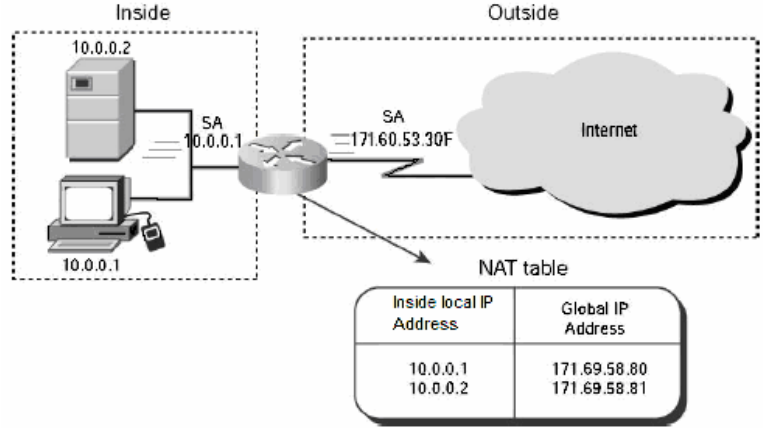
Сл. 2.15: DMZ Firewall околина

DMZ служат како приклучни точки за компјутерите што имаат потреба да пристапуваат и внатре и надвор, но кои не смеат да се сместат во внатрешната заштитена мрежа. На пример, организацијата може да употреби граничен рутер - firewall и два внатрешни firewall-и, и да ги смести сите сервери кои се достапни однадвор во надворешната DMZ - помеѓу рутерот и првиот firewall. Граничниот рутер ќе филтрира пакети и ќе овозможи заштита на серверите, а првиот firewall ќе обезбеди пристап до и заштита од серверите во случај да тие бидат нападнати. Организацијата може да ги смести другите внатрешни сервери во внатрешната DMZ зона, лоцирани помеѓу двата внатрешни firewall-и; firewall-те може да обезбедат заштита и контрола на пристап за серверите, заштитувајќи ги и од надворешни и од внатрешни напади. Оваа околина е прикажана на Сл. 2.15.

2.4.10 Мрежно преведување на адреси (NAT)

Мрежното преведување на адреси (Network address translation - NAT) е многу важен концепт кај компјутерските мрежи, особено во firewall-околини (Сл. 2.16). Прво, NAT е ефективна алатка за сокривање на адресната шема што се наоѓа позади firewall-от. Во суштина, NAT им овозможува на организациите да користат

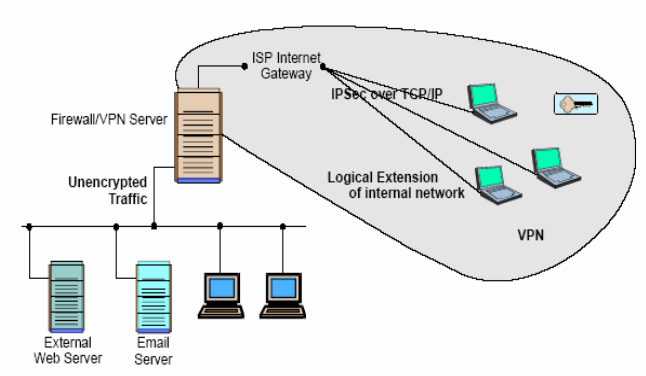
произволна адресна шема позади firewall-от, но сеуште да можат да се конектираат кон надвор преку firewall. Второ, ограниченото множество на IP-адреси придонело да некои организации го користат NAT за пресликување на не-рутабилните IP-адреси во помало множество од легални адреси. Како firewall администратор, не би сакале некои надворешни компјутери да ги знаат вистинските IP-адреси на вашата внатрешна мрежа. Агенцијата за доделување глобални адреси (IANA) го резервирала следниот блок IP-адреси за приватни Internet-и: 10.0.0.0 до 10.255.255.255, 172.16.0.0 до 172.31.255.255, и 192.168.0.0 до 192.168.255.255 - познати како "глобални не-рутабилни адреси". NAT е алатка што се користи за маскирање на вистинските IP-адреси со примена на овие внатрешни адреси. NAT ја конвертира приватната IP-адреса во регистрирана "вистинска" IP-адреса. Повеќето firewall-и не содржат NAT можности. NAT исто така се користи кога корпорациите користат приватни адресни рангови за внатрешните мрежи - не е дозволено овие рангови да бидат рутабилни на Internet.



Сл. 2.16: Илустрација на NAT - мрежно преведување на адреси

2.4.11 Виртуелна приватна мрежа

Друга корисна примена на firewall-от и неговата околина е конструкцијата на виртуелна приватна мрежа (VPN). Виртуелната приватна мрежа се конструира врз постоечките мрежни медиуми и протоколи со примена на додатни протоколи и по можност, енкрипција. Ако VPN е криптирана, може да се користи како проширување на внатрешната заштитена мрежа. Во повеќето случаи, виртуелна приватна мрежа се користи за да обезбеди сигурни мрежни линкови помеѓу мрежи кои се на оддалечени локации. На пример, виртуелната приватна мрежа сè почесто се користи за да овозможи далечински пристап на корисниците до организациската мрежа преку глобалниот Internet. Оваа примена добива на популарност, заради трошоците што би ги имале кога би правеле друг тип приватни конекции, како на пр. безброј модеми. Со примена на виртуелна приватна мрежа, организацијата плаќа само една конекција до Internet, и таа конекција ќе овозможи да корисниците далечински се логираат на приватната мрежа и да ги користат нејзините ресурси. Единствената Internet конекција може исто така да обезбеди и други типови на услуги. Како резултат на ова, овој механизам се смета за многу економичен (cost-effective).

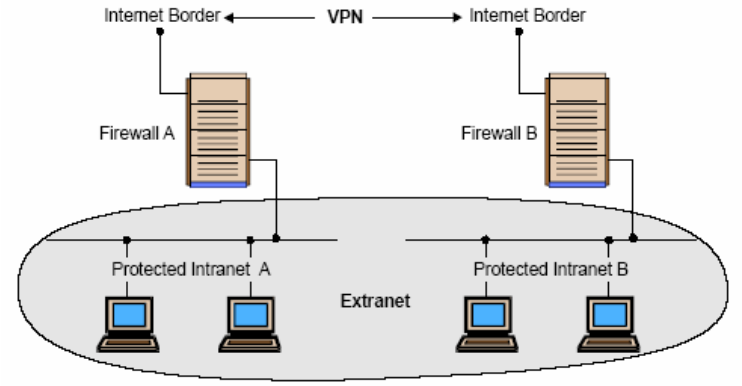


Сл. 2.17: Пример за VPN.

Виртуелната приватна мрежа честопати се користи за креирање сигурни мрежи помеѓу организации или агенции, како на Сл. 2.17. На протоколско ниво, постојат неколку опции за избор на виртуелна приватна мрежа. Првата, и можеби најупотребувана опција е протоколот IPSec11 (Internet Protocol Security). IPSec стандардите се состојат од IPv6 сигурносни особини нанесени врз IPv4, тековната верзија на IP што се користи за Internet. Други VPN протоколи се: PPTP (Point-to-Point Tunneling Protocol), - Microsoft стандард и L2TP (Layer 2 тунелски протокол).

2.4.12 Интранет

Интранет претставува мрежа што користи ист тип на сервиси, апликации, и протоколи како Internet, со тоа што нема надворешна конекција кон светот. На пр., една корпорациска мрежа што го користи протоколот TCP/IP, заедно со HTTP за достава на информации би можела да се смета за Intranet. На Слика 2.18, внатрешните заштитени мрежи се пример за intranet конфигурација. Повеќето организации користат некаков intranet, иако не го нарекуваат така. Во внатрешната мрежа (intranet), можат да се креираат повеќе мали intranet-и со помош на внатрешни firewall-и. На пример, една организација може да ја заштити мрежата на еден свој Сектор со внатрешен firewall, и добиената заштитена мрежа може да се нарече Секторски intranet.



Сл. 2.18: VPN што поврзува два Intranet-а.

2.5 СИСТЕМИ ОТПОРНИ НА ГРЕШКИ

2.5.1 RAID

RAID е кратенка од *преголем низ на независни дискови*. Неговата примарна цел е да овозможи толеранција на грешки и заштита од паѓање на хард-дискот на фајл-серверот. Некои видови RAID секундарно ги подобруваат перформансите на системот со запишување во кеш меморија и дистрибуирање на податоците вчитани на дискот - од повеќе дискови што работат заедно, за да ги зачуваат фајловите истовремено. Всушност, RAID ги одвојува податоците во повеќе единици и ги вчитува на повеќе дискови, користејќи процес наречен „распоредување (striping)“. Тој може да се имплементира или како хардверско или како софтверско решение, но како што ќе видиме, секој вид на имплементација има свои проблеми и придобивки. Советодавниот одбор на RAID има дефинирано три класификации на RAID: диск-системи отпорни на откажување (ДСОО) (Failure Resistant Disk Systems - FRDSs), диск-системи толерантни на откажување и диск-системи толерантни на катастрофа. Од горенаведените само првиот (FRDS) е постоечки стандард, а другите сеуште чекаат на усвојување. Сега ќе зборуваме за различните нивоа на имплементација на FRDS.

Диск-систем отпорен на откажување

Основната функција на еден FRDS е да ги заштити фајл-серверите од губење на податоци и губење на достапноста поради откажување на дискот. Тој дава можност да се реконструира содржината на еден диск што откажал на диск-замена и овозможува дополнителна заштита од губење на податоци поради откажување на многу делови на хардверот на серверот. Една од карактеристиките на FRDS е дека тој овозможува постојан мониторинг на овие делови и алармирање за нивното откажување.

Диск-систем плус отпорен на откажување

Ажурираната верзија на стандардот FRDS се нарекува FRDS+. Оваа ажурирана верзија ја додава и можноста за автоматска топла размена (разменување додека серверот сеуште работи) на дисковите што откажале. Тој исто така додава и заштита од опасности во околината (како што се температурата, состојба на надвор-од-опсегот и надворешен прекин на струјата) и вклучува серија аларми и предупредувања за ваквите откажувања.

2.5.2 Преглед на десетте нивоа на RAID

RAID-нивото 0 создава еден голем диск користејќи неколку дискови. Овој процес се нарекува *распоредување*. Тој ги распоредува податоците преку сите дискови (но не дава преобилност) користејќи го целиот достапен простор на дрејвот за да создаде максимална големина на употреблив волумен на податоци и за да го зголеми перформансот за вчитување/впишување. Еден од проблемите со ова ниво на RAID е дека тој всушност ја намалува толеранцијата на грешки на

диск-системот а не го зголемува – целиот волумен на податоци е неупотреблив ако еден драјв во сетот откаже.

RAID-нивото 1 обично се нарекува пресликување. Тоа ги пресликува податоците од еден диск или сет од дискови така што ги дуплира податоците на друг диск или сет од дискови. Ова често се имплементира со еден–за–еден диск на диск сооднос: секој драјв се пресликува на еднаков драјв-партнер што постојано се ажурира со тековни податоци. Ако еден драјв откаже, системот автоматски ги зема податоците од другиот драјв. Главниот проблем со ова ниво на RAID е дека сообносот еден-за-еден е многу скап и резултира во најголем трошок по мегабајт од капацитетот за податоци. Ова ниво ефективно го дуплира количеството на хард-драјвови што ви е потребно, па оттука обично е подобро за системи со помал капацитет.

RAID-нивото 2 се состои од вметнати бит податоци на повеќе дискови. Паритетната информација се создава користејќи хемингов код што открива грешки и утврдува кој дел од кој драјв има грешка. Тој дефинира еден систем на диск-драјв со 39 дискови: 32 дискови на складирање за корисникот и седум дискови за кодирање на обновувањето на грешките. Ова ниво не се користи во праксата и беше брзо заменето со пофлексибилните нивоа на RAID што следуваат подолу.

RAID-нивоата 3 и 4 се разгледуваат заедно, бидејќи функционираат на ист начин. Единствената разлика е дека нивото 3 се имплементира на ниво на бајти, а нивото 4 обично се имплементира на блок-нивото. Во ова сценарио, податоците се распоредени преку неколку драјвови и битот за проверка на паритетот се впишува на паритетен драјв резервиран за тоа. Ова е слично на RAID 0. И двата имаат голем волумен на податоци, но додавањето на паритетен драјв резервиран за тоа овозможува преобилност. Ако еден хард диск откаже, податоците можат да се реконструираат користејќи ја бит-информацијата на паритетниот драјв. Главниот проблем со ова ниво на RAID е дека постојаното впишување на паритетниот драјв може да создаде performance hit. Во оваа имплементација, резервните драјвови можат да се употребат за да се заменат паднатите драјвови.

RAID-нивото 5 ги распоредува податоците и паритетната информација на блок-нивото преку сите драјвови во сетот. Тој е сличен на RAID 3 и 4, само што паритетните информации се впишуваат на следниот достапен драјв, а не на драјвот резервиран за тоа, користејќи вметнат паритет. Тоа овозможува повеќе флексибилност во имплементацијата и ја зголемува толеранцијата на грешки бидејќи паритетниот драјв не е единствената точка на откажување, како што е случајот со RAID 3 или 4. Вчитувањата и впишувањата на дискот исто така се прават истовремено, со што се зголемува перформансот над нивоата 3 и 4. Со резервните драјвови што ги заменуваат драјвовите што откажале обично може да се направи топла размена, што значи дека можат да се заменат на серверот додека системот е подигнат и работи. Тоа е веројатно најпопуларната имплементација на RAID денес.

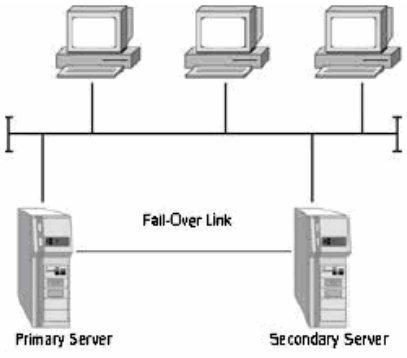
RAID-нивото 7 е варијација на RAID 5 во кој што низот функционира како *единствен виртуелен диск* во хардверот. Тоа понекогаш се симулира така што софтверот работи преку хардверска имплементација RAID-ниво 5. Тоа му

овозможува на низот дрејвови да продолжат да работат ако кој било диск или која било патека до кој било диск откаже. Исто така овозможува заштита на паритетот.

Многу снабдувачи креираат разни други имплементации на RAID за да ги комбинираат карактеристиките на неколку RAID-нивоа, иако овие нивоа не се официјално дефинирани. Нивото 10 е креирано, така што се искомбинирани нивото 0 (распоредување) со нивото 1 (пресликување). Нивото 6 е креирано, така што се искомбинирани нивото 1 (пресликување) со нивото 5 (вметнување).

2.5.3 Други видови на системи толерантни на серверски грешки

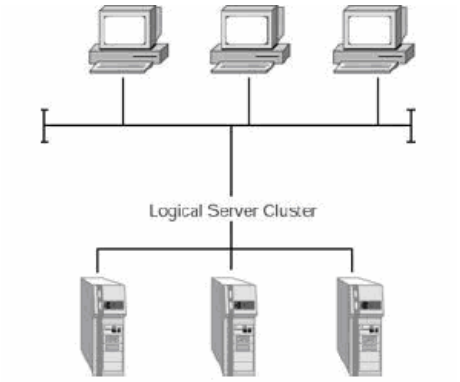
Преголеми сервери. Имплементацијата на преголем сервер го зема концептот на RAID 1 (пресликување) и го применува на пар сервери. Примарниот сервер ги пресликува своите податоци на секундарен сервер, и на тој начин му овозможува на примарниот да се „префрли“ на секундарниот во случај примарниот сервер да откаже (секундарниот сервер влетува и ја презема работата наместо примарниот сервер). Ова префрлување може да биде жешко или топло (т.е., префрлувањето може но не мора да биде транспарентно за корисникот), во зависност од имплементацијата на оваа преобилност на снабдувачот. Ова е исто така познато како толеранција на грешки на серверот. Вообичаени вакви имплементации се: SFTIII на Novell, Октопод (Octopus) и стенд-бај серверот на Vinca.



Сл. 2.19: Вообичаена имплементација на преголем сервер.

Кластеринг на сервери. Кластер на сервери е група независни сервери што се управуваат како еден систем, што овозможува повисока достапност, полесно управување и поголема scalability. Концептот за кластеринг на сервери е сличен на имплементацијата на преголем сервер за која претходно зборувавме, со таа разлика што сите сервери во кластерот се он-лајн и учествуваат во процесирањето барања за услуга. Оспособувајќи ги секундарните сервери да обезбедуваат време на процесирање, кластерот дејствува како интелигентно тело и го балансира оптоварувањето на сообраќајот за да ги подобри перформансите. Кластерот изгледа како еден сервер од точката на гледиште на корисникот. Ако некој сервер во кластерот падне, процесирањето продолжува транспарентно, но сепак кластерот ќе претрпи одредена деградација во перформансот. Оваа имплементација

понекогаш се нарекува „фарма на сервери“. Примери за овој вид имплементација се: Microsoft кластер сервер („Wolfpack“), Oracle паралелен сервер и Tandem нон-стоп.



Сл. 2.20: Еден вид на кластеринг на сервери.

□

3. КРИПТОГРАФИЈА

3.1 ВОВЕД

Криптографијата има долга и фасцинантна историја. Криптографијата, низ годините била уметност која била практикувана од многумина кои измислиле повеќе техники за да одговорат на некои од барањата во врска со сигурноста. Последните дваесет години беа период на транзиција, со тоа што дисциплината преминува од уметност во наука. Сега постојат неколку интернационални научни конференции кои се посветени исклучиво на криптографијата, а исто така и интернационална научна организација, - Интернационална Асоцијација за Криптографско Истражување (IACR), насочена кон надгледување на истражувањата во областа.

Напредокот на компјутерите и комуникациските системи во 1960-те донесе со себе и барања од приватниот сектор во поглед на заштитата на информациите во дигитална форма и обезбедување на сигурносни сервиси. Започнувајќи со работата на Feistel во IBM во раните 1970-ти и со кулминација во 1977 со усвојување на U.S. Federal Information Processing Standard за енкрипција на доверливите информации - DES (Data Encryption Standard) е најдобро познатиот криптографски механизам во историјата. Останува најдобар стандард за обезбедување на електронската трговија за многу финансиски институции низ целиот свет.

Математичките методи кои се користат за трансформација на податоци (енкрипција и декрипција) со едно име може да ги именуваме како криптографија. На таков начин, обичниот текст се трансформира во сигурен формат т.н. шифриран текст, кој обезбедува приватност и заштита. Јачината на енкрипциските алгоритам, т.н. шифрер (cipher), е мерка за степенот до кој шифрираниот текст може да ги издржи криптографските анализи насочени кон разбивање на кодот и откривање на кодираниот текст.

Со тек на време се развило елаборирано множество протоколи и механизми креирани за справување со сигурноста на информациите, кога информацијата се спроведува по физички пат преку пишани документи. Најчесто, информационата сигурност не може да се постигне само со математички алгоритми и протоколи, туку има потреба и од процедури, техники и соодветна законска регулатива за да се постигне сакниот резултат. На пример, приватноста на писмата се постигнува со ставање во запечатени пликови кои потоа ги испорачува поштенската служба. Законската регулатива го заштитува писмото на тој начин што утврдува дека е прекршок да се отвори пликот без претходно одобрение.

Концептуално, начинот на кој се запишуваат информациите не се сменил многу. Порано информациите се запишувале на хартија, а денес голем дел од нив се наоѓаат на магнетни медиуми и се пренесуваат преку телекомуникациски системи. Она што навистина се смени е можноста за копирање и промена на информациите. Може да се направат илјадници идентични копии од некоја информација запишана на електромагнетен медиум и ниедна од нив нема да се разликува од оригиналот.

Со информација која се наоѓа на хартија, тоа е далеку потешко изводливо. За општество во кое информациите се чуваат и пренесуваат по електромагнетен пат, потребен е начин за обезбедување сигурност независно од физичкиот медиум кој ја чува или пренесува информацијата. Една од фундаменталните алатки кои се користат во информационата сигурност е потписот. Потписот е замислен како единствен за секоја индивидуа и служи за идентификација, авторизација и валидација. Кај електромагнетните информации - концептот на потпис треба да се преиспита; потписот не може да биде уникатен за потпишувачот независно од типот на информација која е потпишана. Електронската репродукција е толку лесна што манипулацијата и фалсификувањето на потпишан документ е тривијална работа. Потребата од соодветна заштита е јасна, а техничките методи за таквата работа ги обезбедува криптографијата. Основната цел на криптографијата е адекватно да ги обработи конкретните области на интерес (доверливост, интегритет на податоци, автентификација). Самата причина за постоење на криптографијата е откривање и превенција на измама и останати малициозни дејства.

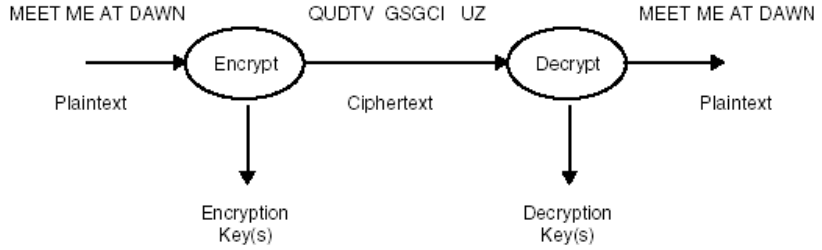
3.1.1 Прикривање

Еден од првите технолошки одговори на потребата за доверливост и интегритет на информациите била криптографијата, или "тајното" пишување. Историјата на тајното пишување се протега наназад сè до 1900 година п.н.е., почнувајќи од тајниот напис на гробот на египетскиот благородник Khnumhotep II. Првите апликации биле само трансформација на хиероглифите најверојатно за да се потенцира нешто во калиграфски, декоративни и други цели. Употребата на такви трансформации за сигурносни потреби од страна на Египќаните, најверојатно оригинално замислени како некој вид игра или загатка, најверојатно е пра-почетокот на криптографијата како алатка за прикривање на информации.

Еден од најсигурните начини за заштита на тајноста на податоците е да се скријат толку ефективно што тие кои ги бараат да не можат да ги препознаат. Криењето на пораки креира т.н. concealment cipher или null cipher. Бидејќи пораките на крајот се сведуваат на секвенци од единици и нули, било која шема на бројки може да се искористи за криење информации. Генералниот термин за науката за криење цифри е стеганографија. Почнаа да се појавуваат и компјутери кои употребуваат стеганографски алгоритми. Една од тие рутини го заменува најмалку значајниот бит од бит-стринговите што го дефинираат секој графички пиксел - со секвенца од нули и единици кои ја сочинуваат тајната порака. Бидејќи повеќето графички кодирања овозможуваат повеќе бои одошто човечкото око може да регистрира, промената на најмалку значајниот бит (со цел запишување на порака) нема видливо да ја оштети сликата. На ваков начин, порака од 64 KB лесно може да се скрие во графика од 1024 x 1024 пиксели, со помош на софтвер кој е лесно достапен. Доколку сликата биде пресретната, не е многу веројатно дека другата страна ќе знае дека во неа воопшто има порака освен ако не се знае со сигурност дека е употребена стеганографија.

3.1.2 Први принципи

Криптологија е наука за кодови и цифри кои се употребуваат за таен пренос на пораки од испраќачот до примачот, независно дали се работи за комуникација помеѓу луѓе, помеѓу човек и машина или помеѓу два процеси во компјутерски систем или мрежа. Шифрерите (ciphers) се методи или системи за обезбедување "тајност" на податоците и можат да бидат шифрери со криење, кои беа дискутирани претходно, или шифрери за транспозиција и супституција. Кодовите се специјална форма на шифрери во кои симболи или групи на симболи заменуваат групи на битови или букви - од оригиналната порака со помош на кодна книга. Креирањето на кодна книга бара идентификациски зборови, фрази, реченици, па дури и цели пораки и доделување на специфичен симбол (земен од табела) или група на симболи за секоја порака. Така на пример пораката "Meet me at dawn" може да се претстави како "QQRST" во кодната книга.



C

Сл. 3.1: Едноставен енкрипциски систем

Било да се работи за шифрер или за код, оригиналната порака која се праќа и прима се нарекува plaintext или cleartext, а заштитената (или скриена) порака која се пренесува - се нарекува шифриран текст. Процесот (алгоритмот) за конверзија на plaintext во шифриран текст се нарекува енкрипција или encipherment. Откривањето на оригиналната порака се изведува со помош на декрипциски (decipherment) алгоритам. Криптологијата се состои од *криптографија* – наука за сигурноста на пораките, и *криптоанализа* – наука за разбивање на пораките (т.е. откривање на оригиналната порака со претходни детални предзнаења за системот кој се користел за енкрипција на пораката). Успешната криптографија која не е многу подложна на криптоанализа обезбедува приватност. Мора да се напомене дека криптографијата сама по себе не може да ги реши сите проблеми во смисол на заштита на компјутерските системи. Не осигурува достапност, па denial-of-service нападите се сеуште опасни. Генерално, не може ниту да пружи заштита од вируси иако може доста да помогне во таа насока. Има два типа на криптографски алгоритми: secret key (или симетрична) криптографија, која користи еден клуч (one-key) и public key (асиметрична) криптографија која користи два математички поврзани клуча, на сличен начин како што тоа се изведува со сигурносните кутии во банките. Се сугерира дека од шесте состојби на информатичко процесирање – влез, излез, приказ, складирање, комуникации и процесирање, криптографијата може да заштити само два: складирање и комуникации.

3.2 ОСНОВНИ ТЕРМИНОЛОГИИ И КОНЦЕПТИ

Научните студии на било која дисциплина мора да бидат изградени врз основа на ригорозни дефиниции кои потекнуваат од фундаментални концепти. Во продолжение следат основните концепти на криптографијата.

3.2.1 Енкрипција на домени и кодомени

• A означува конечно множество - наречено азбука на дефиниции. На пример A={0,1}, бинарната азбука, е честопати користена азбука за дефиниции. Секоја азбука може да се кодира на начинот кој го дава бинарната азбука. На пример, бидејќи постојат 32 бинарни стрингови со должина пет, на секоја буква на англиската азбука може да и се препише единствен бинарен стринг со должина пет .

• M означува множество, т.н. место за порака. M содржи низа на симболи од азбуката на дефиниции. Елементите од M формираат празна порака или едноставно празно место. На пример, M може да се состои од бинарни стрингови, пишан текст, компјутерски код, итн.

• C означува множество, кое се нарекува празно место на шифер-текст. C се состои од низи на симболи од азбуката на дефиниции, која може да се разликува од азбуката на дефиниции за M. Елементите од C се нарекуваат шифер-текст.

3.2.2 Енкрипциски и декрипциски трансформации

• K означува сет наречен *празно место*. Еден елемент на K се нарекува клуч.
• Секој елемент $e \in \kappa$ единствено детерминира биекција од *M* до *C*, означена со $\mathrm{E}e$. $\mathrm{E}e$ се нарекува *енкрипциска функција* или *енкрипциска трансформација*. $\mathrm{E}e$ мора да биде биекција, бидејќи процесите се реверзибилни. Притоа единствена празна порака се доделува за секој различен шифертекст.
• За секој $d \in \kappa, Dd$ означува бијекција од *C* во M($Dd : C \to \mathrm{M}$). Dd се нарекува декрипциска функција, или декрипциска трансформација.
• Процесот од нанесување на трансформацијата $\mathrm{E}e$ на пораката $m \in M$ обично се нарекува *енкриптирање m* или *енкрипција* на *m*.
• Процесот од нанесување на трансформацијата Dd на шифертекстот *c* обично се нарекува *декриптирање c* или *декрипција* на *c*.
• *Енкрипциска* шема се состои од сет $\{\mathrm{E}_e : e \in \kappa\}$ на енкрипциски трансформации и одговарачки сет $D_d : d \in \kappa$ на декрипциски трансформации, каде што за секој $e \in \kappa$ постои уникатен клуч $d \in \kappa$ каков што е $Dd = \mathrm{E}_e^{-1}$; т.е. $D_d(\mathrm{E}_e(m)) = m$ за сите $m \in M$. Енкрипциската шема понекогаш се однесува како *шифрер*.
• Клучевите *e* и *d* во претходната дефиниција се дадени како пар клучеви и понекогаш се означени како (*e*, *d*). *e* и *d* може да бидат исто.

• За да се конструира енкрипциска шема треба да се додели место за пораката M, шифертекст-место *C*, клуч-место *K*, сет на енкрипциски трансформации $\{\mathrm{E}_e : e \in \kappa\}$, и одговарачки сет на декрипциски трансформации $D_d : d \in \kappa$.

3.2.3 Постигнување доверба

Енкрипциската шема може да биде користена на следниот начин за постигнување доверба. Две страни А и Б прво тајно избираат или тајно си разменуваат пар клучеви. После тоа, ако А сака да испрати порака $m \in M$ на Б, таа пресметува $c=E_e(m)$ и го пренесува тоа на Б. Штом ќе го прими с, Б пресметува $Dd(c)= m$ и оттаму ја добива оргиналната порака m.

Прашањето е зошто се неопходни клучевите? (Зошто едноставно да не се избере една енкрипциска функција и декрипциска функција која ќе одговара на неа?). Кај алгоритмите кои користат клучеви значи дека - ако некоја одредена енкрипциска/ декрипциска трансформација е откриена, тогаш не мора да се дизајнира повторно целата шема - туку само да се смени клучот. Криптографска пракса е да се менува клучот многу често (а не енкрипциско-декрипциската трансформација). Како физичка аналогија, се зема едноставна брава со менливи комбинации. Структурата на бравата е достапна до секој, но комбинацијата е избрана и наместена од сопственикот. Ако сопственикот се посомнева дека комбинацијата е откриена, може лесно да ја смени без да мора да го менува целиот физички механизам. Слика 3.2 покажува прост пример на двострана комуникација со користење на енкрипција.

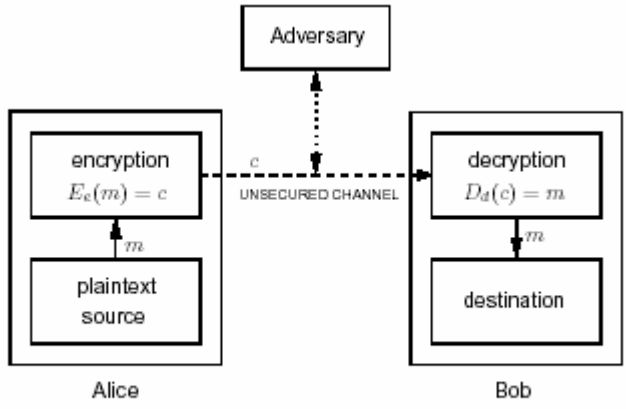


Figure 1.6: *Schematic of a two-party communication using encryption.*

Сл. 3.2: Криптирана комуникација помеѓу 2 страни

3.2.4 Учесници во комуникацијата

Во однос на слика 3.2, е дефинирана следната терминологија:
• *Ентитет* или субјект, е некој (или нешто) што испраќа, прима, или манипулира информации. Ентитетот може да биде некоја личност, компјутерски терминал итн.

• *Испраќач* е ентитет во двострана комуникација, кој е легитимен трансмитер на информации.
• *Примател* е ентитет во двострана комуникација, кој е намерниот примател на информацијата.
• *Противник* е ентитет во двострана комуникација, кој не е ниту испраќач ниту примател, и кој се обидува да го наруши системот за безбедност на информацијата што се спроведува помеѓу испраќачот и примателот. Се користат и други имиња наместо противник, како што се непријател, напаѓач, конкурент, прислушкувач, натрапник и наметнувач. Противникот честопати се обидува да игра улога на вистински испраќач или примател.

3.2.5 Канали

• *Канал* е начин за пренесување на информации од еден ентитет до друг.
• *Физички безбеден канал* или *безбеден канал* е тој што физички не е достапен за натрапникот.
• *Несигурен канал* е тој што има и други странки кои сакаат информацијата да ја снимат, избришат, да додадат во неа, или да ја прочитаат.
• *Безбеден канал* е тој каде што противникот нема можност да снима, брише, додава или да ја чита информацијата. Треба да се забележи разликата помеѓу физички безбеден канал и безбеден канал. Обичниот безбеден канал може да биде сигурен преку физички или криптографски техники. Се смета дека некои канали се физички безбедни. Ова вклучува доверливи доставувачи, лични контакти помеѓу страните кои комуницираат, и линк посветен за комуникацијата.

3.2.6 Безбедност

Основна претпоставка во криптографијата е тоа што множествата $\mathrm{M}, C, K, \{\mathrm{E}_e : e \in K\}, \{D_d : d \in K\}$ се јавно познати. Кога две страни сакаат да комуницираат безбедно со користење на енкрипциска шема, едиснтвената работа која е тајна - е дадениот пар на клучеви што ги користат и кои мора да ги изберат. Може да се добие поголема безбедност ако таинствено се чуваат и енкрипциските и декрипциските трансформации, но не треба да се базира целосната безбедност на овој пристап. Историјата покажала дека одржувањето во тајност на трансформациите е навистина тешко.

Енкрипциската шема може да биде лесно кршлива ако трета страна, без познавање на клучевите може систематски да го земе целиот празен текст од шифер-текстот кој одговара на одредена временска рамка. Временската рамка која одговара, претставува функција од животниот тек на податоците кои се заштитени. На пример, информацијата за купување на одредена стока ќе треба да биде чувана како тајна само неколку минути, додека државните тајни ќе треба да останат тајни засекогаш.

Енкрипциската шема може да биде скршена со пробување на сите можни клучеви за да се види кој од комуникациските странки се користат (претпоставувајќи дека класата на енкрипциски функции е јавно позната). Ова се нарекува исцрпно барање на клучот. Затоа е потребно да бројот на клучеви (т.е. големината на

клучот) биде доволно голем, за да се направи овој пристап пресметливо недостапен. Дали ова ќе биде најдобриот начин за пробивање на системот, зависи и од типот на енкрипциската шема. Во литературата честопати се спомнуваат правилата на Kerckhoffs, сет на барања за шифрер системи. Во продолжение се дадени како што Kerckhoffs оргинално ги напишал:

1. Системот треба да биде, ако не теоретски нескршлив, барев нескршлив во пракса;
2. Деталите на криптографскиот алгоритам не треба да се битни за страните што комуницираат;
3. Клучот треба да биде лесен за памтење без запишување и лесно променлив;
4. Енкрипцискиот уред (алгоритам) да може да се носи и да се управува од страна на еден човек;
5. Системот треба да биде лесен, барајќи ниту знаење, ниту долга листа на правила, ниту умствен напор.

Оваа листа на барања била артикулирана во 1883 и во најголем дел, останува корисна и денес. Точката 2 овозможува да класата на енкрипциските трансформации што се користат - да бидат јавно познати, а безбедноста на системот треба да остане само во избраниот клуч.

3.2.7 Општи информации за безбедноста

Досега терминологијата е ограничена на енкрипција и декрипција со цел да се обезбеди приватноста. Безбедноста на информациите е многу поширока област, вклучувајќи во себе работи како што се автентикација и интегритет на податоци.

• *Сервисот за безбедност на информациите* е метод за спроведување на некои специфични аспекти од безбедноста. На пример, интегритетот на пренесените податоци е дел од безбедноста, а методот кој го обезбедува овој дел - е сервис за безбедност на информациите.
• *Пробивање на сервисот за безбедност на информации* (кој честопати вклучува повеќе отколку едноставна енкрипција) претставува разоткривање на дадениот сервис.
• *Пасивен противник* е противник кој може само да ја чита информацијата од несигурен канал.
• *Активен противник* е противник кој исто така може да пренесува, модифицира или да брише информации од несигурен канал.

3.2.8 Криптологија

• *Криптоанализа* е проучување на математичките техники, со цел да се открие (разбие) криптираната порака.
• *Криптоаналитичар* (пробивач на шифри) е некој кој се занимава со криптоанализа.
• *Криптологија* е наука за криптографијата и криптоанализата.

• *Криптосистем* е општ назив кој се однесува на сет од криптографски методи кои се користат за спроведување на сервисите за безбедност на информации. Најчесто терминот се користи за опис на методите за спроведување доверливост, т.е. енкрипција. Криптографските техники се типично поделени на два главни: методи со *симетричен клуч* и методи со *јавен клуч*.

3.3 ПРОТОКОЛИ И МЕХАНИЗМИ

Дефиниција - Криптографски протокол е дистрибуиран алгоритам дефиниран со низа на последователни чекори, точно специфицирајќи ги потребните акции на два или повеќе ентитети за постигнување на одредена безбедносна цел.

Забелешка (protocol vs. mechanism). Како спротивност на протокол, механизам е поопшт термин кој ги опфаќа протоколите, алгоритмите (специфицирајќи ги чекорите кои ги следи ентитетот), и не-криптографските техники (т.е. заштитен хардвер и процедурални контроли) за да се постигне одредена цел на безбедност. Протоколите имаат голема улога во криптографијата и се многу важни во постигнување криптографски цели. Енкрипциските шеми, дигиталните потписи, hash функциите и генерирањето на случајни броеви - се едни од начините кои може да бидат искористени во изградбата на еден протокол.

Пример - А и В избрале енкрипциска шема со симетричен клуч за да ја користат во комуникацијата преку несигурен канал. За енкриптирање на информацијата потребен им е клуч. Протоколот за комуникација е следниот:
1. В конструира енкрипциска шема со јавен клуч и преку канал - на А му го испраќа својот јавен клуч.
2. А генерира клуч за енкрипциска шема со симетричен клуч.
3. А го енкриптира клучот со користење на јавниот клуч на В и го испраќа енкриптираниот клуч на В.
4. В го декриптира со користење на неговиот приватен клуч и го добива симетричниот (таен) клуч.
5. А и В започнуваат да комуницираат приватно, со користење на системот за симетричен клуч, т.е. договорениот таен клуч. Овој протокол користи основни функции за реализација на приватна комуникација преку несигурен канал.

Во примеров се користени методи на енкрипциски шеми со симетричен клуч и јавен клуч. Протоколот има недостатоци, вклучувајќи го и нападот со имитирање, но ја дава основната идеја за протокол. Честопати, улогата на енкрипција со јавен клуч во приватните комуникации е точно онаа што ја има во горниот пример – енкрипцијата со јавен клуч се користи како начин за размена на клучеви кои ќе се употребуваат во енкрипцијата со симетричен клуч; ова е мотивирано од разликите во изведбата на енкрипцијата со симетричен и со јавен клуч.

3.3.1 Пад на протоколи и механизми

Дефиниција. *Пад на протокол* или *пад на механизам* се случува кога механизмот нема да успее да ги исполни целите за кои бил наменет, т.е. кога натрапникот ќе добие предност и тоа не со директен напад, како на пример напад на

енкрипцискиот алгоритам, туку со манипулирање на самиот протокол или механизам.

Пример - А и В комуницираат со користење на stream шифрер. Познато е дека пораките што ги енкриптираат имаат специјална форма: првите дваесет битови носат информација што претставува сума на пари. Активниот противник може едноставно да направи XOR на првите дваесет битови од шифрер текстот и да ја промени сумата. Иако натрапникот не е во можност да ја прочита дадената порака, тој може да ја промени информацијата. Енкрипцијата не е нарушена, но протоколот не успеал да работи исправно; претпоставката дека енкрипцијата спроведува интегритет на податоците е неточна.

Пример - Претпоставете дека во електронска банка - вредноста на 32-битно поле што ја содржи трансакцијата ќе биде енкриптирана со користење на шема со јавен клуч. Овој едноставен протокол треба да ја заштити приватноста на полето со вредноста - но дали го прави тоа? Противникот може лесно да ги заземе сите 32 можни влезови кои може да бидат празни во ова поле и да ги енкриптира со користење на јавна енкрипција. (Треба да се знае дека во самата природа на енкрипцијата со јавен клуч - оваа функција му е достапна на противникот). Со споредба на секој од овие 32 шифрер текстови со кои тој е всушност енкриптиран во трансакцијата, противникот може да го одреди празното поле. Овде функцијата за енкрипција со јавен клуч не е компромитирана, туку начинот на кој се користи. Нападот се однесува директно на автентикацијата, т.е. за целите на контрола на пристап.

Забелешка (*причини за пад на протокол*). Протоколите и механизмите може да бидат неуспешни поради голем број на причини, вклучувајчи ги и:
1. Слабост во одреден криптографски метод, која може да биде предизвикана од протоколот или механизмот.
2. Потврдени или претпоставени гаранции за безбедност, кои се претерани или не сосема разбрани; и
3. Пропуст на некои основни апликативни класи, како на пример енкрипцијата.

Забелешка (*протокол дизајн*). Кога се дизајнираат криптографски протоколи и механизми, следните два чекори се многу важни:
1. Идентификување на сите претпоставки во дизајнот на протоколот или механизмот; и
2. За секоја претпоставка, да се одреди последицата по безбедноста - ако таа претпоставка е прекршена.

3.4 HASH ФУНКЦИИ

Еден од основните начини во модерната криптографија е криптографската hash функција, која најчесто се нарекува еднонасочна hash функција. Упростена дефиниција за неа е следната:

Дефиниција - Hash функција е пресметливо-ефикасна функција, која мапира бинарни стрингови со произволна должина - во бинарни стрнгови со некоја

фиксна должина, наречена hash-вредност. Hash функцијата која дава n-битни излезни hash-вредности (пр., n=128 или 160), ја дава веројатноста дека случајно избран стринг ќе биде мапиран на одредена n-bit hash-вредност. Основната идеја е тоа што серверите со hash-вредност служат како компактна репрезентација на стринговите на влезни податоци. За да биде од криптографска корист, hash функцијата h типично се избира да биде пресметливо корисна, т.е. да наоѓа два различни влезни податоци кои се однесуваат на дадена вредност /за два влезни податоци - x и y, за кои h(x)=h(y) и на кои им е дадена hash-вредност y, пресметливо е неизводливо да се најде влезен податок x, таков што h(x)= y/. Најчестите криптографски примени на hash функциите се во областа на дигиталните потписи и интегритетот на податоците. Кај дигиталните потписи, долгата порака обично е хеширана (со користење на јавно позната hash функција) и само hash-вредноста е потпишана. Страната која ја добива пораката тогаш ја хешира примената порака, и се уверува дека применият потпис е валиден за оваа hash-вредност. Ова зачувува повеќе време и простор во споредба со директното потпишување на пораката, за што пораката ќе треба да се подели на блокови со соодветни големини и потпишување на секој блок посебно. Забележете дека неможноста да се најдат две пораки со иста hash – вредност оди во прилог на безбедноста, додека потписот на hash-вредноста на една порака ќе биде ист како и на другата порака. Ова овозможува - кога корисникот ќе потпише една порака, подоцна да не може да тврди дека потпишал друга. Hash функциите може да бидат користени за интегритет на податоците на следниот начин: Hash-вредноста која одговара на одреден влезен податок е пресметана во одредена точка на времето. Интегритетот на оваа hash-вредност е заштитен на некој начин. Во следната точка на времето, за да се верификува дека внесените податоци не се нарушени, hash вредноста повторно се пресметува со користење на новите вредности, и се споредува со оргиналната hash вредност. Специфичните апликации вклучуваат и заштита од вируси и софтверска дистрибуција. Трета апликација на hash функциите се користи кај протоколите, вклучувајќи и некакви шеми за дигитален потпис и протоколи за идентификација. Hash функциите, како што беше кажано погоре, се типично јавно познати и не вклучуваат тајни клучеви. Кога се користат за откривање дали податоците од пораката се нарушени, се нарекуваат *детекциони кодови за модификација* (MDCs). Со ова се поврзани hash функциите кои вклучуваат таен клуч, и спроведуваат автентикација за потеклото и интегритетот на податоците, и се нарекуваат *кодови за автентикација на пораки* (MACs).

3.5 ШИФРЕРИ

3.5.1 Транспозициски шифрери

И покрај скоро 4000 години употреба, криптографијата денес сеуште се заснова на две методологии кои се широко познати. Кај transposition ciphers методот, буквите од пораката која тајно се пренесува се скриени, т.е. напишани на некој специфичен начин и пораката се испраќа во сосем поинаква форма од оригиналната. На пример, транспозициските алгоритми ги пишуваат пораките хоризонтално во правоаголни полиња, при што транспонираниот текст се чита вертикално. Примачот го применува истиот процес за да го открие оригиналниот текст:

N	O	W	—	I	S	—	T	H	E	—	T	I	M	E
F	O	R	—	A	L	L	—	G	O	O	D	—	M	E
N	—	T	O	—	C	O	M	E	—	T	O	—	T	H
E	—	A	I	D	—	O	F	—	T	H	E	I	R	—
P	A	R	T	I	E	S	—	S	T	O	P	Z	Z	Z

Ќе биде пренесено во следнава форма:

NFNEP OO—A WRTAR —OIT IA-DI SLC-E -LOOS T-MF- HGE-S
EO-TT -OTHO TDOEP I—IZ MMTRZ EEH-Z

Шемите кои ќе се користат, знаците кои ќе ги означуваат зборовите, реченициte, параграфите, филтрите и сè останато - треба да биде претходно договорено, и го сочинува она што модерната криптографија го нарекува декрипциски алгоритам. Очигледно, возможни се многу сложени алгоритми. Клучните зборови исто така играат своја улога; на пример, ако договориме клучен збор computer (осум букви), оригиналната порака се пишува хоризонтално во поле со димензии осум по осум. Природниот редослед на буквите во клучниот збор (азбучниот редослед) кажува по кој ред ќе се отстрануваат колоните од полето - со цел постигнување на транспозициска енкрипција.

Key Word	C	O	M	P	U	T	E	R
Letter Order	1	4	3	5	8	7	2	6
	M	E	E	T	M	E	A	T
	T	H	E	F	R	O	N	T
	D	O	O	R	O	F	T	H
	H	I	L	T	O	N	H	O
	T	E	L	A	T	9	P	M

На ваков начин обичниот текст “Meet me at the front door of the Hilton Hotel at 9 PM” ќе ја добие следната форма:

MTDHT ANTHP EEOLL EHOIE TFRTA TTHOM EOFN9 MROOT

Употребата на клучни зборови во ваков шифрер многу ја поедноставува неговата операционална употреба. Праќачот и примачот меѓусебно се договараат за методологијата, па за релативно сигурна комуникација со помош на шифрер треба само да се разменат клучните зборови. Секако, од витално значење е да прелиминарната размена на клучни зборови се изведе сигурно, бидејќи секој што го има клучот може да ја де-шифрира пораката. Проблемот на сигурно разменување на клучевите и управување со нив е од огромна важност. Транспозициските шифрери можеме да ги гледаме како множество компјутерски

инструкции, т.е. по една инструкција за секоја буква. Наместо да се прави транспозициска табела со редици и колони, побрзо е веднаш да се помести секоја буква на својата нова, транспонирана положба. Компјутерите ја прават оваа релокација многу брзо – ред на величина: милион во една секунда. Дури и најкомплексните transposition cipher алгоритми имаат едноставно множество на инструкции - познато како транспортациска мапа.

3.5.2 Субституциски шифрери

Во втората методологија, substitution ciphers се креираат со замена на одреден симбол, на пример буква од некоја порака - со друг симбол или буква, според некоја претходно дефинирана шема. Можеме, на пример, да ја поставиме азбуката веднаш до друга "азбука" која е поместена неколку букви надесно:

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

Сега, ја заменуваме првата буква од пораката "Meet me at dawn" - M, со буквата која се наоѓа на истата позиција во другата низа – P, па истото се повторува со сите букви. На крајот, се добива резултат (шифрирана порака) "PHHW PH DW GDZQ". Примачот на пораката, ако го знае клучот, (во случајов за колку места е поместена абецедата), може да ја употреби истата шема, но во обратна насока за да ја добие повторно оригиналната порака. Повторно, со шифтирање три места налево, ќе добиеме нешто вакво:

Обичен текст: NOW IS THE TIME FOR ALL GOOD PEOPLE
Шифриран текст: KLT FP QEB QFJB CLO XII DLLA MBLMIB

Било кој број од 1 до 25 може да се користи како мерка за поместувањето; на таков начин добиваме клуч за оваа т.н. Caesar супституција, наречена така, бидејќи се верува дека Caesar бил оној што прв ја употребил. Покомплексни алгоритми се прават кога би се избрал клуч кој би ја одредил шемата. На пример, ако за клуч го одбереме зборот magnetic би добиле:

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
M A G N E T I C B D F H J K L O P Q R S U V W X Y Z

Бидејќи секоја буква може да се појави во азбуката само еднаш, повторувањата се игнорираат, па така клучот SECURE станува SECUR. Може да се употребат и два клучни зборови за понатамошно комплицирање на супституцијата:

S E C U R A B D F G H I J K L M N O P Q T V W X Y Z
M A G N E T I C B D F H J K L O P Q R S U V W X Y Z

Поместувањата може да се искористат и за избегнување на замена со иста буква:

M A G N E T I C B D F H J K L O P Q R S U V W X Y Z
A C D F G H J K M N O P Q S U V W X Z L I B E R T Y

Комбинацијата од еден или повеќе зборови и едно или повеќе поместувања, ги формираат клучевите. Исто како и кај транспозициските цифри, употребата на клучеви ја поедноставува операционалната употреба на субституциските цифри, но бара одреден сигурносен менаџмент. Ниту транспозициските ниту супституциските цифри, во едноставната форма во која се овде претставени, не претставуваат голем предизвик на евентуалниот напаѓач кој сака да ја открие оригиналната порака, посебно ако кодот е таков да овозможува помош од компјутер. Сепак, може да се употребат комплексни варијации на двете шеми, често и комбинација, за постигнување на импресивно ниво на сигурност.

3.5.3 Продуктни шифрери

Со комбинирање на методологиите на супституција и транспозиција се добива многу посилен шифрер за прикривање, наречен продуктен шифрер, (посилен отколку што продуцира секој од методите сам по себе). Последователната употреба на двата методи ги маскира шемите на енкрипција на обичниот текст и ја прави самата порака потешка за де-шифрирање. Модерните енкрипциски стандарди 3DES (Data Encryption Sandard) и Rijndael употребуваат повеќекратни комбинации од транспозиција и супституција за постигнување на супериорна криптозаштита. Иако супституциските и транспозициските цифри се многу комплексни, сепак може да бидат нападнати со користење на статистички методи. Идеално, шифрираниот текст треба да претставува случајна низа од букви или битови; криптографот треба да ги елиминира сите траги кои можат да помогнат во анализата на кодот. Тоа значи елиминирање на статистичките релации помеѓу шифрираниот текст и обичниот текст кој што е кодиран. *Дифузијата* е дефинирана како дисперзија или распределба на обичен текст на статистички случаен начин врз шифрираниот текст. Најчесто се користи итеративна комбинација на супституција и транспозиција како некој вид продуктен шифрер. Дифузијата го распрснува обичниот текст низ шифрираниот текст; во суштина ги крие неизбежните релации помеѓу текстот и кодот. Принципот на *конфузија* го спречува крипто-аналитичарот од употреба на шифриран текст за дедукција на тајниот клуч. Конфузијата ги крие релациите помеѓу шифрираниот текст и тајниот клуч. Шифрерите кои користат дифузија и конфузија заедно се наречени продуктни цифри. Секоја апликација на конфузија и дифузија е позната како рунда. Постојаното повторување на рундите се вика итерација. Продуктните цифри кои користат многу рунди, како на пример DES, се нарекуваат итеративни продуктни цифри. Добро дизајниран итеративен продуктен шифрер ја енкриптира пораката така што никој, дури ни дизајнерот на крипто-системот, не може лесно да ја декриптира пораката, без да го знае тајниот клуч. Кај итеративните продуктни цифри, статистичката анализа на буквите од шифрираниот текст не е практична опција за пробивање на кодот. Најдобриот напад во ваков случај е да се пробаат сите можни клучеви – неинтелигентен напад, наречен напад на сурова сила (brute force). Криптографскиот метод кој може да се пробие само со brute force напад, (а има толку многу клучеви што таквиот напад практично е неизводлив), се нарекува силен (сигурен) метод. Модерните сигурни крипто-системи се силни, но и тие се подложни на промените во напредната технологија. Силните методи се прават посигурни со јавно објавување, бидејќи на таков начин можат подобро да се проучат и испитаат од крипто-аналитичарите. DES (Data Encription Standard) има

околу 70 квадрилиони (70 x 10^{15}, според US стандарди) потенцијални клучеви и бил, скоро три децении, сигурен против традиционалната крипто-анализа. Не е повеќе сигурен (силен), бидејќи денешен компјутер тестира 70 x 10^{15} комбинации без некои посебни потешкотии. Дизајнерите на крипто–системи мора да ги земат во предвид перформансите, работниот фактор и технолошките ресурси кои би биле употребени против крипто-системот, како и прашањата поврзани со имплементација во мрежна околина, употребливоста и цената на чинење. Безжичните системи претставуваат дополнителен предизвик, бидејќи овозможуваат дополнителни точки на напад и потенцијално повеќе информации за крипто-аналитичарот.

3.5.4 One-Time-Pad шифрер

Еден од најзабележителните шифрери е таканаречениот **one-time-pad** каде што обичниот текст се става бит по бит (или буква по буква) во неповторувачка случајна секвенца со истата должина. One-time-pad се нарекува и Vernam шифрер во чест на G. Vernam кој го развил принципот во 1917 за употреба во телеграфските комуникации. Во Vernam шифрерот, шифертекстот е modulo-2 сума на секој бит од обичниот текст - со неповторувачката случајна секвенца со иста должина како пораката. Дешифрирањето се изведува со извршување на шифрерот по втор пат. Целата оваа процедура нуди перфектната сигурност ако се претпостави напад само врз шифертекстот. Claude Shannon докажал дека дури и со неограничени пресметувачки можности и ресурси - криптоаналитичарот никогаш не би успеал да го препознае кодираниот текст помеѓу мноштво други наизглед безначајни текстови. Првенствениот проблем секако е потребата од неограничен број на клучеви. Друг проблем е почетната тешкотија во правењето на дупликат pad и негова достава до примачот. Се сугерира употреба на синхронизиран stream cipher кој го шифрира текстот употребувајќи псевдо-случајна секвенца со што се елиминира потребата од неограничен клуч. Детерминистички алгоритам наречен key stream генератор, под контрола на таен клуч, може да ја генерира ваквата секвенца. За да биде системот сигурен, потребно е низата на клучеви да не е предвидлива на друг начин, освен со случајно нагаѓање, без оглед на бројот на знаци од низата кои претходно биле познати. Линеарните системи продуцираат секвенци кои се криптографски слабо заштитени. Мора да се комбинираат со нелинеарни трансформации со цел да се добијат комплексни псевдо-случајни секвенци. Основниот принцип на one-time-pad е статистички да се одделат обичниот текст и шифертекстот со употреба на целосно случајна секвенца од клучеви. Направата која емитува ваква случајна секвенца (секвенца во која секој бит може со еднаква веројатност да е 1 или 0, без оглед на претходните битови) се нарекува бинарен симетричен извор BSS (binary symmetrical source). Накратко, BSS на излез дава секвенца која би се добила со фрлање паричка. Криптографскиот систем нуди перфектна сигурност (т.е. се нарекува безусловно сигурен), ако заедничката информација која ја носат оригиналниот текст и шифертекстот е 0, независно од должината на пораката. На таков начин, пресретнувањето на шифертекстот на крипто-аналитичарот нема да му донесе никаква информација за пораката која во него се содржи. Перфектната сигурност може да се одржи сè додека има доволно случајни клучеви за секој бит информација. Операционалните проблеми на ваквиот начин на кодирање довеле до развивање на синхронизирани низи на цифри кои го шифрираат текстот на

сличен начин како one-time-pad, но со детерминистички генерирана случајна секвенца.

3.5.5 Композиција на шифрери

Со цел да се опишат продуктните шифрери, го изложуваме концептот за составување на функциите. Составувањата (композициите) се начин за конструирање на покомплицирани функции од поедноставните.

Композиција на функции

Нека S, T, и U бидат конечни множества и нека $f : S \to T$, и $g : T \to U$ бидат функции. Составувањето на g со f, означено како $g \circ f$ (или едноставно gf), е функција од S до U, како што е покажано на слика 3.3 и дефинирано со $(g \circ f)(x) = g(f(x))$ за сите $x \in S$.

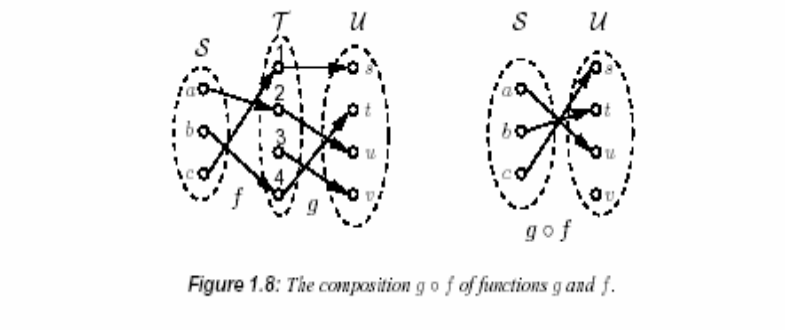


Figure 1.8: The composition $g \circ f$ of functions g and f.

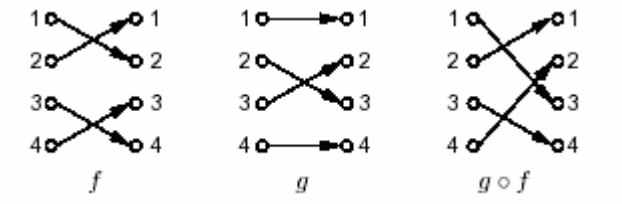
Сл. 3.3: Композиција на две функции

Составувањата може лесно да бидат продолжувани на повеќе од две функции. За функциите $f_1, f_2, \ldots, f_t$, може да се дефинира $f_t \circ \ldots . f_2 o f_1$, дадено преку доменот на еднаквите на него кодомени од f_{t-1} итн.

Композиции и Вметнувања

Вметнувањата беа претставени како едноставна класа на функции со интересна особина: $E_k(E_k(x)) = x$, за сите x во доменот на E_k; т.е. $E_k \circ E_k$ е функција за идентитет.

Забелешка (*composition of involutions*) Составувањето на две вметнувања не е секогаш вметнување, како што е покажано на слика 3.4. Сепак, вметнувањата може да се состават, за да се добијат покомплицирани функции чии инверзни е лесно да се најдат. Ова е важна особина за декрипцијата. На пример ако $E_{k1}, E_{k2}, \ldots E_{kt}$ се вметнувања отколку инверзните на $E_k = E_{k1}, E_{k2} \ldots E_{kt}$ и $E_k^{-1} = E_{kt} E_{kt-1} \ldots E_{k_1}$, составувањето на вметнувањата е во обратен ред.



Сл. 3.4: Композиција на инволуции

3.6 ДИГИТАЛНА КРИПТОГРАФИЈА

Модерната криптографија е скоро исклучиво заинтересирана за заштитата на информации во дигитален формат, т.е. множество секвенци од нули и единици. Еден процес, (или комбинација на два процеси – транспозиција и супституција), може да се примени во комплексен алгоритам и да се употреби клуч, исто така составен од нули и единици - за кодирање на обичниот текст во кодирана порака (cipher). Во следната табела е даден ASCII кодот за пораката “Meet me at dawn”. Ако ова се прочита на вообичаениот начин, ќе добиеме:

0101010101001101010011010101110000000000001010101010011010000000001001001010111000000000000100110001001001010111110101011000110110.

Ако пак ги прередиме или транспонираме битовите, на пример читајќи го секој бит од десно кон лево, така што 01010101 ќе стане 10101010, добиваме низа:
1010101010110010010011010101110000000000001010101110110010000000001
0010010001110100000000000011001010010010111111010011010100110110 0.

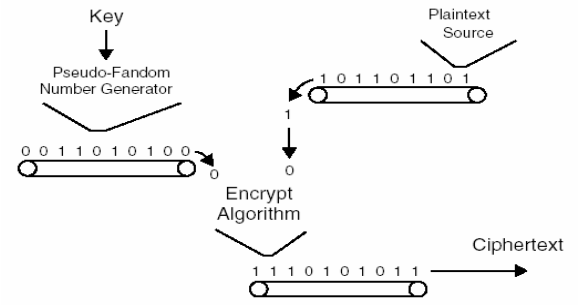
M 01010101	E 01001101	E 01001101	T 01011100	NUL 00000000	M 01010101
E 01001101	NUL 00000000	A 01001001	T 01011100	NUL 00000000	D 01001100
A 01001001	W 01011111	N 01010110	00110110	.	

Ако ја знаеме почетната точка на низата од битови и должината на бајтот кој служи за кодирање - лесно е да се “преврти” секој бајт со цел да се реконструира оригиналната низа. Уште една транспозиција може да се оствари ако се почне од последниот бит и се креира транспонирана низа од битови така што прво ќе се земат сите последни битови одејќи од назад кон напред, па сите претпоследни и така натаму - што би продуцирало ваква низа:
0011000101100111111000000000000011101010110111100111011010011101 1
1000100010100110000000000000000011110110110111100000000000000000.

Оваа низа е исто лесна за конвертирање во оригиналната низа, ако знаеме дека има 16 бајти, секој составен од по 8 бита. Супституциските шифри користат клуч и алгоритам за замена на знаците од пораката - со знаци кои би изгледале беззначајно за примателот (ако претходно не се дешифрираат). Во модерните

комуникациски системи, колата кои ја овозможуваат супституцијата се нарекуваат порти; портите примаат на влез два или повеќе битови, а на излез даваат бит од кој зависи исходот на целата операција.

Ако обичниот текст го гледаме како низа од битови, и ако енкрипциските и декрипциските клуч се идентични, (а енкрипциските и декрипциските алгоритам се идентични исто така) – шифрирањето претставува едноставна XOR операција која лесно се имплементира. За креирање на bitstream од клучеви, може да се користи робусниот псевдо-случаен генератор на броеви. Псевдо-случајните генератори се математички функции кои продуцираат секвенци од броеви кои се навидум случајни - иако се продуцираат детерминистички. Секвенцата продуцирана од псевдо-случајниот генератор поминува низ неколку тестови дизајнирани да детектираат присуство на шеми, кои би можеле да бидат употребени за правење копии од низата броеви и на таков начин да придонесат за разбивање на самата енкрипција. Псевдо-случајниот генератор на броеви (PRNG, Pseudo Random Number Generator) може да се замисли како мала машина која произведува навидум случајни, но всушност детерминистички секвенци од броеви кои енкрипциските алгоритам ги комбинира со секвенцата од единици и нули (т.е. оригиналниот текст на пораката). Ако енкрипциските алгоритам е XOR, процесот е бинарно собирање.



Сл. 3.5: Употреба на PRNG при енкрипција

Секвенцата од битови продуцирани од генераторот се зема во блокови што одговараат на должината на блоковите од текстот што се кодира. Процесот на декрипција, повторно, не е ништо повеќе од обратен процес на енкрипцијата. Во пракса, псевдо-случајните генератори на броеви понекогаш се повторуваат, па затоа треба да се избере функција која не се повторува себеси веќе по неколку кратки секвенци на продуцирани броеви. За да се комплетира сликата за практичен енкрипциско-декрипциски систем, треба да се истакне уште и тоа дека псевдо-случајните генератори на броеви кои се употребуваат, треба да се ограничат со клуч на распределба за секоја случајна секвенца која ќе ја произведат (за да се осигура дека секвенцата која се произведува не е истата). Клучевите за распределба може да се кратки во однос на должината на неповторувачката псевдо-случајна низа, неколку десетини наспроти илјадници или дури милиони броеви.

3.7 ГЕНЕРИРАЊЕ НА ПСЕВДО-СЛУЧАЈНИ БРОЕВИ

Колку и да изгледа чудно, може да се каже дека ништо не е случајно. Случајните броеви играат многу важна улога во криптографијата кога треба да се генерираат криптографски клучеви. Ако имаме 128-битен клуч, ни требаат барем 128 бита случаен материјал. Ако едноставно отчукаме неколку букви на тастатурата, и тие нема да бидат случајни. Испитувањата покажале дека луѓето обично не отчукуваат броеви и големи букви, дека најчесто се фокусираат на букви од средината на тастатурата и дека паровите букви најчесто се комбинации искуцани со левата или десната рака. Можеби ретко се внесуваат повеќе исти букви во еден ред и има 4, 5, 10 или 20 доминантни шеми. Brute force нападот во ваков случај би се фокусирал на барање на клучеви кои ги следат тенденциите на човечкото отчукување. Напаѓачот најчесто доаѓа до решението во првата половина комбинации. Оттука следи дека клучевите избрани на ваков начин не се случајни. Она што ни треба е програма која ги избира броевите по случаен редослед.

3.7.1 Генератор на псевдо-случајни броеви (PRNG)

PRNG (Pseudo Random Number Generator) е алгоритам кој продуцира броеви кои изгледаат случајни, но всушност се репродуктибилни. Сепак, излезот од PRNG ги минува сите тестови за случајни броеви, па затоа се нарекува псевдо-случаен. Ако му се стави одредена распределба, ќе генерира броеви кои се навидум случајни. Со секоја (различна) распределба - се добиваат различни резултати. Повеќето PRNG работат со помош на message digest (математички редуцирана уникатна форма на пораката). На пример, најпрво се преработува распределбата за да се креира почетна состојба. Кога ќе се дојде до генерирањето на рандом бајти, се преработува состојбата. Резултатот на тој digest е првиот дел од излезот. Ако има потреба од повеќе рандом бајти - се ажурира состојбата (на пример со додавање на константа). Дури потоа се дигестира новата состојба и се добиваат нови рандом броеви.

Распределба - 3707446542388966625321...
Процесирање со message digest алгоритам – состојба:
1726398714300234967249 1...
Итерациите на message digest алгоритмот даваат псевдо-случајни броеви -
5423709821369792645233...

Дури и да се знаат некои од случајните бајти, сепак нема да може да се открие целиот редослед. За да се дознаат сите бајти, треба да се знае состојбата која што се чува во тајност, а за да се открие состојбата треба да се знае - или распределбата која се користела при креирањето на самата состојба, или да се "преврти" digest процесот. За сега, digest пооцесот важи за иреверзибилен. Значи, ако се одбере распределба која напаѓачот нема да може успешно да ја анализира (и која ќе се чува во тајност), напаѓачот нема да може да ги дознае следните (или претходните) бајти. Зошто би се заморувале со состојби? Би можеле да ја дигестираме распределбата за да добиеме случаен излез, па ако има потреба од повеќе бајти, да го дигестираме и излезот. Но ако така се постапи - познавањето на некои од случајните бајти би значело познавање и на следните. Ако едноставно го

дигестираме излезот за да го продуцираме новиот излез, истото би можело да го стори и напаѓачот.

Броевите изгледаат случајни ама знаеме дека тоа не е така. Сепак, употребата на иста распределба носи исти резултати, па затоа ги викаме псевдо-случајни. Но за напаѓачот тие се навистина случајни, бидејќи нема начин да дознае кои би биле следните бајти. Зошто се користи digest? Резултатите од message digest се навидум случајни, а ги поминуваат и сите тестови за случајни броеви. Понатаму, може да се користат произволен број распределби и да се добива излез за сите нив. Истотака, дури и многу мала промена на состојбата дава на излез радикално различни резултати. Секој излезен блок е комплетно различен од претходниот. PRNG зема огромно количество податоци на влез, го дигестира и го намалува - и на излез дава навидум случајна низа. Но и распределбата треба да потекнува од случаен извор. Случајните отчукувања на тастатура и системските часовници не се добар избор – имаат шеми кои лесно може да се репродуцираат. Криптограферите го користат терминот ентропија – термин кој го опишува движењето од ред во хаос. Во криптографијата, ентропијата најчесто се изразува во битови. Вистински RNG би имал по еден бит ентропија за секој бит од излезот. Тотално хаотична распределба и тотално случајна.

Фрлањето на паричка, на пример, има еден бит ентропија – т.е. два можни исходи; секое фрлање продуцира или 0 или 1 (петка или глава). Значи, секое фрлање продуцира еден бит т.е. за секој исход (еден бит) имаме еден (случаен) бит ентропија. Друг начин на гледање на работите е прашањето колку brute force напади се потребни за да се открие одговорот? Ако имаме тотална ентропија, вкупниот број на напади потребен да се пробие 128-битна енкрипција би изнесувал $2^{128.}$ Но ако имаме мала ентропија (ентропијата ја земаме како мерка за хаотичност т.е. случајност во системот), на пример 2 бита ентропија на секои 8 бита излез (значи однос 1:4, а не 1:1 како претходно) тогаш и бројот на потребни напади се намалува четирикратно, па сега ни требаат само 2^{32} итерации.

Сакаме да креираме 128-битен клуч. Убаво би било да имаме 128 бита ентропија со што клучот би бил целосно случаен. Ако немаме RNG, ќе користиме PRNG. Би претпоставиле дека - бидејќи излезот изгледа случаен, напаѓачот нема да се обидува да го пробие кодот со brute force напади. Сепак, поверојатно е дека кодот генериран од PRNG ќе биде полесен за откривање, доколку распределбата не содржи доволно ентропија. Случајните отчукувања на тастатура, како и системското време имаат некој ред - значи имаат мала ентропија. За да се добие добра распределба, ни треба извор со висока ентропија. Или извор со ниска ентропија, но во големи количини. На пример, ако утврдиме дека случајното отчукување има една десетина од бит ентропија, за секоја буква (8 бита), за клуч од 128 бита ќе требаат 1280 отчукувања. За да го открие клучот, напаѓачот треба да открие 1280 отчукувања и тоа во правилен редослед; бидејќи секое отчукување додава 8 бита на распределбата, откривањето би барало 2^{1280x8} итерации со brute force напад. Секако, напаѓачот нема да се обидува со сите можни комбинации – некои се невозможни, а други се многу малку веројатни. Мерката за ентропија индицира дека ова е еквивалентно на 2^{128} brute-force напад – истата работа е потребна да се изврши напад на самиот клуч. Значи, откривањето на пораката со

разбивање на распределбата е исто што и откривањето и разбивање на клучот. Доброто шифрирање налага користење на неколку методи за добивање на распределба и ставање во неа - одреден процент од изворната порака – ова ја зголемува ентропијата и го намалува ризикот од откривање, ако еден од искористените извори на распределба потфрли во работата.

3.8 МАТЕМАТИЧКИ ОСНОВИ

Алгоритмите за криптирање можеме генерално да ги класифицираме на два начини: по тежината на нивниот математички систем и по нивната криптографска намена. Во првата класификациска шема има три типа математички методи кои се сметаат сиурни и ефикасни. На нив се базира практичната криптозаштита, а тие се:

- **Факторизација на цели броеви -** Integer factorization problem (IFP). RSA е основниот и најпознат криптосистем во оваа категорија.
- **Дискретен логаритамски проблем -** Discrete logarithm problem (DLP). Тука спаѓаат Digital Signature Algorithm (DSA), Diffie-Hellman методата, El Gamal енкрипција и Schnorr шема за дигитален потпис.
- **Дискретен логаритамски проблем на елипсоидна крива -** Elliptic curve discrete logarithm problem (ECDLP)**.** Примери за овој тип би биле аналогијата на DSA со елипсоидна крива (ECDSA), аналогијата на Diffie-Hellman шемата со елипсоидна крива (ECDH), El Gamal енкрипцијата и шемите за потписи (ECEG) и Schnorr шемата за потписи (ECSS).

Вториот класификациски метод ги дели криптографските алгоритми по нивната криптографска намена или функционалност:

- Симетрични
- Асиметрични
- Системи за автентификација
- Дигитални потписи

3.8.1 Системи за факторизација на цели броеви

Diffie и Hellman го откриле концептот на криптографија со јавен клуч во 1976. Првата практична имплементација на самиот систем е изведена од Ron **R**ivest, Adi **S**hamir и Len **A**dleman на MIT; системот е наречен RSA во чест на неговите творци. RSA е најпознат од цела фамилија на системи чија сигурност се заснова на проблемот на факторизација на цели броеви. Проблемот е дефиниран на следниот начин: нека p е прост број, а n е цел број таков што n = p x q, при што и q е прост број. RSA алгоритмот се состои од пар (n, m), при што m е број помеѓу 1 и n-1, а n е производ на два големи прости броеви p и q. Се смета дека за генерално разбивање на RSA треба да се реши проблемот за факторизација за целиот број n; овој проблем бил проучуван преку 300 години и досега не е откриен некој многу ефикасен метод за пресметување. Поради непостоењето на ефикасен алгоритам за факторизација, треба само да се одбере доволно голем број n за да се осигура сигурност на системот. За краткорочна сигурност, n треба да биде долг барем 300 децимални цифри (значи отприлика 1024 бита). При употребата на RSA, или било кој друг систем што го користи проблемот на факторизација - треба да се

употреби модуларна аритметика. Модуларното собирање и множење работат исто како и класичното собирање и множење, со таа разлика што резултатот на крај се дели со модулот n и како краен резултат се зема остатокот од тоа делење. Оттаму, резултатот е секогаш помеѓу 0 и n-1. Кај RSA се користи степенување по модул n: ако m е број од 0 до n-1 и ја претставува пораката, мора да се пресмета степенувањето m^X(mod n) за некој број x, кога го трансформираме m. Оваа операција одзема најмогу време во целиот систем на RSA кодирање, така што времето потребно за степенување всушност е и време потребно за изведување на целото кодирање со RSA. Накратко, сигурноста на RSA зависи од тешкотијата на факторирање, а ефикасноста од брзината со која се степенува.

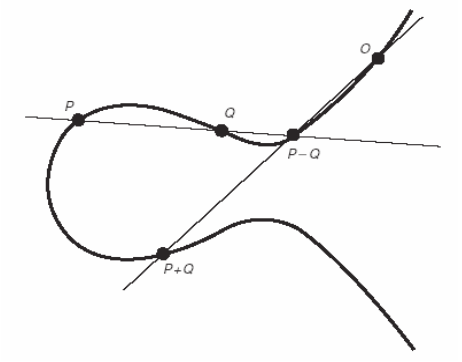
3.8.2 Дискретни логаритамски системи

Уште еден математички проблем дефиниран во рамките на модуларната аритметика е дискретниот логаритамски проблем по модул p. Ако p е прост број, а g е број од 0 до p-1, тогаш резултатот од степенувањето е $y = g^X$ (mod p) за некој број x. Проблемот во случајов е одредувањето на x, ако се познати y и p. Бројот p треба да е долг барем 150 децимални цифри (околу 500 бита) за да се обезбеди минимална сигурност. Исто како и кај факторизацијата на цели броеви, и овде нема ефикасен алгоритам кој би го решил логаритамскиот проблем за прост број p. Taher El Gamal прв предложил криптосистем базиран на овој проблем. Всушност, El Gamal предложил два различни системи - еден за енкрипција и еден за дигитален потпис. Во 1991 Claus Schnorr открил варијанта на El Gamal системот за дигитален потпис која нуди додатна ефикасност во однос на оригиналниот систем. Алгоритмот за дигитални потписи DSA (Digital Signature Algorithm) е истотака базиран на El Gamal.

3.8.3 Криптосистем со елипсоидна крива (ECC)

Математичките теории поврзани со елипсоидните криви датираат од 17-ти век, кога математичарите ги истражувале различните структури и форми на геометриски формули. Основата за ECC (Elliptic Curve Cryptography) лежи во својствата на елипсоидната крива. Иако теоремите биле оригинално развиени околу 1650 година, дури во 1955 година јапонскиот математичар Yutaka Taniyama ги употребил елипсоидните криви во теоријата на Fermat. Taniyama употребил елипсоидна крива за решавање на последната теорема на Fermat ($x^n + y^n = z^n$). Сегашниот ECC систем започнал да се развива паралелно од двајца математичари: Victor Miller од IBM и Neil Koblitz од Универзитетот во Вашингтон. Нивната работа го користи проблемот на дискретно логаритмирање на точки од елипсоидната крива. Ова значи дека ECC може да обезбеди и енкрипција и систем за дигитален потпис. Ова претставува алтернатива на традиционалниот приод кон криптографијата со јавен клуч. Системите со елипсоидна крива користат варијанта на **Д**искретниот **Л**огаритамски **П**роблем (DLP). Но наместо целобројната алгебра, овие системи користат алгебарска формула за одредување на врската помеѓу јавните и приватните клучеви во универзум креиран од елипсоидната крива. Проблемот на дискретно логаритмирање по модул p е опишан во модуларната аритметика како остаток при делење со p. Ова не е единствената математичка структура која ја формира основата за дискретните логаритамски проблеми.

Сигурноста на ECC се потпира врз DLP - аплициран на точки од елипсоидната крива и нуди многу моќни и уникатни особини кои се погодни за употреба во криптографските системи.



Сл. 3.6: Пример за елипсоидна крива

Елипсоидна крива, дефинирана со модул по прост број p е множество од решенија на равенка од облик $y^2 = x^3 + ax + b \pmod p$, за дадени два броја a и b. Ако парот (x,y) ја задоволува горната равенка тогаш P=(x,y) е точка од кривата. Елипсоидна крива може исто да се дефинира како конечно поле кое се состои од 2^m елементи. Таквата репрезентација носи поголема ефикасност во работата на ECC. Може да се дефинира и собирање на две точки од кривата. Ако P и Q се две точки кои припаѓаат на кривата, тогаш и точката P+Q ќе припаѓа на кривата. Проблемот на дискретно логаритмирање кај елипсоидна крива може да се опише на следниот начин: нека p е прост број; xP е точката P додадена сама на себеси x пати (значи помножена со x). Нека Q е број таков што Q=xP за некое x. Проблемот на дискретно логаритмирање кај елипсоидна крива е да се одреди x ако се познати P и Q. Сигурноста на ECC зависи во потполност од тежината на логаритамскиот проблем. Исто како и во претходните два случаи, и кај ECC не постои некој ефикасен алгоритам кој би го решил проблемот. Една од предностите на ECDLP е тоа што проблемот е потежок - и од проблемот на факторизација со цели броеви, и од проблемот на дискретен логаритам по модул p.

Процесот на додавање на точки на кривата бара малку модуларни калкулации. Бидејќи кај сите три системи криптографскиот систем зависи од ефикасноста на модуларната аритметика, интересно е да се напомене дека простиот број p кој се користи кај ECC - може да е помал од броевите кои ги бараат другите системи, па уште една предност на ECC е тоа што модуларните пресметки се изведуваат за помал модул, што води кон значително подобрување на ефикасноста на ECC во споредба со другите два системи. Ова значи дека ECC е засега еден од најсилните криптографски системи со јавен клуч.

Табела 3.1: Споредба на криптирачки алгоритми

Алгоритам	Системски параметри	Public key (битови)	Private key (битови)	Должина на потпис (битови)
RSA	n/a	1088	2048	1024

DSA	2208	1024	160	320
ECC	481	161	160	320

ECDLP е добар избор за многу безжични уреди поради нивните ограничувања со напојување, простор и меморија, поради можноста со помали клучеви да се обезбеди високо ниво на сигурност. Крајната цел на сигурната инфраструктура е да се добие комплетно end-to-end решение кое ќе понуди апсолутна сигурност без да ги исцрпи сите достапни ресурси. Бидејќи мрежниот систем има корист од алгоритми кои штедат проток и процесорско време, можноста да се намали должината на клучот без да се намали ефективноста и степенот на заштита што ги овозможува самиот алгоритам е од голема важност кај безжичните мрежи. ECC е идеален за употреба кај мали апликации со мала меморија и процесорски способности како на пример мобилни телефони, smart картици и други уреди.

3.8.4 Криптографија вградена во хардвер: FPGA и ASIC

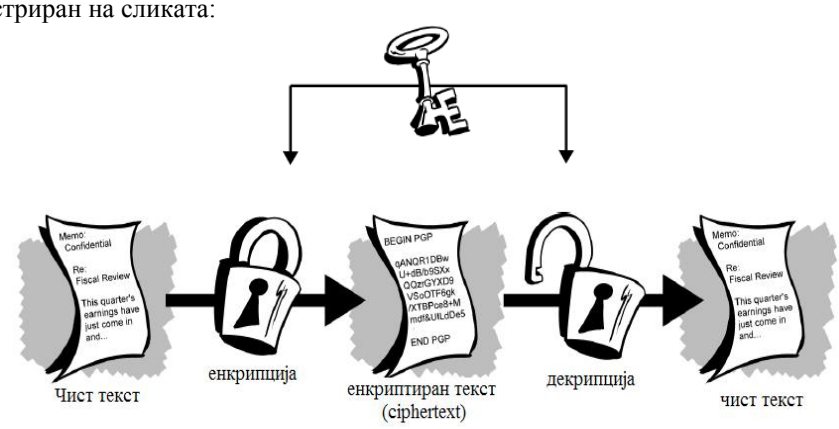
Доста интересни криптографски истражувања се вршат и во хардверскиот домен. Во 2001, Kris Gaj и Pawel Chodowiec ги имплементирале сите 5 AES алгоритми со помош на Field Programmable Gate Arrays (FPGA), со цел да се оценат нивните перформанси. Мерката за перформанси е земана во однос на протокот и доцнењето при креирањето на клучеви. Протокот се смета како количина на податоци процесирана во единица време, а доцнењето е време кое е потребно за да започне енкрипцијата откако се добиле влезните клучеви. FPGA технологијата има потенцијал да ги обезбеди перформансите што ги нуди ASIC (Application Specific Integrated Circuits) плус флексибилноста на процесорите. Оваа технологија овозможува креирење на специфични хардверски кола по потреба - за да се задоволат пресметувачките и конекциските барања на одредена апликација. Понатаму, овие хардверски кола можат парцијално или целосно да се модифицираат според потребата. Криптографските системи со приватен клуч одлично се сложуваат со карактеристиките на FPGA, што е особено изразено кај безжичните апликации. Грануларноста на FPGA одлично одговара со операциите кои ги бараат криптографските алгоритми со приватен клуч, како што се бит-пермутации, бит-супституции, читање на look-up табели и др. Повеќекратни операции можат да се извршуваат истовремено што резултира со повисок проток во однос на инсталациите базирани само на софтвер. На крајот, колото за конфигурирање на клучевите може да работи истовремено со криптографското јадро што резултира со мало доцнење и агилен key-context switching.

Процесорите и ASIC се двете главни пресметувачки парадигми денеска; процесорите служат за поопшта намена и можат да извршат секаква операција. Сепак, нивните перформанси се ограничени со инструкциското множество, податочните патеки и интерконекцијата. ASIC се специфични за секоја апликација и можат да постигнат супериорни перформанси во споредба со процесорите. Сепак, функционалноста на ASIC дизајнот е ограничена од параметрите кои се сетираат фабрички. Надградбите на ASIC платформите се многу скапи, па затоа на самиот приод му фали флексибилност. FPGA има потенцијал да ја спои процесорската супериорност на ASIC со флексибилноста на процесорите. Основното својство на FPGA е програмабилниот логички елемент кој се реализира

со anti-fuse технологија или со SRAM-контролирани транзистори. FPGA има матрица од логички ќелии поврзани со мрежа од жици; пресметувањето на ќелиите и интерконекцијата на жиците може да се конфигурираат. Сигурноста истотака ги прави FPGA имплементациите супериорни во однос на софтверските решенија. Енкрипциските систем кој работи на некој компјутер нема физичка заштита. Хардверските криптографски уреди може сигурно да се енкапсулираат за да се спречи било каква модификација на сигурносниот алгоритам. На крајот, дури и ако ASIC постигнува супериорни перформанси во споредба со FPGA, флексибилноста на ASIC е ограничена; FPGA алгоритмите се далеку пофлексибилни за модификација и надградба. Секако, ако акцентот во системот се стави на перформансите, ASIC е подобро решение. Како што и наведовме во погорниот дел од текстот, постојат два типа на енкрипција: симетрична – со таен клуч, и асиметрична – со јавен клуч.

3.9 ЕНКРИПЦИЈА СО СИМЕТРИЧЕН И АСИМЕТРИЧЕН КЛУЧ

Повеќето луѓе кога зборуваат за енкрипција всушност мислат на криптографски системи со симетричен клуч. Симетричниот клуч, исто така наречен и приватен или таен клуч, се заснова на еден единствен клуч и алгоритам кој се дели помеѓу страните кои разменуваат енкриптирани информации. Истиот клуч се користи и за енкриптирање и за декриптирање на пораките. Овој концепт е илустриран на сликата:



Сл. 3.7: Процес на симетрична енкрипција/декрипција

Силата на алгоритамот во многу зависи од големината на клучот и од неговото чување во тајност. Генерално, колку е поголем клучот, толку е посигурна шемата. Покрај ова, енкрипцијата со симетричен клуч е релативно брза. Главната слабост на системот е што клучот или алгоритмот мора да се делат. Не можете да ја делите тајната информација по пат на несигурна мрежа, без да го компромитирате клучот. Како резултат на ова, крипто-системите со приватен клуч не се баш најдобри за спонтана комуникација преку отворена и несигурна мрежа. Исто така, симетричната енкрипција нема никаков вид на автентификација или не-одрекување. Не-одрекување е способноста да се спречат индивидуи или ентитети да негираат дека пораката е пратена, т.е. примена или пак дека е влезено во некој фајл, кога всушност тоа е направено. Оваа способност е особено важна кога се

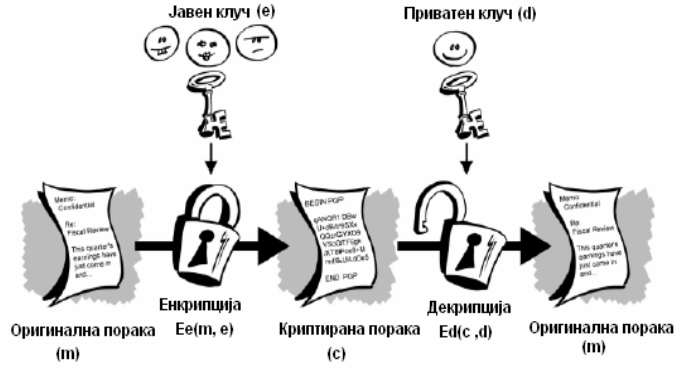
работи за е – бизнис. Примери за широко распространети крипто-системи со симетричен клуч се DES, IDEA, Blowfish, RC4, CAST и SKIPJACK. Во табелата 3.2 се дадени некои предности и недостатоци на алгоритмот со симетричен клуч.

Табела 3.2: Особини на симетрична енкрипција

Предности	**Недостатоци**
Брзина	Бара делење на тајна
Релативно сигурна	Комплексна администрација
Широко разбрана и прифатена	Нема автентификација
	Нема не - одрекување

3.9.1 Енкрипција со асиметричен клуч – системи со јавен клуч

Со векови, целата криптографија била базирана на крипто-системи со симетричен клуч. Сè до 1976, кога два компјутерски научници, Whitfield Diffe и Martin Hellman од Stanford University, не го претставиле концептот на асиметрична криптографија. Асиметричната криптографија е исто така позната и како криптографија со јавен клуч. Криптографијата со јавен клуч користи два клуча, за разлика од едниот кај симетричните системи. Кај оваа криптографија имаме јавен и таен клуч. Како што може и да претпостави од нивните имиња, едниот клуч се чува тајно, а другиот е потполно јавен. Знаењето на јавниот клуч не го открива и тајниот клуч. Пораката енкриптирана со таен клуч - може да се декриптира само со одговарачкиот јавен клуч. Конверзивно, порака енкриптирана со јавен клуч - може да се декриптира само со тајниот клуч. Овој процес е илустриран на сликата 3.8.



Сл. 3.8: Процес на асиметрична енкрипција/декрипција

За разлика од DES, ако се знае еден клуч од парот клучеви - тоа никако не може да помогне во откривањето на другиот. Доколку се запази тајноста и сигурноста на клучевите, системот овозможува дури и јавно објавување на едниот од клучевите, сè додека другиот се чува во тајност. Така, секој што сака да му прати порака на

сопственик на таен клуч - може да ја шифрира со помош на јавниот клуч без ризик по сигурноста, бидејќи пораката ќе може да биде дешифрирана само од сопственикот на тајниот клуч. Ваквите шеми генерално се викаат енкрипциски системи со јавен клуч. Методот Diffie-Hellman е базиран на концептот на пар од клучеви – едниот јавен, а другиот приватен. Протоколот започнува со тоа што секоја страна си креира свој приватен клуч; потоа секоја страна продуцира по еден јавен клуч врз база на математичката функција на соодветниот приватен клуч. Потоа ги разменуваат јавните клучеви. На крај, пресметуваат комбинација од сопствениот приватен клуч и јавниот клуч од другата страна. Математиката е таква што секогаш се добива истата вредност на двете страни, изведена од соодветните приватни клучеви. За сето ова да биде сигурно, јавниот клуч мора да се пресметува како неповратна функција од приватниот клуч зошто во спротивно - прислушувањето на комуникацијата може да доведе до пресретнување на јавните клучеви; со тоа би се добил еден од приватните клучеви и на крајот и клучот за самата порака. Исто така, не може да се користи било која неповратна функција, бидејќи мора да биде погодна за генерирање на клуч. Методот на Diffie и Hellman користи степенување во модуларна аритметика за пресметување на јавните клучеви и клучот за пораката. Модуларната аритметика е слична на стандардната аритметика, освен во тоа што користи броеви кои во опсегот од 0 до N се нарекуваат модули. Кога операцијата ќе продуцира резултат поголем или еднаков на N, N последователно се одзема од резултатот додека не се стигне до вредност која влегува во опсегот од 0 до N-1 (значи делење со N, крајната вредност која е во опсегот, е остатокот). На пример 5+4 mod 7 = 2. Во модуларната аритметика - степенувањето е еднонасочна (неповратна) функција. Значи, не е многу тешко да се пресмета вредноста y = g^X mod N за некој број x којшто е таен, но многу е потешко да се пресмета x врз база на y (претпоставуваме дека g и N се познати), ако броевите се доволно долги, на пример неколку стотини цифри. Ова се нарекува дискретен логаритамски проблем бидејќи x = $\log_{g \bmod N}$ y (логаритам од y за база g (mod N)), а броевите се цели и конечни. За подобра илустрација на Diffie-Hellman методот ќе се послужиме со едноставен пример – комуникација на Страна A и Страна B:

1. Страна A генерира свој таен клуч **xa,** а Страна B таен клуч **xb.**
2. Страна A го пресметува својот јавен клуч **ya=g^{xa} mod p**, каде **p** е прост број.
3. Страна B го пресметува својот јавен клуч **yb=g^{xb} mod p.**
4. Двете страни ги разменуваат јавните клучеви.
5. Страна A го степенува јавниот клуч на Страна B користејќи го својот приватен клуч како експонент со модул **p,** а истото го прави и Страна B, т.е. **K = yb^{xa} mod p = xa^{yb} mod p.**
6. И двете страни го добиваат истиот резултат **$g^{xa[xb]}$** кој се користи како податочен клуч **K**.
7. Изразено математички:
   K = yb^{xa} mod p = $g^{xb\ [xa \bmod p]}$ mod p = $g^{xa\ [xb \bmod p]}$ mod p = xa^{yb} mod p = K.

Методот Diffie-Hellman и негови варијанти се користат во неколку мрежни протоколи и комерцијални продукти, вклучувајќи го и AT&T 3600 Telephone Security Device. Една од поатрактивните можности на протоколот е тоа што може да се користи без долготрајни клучеви. Сите клучеви може да се генерираат “on the

fly" и да се отфрлат веднаш штом се прекине комуникацијата. Криптографијата со јавен клуч донекаде го решава проблемот на управувањето со клучевите. Клучевите сеуште мора да се креираат со помош на сигурни процеси за да се осигура приватноста на тајните клучеви. Сепак, нема потреба од скапи и гломазни системи за дистрибуција и чување на клучевите, бидејќи јавните клучеви воопшто не мора да се чуваат за да се обезбеди сигурност и доверливост на целата шема. Се поставува прашање зошто сите не почнат да го користат овој метод секогаш кога има потреба од криптографија? Еден од одговорите лежи во релативната ефикасност на алгоритмот – симетричната енкрипција генерално е многу побрза од енкрипцијата со јавен клуч. Разликата во брзината не се чувствува многу ако се работи со мали пораки, меѓутоа станува значителна ако пораките се големи. Така, ако е потребна обемна енкрипција, симетричната енкрипција е многу попрактична за сигурно испраќање на големи количества информации. Клучевите за симетрична енкрипција се релативно мали; дури и ако клучевите се одберат така да спречуваат криптографски напад - тие ќе бидат долги само неколку стотини или илјади бита. Можат да се шифрираат брзо и лесно, па потоа, откако со помош на криптографија со јавен клуч ќе се испратат до "другата страна", ќе се искористат за масовна енкрипција со помош на побрзите симетрични рутини. Од технолошки аспект, ова го решава проблемот на управувањето со клучеви.

Табела 3.3: Сличности и разлики помеѓу Secret key и Public/Private key

	Secret Key	Public/Private Key
Години на употреба	Илјадници	Помалку од 50
Главна употреба	Масовна енкрипција на податоци	Размена на клучеви, дигитални потписи
Стандард	DES, Triple DES, Rijndael	RSA, Diffie-Hellman, DSA, Elliptic curves
Енкрипција/Декрипција	Брза	Спора
Клучеви	Се разменуваат тајно помеѓу двете страни	Private: Се чува во тајност Public: Познат на сите
Размена на клучеви	Комплицирана и ризична при трансферот на тајниот клуч	Лесна и помалку ризична, јавниот клуч се пренесува насекаде, приватниот не се пренесува воопшто
Должина на клучеви	128 бита се смета за доволно сигурна	1024 бита (предложено од RSA), а многу корисници бараат 2048 бита
Доверливост, Интегритет	Да	Да
Напади	Да	Да

3.9.2 Криптографија со симетричен клуч наспроти јавен клуч

Енкрипциските шеми ос симетричен и јавен клуч имаат различни предности и недостатоци, од кои некои се вообичаени и за двете. Овде ќе

разгледаме одреден број и ќе ги сумаризираме особините што беа назначени во претходните поглавја.

Предности на криптографијата со симетричен клуч

1. Шифрерите со симетричен клуч може да бидат дизајнирани за да имаат висока стапка на поврзани податоци. Некои хардверски имплементации постигнуваат енкрипциски стапки по стотина мегабајти во секунда, додека софтверските имплементации може да постигнат поврзани податоци само до 1 мегабајт.
2. Клучевите за шифрерите со симетричен клуч се релативно кратки (на пр.128-битен клуч би го натерало и најбрзиот компјутер да "врти" повеќе години, ако сака со brute force да ја пробие пораката).
3. Шифрерите со симетричен клуч може да служат како начини за конструирање на различни криптографски механизми, вклучувајќи и псевдо-рандом генератори, hash функции и пресметувачко-ефикасни шеми на дигитални потписи.
4. Шифрерите со симетричен клуч може да бидат составени за да дадат посилни шифрери. Едноставни трансформации кои лесно може да се анализираат, (но на нивна штета), може да се искористат за конструирање на силни продуктивни шифрери.
5. Енкрипцијата со симетричен клуч се смета дека има долга историја (претставник е ротор-машината Енигма), иако мора да се признае дека, голем дел од знаењето во оваа област било постигнато постепено - со појавата на дигиталниот компјутер, и со дизајнот на Data Encryption Standard во раните 1970-ти.

Недостатоци на криптографијата со симетричен клуч

1. Кај двостраната комуникација, клучот мора да остане таен на двата краеви.
2. Во голема мрежа, има многу парови на клучеви кои треба да се следат. Заради тоа, ефикасното подредување на клучеви бара користење на безусловно доверливиот TTP.
3. Во двострана комуникација помеѓу ентитетите А и Б, криптографската пракса покажува дека клучот треба да се менува постојано, и по можност за секоја комуникациска сесија.
4. Механизмите на дигитален потпис кои потекнуваат од енкрипцијата со симетричен клуч типично бараат поголеми клучеви за верификација на јавната употреба на TTP.

Предности на криптографијата со јавен клуч

1. Само приватниот клуч може да се чува како тајна (автентичноста на јавните клучеви мора да биде загарантирана).
2. Администрацијата за клучеви на мрежата бара присуство на функционално доверлив TTP, како спротивност на нефункционалниот доверлив TTP. Во зависност од начинот на користење - TTP може да биде потребен само на "off-line" начин, а не во реално време.
3. Во зависност од начинот на користење, парот на приватен/јавен клуч може да остане непроменет за одреден период на време, т.е. повеќе сесии (дури и неколку години).

4. Многу шеми со јавен клуч произведоа релативно ефикасни механизми за дигитален потпис. Функцијата на клучот што се користи за опис на јавната верификација е типично многу помала, отколку за копијата за симетричниот клуч.
5. Во големите мрежи, бројот на неопходни клучеви може да биде значително помал отколку кај шемите со симетричен клуч.

Недостатоци на енкрипцијата со јавен клуч

1. Во рангирањата за најпопуларни методи за енкрипција со јавен клуч - има неколку правила: клучот е поголем отколку кај шемите со симетричен клуч.
2. Големините на клучевите се типично многу поголеми отколку кај енкрипцијата со симетричен клуч, а потписот со јавен клуч е поголем отколку јазлите кои даваат автентикација за потеклото на податоците преку техники со симетричен клуч.
3. Ниту една шема со јавен клуч не е докажано дека е сигурна (истото може да се каже и за блок-шифрерите). Најефикасните шеми на енкрипција со јавен клуч - ја базираат својата безбедност на претпоставена сложеност на нумеричко-теоретските проблеми.
4. Криптографијата со јавен клуч нема долга историја како енкрипцијата со симетричен клуч, која е откриена во средината на 1970-тите.

3.9.3 Преглед на споредбите

Енкрипцијата со симетричен клуч и јавен клуч имаат одреден број на предности. Моменталните криптографски системи ја експлоатираат силата на секоја од нив. Техниките за енкрипција со јавен клуч може да се користат за поставување на клуч за систем со симетричен клуч, кој ќе се користи од ентитетите А и В. Во овој случај - А и В може да имаат корист од долгорочната природа на јавните/приватни клучеви од шемата со јавен клуч и ефикасноста на перформансите на шемата со симетричен клуч. Бидејќи симетричната енкрипција на податоци зафаќа најголем дел од времето, шемата со јавен клуч за поставување на клучеви, е мал дел од целосниот процес на енкрипција помеѓу А и В. До денес, пресметувачките способности на енкрипцијата со јавен клуч се никакви во споредба со тие на енкрипцијата со симетричен клуч. Сепак, ова не мора секогаш да биде така. Важни работи во праксата се:
1. Криптографијата со јавен клуч ја олеснува ефикасноста на потписите и поставувањето на клучеви, и
2. Криптографијата со симетричен клуч е ефикасна за енкрипција и некои апликации за интегритет на податоци.

Со помош на криптографијата со јавен клуч, можно е да се воспостави сигурна комуникација со секоја индивидуа или ентитет, користејќи соодветен софтвер и хардвер. На пример, нека А и В сакаат да разменуваат доверливи информации по пат на мрежна комуникација. И двајцата имаат пар од клучеви, јавен и таен. Ако В сака да му испрати некој фајл на А, тогаш истиот го енкриптира со јавниот клуч на А. А, откако го примил енкриптираниот фајл, го декриптира истиот со користење на сопствениот таен клуч. Впрочем, тоа е и единствениот начин да се енкриптира фајл кој е енкриптиран со неговиот јавен клуч. Дури и некој трет да ја пресретне

пораката помеѓу двете страни, би било невозможно да ја декриптира, бидејќи А е единствениот кој го поседува тајниот клуч.

Додека криптосистемите со симетричен клуч се ограничени во обезбедувањето на приватноста на информациите, асиметричната криптографија има многу поголеми можности. Крипто-системите со јавен клуч можат да обезбедат средства за автентификација и претставуваат силна основа за дигиталните сертификати. Кај дигиталните сертификати, системите со јавен клуч го зајакнуваат не-одрекувањето. За разлика од симетричната енкрипција, јавните клучеви дозволуваат безбедна и спонтана комуникација во услови на мрежа. Исто така, многу се подобри за големи системи (десетици милиони), отколку системите со симетричен клуч. Кај симетричните системи - администрацијата со клучот е многу комплексна за големи системи. Во табелата 3.4 се дадени предностите и недостатоците на крипто-системите со јавен клуч.

Постојат 3 системи со јавен клуч кои се во широка употреба – Diffie-Hellman, RSA, Digital Signatture Algoritam (DSA) .

Табела 3.4: Особини на асиметрична енкрипција

Предности	**Недостатоци**
Нема потреба од делење на тајна	Побавни и со интезивни пресметки
Поддржуваат автентификација	Потребен е Certificate Authority
Обезбедуваат не-одрекување	
Скалабилни	

3.9.4 Сила на енкрипција и должина на клуч

Генерално, силата на енкрипцијата се поистоветува со тежината на откривањето на клучот, кое што пак зависи од алгоритмот кој што се користи и од должината на клучот. Енкрипциската сила често се поистоветува со должината на клучот кој се користи при енкрипција. Генерално земено, подолги клучеви обезбедуваат посилна енкрипција. Должината на клучевите се мери во битови. На пример, 128-битните клучеви што се користат за RC4 симетричниот алгоритам поддржан од SSL (Secure Sockets Layer) обезбедуваат значајно подобра криптографска заштита отколку 40-битните клучеви, користени во истиот алгоритам. Грубо кажано, 128-битната енкрипција е 3 x 10^{26} пати посилна од 40-битна енкрипција. Различни алгоритми бараат различни должини на клучеви - за да го постигнат истото ниво на јачина. RSA алгоритмот што се користи за енкрипција со јавен клуч, може да користи само подмножество од сите вредности на клучот, заради природата на математичкиот проблем на кој што се базира.

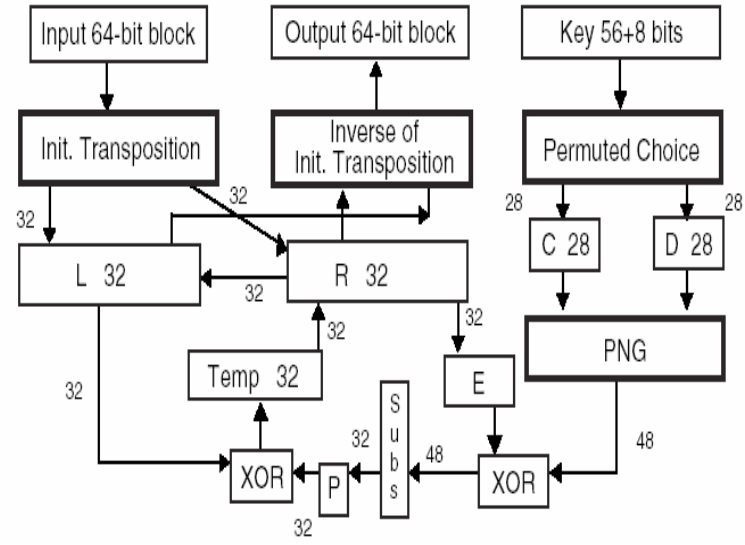
Останатите алгоритми, како оние што се користат за симетрична енкрипција, можат да ги користат сите вредности на клучот. Па така 128-битен клуч што се користи во алгоритам за симетрична енкрипција, ќе обезбеди посилна заштита отколку 128-битен клуч користен во во алгоритмот на RSA. Оваа разлика објаснува зашто RSA алгоритмот со јавен клуч мора да користи 512-битен клуч (или подолг) за да се смета за енкрипциски силен, а од друга страна пак,

симетричните алгоритми можат да ја достигнат приближно истата јачина со 64-битен клуч.

3.10 DATA ENCRYPTION STANDARD (DES)

Има две иновации во компјутерската криптографија кои ги промениле принципите на прикривање на пораки стари повеќе од 3000 години. Едната од нив е појавувањето на DES, а другата е откритието на криптографијата со јавен клуч. И двете иновации се појавиле во 1977 година.

Data Encryption Standard (DES) е алгоритам за енкрипција и декрипција базиран на рутината наречена Луцифер, оригинално развиена од IBM во почетокот на седумдесетите. DES е земен за стандард на 23 ноември 1976, официјалниот опис е објавен на 15 јануари 1977, а станал ефективен шест месеци подоцна. DES е блок шифрер кој енкриптира и декриптира блокови од 64 бита. Енкрипцискиот и декрипцискиот алгоритам се идентични. Клуч од 56 бита се користи за енкрипција и декрипција на текстот, а дополнителни 8 бита се употребуваат за проверка на парност. Секој 56-битен број може да се употреби како клуч, но неколку од нив се слаби и треба да се избегнуваат. Сигурноста на шифрерот се потпира целосно на клучот, бидејќи алгоритмот е општо познат. Ако му се проследи блок текст од 64 бита, DES прави почетна транспозиција и прави scrambling на битовите. Резултантниот 64-битен блок е поделен на два блока од по 32 бита, а тоа се повторува 16 пати и тоа секогаш со метод на транспозиција и супституција, кои се базирани на клучот кој се употребува. По завршувањето на 16-те циклуси, резултантните половини се спојуваат и шифрирањето се комплетира со финална транспозиција која е инверзна на почетната.



Сл. 3.9: Тек на процесот кај DES алгоритамот

Во секоја рунда - битовите од клучот се шифтираат и се селектираат 48 од 56-те битови. Десната 32-битна половина од транспонираниот текст (резултат на почетната транспозиција) се експандира по посебна шема до 48 бита и потоа се комбинира со XOR функција со 48-те бита селектирани од шифтираниот клуч. Следните осум симултани суптитуции го конвертират секој 6-битен суб-блок во 4-битен излез. Резултантните осум 4-битни излези се комбинираат во еден 32-битен блок кој потоа се транспонира и комбинира со левата половина со XOR функција. Резултантните 32 бита стануваат нова десна половина, а старата десна половина станува лева половина со што се комплетира една рунда. Транспозициите во рундата се линеарни, па брзо би подлегнале на нападите на криптоанализата, ако ја нема нелинеарноста која е застапена во супституциите. Почетната вредност на клучот од страна на алгоритмот е поделена на две половини, кои потоа се шифтираат независно една од друга. Консеквентно, ако сите битови во секоја половина се единици и нули, истиот клуч ќе се употребува за секоја рунда. Четирите слаби клучеви кои треба да се избегнуваат се:

0000000 0000000, 0000000FFFFFFF, FFFFFFF 0000000, и FFFFFFF FFFFFFF.
Неколку пара клучеви даваат идентичен шифертекст, па со едниот од нив од може да се декриптираат пораките енкриптирани со другиот, а тие се:

01FE01FE01FE01FE и FE01FE01FE01FE01,
1FE01FE00EF10EF1 и E01FE01FF10EF10E,
01E001E001F101F1 и E001E001F101F101,
1FFE1FFE0EFE0EFE и FE1FFE1FFE0EFE0E,
011F011F010E010E и 1F011F010E010E01,
E0FEE0FEF1FEF1FE и FEE0FEE0FEF1FEF1.

Други 48 клучеви продуцираат само 4 суб-клучеви од кои секој се употребува четири пати. Ова значи дека 64 од 72,057,594,037,927,936 можни клучеви мора да се избегнуваат, што и не е некој голем проблем. DES и останатите блок шифрери со таен клуч имаат многу ефективно криптографско својство наречено ефект на лавина (avalanche effect). Во суштина, ова значи дека за секоја голема промена во оригиналниот текст, криптографскиот алгоритам прави промени во повеќе од половината шифертекст-битови. Во идеален случај, сите шифертекст-битови би требало да се променат при промена на оригиналниот текст кој се внесува во алгоритмот. Ефектот на лавина дава потврда дека DES е добар randomizer; пример за ефектот на лавина би бил:

Оригинална порака 1:	100000000001 000101010001
Оригинална порака 2:	100001000001 000101010001
DES Ciphertext порака 1:	100100001111 010111000001
DES Ciphertext порака 2:	101001111001 011111011000

Оригиналниот текст може да се разликува само во еден бит, но шифра-текстот кој се добива како излез е многу изменет.

Во јули 1998 година, финансиската и другите индустрии кои користат криптографски продукти базирани на DES, беа шокирани од објавувањето на DES Cracker проектот од страна на Electronic Frontier Foundation (EFF). EFF

организирале проект за изработка на специјализиран DES Cracker за помалку од 250.000 долари. Под раководство на Paul Kocher, претседател на Cryptography Research, DES Cracker проектот победил на натпреварот во разбивање на DES шифри - пронајдувајќи 56-битен клуч за 56 часа и тоа пребарувајќи само 24.8 % од вкупниот број клучеви т.е. со тестирање на 88 милијарди клучеви во секунда. Машината со која е изведен овој потфат се состоела од 27 плочи, секоја со 64 custom чипови на себе, поврзани преку кабел на PC кој го контролира целиот процес. Секој custom чип, наречен Deep Crack, има 24 пребарувачи од кои секој е способен да тестира 2.5 милиони клучеви во секунда, работејќи на такт од 40 MHz. Машината е речиси 100 пати побрза од Cray T3D суперкомпјутерот и повеќе од 100 пати поевтина. Ова е одличен доказ дека дизајнерите на криптографски продукти не треба повеќе да дизајнираат продукти базирани на single DES. Поефикасни верзии кои се развиени се 3DES (троен DES) и AES.

3.11 НАПРЕДЕН ЕНКРИПЦИСКИ СТАНДАРД

Во 1998 година, истражувачите од 12 различни држави поднеле 15 предлози за стандардот наречен Advanced Encryption Standard (AES) – новиот шифрирачки метод (наследник на DES/3DES) кој би бил прифатен како федерален стандард во САД. Од 1998, криптографите се обидувале да најдат начин за напад на AES шифрирањето и барање на слабости кои би ги компромитирале шифрираните информации (бројот на алгоритми што преживеале бил намален од 15 - на 5). AES е јавен алгоритам дизајниран за заштита на чуствителни владини информации кој треба да го замени DES. DES и 3DES се употребуваат и во приватниот сектор посебно во финансиските индустриски гранки. Лабораторијата за Информациона Технологија ги избрала следните предлози како финалисти за AES:

- **MARS,** развиен од IBM (САД),
- **RC6,** развиен од RSA Laboratories (САД),
- **Rijndael,** развиен од Joan Daemen и Vincent Rijmen (Белгија),
- **Serpent,** развиен од Ross Anderson (В. Британија), Eli Biham (Израел) и Lars Knudsen (Норвешка),
- **Twofish** развиен од Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall, and Niels Ferguson.

При иницијалната анализа на сите пет алгоритми, кај ниеден од нив не се пронајдени ранливости и секој од петте предлози нудел технологија потенцијално супериорна во заштитата на чувствителни информации ви 21 век. Секој од алгоритмите-кандидати за AES поддржува криптографски клучеви со големина од 128, 192 и 256 бита (за 128-битен клуч има околу 34 x 10^{37} комбинации). Победникот е објавен на 2 октомври 2002: алгоритмот Rijndael**.** Rijndael е блок шифрер дизајниран од Joan Daemen и Vincent Rijman. Шифрерот има променлива големина на блок и должина на клуч. Досега постојат спецификации за користење на 128, 192 или 256-битни клучеви за енкрипција на 128, 192 или 256-битни блокови текст (сите 9 комбинации). И должината на клучот и големината на блокот можат да се продолжуваат (да се мултиплицираат).

3.12 КРИПТОГРАФСКИ НАПАДИ - КРИПТОАНАЛИЗА

Со тек на годините, се идентификувани многу различни видови на напади на криптографските алгоритми и протоколи. Дискусијата тука не се однесува на нападите на енкрипцијата и протоколите. Ќе ги разгледаме улогите на активен и пасивен противник. Нападите кои овие противници можат да ги направат се класифицирани на следниот начин:

1. *Пасивен напад* е тој каде што противникот само ја надгледува комуникацијата на каналот. Пасивниот противник може само да ја загрози доверливоста на податоците.
2. *Активен напад* е кога противникот ќе се обиде да избрише, додаде, или во некој друг случај да ја пренасочи трансмисијата на каналот. Активниот противник се заканува на интегритетот, автентикацијата како и на доверливоста на податоците. Активниот напад може да биде поделен на многу поспецијализирани напади за откривање на шифрираниот текст.

3.12.1 Напади на енкрипциски шеми

Целта на нападите е систематски да добијат обичен текст од шифрираниот, или уште подрастично, да го добијат клучот за декрипција.
1. *Ciphertext-only* е кога противникот (или криптоанализаторот) се обидува да го најде клучот за декрипција или да добие обичен клуч - само за набљудување на кодираниот текст. Секоја шема за енкрипција која е ранлива од овој вид на напад - се смета дека е комплетно несигурна.
2. *Known-plaintext* напад е кога противникот има количина на обичен текст и кодиран текст кој одговара на него. Овој тип на напад е малку потежок за изведување.
3. *Chosen-plaintext* напад е кога противникот избира обичен текст и после му го дава кодираниот текст кој му одговара. Потоа, противникот ја користи било која земена информација со цел повторно да добие обичен текст кој одговара на претходниот невиден кодиран текст.
4. *Adaptive chosen-plaintext* напад каде што изборот за обичен текст ќе зависи од кодираниот текст добиен од претходните барања.
5. *Chosen-ciphertext* напад е тој каде противникот го избира кодираниот текст и после му го дава обичниот текст кој му одговара. Целта на ваквиот напад е противникот да добие пристап до опремата која се користи за декрипција (но, не и клучот за декрипција, кој може сигурно да биде вграден во опремата). После тоа, и без пристап до ваквата опрема, ќе се добие обичниот текст од (различен) кодиран текст.
6. *Adaptive chosen-ciphertext* напад се прави со кодиран текст каде што изборот на кодираниот текст може да зависи од обичниот текст добиен од претходните барања. Повеќето од овие напади исто така напаѓаат и шеми на дигитални потписи и кодови за автентикација на пораки. Во овој случај, целта на напаѓачот е да фалсификува пораки или MACs.

3.12.2 Напади на протоколи

Следи делумна листа на напади кои можат да се извршат на повеќе протоколи. Сè додека протоколот докажува дека може да го изврши потребниот сервис, листата на можни напади никогаш нема да биде комплетна.

1. *Known-key attack*. Во овој напад - противникот зазема некои клучеви кои претходно биле користени и ја користи таа информација за добивање на нови клучеви.
2. *Replay*. Во овој напад, противникот снима комуникациска сесија и повторно ја пушта целата сесија, или само дел, некое време подоцна.
3. *Impersonation*. Овде противникот се претставува како идентитетот на една од легитимните странки во мрежата.
4. *Dictionary*. Ова е вообичаен напад против лозинки. Типично, лозинката е зачувана во фајл во компјутерот како маска на една незаклучена hash функција. Кога корисникот ќе се приклучи и ќе внесе лозинка, се хешира и маската се споредува со зачуваната вредност. Противникот може да направи листа на можни лозинки, да ги хешира сите влезови во таа листа, и потоа да го спореди тоа со листата на вистинските криптирани лозинки со надеж дека ќе најде иста.
5. *Forward search*. Овој напад е сличен со претходниот и се користи за декриптирање на пораки.
6. *Interleaving attack*. Овој тип на напади вклучуваат некоја форма на имитирање во автентикацискиот протокол.

Модели за проценување на безбедноста
Безбедноста на криптографските цели и протоколи може да биде проценета според неколку различни модели. Нивото на доверба на безбедносниот механизам се базира на зголеменото време потребно за истражување на шемата. Сепак, времето не е доволно ако неколкумина добро го анализирале методот.

Безусловна безбедност
Најстрогата мерка е информацијата (теоретска мерка) – без разлика дали системот има или нема безусловна безбедност. Се претпоставува дека противникот има неограничени пресметливи ресурси, и прашањето е дали има доволно пристапни информации за да го победи системот. Безусловната безбедност за енкрипциските системи се нарекува совршена таинственост. За совршената таинственост, несигурниот дел е обичниот текст, т.е. не смее да дава информации на противникот, после набљудувањето на кодираниот текст. Неопходен услов за енкрипциска шема со симетричен клуч да биде безусловно безбедна, е клучот да биде долг барем колку и пораката. One-time pad е пример за безусловно сигурен енкрипциски алгоритам. Воопшто, енкрипциските алгоритми не нудат совршена таинственост, и секој набљудуван карактер на кодираниот текст ја зголемува теоретската несигурност во обичниот текст и енкрипцискиот клуч. Шемите за јавна енкрипција не можат да бидат безусловно безбедни, откако, за даден кодиран текст - неговиот обичен текст може да биде откриен со енкриптирање на сите можни обични текстови додека не се добие *c*.

Комплексно-теоретска безбедност
Дефиниран е соодветен модел за пресметување и противниците се моделирани со имање полиноминална моќ за пресметување. (Тие градат напади со вклучување на времето и просторот полиноминално со големината на соодветните безбедносни параметри). Конструиран е доказ за безбедноста кој е релативен со моделот. Целта е да се дизајнира криптографски метод базиран на најслабите можни претпоставки, кои ги очекува моќен противник. Се користат асимптомски анализи и worst case анализи, па затоа мора да се вежба грижата за да се одреди кога доказите имаат практичен потпис. Во спротивност, полиноминалните напади кои се изводливи теоретски, во пракса, сеуште се пресметливо неизводливи. Безбедносните анализи од овој тип, иако не се од практична вредност во сите случаи, сепак можат да го направат подобро разбирањето на безбедноста. Комплексно-теоретските анализи се непроценливи во формулирањето на основните принципи. Ова е како и многу други науки, чии практични техники се откриени рано во развојот, многу пред да бидат постигнати теоретските основи и разбирањето.

Докажана безбедност
За криптографскиот метод се вели дека е докажливо сигурен, ако тешкотијата на разбивање се докаже дека во основа е тешка колку и решавањето на добро познат и доволно тежок (типично со теоретски броеви) проблем, како факторизација на цел број или пресметките на дискретни логаритми. Овој пристап - од некои се смета како добар за практични анализи на техниките што постојат. Безбедноста што се докажува може да се смета како специјална под-класа од голема класа на докажливо-безбедни проблеми.

Пресметлива безбедност
Оваа безбедност ја мери количината на бараниот труд за пресметување (со моментално најдобрите познати методи), за покорување на еден систем; овде мора да се претпостави дека системот бил добро проучен за да одреди кои напади се релевантни. Предложената техника е пресметливо-безбедна, ако бараното ниво на пресметливост за покорување (со користење на најдобриот напад кој е познат) се зголеми, до соодветна граница на пресметливите ресурси на претпоставениот противник. Често методите во оваа класа се поврзани со тешки проблеми, но, за разлика од докажаната безбедност - нема добро познат метод за еквиваленција. Повеќето од најдобро познатите шеми на јавни клучеви и симетрични клучеви во сегашна употреба, се во оваа класа. Оваа класа понекогаш се нарекува и практична безбедност.

Ad hoc Безбедност
Овој пристап содржи голем број на аргументи кои бараат - секој алгоритам да има ниво на ресурси (т.е. време и простор) - поголемо од фиксните ресурси на противникот. Криптографските начини и протоколите кои преживуваат вакви анализи се вели дека имаат хевристичка безбедност, т.е. имаат типична безбедност во пресметувачка смисла. Се дизајнираат начини и протоколи за противнапад на стандардните напади. Додека можеби најчесто-користениот пристап (посебно за протоколи), е на некој начин, тој што њамалку задоволува - тврдењата за безбедноста обично остануваат под знак прашање и непредвидените напади продолжуваат да бидат закана.

3.12.3 Класична крипто-анализа

Класичната криптографија имала слабост фатална за сигурноста – лингвистички шеми или повторувања. Уникатните атрибути и нивната употребата во букви и зборови им помогнала на крипто-аналитичарите да ги декриптираат тајните пораки стари повеќе од 3000 години. Обидот за крипто-анализа се нарекува напад. Криптолозите секогаш претпоставуваат дека непријателот ги знае алгоритмите за шифрирање и дешифрирање, па сигурноста се базира единствено на клучот или клучевите кои се користат за шифрирање. Ова е конзервативна претпоставка – непријателот нема секогаш да ги знае сите детали на алгоритмот и неговата имплементација, но паметно е да се направи таква претпоставка кога се дизајнираат шифрите, така да не можат да бидат пробиени - дури и ако претпоставката се покаже точна. Ако ја знаеме фреквенцијата со која се појавуваат поедини букви во англискиот јазик, можно е да се одреди скоро веднаш дали некој шифрер е транспозиција или супституција. На пример, ако E не е најчестата буква во англискиот јазик, шифрерот скоро сигурно е супституција. Со последователна замена на буквите според фреквенцијата на нивно појавување во шифрираниот текст, едноставните субституции може да се разбијат со случајни проби. Пробивањето на едноставни шифри денес е хоби на голем број ентузијасти. Шифрерите се разбиваат со анализа базирана на одредени регуларности во англискиот јазик. Сите јазици имаат слични регуларности, па може статистички да се одреди кој јазик е употребен, дури и ако не се знае изворот на пораката.

Табела 3.5: Процентуална застапеност на вокали во светските јазици

Англиски	Германски	Француски	Италијански	Шпански	Португалски
			Вокали:		
40 %	40 %	45 %	48 %	47 %	48 %
L	N	K	R	S	T
33 %	34 %	34 %	30 %	31 %	29 %

□

4. АВТЕНТИКАЦИЈА

4.1 АВТЕНТИКАЦИЈА И ИДЕНТИФИКАЦИЈА

Автентикација е термин кој се користи во доста широка смисла. Сам по себе има мало значење во споредба со преносната идеја - гаранција дека ентитетите се тие кои тврдат дека се, или дека информацијата не била манипулирана од неовластени страни. Автентикацијата е специфична за безбедносните цели кои треба да се постигнат. Примери за специфични цели вклучуваат: контрола на пристап, автентикација на ентитети, автентикација на пораки, интегритет на податоци, не-признавање, и автентикација на клучеви. Автентикацијата е една од најважните информации кај сите цели на безбедност. Сè до средината на 1970-те, се верувало дека таинственоста и автентикацијата се неопходно поврзани. Со откривањето на hash функциите, и дигиталните потписи, се увидело дека таинственоста и автентикацијата се одделни и самостојни информации на целите на безбедноста. На почеток можеби нема да изгледа важно да се одделат двете, но постојат ситуации каде што тоа не само што е корисно, туку е и пресудно. На пример, ако се одвива двострана комуникација помеѓу А и В кога А е во една земја, а В во друга. Хостот на земјите можеби нема да дозволи таинственост на тој канал; едната или двете страни можеби ќе сакаат да бидат сигурни во нивните идентитети, и за интегритетот на потеклото на информациите кои ги примаат и испраќаат. Овој тип на автентикација често се нарекува автентикација на ентитет или едноставно идентификација. За втората можност - не е соодветно да се прати и да се чека одговор, и уште повеќе - патот на комуникација треба да биде единствен во таа насока. Денес се достапни различни техники за да се автентицира испраќачот на пораката. Овој начин на автентикација се нарекува автентикација за потеклото на податоците.

4.1.1 Идентификација

Техниката на идентификација или автентикација на идентитет - го осигурува идентитетот на едната страна (преку добивање на соодветни докази) кај втората страна која е вклучена; при тоа - втората страна била активна во времето кога доказот бил направен или потребен. Типично - единствените податоци кои се пренесуваат, се само неопходните за идентификација на двете страни кои комуницираат. Ентитетите се активни во комуникацијата, давајќи безвременска гаранција.

Пример (*идентификација*). А се јавува на В по телефон. Ако А и В се познаваат - тогаш автентикацијата на ентитети се врши преку распознавањето на гласот. Иако не е сосема докажано, ова работи доста добро во пракса.

Пример (*идентификација*). Личноста А носи до банкоматот број за лична идентификација (PIN), заедно со магнетната лента на картичката која содржи информации за лицето А. Банкоматот ги користи информациите од картичката и PIN за верификација на идентитетот на сопственикот на картичката. Ако верификацијата е успешна, на А и се дава пристап до различни сервиси кои ги нуди машината.

4.1.2 Автентикација на потекло на податоци

Техниките за автентикација на потеклото на податоците, или автентикација на порака, на страната која ја прима пораката и даваат сигурност (преку сигурносни докази) за идентитетот на странката од која потекнува пораката. Честопати се праќа порака до B, заедно со додатна информација која може да го одреди идентитетот на ентитетот кој ја испраќа пораката. Оваа форма на автентикација типично не дава никаква гаранција за постојаност, но е корисна во ситуации кога една од страните не е активна во комуникацијата.

Пример (*потреба за автентикација на потеклото на податоците*). A праќа до B електронска порака (e-mail). Пораката може да патува низ различни мрежни системи за комуникации и да биде зачувана - и B да ја добие после некое време. A и B обично не се во директна комуникација. B сака на некој начин да се увери дека применатa порака испратена од A - е навистина креирана од A. Автентикацијата на потеклото на податоците - имплицитно дава интегритет на податоците; на пр. ако пораката била модифицирана за време на трансмисијата, A веќе нема да биде креаторот.

4.2 СИСТЕМСКА И МРЕЖНА АВТЕНТИКАЦИЈА

Мрежната автентикација почнува на ниво на индивидуален систем. Како што се вели во старата поговорка - синџирот е онолку силен, колку што е силна неговата најслаба алка, мрежата не е ништо друго - туку синџир на системи. Како резултат на ова, за мрежата да има голем степен на сигурност, сите системи во мрежата мора да бидат соодветно администрирани и набљудувани. Многу малку организации адекватно ги администрираат и набљудуваат системите кои се наоѓаат во мрежата. Овој пристап на одбрана во длабочина - бара многу поголема посветеност на безбедноста отколку што повеќето организации сакаат да направат. Клучот на овој пристап на одбрана претставува примена на поопширна стратегија за мрежна и системска безбедност. Наместо тоа, повеќето организации одбираат периметарска одбрана.

Автентикација е процес на одредување на идентитетот на корисникот. Терајќи го да докаже дека ја знае тајната што треба да ја знае само вистинскиот корисник, докажува дека е навистина тој што вели дека е. Автентикацијата се користи да се верификува идентитетот на корисниците, за контрола на пристапот до ресурси, за спречување на неовластени корисници да добијат пристап до системот, и за запис на активностите на корисниците со цел да се држат одговорни за нивните активности. Се користи за автентикација на корисници кои се логираат на компјутер, се користи за осигурување дека софтверот кој го симнувате од Интернет доаѓа од уважен извор, и се користи за да се обезбеди дека личноста која ја испраќа пораката е всушност оној кој вели дека е. При мрежна комуникација - треба да се запрашаме две работи:

1. Со кого комуницирам?
2. Како сум сигурен дека тоа лице е баш она за кое се претставува дека е?

Ако немаме одговор на второто прашање - тогаш огромни се шансите дека грешиме и во однос на првото. При најавување на мрежа, три основни шеми се користат за автентикација:

- *Нешто што знаеме:* Типично, нешто што знаеме и што го потврдува нашиот идентитет е лозинка, код или секвенца. Безбедноста е заснована на идејата дека ако ја знаете тајната лозинка или код, тогаш вие мора да сте тој што тврдите дека сте и сте овластени да влезете во системот или мрежата. Лозинките се веројатно најнедоверлива форма на автентикација која се користи, но исто така се и најлесно имплементирана форма – тие не бараат специјализиран хардвер или софистицирани алгоритми за основна употреба. Но тие лесно се погодуваат, дури и ако се внимателно одбрани - сеуште е возможно лесно да се погоди целиот опсег на можни лозинки.

- *Нешто што поседуваме:* бара клуч, бец, картичка со token, или некој уред или предмет кој ви обезбедува пристап. Безбедноста е заснована на концептот дека само овластени лица или ентитети имаат пристап до одреден уред. Ова не е толку чест, но посигурен метод на автентикација кој подразбира физички да се поседува уникатен клуч. Ова е аналогно на повеќето физички брави. Во компјутерските безбедносни системи, клучеви се големи броеви генерирани од специјални алгоритми кои инкорпорираат информации за корисникот, и кои се чувани на подвижен медиум, како паметна картичка. Проблемот е што можат да бидат изгубени или украдени. Но, во комбинација со лозинка - тие се многу сигурни и тешки за пробивање.

- *Нешто што сме:* се потпира на некои физички или карактерни особини. Ова се нарекува биометриска автентикација, и се потпира на уникатни и неменливи физички особини на човекот, како отисок на прст, рака, лице итн. Биометриска автентикација е најдоверлива форма на автентикација, бидејќи е лесна за употреба, скоро невозможна за да се излаже, и не може да се заобиколи од корисникот дури и да сака. Некои форми на биометриска автентикација се полесни за фалсификат од други и наивната имплементација може да биде штетна. Но ако добро се примени - биометриската автентикација е најсигурна форма на автентикација и единствена која може уникатно и без грешка да го идентификува корисникот.

4.2.1 Лозинки

Прва мерка на системска безбедност е автентикацијата и идентификацијата на корисниците. Најчесто користената шема е нешто што знаеме, а најшироко иплементирана варијација на оваа шема е употребата на лозинки.

Лозинките се користени скоро од секој систем и мрежа како прво, а најчесто и единствено средство за идентификација и автентикација. Иако лозинките се најшироко применета шема за автентикација, тие се можеби и најслабата алка во безбедносната шема. Но, постојат голем број на активности кои можат да се преземат за да се намали ризикот во врска со употребата на лозинки. Секоја организација мора да има полиса за одредување на одговорностите на корисникот

- за одржување на тајноста на лозинката и за последиците ако тоа не го исполнува. Во меѓувреме, луѓето премногу често користат лозинки кои се премногу кратки и/или премногу лесни за погодување или дешифрирање, или пак едноставно никогаш не ги менуваат. Има програми познати како cracker-и кои лесно се симнуваат од Интернет и кои се компатабилни за секој систем и лесно ја пронаоѓаат лозинката. Дури и лозинката да е енкриптирана при емитување помеѓу клиентот и серверот, може да биде пресретната и ре-емитувана покасно, како дел од последователен напад.

4.2.2 Избор на лозинките

Кога се избира лозинка - треба да се избегнат следниве:

- Вашето име, прекарот или името на партнерот,
- Името на домашното милениче или на детето,
- Имиња на пријатели и блиски соработници,
- Името на компанијата, училиштето, оделот или групата,
- Името на омилениот цртан лик,
- Името на оперативниот систем кој го користиме,
- Името на компјутерот,
- Телефонскиот број или бројот на регистарската таблица,
- Датумот на раѓање,
- Било која лична информација,
- Лозинка составена од една иста буква,
- Букви од тастатурата кои се многу блиску поставени на тастатурата,
- Имиња на места или познати поими кои можат да се најдат во најобичен речник.

Во филмот "Вистински генијалец", пробиваат во многу таен Владин компјутер со користење на телефон и погодување на лозинки. Почнуваат од лозинката AAAAAA па AAAAAB, па AAAAAC итн., сè додека не ја најдат вистинската. Во реалноста овие напади се многу пософистицирани. Наместо да ги внесуваат сите можни комбинации - хакерите ги користат своите компјутери за да се поврзат мрежно и потоа ги пробуваат лозинките, користејќи листа на познати лозинки и зборови. Дури и скромен домашен компјутер може да испроба илјадници лозинки за помалку од еден ден. Некои листи кои се користат од напаѓачите се големи и по неколку стотици илјади зборови, и содржат зборови на различни светски јазици. Следува дека, лозинка што би можел да ја користи било кој во светот е лоша за употреба. Во спротивно, доколку сакаме да го искористиме компјутерот за испробување на сите лозинки со должина 6 карактери, ќе треба да испроба 308,915,776 различни комбинации. Ако пробува една лозинка во секунда - ќе му бидат потребни 10 години за да ги испроба сите.

Добри лозинки се оние кои се тешки за погодување. Најдобрите лозинки се најтешки за погодување, бидејќи содржат некое подмножество од следниве карактеристики:

- Имаат и големи и мали букви,

- Имаат бројки и/или знаци за интерпункција како и букви,
- Може да содржат контролни карактери и/или празни места.

Во некои случаи - користењето на празни места може да биде проблематично. Напаѓач кој е во позиција да слуша внимателно може да одреди разлика помеѓу звукот на space bar и било кое друго копче.

- Лесни се за помнење, па не мора да се запишуваат,
- Долги се 7 или 8 карактери,
- Може да се искуцаат брзо, така што некој кој ве набљудува нема да може да види што куцате на тастатура.

Ако имате неколку комјутерски account-и, може да употребувате иста лозинка за секоја машина. Ова се нарекува синхронизација на лозинки. Синхронизавијата на лозинки може да ја зголеми безбедноста, доколку синхронизацијата дозволува употреба на силна лозинка која е тешка за погодување. Системите кои овозможуваат автоматска синхронизација на лозинка - многу ја олеснуваат промената на лозинката на целиот систем. Од друга страна, синхронизацијата на лозинки можеа да ја намали безбедноста - ако лозинката е пробиена, тогаш сите account–и ќе бидат ранливи.

Синхронизацијата на лозинки е проблематична и за кориснички имиња и лозинки кои се користат за веб сајтови. Многу луѓе користат исто корисничко име и лозинка за многу сајтови, дури и за сајтови кои се направени и управувани од сомнителни индивидуи и организации. Најлесен начин за откривање на корисничкото име и лозинката е да се направи сајт кој ќе нуди шанса за освојување на 10000$ за секој што ќе се пријави со e–mail адреса и ќе внесе лозинка на влез.

Ако се исклучат неколку контролни знаци кои не смеат да се користат во лозинката, сеуште е можно да се направат повеќе од 5,000,000,000,000,000 уникатни 8-карактерни лозинки. Комбинирањето на речник од 10 различни светски јазици, плус тие зборови напишани наопаку, напишани со големи букви, со бројка на крајот, и малку модифицирани, резултира со малку помалку од 5,000,000 зборови. Од овие бројки гледаме дека корисниците кои имаат слаби лозинки - во многу им олеснуваат на хакерите, тие го намалуваат просторот за пребарување на 0,000000001% од можните лозинки. Една студија за лозинките направена во произволна средина, покажала дека корисниците користат лозинки со контролни карактери само во 1.4%, а со интерпункциски знаци и празно место само во 6%.

4.2.3 Имплементација на лозинки кај Windows OS

Кај Windows OS секој корисник, група или компјутер кој може да иницира акција - е безбедносен објект. Безбедносните објекти имаат account-и, кои можат да бидат локални на комјутерот или пак domain-базирани. На пример, Windows OS компјутери учествуваат во мрежен domain преку комуникација со domain контролер, дури и ако нема најавени корисници. За да ја иницираат комуникацијата, компјутерите мора да имаат активен account на domain-от.

Безбедносниот контекст на корисник или компјутер варира од еден комјутер до друг, како кога корисникот се најавува на сервер или работна станица, различни од неговата работна станица.

Оперативниот систем Windows овозможува лесна и широка употреба на лозинките за заштита, како на индивидуалниот компјутер, така и за заштита на мрежната структура на корисници. Windows 2000 Server и Windows XP Professional поддржуваат неколку протоколи за верификација на идентитетот на корисниците кои тврдат дека имаат account на системот. Но, следниве два протокола се примарни избори за мрежна автентикација помеѓу Windows NT4, Windows 2000 и Windows 2000 server domain–и, и Windows XP Professional клиенти:

- Kerberos V5 protocol - default автентикациски протокол за Windows 2000 и Windows XP.
- NTML protocol – default автентикациски протокол во Windows NT 4.0.

Иако протоколот Kerberos V5 е default за Windows 2000 и Windows XP, мора и мрежниот domain контролер и клиентските компјутери да имаат Windows 2000 или Windows XP, за да се искористи овој протокол. Алтернативниот NTML протокол се користи за автентикација во следниве случаи:

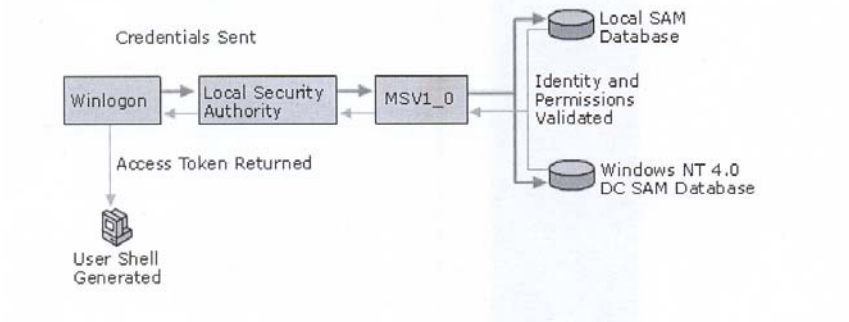
- Компјутери кои имаат Windows 3.11, Windows 95, Windows 98, или Windows NT 4.0, го користат NTML за мрежна автентикација на Windows 2000 domain.
- Компјутери со Windows 2000 или понов систем, го користат NTML за да се автентикуваат на сервери со Windows NT 4.0.
- Компјутери кои имаат Windows 2000 или понов, или пак Windows 2000 Server или понов, го користат NTML протоколот кога не партиципираат во domain.

По default, Windows XP не бара корисниците со локални account-и, вклучувајќи ги тука и администраторите, да имаат лозинки. Корисниците можат да си стават самите лозинки, или пак тоа да го направи администраторот. Кај Windows XP, корисниците кои имаат бланко лозинки не можат да се најават на далечински компјутер преку мрежа. Ова до сега не беше случај, но Windows XP има воведено посебна мерка за овие account-и. На сликата 4.1 е прикажан стандарден екран за најавување кај Windows XP Professional. Можеме да избереме дали ќе се најавиме локално на нашата машина или пак на domain-от.

Сл. 4.1: Типичен Windows logon dialog box

При процесот на интерактивно најавување со NTML се случуваат следните активности:

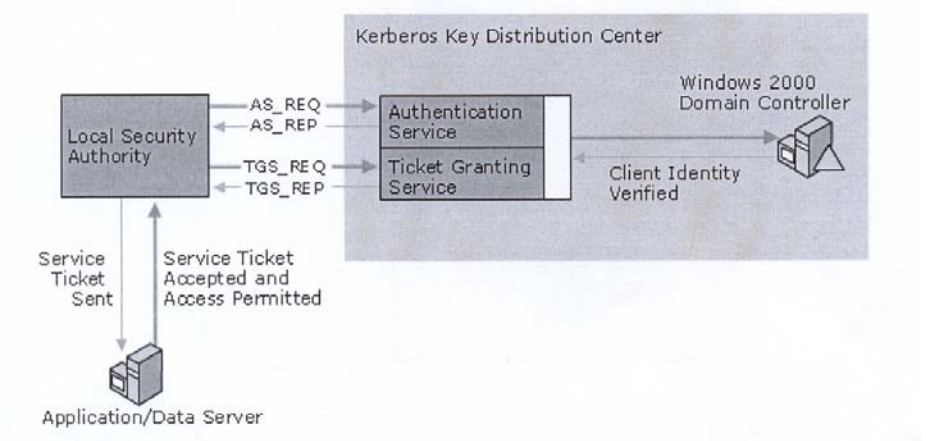
1. Корисникот притиска Ctrl+Alt+Del, што е Secure Attention Sequence – SAS на компјутери кои имаат стандардна Windows XP Professional конфигурација. Winlogon повикува Graphical Identification and Authentication GINA dynamic link library (DLL), да го покаже интерфејсот за најавување.
2. Откако корисникот ќе ги внесе корисничкото име и лозинката, Winlogon ја праќа информацијата до LSA – Local Security Authority.
3. Ако корисничкиот account е локален на компјутерот, LSA го користи MSV1_0 автентикацискиот пакет за да ја спореди информацијата при најавувањето на корисникот - со податоците во базата SAM. Ако корисникот не е локален на компјутерот, LSA ги верификува корисничките податоци со користење на MSV1_0 автентикацискиот пакет и сервисот Net Logon - за да упати query на Windows NT domain контролерот.
4. Ако корисничкото име и лозинката се валидни, SAM ја враќа оваа информација до LSA, заедно со корисничкиот безбедносен идентификатор (SID) и SID – овите кои содејствуваат со групата на која припаѓа корисникот. LSA ја користи оваа информација за да креира access token кој ги содржи корисничките SID – ови.
5. Winlogon ја стартува корисничката shell заедно со прикачен token.



Сл. 4.2: Процес на автентикација кај NTML протокол.

Автентикацискиот процес кај Kerberos ги вклучува следниве активности:

1. Корисникот притиска Ctrl+Alt+Del, што е Secure Attention Sequence – SAS на компјутери кои имаат стандардна Windows XP Professional конфигурација. Winlogon повикува Graphical Identification and Authentication GINA dynamic link library - DLL, да го покаже интерфејсот за најавување.
2. Откако корисникот ќе ги внесе корисничкото име и лозинката, Winlogon ја праќа информацијата до LSA – Local Security Authority.
3. Кога барањето за најавување ќе дојде до LSA, тој го проследува до Kerberos автентикацискиот пакет. Клиентот праќа иницијално барање за автентикација (AS_REQ), кое содржи податоци за корисникот и енкриптирана timestamp до KDC (Key Distribution Center). Ова е барање за автентикација и TGT.
4. KDC го користи тајниот клуч за да го декриптира timestamp и издава TGT на клиентот. Овој TGT (AS_REP), содржи сесиски клуч, името на корисникот на кого му е издаден сесискиот клуч, максималниот животен век на тикетот, и било кои додатни полиња за податоци или подесувања кои може да бидат потребни. AS_REP се енкриптира со корисничкиот клуч и се враќа кај корисникот. Тикетот е енкриптиран со клучот на KDC и приложен во AS_REP. Делот со податоците за авторизација од TGT ги содржи SID-от на корисникот и на групите, на кои тој account припаѓа.
5. Кога корисникот се обидува да влезе во ресурс, клиентскиот систем го користи TGT за да побара сервис тикет (TGS_REQ) од Kerberos ticket - granting service на domain контролерот. TGS тогаш издава сервис тикет (TGS_REP) до клиентот. Сервис тикетот е енкриптиран со серверскиот таен клуч. SID – овите се копираат од страна на Kerberos service од TGT - во сите подсеквентни сервисни тикети добиени од Kerberos service.
6. Клиентот го презентира овој сервис тикет директно до бараниот мрежен сервис. Сервис тикетот го докажува идентитетот на корисникот на сервисот, како и идентитетот на сервисот на клиентот.

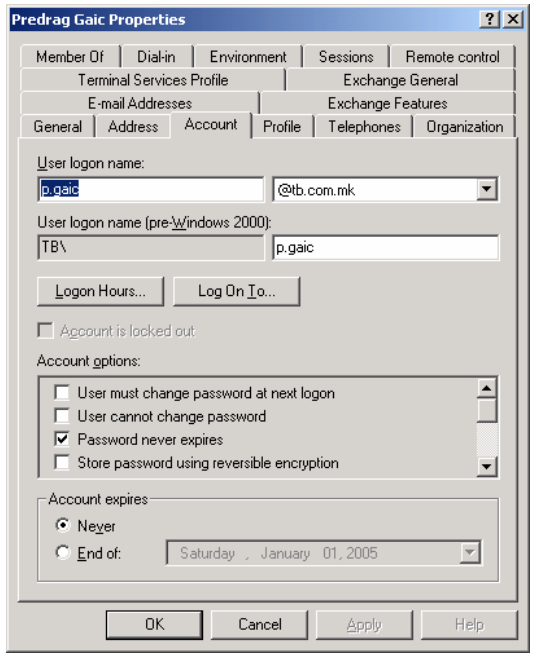


Сл. 4.3: Процес на автентикација кај Kerberos протокол

Секој корисник може да ја промени својата лозинка со притискање на Ctrl+Alt+Del и избор на опцијата Change Password. По ова, сè што треба е да се внесат старата и новата лозинка. Секој корисник може локално на својот компјутер да подеси безбедносна полиса т.е. правила за лозинката на својот локален User account. Сите подесувања на лозинката се наоѓаат на посебна локација Local Security Settings. Windows OS овозможува корисникот да може да подеси неколку категории и тоа:

- Enforce password history
- Maximum password age
- Minimum password age
- Minimum password length
- Password must meet complexity requirements
- Store password using reversible encryption for all users in the domain

Ова се однесува на локалниот User account. Но, во една организациска мрежна структура, најчесто корисниците се поврзани на domain и се најавуваат на Domain user account-и. Во основа, за некој корисник да може да се најави на domain-от, мора да има претходно отворен User account во кој се наведени некои основни информации за него, а меѓу другото и корисничкото име и лозинката. На следната слика е даден пример како во Windows 2000 Server е овозможено подесување на некои предефинирани правила кои ја креираат политиката на употреба на лозинката за одреден корисник.



Сл. 4.4: Администраторски подесувања на User account properties.

Како што може да се види систем администраторот има избор од повеќе опции кои ги селектира при креирањето на секој user account. Од посебен интерес се:

- **User must change password at next logon**

Со оваа опција, корисникот мора да ја менува лозинката на секое наредно најавување. Многу ретко се користи, бидејќи е непрактична и предизвикува огромно негодување кај корисниците.

- **User cannot change password**

Оваа опција го оневозможува корисникот да ја промени лозинката. Негативно е што со тоа кориснкот е приморан постојано да користи иста лозинка и ја одведува во прашање безбедноста на системот. Се користи најчесто кај проблематични корисници кои се обидуваат да направат одредена манипулација со системските подесувања.

- **Password never expires**

Со оваа опција - кога корисникот ќе ја промени лозинката, системот не го тера да направи наредна промена, додека корисникот не реши да ја направи самиот. Најчесто оваа опција ја имаат систем администраторите и другите вработени во службата за ИТ, т.е. корисници кои се свесни за потребата од честа промена на лозинката; со ова ја избегнуваат системската порака која се јавува при секое најавување на системот.

- **Account is disabled**

Со ова се блокира корисничкиот account и се оневозможува било каква употреба на истиот за користење на мрежни ресурси. Оваа опција се користи во случај корисникот да е извесно време отсутен од своето работно место, најчесто поради користење на боледување.

- **Account is locked out**

Оваа опција го заклучува account-от и привремено го оневозможува корисникот да се најави. Оваа состојба трае сè додека администраторот не го отклучи account-от, или пак не измине предвиденото време и системот сам не го отклучи.

Добрата страна на употребата на Windows OS во domain околина е што овозможува подесување на групни полиси за сите корисници на domain-от. Овие подесувања спаѓаат во безбедносната полиса на самиот domain.

Maximum password age – бројот на денови во кои лозинката може да се користи пред корисникот да мора да ја смени. Постојаното менување на лозинката е еден начин да се спречи компромитирање на лозинката. Најчесто оваа вредност варира од 30 до 42 дена.

Enforce password history – ова е бројот на уникатни, нови лозинки кои мора да се поврзани со корисничкиот account, пред да може да се употреби старата лозинка. Кога се користи во координација со minimum password age, ова подесување

спречува користење на една иста лозинка постојано. Најчесто оваа вредност се подесува да биде поголема од 10.

Minimum password age – бројот на денови во кои лозинката може да се користи пред да биде сменета. Препорачливо е оваа вредност да се подеси на неколку дена. Особено е ефикасно ако се користи во координација со enforce password history.

Minimum password length – минималниот број на карактери кои корисникот мора да ги употреби при креирањето на лозинка. Најчесто користена и препорачлива бројка е 7.

Paswords must meet complexity requirements – Филтерот за лозинки кај Windows 2000 Server и Windows XP Professional бара лозинката да ги има следниве карактеристики:

- да не го содржи вашето име или корисничкото име,
- да содржи барем 6 карактери,
- да содржи карактери од секоја од следниве групи - големи и мали букви, бројки и симболи.

Account lockout policy опцијата го блокира account-от по одреден број на погрешни обиди за најава. Користењето на овие опции помага во детекцијата на обиди за пробивање на лозинки.

Ackount lockout treshold – ова е бројот на погрешни најавувања пред корисничкиот account да биде заклучен. Заклучен account не може да се користи сè додека администраторот не го ресетира, или додека времетраењето на заклучувањето не истече. Можеме да подесиме вредности помеѓу 1 и 999 погрешни обиди за најавување, или можеме да специфицираме дека acount-от никогаш не се заклучува. Оваа опција е оневозможена во default domain group policy и во local secutiry policy за работни станици и сервери. Мора да ја овозможиме за да проработи заклучувањето на account. Неуспешните обиди за најавување на компјутер кој е заклучен со користење на Ctrl+Alt +Del, или пак со Screen saver заштитен со лозинка, не се бројат како неуспешни обиди во ова подесување на полисата.

Account lockout duration – бројот на минути (од 1 до 99999) во кои account-от останува заклучен пред да се отклучи Со подесување на оваа вредност на 0, можеме да специфицираме дека account-от останува заклучен додека администраторот не го отклучи.

Reset account lockout counter after – одредува колку минути (1 до 99999) мора да поминат по неуспешен обид за најавување, па сè додека бројачот не се ресетира на 0 неуспешни обиди. Оваа вредност мора да биде помала или еднаква на account lockout duration. Типично, време на ресетирање од 30 минути е доволно, бидејќи целта на заклучувањето е да се одолговлече нападот на лозинката.

Некои системи можат да создадат лозинки кои се состојат од прозволна комбинација на бројки и букви. Систем-генерираните лозинки обично не се подложни на напади со речник. Но, тие се тешки за паметење, што предизвикува корисниците да мораат да ги запишуваат со што се создава огромна безбедносна дупка. Ако корисникот не ја избере лозинката, тогаш таа нема значење и е тешко

да се направи лесно паметлива. Кога корисниците не можат да запаметат лозинка, ги запишуваат на жолти стикерчиња и ги лепат на мониторите, или пак секој ден се јавуваат во ИТ секторот и бараат нова лозинка. Во пракса, понекогаш е потребно да се дели лозинка од привилегиран account со некој надвор од вашата организација. Најчесто, тоа е потребно кога се инсталира нов хардвер и софтвер - од фирмата која го доставува и одржува. Во овие услови, препорачливо е да се смени лозинката за тој account во нешто безопасно, но да ја смените лозинката веднаш кога ќе завршат со работа. Индивидуи надвор од организацијата никогаш не смеат да имаат лозинка на системот. Многу системи, кога се инсталираат, имаат системски или администраторски account со однапред сетирана лозинка или пак се без лозинка. Ако овие account-и не се потребни - препорачливо е веднаш да се избришат. Во спротивно треба да се ресетираат.

Во денешните големи организации корисниците може да имат неколку account-и на различни системи и мрежи. Понекогаш луѓето имаат 3 или пак 5 различни account-и и за сите од нив им требаат лозинки. Некои администратори препорачуваат употреба на различни лозинки за сите account-и. Ова колку што има добри страни, толку има и лоши. Главниот проблем е што кога корисниците имаат повеќе лозинки тогаш тешко ги помнат сите и мораат да ги запишуваат, па потоа ги чуваат на лесно видливи места итн. Една од добрите алтернативи за ова е да се имплементира single sign-on систем.

4.2.4 One-Time лозинки

Најефективен начин да се минимизира опасноста од лоши лозинки е да не се употребуваат конвенционалните лозинки. Наместо нив, може да се инсталира софтвер и/или хардвер за користење на *one-time* лозинки. Тоа е лозинка која се користи само еднаш. Постојат две техники кои се користат за имплементирање на one-time password-и:

- Хардверски прстени:

Пример е RSA SecureID картичката, која дава нова лозинка или PIN за секоја најава. Некои системи базирани на прстени даваат нов код секоја минута. Други системи изгледаат како мали калкулатори. Кога ќе се обидете да се најавите, ви дава мала шифра. Ја внесувате оваа шифра во калкулаторот, го внесувате вашиот идентификациски број, и потоа го внесувате бројот кој се добива како резултат - во компјутерот.

- Кодни книги:

Ова се листи на валидни лозинки. Секоја лозинка е пребришана, откако ќе биде искористена.

One-time лозинките можат да се применат како замена за конвенционалните лозинки или како нивни додаток. Во типична S/Key околина, ја внесувате лозинката наместо стандардната Unix лозинка. На пример:

login: **darrel**
Password: **says rusk wag hut gwen loge**

Last login: Wed Jul 5 08:11:33 from r2.nitroba.com
You have new mail.

Сите овие системи за one-time лозинки обезбедуваат голем напредок во безбедноста, во однос на конвенционалните системи. Но за жал, бидејќи бараат инсталација на специјален софтвер или набавка на специјален хардвер, не се толку распространети колку што би требало.

4.2.5 Напади на лозинки

Дури и лозинките да се енкриптирани при трансмисија помеѓу клиентот и серверот, сеуште можат да бидат пресретнати и ре-емитувани како дел од последователен напад. Контра-мерките за ова се One time лозинка, прстени и Керберос. Има 4 главни типови на напад врз лозинките:

- *Brute force* – напад на сила
- *Dictionary-based* – напад со речник од лозинки
- *Password sniffing* – прислушкување на лозинки
- *Social engineering* – социјален инжинеринг

Brute Force

Brute-force нападите се обидуваат да влезат во системот со пробување на сите можни комбинации од букви и бројки - додека не се најде вистинката лозинка. Нападот со чиста сила е најефективен ако лозинките се кратки и ако се составени само од букви или бројки, а не се комбинација од двете. Колку е подолга лозинката - толку повеќе напор треба за да се пробаат сите комбинации. Ако имаме лозинка од букви, бројки, и специјални знаци - тогаш се зголемува заштитата експоненцијално.

Dictionary-Based

Dictionary-based нападите се многу поефективни од пристапот на чиста сила. Многу од оперативните системи имаат фајл за лозинки. Овој фајл за лозинки е база на кориснички имиња и лозинки. Лозинките скоро секогаш се сместени во овој фајл во енкриптирана форма. Dictionary-based нападите, всушност применуваат програми кои ги споредуваат енкриптираните лозинки во фајлот со енкриптирани зборови во речникот. Кога ќе најдат совпаѓање, ја пронашле и лозинката. Очигледно е дека овој тип на напади се најефективни против лозинки кои се составени од обични зборови, имиња, или изрази. Некои системи се трудат да го решат проблемот со тоа што не користат фајл за лозинки или пак воопшто не ги зачувуваат лозинките. Windows NT на пример, не ги чува лозинките во фајл. Наместо тоа, NT чува hashed вредности од лозинките. Но, програми за разбивање на лозинки постојат за сите оперативни системи.

Password Sniffing

Како што е познато, мрежното (или пакетно) прислушкување е процес на набљудување на мрежата за собирање на информации кои може да се корисни за

напад. Една од работите кои можат да се набљудуваат се лозинките. Со соодветни алатки, хакерот може да ги набљудува мрежните пакети за да добие лозинки и IP адреси. Password sniffing е особено закана за корисници кои се најавуваат на мрежа со користење на telnet, Rlogin, ftp, или терминалски емулатор. На пример, кога корисникот се најавува на UNIX систем преку мрежа со користење на telnet, лозинката се емитува до системот во cleartext. Системот ја проследува ваквата cleartext лозинка до алгоритмот за енкрипција на лозинката и ја споредува со вредноста во фајлот за лозинки. Ако се совпаѓаат тогаш се дозволува влез во системот. Најчесто програмите како telnet, rlogin, и терминал-емулаторите не ги енкриптираат лозинките при најавување кога ги пренесуваат низ мрежа. Како резултат на ова, секој што го набљудува системот со sniffer може да ја прочита лозинката. Ризикот поврзан со telnet и ftp не се однесува само на Unix. Овие програми се користат и за поврзување на Windows NT или 2000 Сервер. Windows графичкиот кориснички интерфејс, со неговите кликни-и-влечи можности, ги прави telnet и ftp непотребни. Но, дури и лозинките на Windows можат да бидат ранливи ако се пресретнат од некој преку пакетно прислушкување. Кога корисникот се најавува на Windows NT - лозинката е hashed на работната станица пред да биде емитувана до серверот. Windows NT го применува MD4 алгортимот. Кога Windows NT серверот ќе ја прими hashed вредноста, тој ја споредува со вредноста зачувана во hash фајлот. Протоколот challenge-response се користи за да се верификува лозинката која корисникот ја внел. Ако се совпаѓаат, корисникот е автентикуван и дозволен му е пристап во системот или мрежата. Корисникот кој се најавува на Windows NT сервер, ги праќа своето коисничко име и domain преку мрежата во cleartext. Ако некој во мрежата има прислушкувач - може да го пресретне cleartext-от и challenge-response. Ако може да бидат пресретнати, тогаш challenge-response може да биде искористен за откривање на hashed вредноста на корисничката лозинка. Hashed вредноста може потоа да се искористи за dictionary-based напад. Windows NT дозволува алтернативен протокол за автентикација, како што е NT LAN Manager (NTLM). NTLM е примарниот протокол за автентикација употребен од NT. Во Windows 2000, Microsoft го замени со Kerberos како примарен безбедносен протокол за пристап до ресурси во Windows 2000 сервер домени. Но, Kerberos може да се употребува единствено помеѓу системи кои користат Windows 2000. Сите останати Windows клиенти мора да користат NTLM. Исто така, Microsoft е критикуван за користење на приватни формати на податоци во својата имплементација на Kerberos.

Social Engineering

Зачудувачки е колку лесно може да натераме некого да ни ја каже лозинката преку телефон. Хакерите кои се претставуваат како систем администратори и кои се јавуваат на корисниците (или ги искористуваат корисниците кои се јавуваат во ИТ службата), се многу ефикасни во нивните обиди за добивање на лозинките за системот. Овој проблем е еден од најтешките за контролирање, бидејќи потребно е да се менува однесувањето на луѓето, а нема технологија која може да го направи тоа. Повеќето луѓе лесно веруваат и се незаштитени од ваков тип на измама. Единствен начин да се спречи ова е да се едуцираат и обучуваат корисниците.

4.2.6 Контрамерки за прислушкувањето на лозинки

Има неколку чекори кои можат да се превземат за да намалат или елиминираат заканите од прислушкување на лозинки. Една од нив е да се користат мрежни switch -ови наместо мрежни hub-ови. Switch-овите се користат за да ја сегментираат мрежата и да креираат виртуелни LAN (VLAN), кои го делат switch-от во мрежни сегменти кои не можат да си ги видат меѓусебните пакети.

Друга опција е да се употреби VPN. Можат да се користат и програми како SSH, кој е Unix програм направен за да обезбеди силна автентикација и безбедна комуникација преку небезбедна мрежа. SSH е дизајниран за да се користи како замена за други програми од типот на telnet, rlogin, rsh и rcp. SSH комуникацијата може да се енкриптира со IDEA, DES, 3DES, или RC4. Енкрипциските клучеви се разменуваат со користење на RSA key exchange. SSH може да ве заштити од IP spoofing, IP source routing, DNS spoofing, и од пресретнување на лозинки во cleartext. Друга заштита од прислушкување на лозинки е употребата на one-time лозинки. Има неколку широко применети шеми за one-time лозинки. Најпопуларните се употребата на паметни картички или токен картички.

4.3 ПРОТОКОЛИ ЗА АВТЕНТИКАЦИЈА

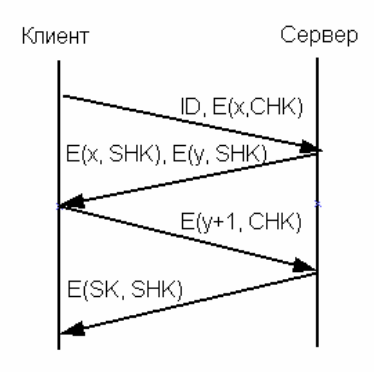
Автентикација е процес на утврдување на идентитетот на двете страни во мрежната комуникација. Како што знаеме, пред да се воспостави врска меѓу клиентот и серверот пожелно е да се утврди идентитетот т.е. дали се тие што тврдат дека се. Со ова се занимаваат протоколите за автентикација. На пример, серверот треба да утврди дека клиентот е тој што тврди дека е, пред да му дозволи пристап до важни ресурси. Но истото важи и за клиентот кој би требало да го утврди идентитетот пред да започне да испраќа важни податоци. За уврдување на идентитетот на клиентот и серверот можеме да се послужиме со неколку стандардни методи на автентикација. Во продолжение ќе се посветиме на два методи кои се базираат на симетричен (DES) и еден со асиметричен (RSA) криптографски алгоритам.

4.3.1 Едноставно тринасочно ракување

Наједноставно решение за да се утврди идентитетот на двете страни вклучени во комуникацијата е кога клиентот и серверот веќе делат некој таен клуч. Идејата е овој таен клуч да се искористи за меѓусебна идентификација, а понатамошната комуникација да се одвива со помош на таканаречен сесиски клуч.

За да го илустрираме едноставното тринасочно ракување, со E(x, K) ќе го означиме процесот на енкриптирање на пораката x со клуч K, а спротивниот процес на декрипција со D(x, K).

- CHK – Клиентски клуч за ракување (Client Handshake Key)
- SHK – Серверски клуч за ракување (Server Handshake Key)
- SK – Сесиски клуч (Session Key)



Сл. 4.5: Тринасочно ракување

Идејата на тринасочно ракување лежи во постоењето на пар тајни клучеви за ракување, еден серверски и еден клиентски, кои се користат во иницијализацијата на криптираната комуникација. Овие клучеви за ракување, се користат за да се дистрибуира еден сесиски клуч, кој понатаму ќе се користи за да се одвива криптирана комуникација помеѓу двете точки. Методот на енкрипција е симетричен, и затоа е потребно, серверот да го знае клиентскиот клуч за ракување, како што и клиентот е потребно да го знае серверскиот клуч за ракување.

Во првиот чекор, клиентот избира случаен број x, кој го криптира со помош на клиентскиот клуч за ракување, и заедно со клиентскиот идентификациски број го испраќа до серверот. Серверот во следниот чекор, во користи клиентскиот идентификациски број за да го лоцира клиентскиот клуч за ракување кој му припаѓа на соодветниот клиент, ја декриптира пораката, го инкрементира бројот x за 1, и го праќа повторно до клиентот енкриптиран со серверскиот клуч за ракување. Покрај повратниот број x+1, серверот праќа уште еден случаен број y енкриптиран исто со серверскиот клуч за ракување.

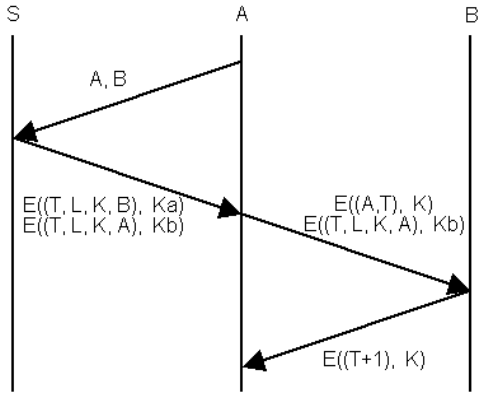
Откако ќе ги добие од серверот двете пораки со броевите x+1 и y енкриптирани со серверскиот клуч за ракување, клиентот ги декриптира и ја споредува вредноста на испратениот случаен број x - со оној кој е вратен од страна на серверот. Со ова клиентот е сигурен дека серверот е автентичен. Втората порака се користи за серверот да може да биде сигурен дека клиентот е автентичен. За таа намена, клиентот ќе ја декриптира втората порака, ќе го зголеми за 1 случајниот број y и ќе го врати до серверот.

Кога серверот ќе ја добие повратна порака од клиентот, која ја содржи вредноста на случајниот број y зголемен за 1, тој ќе може со сигурност да потврди дека се работи за автентичен клиент, и ќе му прати нов сесиски клуч, кој ќе се користи за енкрипција во тековната сесија. Користењето на сесискиот клуч ја намалува употребата на вистинските клучеви со што напаѓачот не може да собере доволно податоци кои може да ги употреби за напад врз вистинските клучеви.

4.3.2 Kerberos - Надворешен доверлив субјект

Kerberos се базира на типичен метод на авторитет, каде што потои еден надворешен субјект, на кого двете страни кои сакаат да воспостават врска му веруваат. Овој трет член во процесот на автентикација ќе го означиме со знакот S, додека двете страни кои сакаат да воспостават сигурна комуникација ќе бидат A и B. Керберос протоколот претпоставува дека двете страни му веруваат на серверот за автентикација S и соодветно на тоа, поседуваат тајни клучеви познати на серверот (Ka, Kb).

Принципот е многу сличен како и во претходниот пример, со мала разлика што во Керберос, сесиските клучеви имаат време на траење. Исто како и во претходниот случај, E(x, K) ќе означува порака x криптирана под клучот K.



Сл. 4.6: Автентикација со Kerberos

Во првиот чекор, A како иницијатор на комуникацијата, бара од серверот за автентикација да го потврди идентитетот на страната B, како и својот идентитет. Во оваа ситуација, серверот враќа порака составена од Моменталното Време (Timestamp – T), Рок на траење (Lifetime – L), Сесиски клуч (K) и идентификациски број за B. Информацијата за моменталното време T, игра улога на случаен број од претходното едноставно тринасочно ракување, како и почетно време од кое започнува валидноста на сесискиот клуч K. Оваа порака серверот ја испраќа криптирана со заедничкиот клуч помеѓу серверот и A (Ka). Серверот, исто така, испраќа уште една порака, која е наменета за клиентот B, во која се содржат истите податоци, но овој пат криптирани со клучот познат на B. Бидејќи A не може да ја прочита втората порака која е енкриптирана со Kb, A едноставно ја препраќа до B. Во третиот чекор, A ја препраќа втората порака од чекорот два, а заедно со неа ја испраќа својата идентификација (A) и информацијата за моменталното време (T), енкриптирани со сесискиот клуч (K) добиен од авторизацискиот сервер S.

Кога B ќе ја добие порака од серверот S, прво ја декриптира со својот заеднички клуч Kb, од каде што добива информација за моменталното време, идентитетот на A, времетраењето на сесискиот клуч, како и самиот сесиски клуч. Потоа B со помош на сесискиот клуч добиен од претходната порака, ја декриптира пораката

со Моменталното Време (T) и идентитетот на A (A), и ги користи за да ги спореди со информациите добиени од пораката испратена од страна на серверот за автентикација S. Доколку сѐ е во ред, B врши одредена манипулација врз информацијата за моменталното време (T), и ја враќа до A, енкриптирана со сесискиот клуч K. Откако A и B ќе бидат сигурни во идентитетот на спротивната страна, и ќе имаат заеднички клуч, комуникацијата помеѓу овие два клиенти ќе може да се одвива непречено, но само во одреден временски период T+L.

4.3.3 Реализација на Kerbersos кај Windows 2000 Server

Протоколот *Kerberos* е подразбираниот протокол за проверка на автентичноста во Windows 2000 и негов основен безбедносен протокол. Тој на корисниците им овозможува со едно пријавување да пристапат на сите ресурси. Ова се постигнува така што на секој контролер на домени се инсталира Kerberos сервисот, и Kerberos клиент на сите компјутери со Windows 2000.

Кога се користи протоколот Kerberos за проверка на автентичноста, идентитетот на корисникот го проверува Kerberos сервисот од доверба, кој е на серверот. Пред поврзување со серверот, корисникот од сервисот Kerberos кој е т.н. Керберос Центар за Дистрибуција на клучеви (*Kerberos Key Distribution Center, KKDC*), бара **влезница** (*ticket*) која го потврдува идентитетот на корисникот. Корисникот потоа таа влезница ја праќа на одредишниот сервер. Бидејќи серверот има доверба во сервисот Kerberos, тој ја прифаќа влезницата како доказ за автентичноста на корисникот.

Кога се користи протоколот Kerberos за проверка на автентичноста, корисниците повеќе не може да се пријават и потоа да ги користат ресурсите со едноставно понудување на важечката идентификација на корисникот и точна лозинка. Ресурсот сега мора да се пријави кај сервисот Kerberos кој издава влезница која гарантира за корисникот. Сервисот Kerberos функционира како трета страна од доверба која прави клучеви и ги одобрува влезниците за одредени сесии клиент/сервер. Кога сервисот Kerberos ќе издаде влезница, таа ги содржи следните компоненти:

- Клуч на сесијата.
- Име на корисникот на кој е издаден клучот на сесијата.
- Времетраење на важност на влезницата.
- Дополнителни полиња и параметри по потреба.

Времетраењето на важност на влезницата се дефинира со политиките на доменот. Ако влезницата престане да важи во текот на активната сесија, сервисот Kerberos ги предупредува клиентот и серверот да ја обноват влезницата. Сервисот Kerberos потоа прави нов клуч на сесијата и сесијата продолжува.

Следните термини се користат за опис на различните компоненти на сервисот Kerberos.

Учесник (*principal*) е корисник, клиент или сервер со единствено име кој учествува во мрежната комуникација.

Подрачје, област (*realm*) е граница на автентичноста која може да се спореди со домените на Windows 2000. Секоја организација која сака да користи Kerberos сервер, го одредува своето подрачје (област). Доменот на Windows 2000 е подрачје во Kerberos, но се вика домен за да не се менуваат конвенциите кои се претходно утврдени за Windows NT.

Тајниот клуч (*secret key*) е клуч за шифрирање кој клиентот или серверот го дели со третата страна од доверба, за да шифрираат информации кои треба да се пренесат помеѓу нив. Во случајот со Kerberos, третата страна од доверба е сервисот Kerberos. Во случајот на учесник, тајниот клуч обично се базира на хеш или на шифрирана лозинка на учесникот. Тајниот клуч никогаш не се пренесува преку мрежата, туку се пренесуваат само шифрираните податоци.

Клучот на сесија (*session key*) е привремен клуч за шифрирање кој се користи помеѓу два учесници, а траењето му е ограничено со траењето на сесијата со едно пријавување. Клучот на сесија се разменува помеѓу партнерите кои комуницираат, па е познат како делена тајна. Клучот на сесија секогаш се праќа во шифриран облик.

Знакот на автентичност (*authenticator*) е запис кој се користи како потврда дека барањето навистина потекнува од учесникот. Тој содржи информации кои го потврдуваат идентитетот на праќачот и времето на стартување на барањето. Тие информации се шифрирани со делен клуч на сесијата, кој е познат само на учесниците кои комуницираат. Знакот на автентичност обично се праќа со влезницата за да примачот може да се увери дека потенцијалниот клиент пратил барање.

Центарот за дистрибуција на клучеви (*Key Distribution Center, KDC*) има две функции: функција на сервер за проверка на автентичноста (*Authentication Server, AS*) и функција на сервис за издавање на влезници (*Ticket Granting Service, TGS*). TGS ги дели влезниците на клиенти кои сакаат да се поврзат со сервисите на мрежата. Но, за да клиентот може од TGS да добие влезница, прво мора од AS-от да добие посебна влезница т.н. влезница за добивање на влезница (*Ticket Granting Ticket, TGT*).

Сертификатот на атрибути со привилегии (*Privilege Attribute Certificate, PAC*) е структура која содржи безбедносна идентификација на корисникот (*Security ID, SID*).

Влезницата (*ticket*) е запис кој им овозможува на клиентите да се претстават на серверот: тоа е единствен сертификат кој го дава сервисот Керберос. Влезницата е шифрирана така да може да се дешифрира и прочита само од одредишниот сервер. Влезниците го содржат идентитетот на клиентот, временската ознака, клучот на серверската сесија, периодот на важност на влезницата и други информации (како што е **PAC**) кој му помагаат на одредишниот сервер да го провери идентитетот на

клиентот. Влезниците може да се користат повеќе пати во периодот на нивното важење, кое обично трае 8 часа.

Еден начин на употреба на Kerberos е, за секој одредишен сервер од TGS делот на Kerberos, сервисот да побара влезница кога корисникот ќе сака да пристапи до одреден сервер. Кога се користи овој метод, одговорот на барањето содржи клуч на сесијата и други информации кои се шифрирани со корисничкиот таен клуч, па една компонента од корисничкиот таен клуч се изнесува на мрежата со секое барање за влезница.

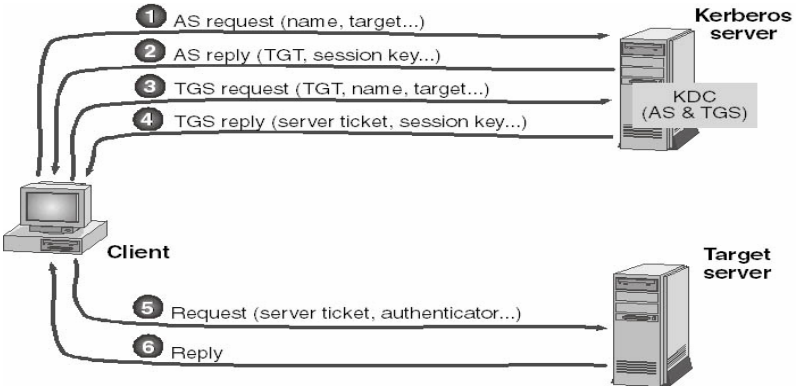
Во Windows 2000 - Kerberos го штити тајниот клуч така што на почетокот ја проверува автентичноста на корисникот, а потоа бара влезница за добивање на влезница.

Влезницата за добивање на влезница (*Ticket Granting Ticket, TGT*) е барање за издавање на влезница и случаен клуч на сесијата која треба да се користи во сесијата со TGS делот од Kerberos сервисот. Кога ќе се добие ваква влезница, корисникот може било кога да го повика сервисот: бараната влезница не доаѓа од AS, туку од TGS. Одговорот е шифриран, но не повеќе со корисничкиот таен клуч, туку со клучот на сесијата кој е добиен од AS-от за користење со TGS-от.

Кога се користи протоколот Kerberos, серверите не мора да ја проверуваат **автентичноста на проследувањето** (*pass-through authentication*). Серверот со Windows 2000 може да ги провери податоците на клиентот со помош на влезниците кои ги дава клиентот и не мора да го повикува сервисот Kerberos, бидејќи клиентот од контролерот на домен веќе добил Kerberos влезница која серверот може да ја употреби кога го прави пристапниот **токен** (влезна карта) на клиентот. Бидејќи серверот има помалку работа при воспоставување на врската, полесно може да прифати поголем број на истовремени барања за поврзување.

Протоколот Kerberos овозможува **двострана проверка на автентичноста** на клиентите и серверите. Windows-овиот протокол за проверка на автентичност NTLM овозможува само проверка на автентичноста на клиентот и се подразбира дека во сите сервери има доверба. Тој не го проверува идентитетот на серверот со кој клиентот се поврзува. Но, претпоставката дека во сите сервери може да се има доверба денес не е точна. Двостраната проверка на автентичност на клиентите и на серверите е многу значајна основа за безбедноста на мрежите.

Kerberos постапката на проверка на автентичноста подразбира дека клиентскиот компјутер преговара за размена со одредишниот сервер и со KDC-от. На слика 4.7 се наоѓа преглед на постапката за проверка на автентичноста.



Сл. 4.7: Kerberos постапка за проверка на автентичноста

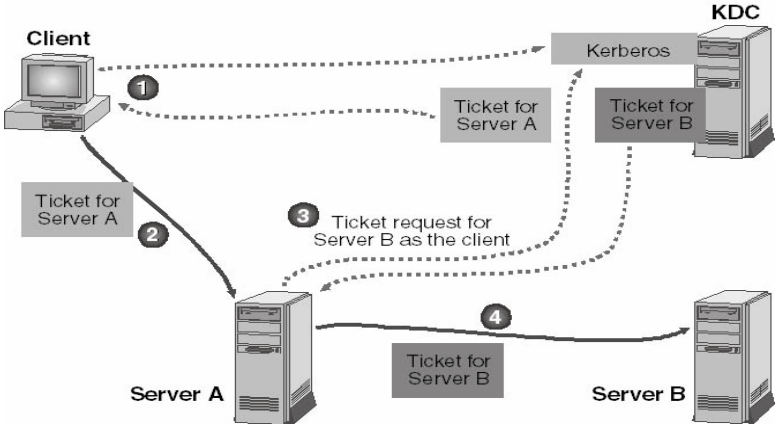
Kerberos постапката за проверка на автентичноста е следна:

1. Клиентот го праќа почетното AS барање на AS делот од Kerberos. AS барањето го содржи името на клиентот-учесник и името на одредишниот сервер-учесник за кој се бара влезница.
2. Сервисот Kerberos прави AS одговор и го праќа на клиентот. Одговорот ги содржи следните информации:
   - TGT за TGS делот од сервисот Kerberos. TGT е шифриран со помош на тајниот TGS клуч. TGT го содржи корисничкиот SID. Со шифрирање на TGT-от со помош на тајниот TGS клуч се спречува клиентот да ги промени својствата на SID.
   - Клуч на сесијата за размена на TGS делот од сервисот Kerberos. Клучот на сесија е шифриран со тајниот клуч на клиентот, кој се добива на основа на неговата лозинка, и е сличен со клучот на сесијата што се користи во NTLM прашањата/ одговорите. Тука шифрирањето го отежнува крадењето на клучот на сесијата.
3. Клиентот прави и праќа TGS барање кое содржи: име на учесниците - клиент и одредишен сервер, подрачје и TGT кој го идентификува клиентот.
4. TGS делот прави и праќа TGS одговор на клиентот. Во TGS одговорот се наоѓа влезницата за одредишниот сервер. Влезницата е шифрирана со тајниот клуч на тој сервер, кој се добива на основа на неговата лозинка која се прави кога серверот пристапува на доменот. Одговорот содржи и други информации, вклучувајќи го и клучот на сесијата.
5. Клиентот го издвојува клучот на сесијата за одредишниот сервер и прави барање до серверот. Барањето го содржи одредишниот сервер и знакот на автентичност кој е шифриран со клучот на сесијата. Клиентот го праќа ова барање до одредишниот сервер преку патеката на преносот.

6. Одредишниот сервер ја дешифрира влезницата со својот таен клуч за да дојде до клучот на сесијата. Серверот потоа со клучот на сесијата го дешифрира знакот на автентичност, заради проверка на клиентот. Ако клентот барал двострана проверка на автентичноста, одредишниот сервер прави одговор и го шифрира со клучот на сесијата за да го прати на клиентот. Со двостраната проверка на автентичноста, серверот го докажува идентитетот на клиентот, а на клиентот му се докажува и идентитетот на серверот.

Понекогаш се јавува потребата еден сервер да воспостави врска со други сервери - на барање на клиентот. Како и кај *методата на превземање на туѓи улоги* (*impersonation*) - и кај делегирањето треба да се обезбеди условот, при барање на апликативниот сервер да се применат точните безбедносни дозволи.

Протоколот Kerberos за проверка на автентичноста, овозможува *делегирање на проверката на автентичноста*. Овој вид на проверка се користи кога трансакцијата на клиентот бара повеќе сервери. Тогаш секој сервер за проверка издава влезница и во името на клиентот ја проверува влезницата за бараниот сервер. Не постои ограничување на бројот на последователни сервери кои ја делегираат проверката на автенитчност. Делегирањето се разликува од методот на превземање на туѓа улога во тоа што серверот во име на клиентот пристапува на оддалечени, а не на локални ресурси. На слика 4.8 е даден прегледот на постапката на делегирање во Kerberos.



Сл. 4.8: Постапка на делегирање во Kerberos

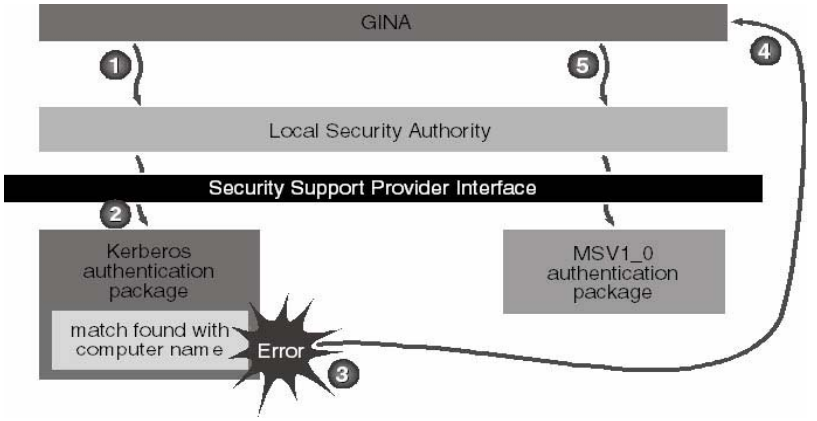
Во следните точки е опишано пристапувањето до ресурсите на два сервери:

1. Клиентот од сервисот Kerberos бара и добива влезница за одредишниот сервер А.
2. Клиентот ја праќа влезницата директно на серверот А.
3. Серверот А праќа барање до сервисот Kerberos, превземајќи ја улогата на клиент, за издавање на влезница за одредишниот сервер

B. Сервисот Kerberos издава влезница која на клиентот му дозволува да пристапи до серверот B.

4. Серверот A потоа може да ја прати влезницата на серверот B, пристапувајќи му на серверот B во улога на клиент.

Кога станува збор за локално интерактивно пријавување, корисникот се пријавува со корисничкиот налог кој постои на локалниот компјутер, а не со корисничкиот налог на доменот. На слика 4.9 е даден преглед на постапката на локално пријавување.

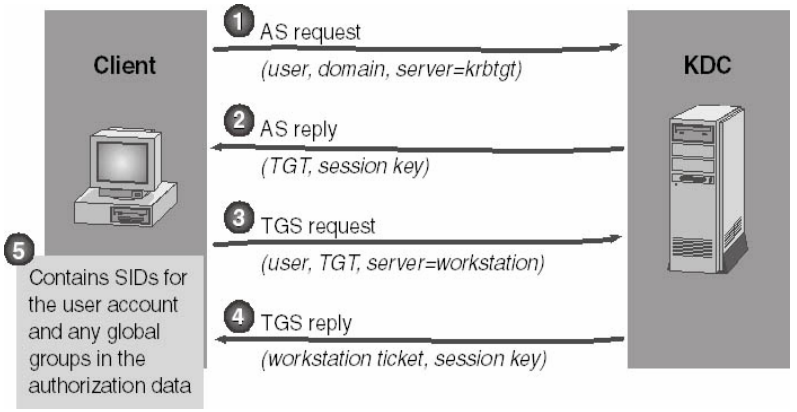


Сл. 4.9: Постапка на локално интерактивно пријавување во Windows 2000

Во следните точки е опишано што се случува при локално интерактивно пријавување.

1. Кога ***DLL GINA*** (*Graphic Identification and Authentication*, Графичко Идентификување и Проверка на Автентичноста) ќе прими барање за пријавување, тој го проследува на **локалниот гарант на безбедност** (*Local Security Authority, LSA*). Во барањето - како пакет за проверка на автентичност се наведува Kerberos, бидејќи тоа е подразбиран пакет за Windows 2000.
2. LSA го обработува барањето и го праќа на пакетот за проверка на автентичност Kerberos.
3. Кога Kerberos ќе прими барање за пријавување, тој враќа порака за грешка, бидејќи е задолжен за проверка на автентичноста за пријавување на кориснички налози на домен, а не на локални кориснички налози.
4. LSA ја прифаќа пораката и ја враќа на DLL GINA.
5. GINA повторно поднесува барање за пријавување до локалниот гарант на безбедност (LSA), но сега како пакет за проверка на автентичноста се наведува **"MSV1_0"**. Постапката на пријавување потоа продолжува како за локално интерактивно пријавување во Windows NT 4.0.

Размената до која доаѓа кога корисникот ќе се пријави на Windows 2000 со кориснички налог за домен, слична е на основната размена на Kerberos. На слика 4.10 е даден преглед на оваа постапка на пријавување.



Сл. 4.10: Постапка на локално пријавување на домен во Windows 2000

Постапката на интерактивно пријавување на домен е објаснета во следните точки:

1. Кога барањето за пријавување ќе стигне до LSA, тој го проследува на пакетот за проверка на автентичност Kerberos. Клиентот го праќа на сервисот Kerberos почетното AS барање, давајќи го името на корисникот и името на доменот. Ова е барање и за проверка на автентичноста и за TGT. Барањето се издава со наведување на името на учесникот krbtgt@<*ime_na_domen*>, каде <*ime_na_domen*> е името на оној домен во кој се наоѓа корисничкиот налог. Првиот контролер на домен во доменот - автоматски го генерира налогот krbtgt@<*ime_na_domen*>.
2. Сервисот Kerberos прави AS-одговор кој содржи TGT (кој е шифриран со Kerberos-овиот таен клуч) и клуч на сесијата за TGS размена (кој е шифриран со клиентскиот таен клуч). Овој одговор се враќа на клиентот. Делот од TGT-от со податоци на одобрување ги содржи SID корисничкиот налог и SID-овите евентуални глобални групи на кои им припаѓа корисникот. SID-овите се враќаат во LSA за да се вклучат во корисничкиот токен пристап. Сервисот Kerberos ги копира SID-овите од TGT-от во напредни влезници кои се издаваат во сервисот Kerberos.
3. Клиентот потоа прави и праќа TGS барање во кое се наоѓа името на клиентот- учесник и подрачјето, TGT кој го идентификува клиентот и името на локалната работна станица како име на одредишниот сервер.
4. Сервисот Kerberos прави и праќа TGS одговор. Овој одговор содржи влезница за работна станица и други информации, влучувајќи го и клучот на сесија (кој е шифриран со клучот на сесија од TGT-от). Освен тоа, делот од TGS со податоци на одобрување содржи SID на кориснички налог и SID-ови на евентуалните глобални групи кои се копирани од првобитниот TGT.

5. Пакетот за проверка на автентичноста Kerberos враќа листа на SID во LSA.

Сервисите на Windows 2000 за проверка на автентичност користат ***SSPI*** (*Security Support Provider Interface*) во режимот на јадро. Наместо директна комуникација со пакетите за проверка на автентичноста од Kerberos, двата сервиси пристапуваат на Kerberos преку **пакетот за проверка** кој е вграден во LSA. Овој пакет се вика ***Negotiate***.

За време на стартување на системот, сервисите ***Server*** и ***Workstation*** го иницијализираат својот интерфејс за пакетот Negotiate од LSA со помош на SSPI. Во текот на оваа постапка - сервисот на серверот собира информации за своите подразбирани налози и лозинки (*credentials*). Меѓумрежната комуникација се врши во два сегменти: *преговарање за протоколот* и *подесување на сесијата*. За да корисникот може да воспостави сесија со серверот, клиентскиот компјутер и сервер мораат да се усогласат околу безбедносниот протокол така што утврдуваат која верзија на безбедност двајцата ја поддржуваат. Кога на клиентот ќе му се провери автентичноста и тој ќе добие влезница, може да воспостави сесија со серверот.

4.3.4 Автентикација со јавен клуч (асиметрична автентикација)

Асиметричната криптографија е најреволуционерниот момент во модерната криптографија кој е откриен од страна на Diffie – Hellman. Според Diffie – Hellman секој ентитет A потребно е да има пар клучеви e и d, за кои постојат соодветни математички трансформации за енкрипција Ee и за декрипција Dd, за кои ќе важи:

Dd (Ee(m, e), d) = m

Важно е да се напомене дека за даден јавен клуч e, времетраењето за пресметка на неговиот соодветен приватен клуч d, треба да биде реално неисплатливо.

Основата на асиметричната криптографија лежи во тоа што ентитетот што испраќа порака, криптира со помош на јавниот клуч, кон ентитетот што треба да ја прими пораката:

c = Ee(m, e)

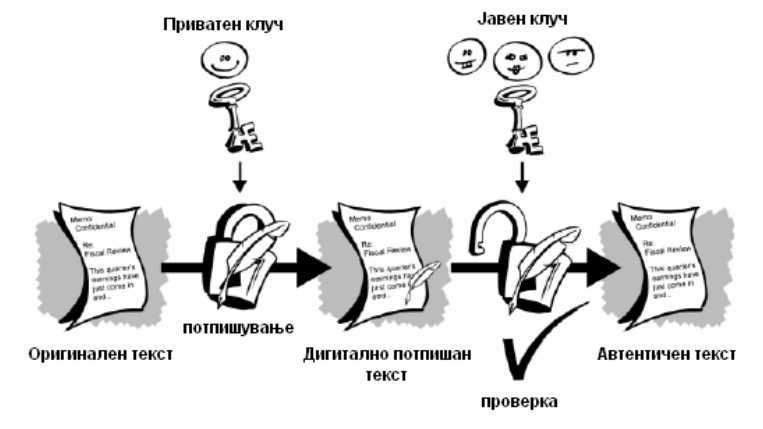
Додека ентитетот што ја прима пораката ја декриптира со својот приватен клуч:

m = Dd (c, d)

Во погорните изрази c ја претставува криптираната порака, која во таква форма се транспортира преку мрежата. Генерално, комуникацијата помеѓу ентитетите A и B се одвива на тој начин што двата ентитети имаат по еден пар јавен и приватен клуч, на пример Kae, Kad и Kbe, Kbd. За да може асиметричната енкрипција да се користи како метод за автентикација, потребно некоја трета страна да гарантира за

автентичноста на јавните клучеви на некој ентитет. Овој процес на гарантирање за валидноста на нечиј јавен клуч, се нарекува сертифицирање на јавниот клуч.

За да послужи како метод за автентикација - јавниот клуч на еден ентитет мора да биде потпишан од страна на трет ентитет кој важи како авторитет во областа на дигитално потпишување. Ентитетите кои гарантираат за автентичноста на јавните клучеви се викаат Certificate Authorities.



Сл. 4.11: Дигитално потпишување со асиметрична енкрипција

Идејата позади Авторитетите за Сертификати е едноставна: Ентитет кој ужива доверба во јавноста, гарантира за автентичноста на јавниот клуч на ентитет кој е непознат за општата јавност. На пример, една компанија може да гарантира за автентичноста на јавните клучеви на своите вработени.

Во процесот на потпишување обично авторитетите, со својот приватен клуч, го потпишуваат јавниот клуч на ентитетот чија автентичност треба да се докаже. Значи за да бидеме сигурни дека се работи за ентитетот со кој сакаме да воспоставиме врска, можеме во секое време да го провериме потписот на неговиот јавен клуч.

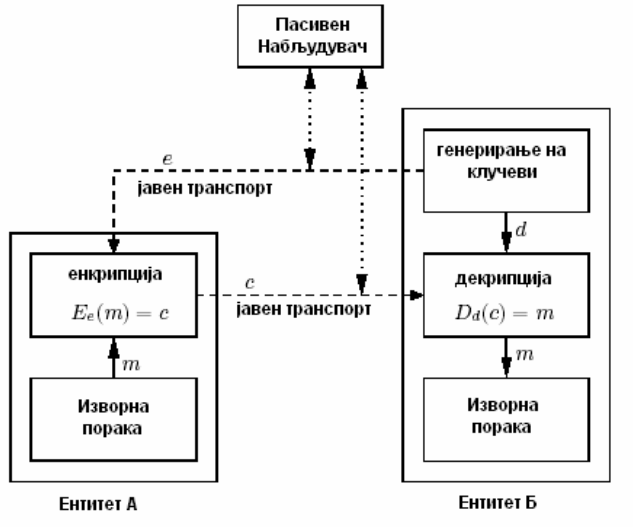
4.3.5 Безбедносни напади кај асиметричната криптографија

Во најопшт случај, нападите врз криптографските протоколи можат да се поделат на неколку групи:

1. *Напад со познат клуч (known-key attack)*. Во овој тип на напад, напаѓачот веќе има пристап до претходно користените клучеви, и оваа информација ја користи за предвидување на новите клучеви
2. *Напад со повторување (replay attack)*. Во некои случаи кога напаѓачот е во позиција да сними една комуникациска сесија помеѓу два ентитети, тој може потоа да се обиде да ја повтори истата постапка за да научи повеќе за начинот на автентикација и криптографските техники, или пак да се здобие со можност на извршување одредена функција врз системот како парче или целина.

3. *Лажно претставување (impersonation)*. Во овој случај напаѓачот ја презема улогата на еден легалните ентитети во мрежата.
4. *Напад со речник (dictionary attack)*. Овој напад најчесто се користи за добивање на лозинки од нивните криптограми. Лозинки често се чуваат во форма на hash криптограми од вистинските вредности, а напаѓачот користи речник врз чии зборови ја применува hash функцијата и потоа го споредува криптограмот со оној од лозинката.
5. *Пребарување напред (forward search)*. Во случај кога множеството на елементи кои се предмет на енкрипција е ограничено, напаѓачот може да го искористи познавањето на јавниот клуч во комбинација со сите вредности од множеството - за да ја добие изворната вредност на криптограмите (исто како и *„Напад со редчник“* за hash функции).
6. *Човек во средина (man in the middle)*. Овој напад е пример кога напаѓачот се претставува како легален ентитет А на ентитетот Б, во исто време и како Б на ентитетот А, а здобиените информации ги користи за лажно претставување на својот идентитет кај двата ентитети.

Од последниот дел за автентикација со јавни клучеви, заклучивме дека најпрактичен начин за дистрибуција на криптографски клучеви е користењето на асиметрични криптографски методи, бидејќи тие немаат потреба од безбедно транспортирање на таен клуч.



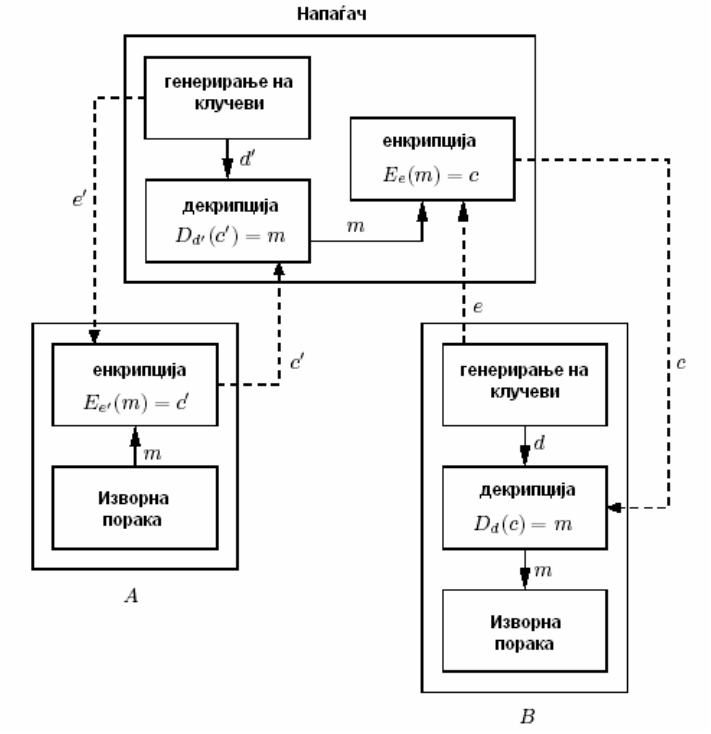
Сл. 4.12: Пасивен набљудувач

На погорната слика јасно се гледа дека пасивните набљудувачи не можат да пристапат до вистинските податоци кои ги носи пораката.

Сепак - и кај асиметричната криптографија постојат одредени проблеми. Најголем проблем за асиметричната криптографија лежи во автентичноста на јавните клучеви. Во случај кога Ентитетот А сака да испрати порака до Ентитетот Б, јавниот клуч со кој А ќе ја енкриптира пораката, важно е да биде клуч кој

потекнува од Б, затоа овој метод е подложен на таканаречениот "Човек во средина" напад (Слика 4.13).

При овој тип на напад, напаѓачот го користи парот јавен-приватен клуч на ентитетот Б, за да ја достави пораката до целта, со што нема да предизвика сомнеж кај А или Б. Во исто време, напаѓачот доставува до А свој јавен клуч (пар клучеви e' и d'), којшто А го користи за енкриптирање на пораката во транспортниот криптограм c'. Напаѓачот потоа ја декриптира пораката со својот приватен клуч d' и повторно ја енкриптира со јавниот клуч на ентитетот Б (e). Од гледна точка на ентитетот А, пораката била успешно енкриптирана под јавниот клуч на Б, и криптограмот бил доставен до целта. Од страната на Б, јавниот клуч е бил искористен за пресметка на криптограмот c и истиот бил доставен до целта - со што Б, успешно ја добил вистинската порака, по наводно сигурен пат. И двата ентитети А и Б, сметаат дека успешно ја завршиле размената на податоците, без сомневање дека надворешен ентитет се здобил со пристап до осетливи информации.



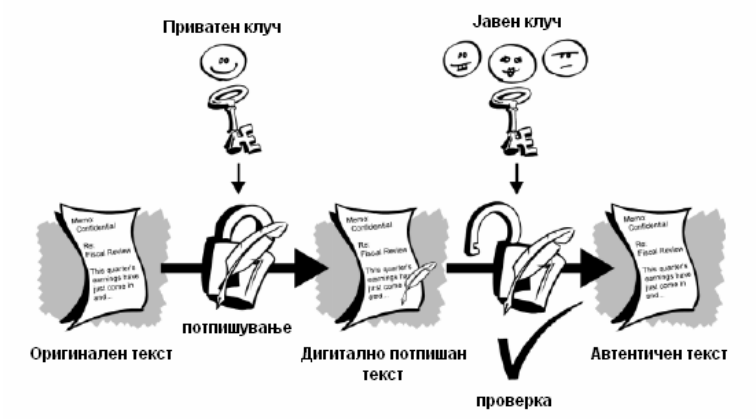
Сл. 4.13: Напад „Човек во средина"

4.4 ДИГИТАЛНИ ПОТПИСИ

При користење на асиметрични криптографски методи за автентикација, се користи посебен систем за одредување на автентичноста на информацијата која потекнува од ентитетот со кој се комуницира. Овој метод се базира на

асиметрични криптографски модели и се нарекува дигитално потпишување на информацијата.

Дигиталните потписи му овозможуваат на примачот на информацијата да ја верифицира автентичноста на изворот на информацијата, и исто така верифицира дали информацијата е оштетена. Затоа, јавните клучеви со дигитален потпис овозможуваат автентификација и интегритет на податоците. Дигиталните потписи исто така овозможуваат non-repudiation, што значи дека го превентира испраќачот од тврдењето дека таа или тој всушност не ја пратил информацијата.



Сл. 4.14: Дигитално потпишување

Бидејќи се работи за асиметрични криптографски методи, секако дека ќе важи следното равенство:

$$Dd\,(Ee(m)) = m$$

каде што Dd е функција за декрипција, Ee – функција за енкрипција, а m е пораката која се криптира. За да можеме да го искористиме овој криптографски модел за потпишување, ќе се послужиме со обратен процес од стандардниот процес на асиметрична енкрипција.

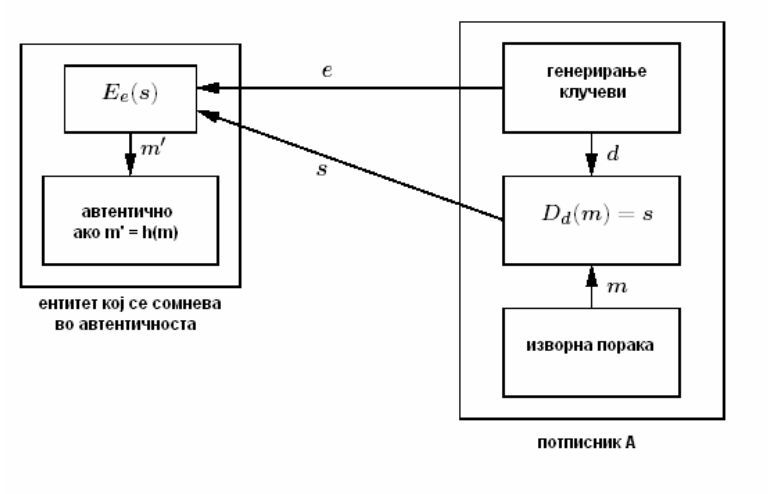
Прво да претпоставиме дека имаме пар јавен-приватен клуч (e,d), кој ќе ни послужи за да ја потпишеме пораката m со потпис s.

Потпишувањето на пораката m ќе го извршиме со функцијата Sa, која ќе биде всушност Dd, така што:

$$s = Dd\,(m, d)$$

За да ја потврдиме автентичноста на пораката m, т.е. да покажеме дека е потпишана од ентитетот сопственик на парот (e,d) ќе дефинираме функција за верификација Va:

$$Va(m, s) = \begin{cases} \textit{валиден}, \text{ ако } Ee(s, e) = m, \\ \textit{невалиден}, \text{ во спротивно.} \end{cases}$$



Сл. 4.15: Дигитално потпишување

Бидејќи во овој општ случај - потпишувањето би траело долго доколку трансформациите се извршуваат врз целата порака, и дигиталните потписи би биле со големина слична на големината на пораките. Затоа во најчест случај, за дигитално потпишување во реалноста, се потпишува само еден дел од целата порака m'. Ова парче од целата порака, најчесто се добива со примена на некоја стандардна еднонасочна hash функција, како MD5, SHA-1 и сл. Со ова, дигиталното потпишување го менуваме во:

$$s = Dd(h(m), d)$$

А функцијата за верификација Va во:

$$Va(m, s) = \begin{cases} \textit{валиден}, \text{ ако } Ee(s, e) = h(m), \\ \textit{невалиден}, \text{ во спротивно.} \end{cases}$$

каде h претставува однапред договорена еднонасочна hash трансформација.

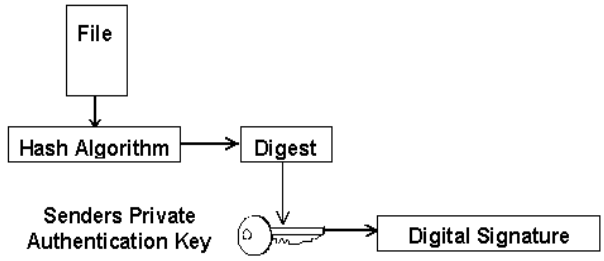
4.4.1 Процес на креирање на дигитален потпис

Кога користиме сервис за обезбедување на нашиот документ, се случуваат следните работи:

1. Најпрво, нашиот документ поминува низ т.н. "hashing" алгоритам кој креира помал "digest" на фајот. Овој digest е број кој што би бил потполно различен - доколку се смени било што во документот и тој повторно се пушти на hashing. Ова се користи при проверка, за да знаеме дека фајлот не бил сменет откако бил пратен т.е. со ова се обезбедува интгретитетот на пораката.

2. Со помош на јавен клуч се енкриптира digest–от. Ова креира дигитален потпис за тој фајл.
3. На крај, нашиот документ се потпишува со додавање на дигиталниот потпис на крајот од документот.

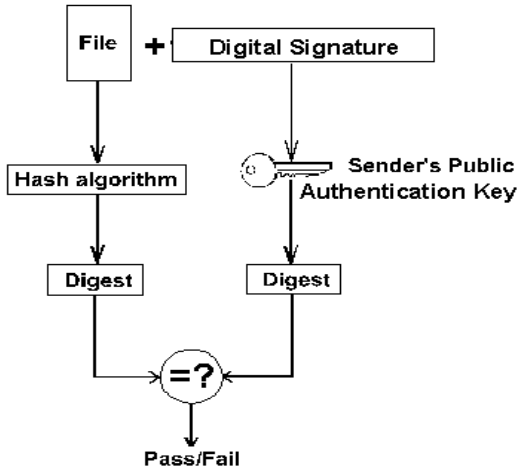
Следниот дијаграм ни го покажува целиот процес:



Сл. 4.16: Процес на креирање на дигитален потпис

4.4.2 Проверка на дигиталниот потпис

За проверка на дигиталниот потпис, сега декриптираниот документ повторно го пуштаме низ истиот hashing алгоритам кој претходно го користевме за добивање на digest пораката, а дигиталниот потпис го пуштаме низ нашиот јавен клуч. Оваа постапка ни дава два резултати кои потоа ги споредуваме. Ако тие не се исти, тогаш знаеме дека пораката е или сменета откако била пратена, или пак била пратена од некое трето неовластено лице.



Сл. 4.17: Проверка на автентичност на дигитален потпис

Ако двата digest-и се исти тогаш знаеме дека пораката има:

- Автентичност, затоа што само ние го имаме тајниот клуч што го креира дигиталниот потпис,

- Интегритет, затоа што ако некој ја пресретнал пораката и направил измени во нејзината содржина, резултатите од hashing – от нема да се совпаѓаат,
- Не-одрекување, затоа што само ние го поседуваме тајниот клуч кој се користи за креирање на потписот, така што не можеме да тврдиме дека некој друг ја испратил пораката.

Силата на дигиталните потписи е дека тие се безмалку невозможни за фалсификување и се лесни за верификување. Но, ако двете страни се странци кои никогаш не комуницирале пред тоа, и едниот го прими јавниот клуч на другиот, а нема ниедно друго средство да верификува кој е праќачот, освен тврдењето на праќачот дека е навистина оној кој се претпоставува, тогаш дигиталниот потпис е неупотреблив за автентикација. Тој сеуште ќе верификува дека пораката пристигнала недопрена, но не може да се користи за автентикација на идентитетот на праќачот. Во случаи каде што двете страни немаат претходно знаење едни за други, потребна е трета доверлива страна за да ги идентификува идентитетот на емитувачките страни.

4.4.3 Стандарди за дигитални потписи

Моментално има два конкурентни стандарди за технологијата на дигитални потписи. Двата система се засноваат на стандардот X.509 на International Telecommunications Union за сертификација на јавни клучеви. Оној кој е на пазарот подолго е стандардот за енкрипција со јавен клуч RSA Data Security, кој стана де-факто стандард во индустријата. RSA Data Security го користи RSA алгоритмот со јавен клуч, и за енкрипција и автентикација. Поново развиениот стандард е DSS на американската влада, кој се заснова на DSA. Тој е избран од страна на National Institute of Standards and Technology (NITS) во 1994 год. Многумина се сомневале во одлуката за избор на DSS. Разбирливо, еден од најгласните опоненти бил RSA Data Security и компании поврзани со RSA. Меѓутоа и многу други се сомневаат во DSS. Крипто-системот DSS е релативно нов и не е уште потполно тестиран. Од таа причина многумина веруваат дека не е сигуирен како RSA стандардот, кој е подложен на ригорозни тестови во изминатите 19 години. Некои дури и се сомневаат во мотивите за изборот на DSS. Одлуката е донесена во координација со NSA, многу тајно и без јавна дебата. Некои дури и тврдат дека DSS е избран затоа што NSA има оставено врата во системот. Иако конкурентните стандарди не претставуваат пречка во имплементирањето на дигиталните потписи во големи мулти-национални организации, тие можат да резултираат со неможност за размена на дигитални потписи помеѓу организации.

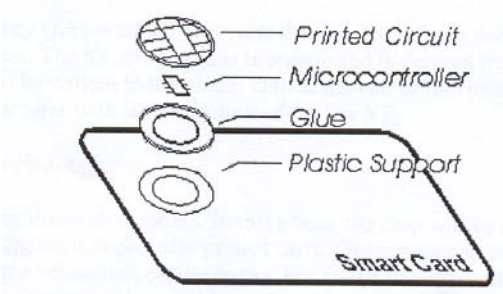
4.5 SMART CARD (ПАМЕТНА КАРТИЧКА)

Паметната картичка, е пластична картичка со големина на кредитна картичка, со вграден чип со интегрирано коло. Self-containement на паметната картичка ја прави отпорна на напади. Поради оваа особина, паметните картички често се користат во различни апликации кои бараат јака безбедносна заштита и автентикација. На пример, паметните картички можат да послужат како средство за идентификација на сопственикот на картичката. Исто така - можат да бидат и

медицинска картичка која ја содржи медицинската историја на корисникот. Уште повеќе, картичката може да се користи како дебитна-кредитна картичка која дозволува off-line транскации. Сите овие апликации имаат потреба - доверливи информации да бидат сместени на картичката, како што се биометриските особини на сопственикот, лични медицински податоци, криптографски клучеви за автентикација итн.

4.5.1 Физичка структура на картичката

Физичката структура на паметната картичка е специфицирана од International Standards Organization (ISO) стандардите 7810, 7816/1 и 7816/2. Генерално е направена од три елементи: базата е пластична картичка со димензии 85.60 mm x 53.98 mm x 0.80 mm. На картичката се вметнати испечатено коло и чип со интегрирано коло. Печатеното коло го исполнува ISO стандардот 7816/3 и обезбедува 5 точки за поврзување на енергија и податоци. Тоа е херметички фиксирано во процеп обезбеден од картичката и е залепено на чип со коло, наполнето со кондуктивен материјал, и запечатено со контактните точки. Печатеното коло го заштитува чипот со колото од механички влијанија и статички електрицитет. Комуникацијата со чипот е остварена преку контакти кои се сместени на печатеното коло.



Сл. 4.18: Преглед на физичката структура на картичката

Капацитетот на картичката е одреден од нејзиниот чип со интегрирано коло. Типично, чипот со интегрирано коло се состои од микро-процесор, ROM, нестатичка RAM и електрично-бришлива програмабилна ROM (EEPROM) кој ќе ја задржи својата состојба кога ќе се исклучи напојувањето. Комуникациската линија е би–дирекционалана сериска трансмисиска линија, која го исполнува стандардот 7816/3. Целокупната размена на информации е под контрола на централната процесорска единица во чипот со интегрирано коло. Командите на картичката и влезните податоци се праќаат до чипот кој по добиените команди - одговара со статусни зборови и излезни податоци. Информациите се праќаат во полу-дуплекс мод, кој претставува трансмисија на податоци во еден правец. Овој протокол, заедно со рестрикцијата на бит-ратата, спречува масивни напади на картичката.

4.5.2 Животен циклус на картичката

Во склоп на секоја картичка има оперативен систем кој може да содржи идентификационен број на производителот, тип на компонента, сериски број, информации за профилот итн. Уште поважно, системската област може да содржи различни сигурносни клучеви, како што се клуч на производителот или фабрикациски клуч, персонализациски клуч исл. Сите овие информации се чуваат тајно.

Од производителот и доставувачот на апликација, па сè до корисникот на картичката, создавањето на паметна картичка е поделено во неколку фази. Ограничувањата во преносот и пристапот до податоци се инкрементираат во различни фази, со цел да се заштитат различни области на картичката. Постојат 5 главни фази во животниот циклус на една картичка:

- *Фаза на производство:*

Оваа фаза се спроведува од страна на производителот на чипови. Силиконскиот чип со интегрирано коло се создава и тестира во оваа фаза. Се додава фабрички клуч за да го заштити чипот од модификација, пред да се вметне на пластичната катичка. На крај на оваа фаза - се запишуваат и други податоци за производителот на чипот. По ова чипот е спремен за да се достави до производитеот на картички.

- *Фаза на пред – персонализација:*

Оваа фаза е изведена од снабдувачите на картички. Во оваа фаза, чипот се става на пластичната картичка која може да го има на себе испринтано логото на снабдувачот на апликација. Се реализира врската помеѓу чипот и печатеното коло, и целата единица се тестира. Како додаток на безбедноста - се оневозможуваат инструкциите за физички пристап до меморијата. Пристап до картичката може да се оствари само со користање на логичко адресирање на меморијата. Ова овозможува заштита на системските и фабричките сектори од пристап и модифицирање.

- *Фаза на персонализација:*

Оваа фаза се остварува од страна на корисникот на картичката и го завршува создавањето на логичките податочни структури. Фајловите со податоци и апликациските податоци се запишуваат на картичката. Исто така се вметнуваат и информации за сопственикот на картичката, PIN – от, и деблокирачкиот PIN.

- *Фаза на употреба:*

Ова е фаза на нормална употреба од страна на корисникот. Активирани се апликацискиот систем, контролите за логички пристап до фајловите итн. Пристапот до информации на картичката е ограничен од безбедносните подесувања од страна на апликацијата.

- *Фаза на престанок на живот - инвалидизација:*

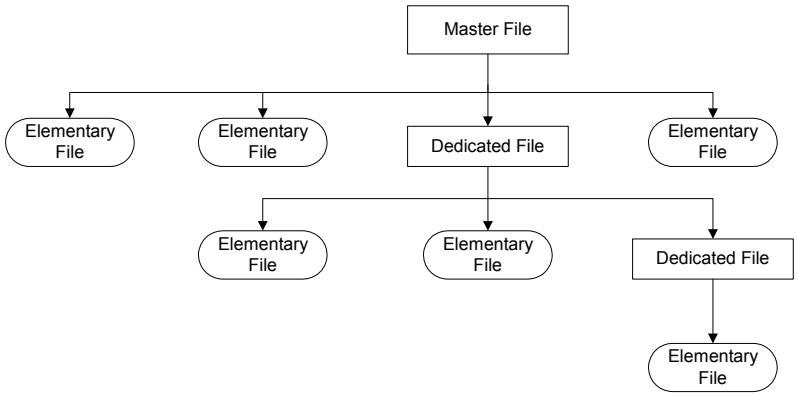
Има два начина да се доведе картичката во оваа фаза. Еден е иницран од страна на апликацијата која го запишува инвалидациското заклучување на индивидуален фајл, или главен фајл. Сите операции, вклучувајќи пишување и ажурирање, се оневозможени од страна на оперативниот систем. Само инструкциите за читање може да останат активни за потреби на анализа. Вториот начин е кога контролниот систем неповратно ќе го блокира пристапот, бидејќи и

PIN-от и деблокирачкиот PIN се блокирани, и тогаш сите операции се блокирани - вклучувајќи и читање.

4.5.3 Логичка структура и контрола на пристап

Откако паметната картичка ќе биде издадена на корисникот, заштитата на картичката се контролира главно од оперативниот систем на апликацијата. Модот за физичко адресирање не е достапен. Пристапот до податоци мора да се направи преку логичката структура на картичката.

Генерално, во однос на чувањето на податоци, паметната картичка може да се разгледува како диск-драјв каде што фајловите се организирани во хиерархиска форма преку директориуми. Слично на MS-DOS, има еден главен или мастер фајл (MF) кој е како root директориум. Под root директориумот, можеме да имаме различни фајлови кои се нарекуваат елементарни фајлови. Можеме да имаме и различни под-директориуми наречени посветени фајлови (DF). Под секој поддиректориум повторно се наоѓаат елементарни фајлови (EF). Главната разлика помеѓу MS-DOS и паметната картичка, е што посветените фајлови можат да содржат податоци.



Сл. 4.19: Организација на фајл системот кај smart card

Во терминологијата на паметни картички, коренот или мастер фајлот, покрај делот со заглавје во кој се опишува себеси, се состои и од тело кое ги содржи заглавјата на сите посветени фајлови и елементарни фајлови кои го имаат MF како родител во хиерархијата. Посветените фајлови се функционално групирани фајлови, кои се состојат од самиот себе и сите фајлови кои се деца на посветениот фајл. Елементарните фајлови едноставно се состојат од заглавје и тело кое ги чува податоците.

Начините на управување со податоци се различни во зависност од оперативниот систем на картичката. Некои од нив може да управуваат со податоци само по должина и offset, други можат да ги организираат податоците со фиксна или променлива должина на записи како кај Global System for Mobile Communication (GSM). Во сите случаи, фајлот мора да биде селектиран пред да се изврши некоја

операција. Ова е еквивалентно со отварање на фајлот. Логичкиот пристап и механизмите на селекција се активираат откако ќе се приклучи картичката на извор на енергија, додека мастер фајлот е селектиран автоматски. Операцијата на селекција дозволува движење во дрвото. Може да биде опаѓачка со избирање на EF или DF, или да биде растечка со избирање на MF или DF. Хоризонтално движење е овозможено со избирање на EF од друг EF. Накратко, структурата на фајлови кај оперативните системи на паметните картички - е слична со онаа на другите оперативни системи како MS-DOS и UNIX. Но, со цел да се обезбеди поголема безбедносна контрола, овозможено е додавање на услови за пристап и полиња за статус на фајл. Уште повеќе, заклучувањето на фајл е возможно со цел да се забрани пристап до фајлот. Овие механизми и алгоритми обезбедуваат логичка заштита на паметната картичка.

4.5.4 Контрола на пристап

Системот за контрола на пристап, го покрива главно пристапот до фајловите. Секој фајл е закачен со заглавје кое ги содржи условите на пристап или барањата на фајлот и моменталниот статус. Основниот принцип за контролата на пристап се базира на коректната презентација на PIN броевите и нивно управување.

PIN-овите се зачувани во два одвоени фајла. Користењето на условите за пристап на овие фајлови може да спречи менување на PIN-овите. PIN-от може да биде сменет со користење на инструкцијата за промена на PIN, заедно со стариот и новиот PIN. Но, за повеќето од оперативните системи на картичките, кореспондирачкиот PIN ќе биде невалидизиран или блокиран, кога фиксен број на инвалидни PIN-ови се последователно презентирани. Бројот на неточни пријавувања варира кај различни системи.

Во овој момент, сите фајлови бараат PIN-от да биде блокиран и недостапен. Деблокирањето мора да биде извршено со знаење на вистинскиот PIN и на специјалниот деблокирачки PIN сместен на картичката. Ако деблокирачкиот PIN биде неточно внесен одреден број на пати - и тој ќе биде блокиран. Тогаш и двата се блокирани и не може да се повратат. Ова се нарекува неповратно блокирање. Некои системи дури може и да ја инвалидираат целата картичка со цел да спречат натамошни напади.

4.5.5 Управување со PIN

За да се достигне горе-споменатата заштита и блокада на PIN-от, два бројачи треба да се имплементираат за секој од верификациските броеви на картичката. Бројачите се направени на тој начин што секоја можна грешка во пишување и читање ќе биде избегната. Има три состојби во управувањето со PIN-от:

- *PIN -от да биде презентиран*

Фајловите или функциите кои имаат PIN презентација како предуслов, можат да се извршат. Секој пат кога ќе се внесе точен PIN, бројачот се рестира на максималниот број на обиди, на пример 3 обида.

- PIN- от не бил внесен или бил внесен неточен

Бројачот ќе биде намален за еден - за секој неточно внесен PIN. Сите операции или функции кои бараат PIN ќе бидат блокирани. Ако бројачот стигне до 0, тогаш PIN се блокира.

- PIN-от е блокиран

Во оваа состојба, сите операции бараат презентација на PIN и дури и инструкцијата за PIN презентација е блокирана. Мора да се изврши инструкција за деблокирање на PIN. Ако е презентиран точен деблокирачки PIN, тогаш бројачот се ресетира на максималниот број на обиди и се враќа на првата состојба. Но, ако неточен деблокирачки PIN се презентира, бројачот за деблокирачки PIN се намалува за еден и кога овој бројач ќе стане нула, PIN-от не може веќе никогаш да се деблокира.

4.5.6 Напади на паметни картички

Како што е наведено и погоре - паметната картичка претставува супериорна алатка за спроведување на системска безбедност и заштита. Една од безбедносните опции кај повеќето оперативни системи за картички се криптографските можности. Тие обезбедуваат енкрипција и декрипција на податоци на картичката, некои од нив дури може да се користат за генерирање на криптографски клучеви. Тајната на криптографскиот алгоритам, на зачуваните клучеви, и контролата на пристап на паметната картичка, се мета за напад. Многу компании и криптоаналитичати тврдат дека можат да ја загрозат паметната картичка и нејзиниот микро-контролер. Некои ја напаѓаат картичката логички, други ја напаѓаат физички, додека пак трети само ја докажуваат својата способност со математички теореми.

Логички напади

Бидејќи целиот клучен материјал на картичката е сместен во електрично бришлива програмабилна ROM, и од фактот дека EEPROM операциите за запишување може да бидат засегнати со големи напони и температури, информациите можат да бидат заробени со менување на волтажата на микроконтролерот. На пример, добро познат напад на PIC16C84 микроконтролерот се состои во тоа дека може да се измени безбедносниот бит на микроконтролерот со бришење на меморијата, што се постигнува со менување на напонот на VCC на VPP –0.5 V. Друг пример е нападот на DS5000 микроконтролерот, каде што мал пад на напонот може да ја ослободи безбедносната брава итн. Од сите овие причини - некои безбедносни процесори имплементираа сензори кои го вклучуваат алармот кога кога ќе настанат промени во околината. Но овие сензори често предизвикуваат лажни аларми кога картичката се употребува и колата се иницираат.

Физички напади

Типични се инвазиските физички напади. Пред да се изврши ваков напад, чипот мора да биде отстранет од пластичната картичка. Ова може да се направи со остар предмет за отстранување на пластиката позади чипот. По вадењето - чипот може да се ипитува и напаѓа директно. Во лабораториите на Cavendish во Cambridge, е развиена техника за обратен инженеринг на чиповите. Функциите и подесувањето на чипот можат да се откријат со користење на оваа техника. Потоа се користи друга техника за набљудување на операциите на чипот. На крај, тајните податоци од чипот се потполно откриени. Покрај овие, постојат и многу други начини за физички напад на картичка. Бришење на безбедносната брава со примена на UV-зраци директно на EPROM-от, пробинг на операциите на колото со употреба на микро-пробинг игли, или користење на микроскопски ласерски секач за чипот итн. Но, повеќето од овие напади се изводливи само во добро опремени лаборатории и за нивно изведување потребни се големи средства.

4.6 БИОМЕТРИКА

Кога станува збор за шеми за автентикација кои се базираат на концептот "нешто што сме", се мисли на биометрика. Автентикација со биометрика е процес на користење на нечија физичка карактеристика, особина, аспект на физичко постоење или однесување, за автентикација на идентитетот. Најпознат процес е концептот на користење на отисок од прст за идентификување на индивидуа. Со години МВР го користи отисокот од прст за идентификување на индивидуа и правење на проверки.

Биометриската автентикација генерално спаѓа во две категории:

- Првата е препознавање на физичка карактеристика (physical characteristics recognition – PCR), која се заснова на физичка карактеристика како што е отисок од прст, скен на ретина или ирис, или фацијална геометрија за идентификација и автентикација.
- Втората категорија е препознавање на карактеристика на однесување (behavioral characteristic recognition BCR). BCR се базира на карактеристики на однесување како што се начинот на куцање на тастатура, пишување, или потпишување. Во основа, PCR е многу по-применуван од BCR. Кај повеќето биометриски автентикации - постои процес на регистрација. Ова го подразбира процесот на регистрација или запишување на некоја физичка особина како што е отисок од прст, запис на гласот, или скен на зеница. За време на процесот на регистрација се креира шаблон за дадената особина. Шаблонот е всушност математичка репрезентација на физичката особина. Шаблонот потоа се чува во некоја форма (обично во база на податоци и тоа во енкриптирана форма) за да може покасно да се искористи за споредба со вистинската карактеристика на корисникот, т.е. за автентикација на идентитетот на потенцијалниот корисник. Да претпоставиме дека биометрискиот систем се користи за идентификација и автентикација на корисници во мрежа. Кога корисникот сака пристап до мрежата, тогаш неговиот шаблон (т.е. физичка карактеристика) се чува на серверот. Истиот процес кој се користи за создавање на шаблонот - се користи и за создавање на математичка репрезентација на особината, и кај читачот и кај серверот. Потоа се

споредува со шаблонот кој е зачуван на серверот или на работната станица. Ако се совпаѓаат, тогаш крајниот корисник добива пристап до мрежата. Ова е само апроксимација на процесот. Процесите на автентикација варираат во зависност од дизајнот на системот и производителот.

4.6.1 Доверливост на биометриската идентификација

Кога се разгледува систем со биометриска автентикација, има две критични карактеристики кои треба да се разгледаат пред тој да се примени. Тие се:

- Рата на погрешно прифаќање - False Acceptance Rate (FAR)
- Рата на погрешно одбивање - False Rejection Rate (FRR)

FAR е ратата до која системот неправилно прифаќа или препознава потенцијален корисник како авторизиран за пристап на системот, кога тој всушност не е. Со други зборови, колку често системот пропушта некого што не треба? Повеќето производители на направи за биометриска автентикација го даваат FAR за нивните производи. Во спротивно, секој корисник може да го побара тоа од нив. Многу често FAR е даден во проценти. FAR за било кој биометриски систем за идентификација и автентикација мора да биде многу прецизно пресметан. Производителот може да даде FAR кој изгледа дека е многу мал, но бројките може да залажуваат. На пример, FAR од само 1% значи дека еднаш од 100 пати системот неправилно прифаќа неовластен корисник. Оваа рата на погрешно прифаќање е преголема. FAR od 1% значи дека ако хакерот направи 100 обида - барем во еден од нив ќе успее. Дури и FAR од 0,1% е преголем. Тоа значи дека еден обид од 1000 ќе биде успешен (ова оди многу повеќе во прилог на хакерот, отколку шансите хакерот да погоди лозинка од 8 карактери). На пример, дури и ако ги исклучиме буквите од азбуката и специјалните знаци и користиме само броеви за лозинка од 8 знаци, сеуште ќе имаме преку 99 999 999 лозинки.

Друга важна карактеристика на секој биометриски систем за идентификација и автентикација е FRR, ратата со која системот неправилно одбива легитимен корисник. Иако таа не е критична како FAR, FRR е важна во секоја примена на системот за биометриска автентикација. Ако FRR на системот е преголема, може да предизвика фрустрација кај корисниците. Фрустрацијата води кон послаби системи за автентикација за да се избегне биометриката. Ова пак води до потенцијална дупка во безбедносниот систем и до пробив на системот. Кога се разгледува биометриска шема за автентикација, мора да земеме во предвид како да се справиме со природните промени на луѓето. Ова е особено точно за PCR биометриските системи (препознавање на лице). На пример, да претпоставиме дека системот користи препознавање на лице и имаме некој што имал брада и решава да ја избричи. Дали тогаш ќе може да влезе во системот?

Како луѓето стареат, така доаѓа до физички промени кај нив. Каде и да е имплементиран системот - тој мора да биде во состојба да го обновува шаблонот со субтилните промени што природно се случуваат, и тоа секогаш кога ќе автентикува корисник. За да биде потполно ефективен, секој биометриски систем мора да биде доволно софистициран за да забележи измама. Како резултат, употребената технологија во системот мора да биде обемна и напредна. На

пример, систем кој користи само оптичка слика за отисок од прст, препознавање на лице, или геометрија на рака, нема да може да детектира украдена или фалсификувана карактериситка ако корисникот е мртов. Пософистицираните системи бараат неколку елементи на физичката карактеристика. На пример, читач на рака кој не само што ќе ја споредува геометријата на раката, туку и ќе ја мери температурата и крвниот притисок. Овој подетален пристап го прави системот многу потежок за измама со нешто како на пр. пластична макета на раката.

4.6.2 Backup автентикација

Ефективниот систем за биометриска автентикација мора да е во можност да се справи со привремени физички промени. Ако употребувате отисок од прст за автентикација, што се случува ако корисникот го изгори прстот? Или пак ако некој скрши рака, а системот се базира на геометрија на рака? (Нема да можат да добијат пристап до системот со завој или гипс на раката). Мора да се разгледаат и backup методи за автентикација на корисникот во случај да биометриката не успее. Исто така, мора да се разгледа и тоа - колку е лесно да се активира backup методата. Не смее да се дозволи корисникот да се најде заклучен надвор - без алтернативен метод на автентикација. Ако имаме backup метод, лозинка на пример, како ќе спречиме некого да го користи цело време, или пак како ќе спречиме некого да да го компромитира бекап методот и да го надмудри биометрискиот систем? *Биометриски систем кој може да се надмудри е безвреден.*

4.6.3 Услови на околината

Уште еден елемент, кој мора да се разгледа пред имплементација на биометриски систем за автентикација, е околината во која ќе дејствува. Временските услови, буката, влагата, и нечистотијата може значително да влијаат на системите. Фабричка установа каде што работниците се во постојан допир со малсо и нечистотија, не е најидеална средина за систем со отисок на прст или читач на рака. Овие системи би биле непогодни и на места каде што работниците носат ракавици. Слично, скенер на зеница или геометрија на лице не би бил препорачлив во средина во која вработените носат маски или заштитни очила. Читач на глас не се става во средина со голема бука. Овие предуслови мора да земат во предвид пред да се имплементира системот.

4.6.4 Прифатеност на системот кај корисниците

За да се достигне успешна примена на биометриски автентикациски систем, важно е да се оствари добра прифатеност на технологијата од страна на корисниците. Корисниците можат да бидат неудобни со скенери на зеница или пак да сметаат дека снимњето на отисок е мешање во приватноста. Пред имплементација - мора да се земе предвид колку нападна ќе биде технологијата. Како што може и да се очекува, по-нападна технологија е понеудобна за корисниците. Иако скенирањето на зеница е далеку поефективно од отисок на прст, корисниците се далеку позадоволни со употреба на читач на отисок. Друга работа која мора да се запази пред примена на системот, е генералната хигиена во

организацијата. Ова е особено важно прашање за биометриските уреди кои се користат за автентикација на централна локација, како што е главен влез во некоја установа.

4.6.5 Безбедност на биометрискиот систем

Друг критичен фактор кај системите за биометриска автентикација е како да се справиме со комуникацијата и чувањето. Мора да се земе предвид како е имплементиран постоечкиот систем. На пример, ако е спроведен во LAN, дали тој комуницира со сервер за автентикација, а ако е така - тогаш комуникацијата помеѓу серверот и читачот е многу важна, бидејќи биометрискиот систем може да биде подложен на напад. Треба да се води сметка дали комуникацијата е енкриптирана, дали може да се снима од некаде итн. На пример, ако А се идентификува себеси на мрежа со користење на читач на отисок на нејзината тастатура - математичката репрезентација на нејзиниот отисок се праќа до серверот за идентификација и автентикација. Но, Б ставил прислушкувач на мрежата и ја пресретнал математичката репрезентација на отисокот на пат кон серверот. Сега Б ја има информацијата и може да ја емитува до серверот кога сака и да добие пристап до мрежата како А. Дури и трансмисијата да била енкриптирана, Б сеуште ќе биде во можност да ја пресретне и копира. Секако, постојат многу начини производителот да ги избегне овие проблеми. Еден метод е да се користат временски паузи во алгоритмот за енкрипција. Друг метод би бил да се зачува шаблонот на локалниот систем. Но тоа би било функционално само за корисници со локални машини – без мрежа. Исто така, чувањето на шаблонот на локалиот хард диск ќе предизвика други безбедносни проблеми. Ако шаблоните се чуваат на сервер - треба да се разгледа и начинот на нивно чување и безбедносните мерки применети за нивна заштита. Сето ова се работи кои администраторот мора да ги земе во предвид пред да се примени биометриски систем за автентикација.

4.6.6 Интероперабилност

Една од работите кои се тешки за решавање е фактот дека не постои никаква интероперабилност помеѓу биометриските системи. Секој производ е приватен. Тешко е да се најде производ кој има системска интероперабилоност. Како резултат на ова, во големите организации мора да се воведе систем кој ќе може да се примени во целата организација.

4.6.7 Трошок наспроти заштеда

Трошокот за примена на овие системи е значаен фактор во недостатокот на широка прифатеност на биометриската идентификација и автентикација. Но, ако се земе во предвид трошокот потребен за одржување на системи со лозинки, можеме значително да заштедиме со системите за биометриска автентикација. Ако се користат Gartner-овите пресметани трошоци од 340$ за корисник годишно за администрирање на лозинки, би требало да заштедите исто толку по корисник кај биометрискиот систем. Ако се работи за компанија со 1000 вработени, се заштедува 340000$ годишно. Повеќето компании создаваат големи трошоци за ИТ, но ги амортизираат во период од 3-5 години. Ако го амортизираме системот 3

години, ќе заштедиме 1020000$. За таа сума на пари - може да се имплементира далеку подобар систем за биометриска автентикација.

И покрај своите корисни особини, биометриските системи имаат скромен успех во имплементацијата. Сеуште има премногу пречки за широка прифатеност на организациско ниво. Но, биометриката зазема голем удел во владини организации, војска и здраствени установи. Системите за биометриска автентикација многу ветуваат, но имаат уште многу за развој. Користени заедно со друго средство на идентификација или метод на автентикација, како што се лозинки, токени, и енкрипција со јавен клуч, биометриските системи можат многу да ја зголемат компјутерската и мрежна безбедност.

4.6.8 Што е Secure Identification Card - SIC?

Без разлика дали станува збор за возачка дозвола или пак картичка за летање со попуст, SIC е личен документ за идентификација, кој верификува дека личноста е она која што се претставува дека е, и дека има авторизација за одреден сервис или активност. Авторизацијата за бараниот сервис, или пак активност, мора да е одредена од апликацијата и да е периодично ре-валидирана за време на нејзиното траење. Ова бара некоја форма на проверка на национална база на податоци, на ниво соодветно со безбедносните потреби на авторизацијата. Овие проверки исто така ќе утврдат дали некоја личност е потенцијална закана.
Верификацијата дека личноста е она која се претставува дека е - бара три работи:

1. Secure Identification Card која не може да биде лесно нападната.
2. Биометриска особина, за да не поврзе со лицето на кое му е издадена картичката.
3. Безбеден автоматизиран интерфејс за верификација дека личноста и податоците на картичката се валидни.

За да се одбегне нарушување на приватноста, базите на податоци кои се користат за време на аплицирањето треба да се оние кои се важни за бараниот сервис. Сите други лични информации, вклучувајќи ги и биометриските идентификатори, треба да се останат тајни и сместени на SIC.

Кога некој ќе побара одреден сервис или привилегија, се поднесува барање кое се разгледува, и евентуално одобрува. Потоа, на корисникот му се издава картичка која содржи повеќекратни биометриски идентификатори, кои можат да се читаат и верификуваат од автоматски читачи на контролните точки. Кога корисникот ќе побара одредена услуга, неговиот идентитет брзо се проверува во базата на податоци без да се емитува било каква информација содржана на картичката. Движејќи се низ контролните точки, корисникот се споредува со една или повеќе биометриски особини кои се наоѓаат на картичката – отисок од прст, скен на зеница, лице, рака или геометрија на прст. Времето потребно за ваква споредба е помалку од 5 секунди. Исто така, треба да се напомене дека различни локации може да бараат различен метод на идентификација. Всушност, особено е поволно да се користи случајна комбинација на биометрика со цел корисникот да не знае кој дел од биометриката се испитува во одреден момент.

LaserCard има најголем мемориски капацитет од сите стандардни формати на картички. Капацитетот на овие картички е 200-500 пати поголем од најблискиот конкурент. Како резултат на способноста на оптичките картички да чуваат повеќекратни биометриски податоци и примероци, сите индустриски биометриски уреди користат оптички картички и најчесто се користат повеќе од еден тип на биометриски податоци. Перманентниот, не-бришлив медиум на кој ласерски се запишува, ги прави оптичките картички природна основа за безбедни картички кои се базираат на биометриката. Најзначаен пример за примена на овој метод на автентикација е US Immigration and Naturalization Service's Permanent Resident Card ("Green Card"), која содржи околу 80000 бајти на биометриски информации. Во потрага побезбедна технологија за сегашната генерација на Permanent Resident Card и Border Crossing Card (Laser Visa), DHS и US Department of State, после опширни испитувања, ја избрале Optical Memory Card од производителот LaserCard Systems Corporation. Оваа технологија на картички е избрана врз база на нејзините добри особини:

- Широк избор на безбедносни опции, кои ја инкорпорираат физичката безбедност, уникатната природа за зачувување на податоци кои обезбедуваат непроменлива енкрипција на податоци, без никаква можност за промена на податоците.
- Силна визуелна автентикација, која во дизајнот на DHS/State овозможува сместување на слики на површината на картичката како и на оптичката лента.
- Голем капацитет на дигитална меморија, која дозволува големи количини на податоци дигитално да се сместат на картичката. Ова е пресудно за сегашните и идните потреби на Граничната безбедност, каде што додатни ID слики (лице, отисок од прст, зеница итн.) треба да се снимаат.
- Ненадминлива издржливост, бидејќи картичките ја докажале својата издржливост во период од 5 години во реални услови.

Биометриските податоци се сместени во INS партицијата на картичката, до која се пристапува само со INS контролирани читачи. Во оваа податочна зона се сместени:

- Високо квалитетна колор слика на сопственикот на картичката (како што е испечатено на површината на картичката),
- Слика од отисокот на сопственикот, земена од базата на податоци на MBP,
- Дигитална слика од потписот на сопственикот на картичката.

Слика 4.20 ни покажува типична структура на INS партицијата на Lasercard картичката која се користи како Green Card во САД. Како што може да се забележи, на горниот дел од картичката со резолуција од 12000 dpi се вметнати слики на сите досегашни претседатели на САД. На долниот дел пак, со иста резолуција од 12000 dpi се вметнати слики од знамињата на сите држави во САД. Со ова уште повеќе се зголемува автентичноста на картичката и се отежнува било каков обид за фалсификување.

Сл. 4.20: Изглед и составни елементи на INS партиција на LaserCard

До денешен ден, издадени се преку 20 милиони на Lasercard (Permanent Resident Cards - Green Cards и Border Crossing Cards - Laser Visas) и тие имаат докажано два многу битни факта:

1. Визите што се издаваат може да бидат во форма на машински-читливи картички,
2. Оптичката картичка на Lasercard служи како одлично биометриско средство за таа намена.

Уреди како што се Field Reader и Biometric Verification System го завршуваат процесот на биометриска автентикација за помалку од 4 секунди (ако процесот го врши пограничен орган). Возможно е и BVS да се имплементира како киоск за "само-услуга" во контролирана надгледувана околина. Потполната биометриска верификација подразбира верификација на автентичноста на картичката, читање од меморија, прикажување на личните податоци на монитор, читање на шаблонот од отисокот од прстот, индикација на резултатот од верификацијата и враќање на картичката назад на овластеното лице. Доколку се користи систем имплементиран во киоск, автентикацијата се завршува за помалку од една секунда. Овој процес подразбира автентикација на ласерската виза, читање на биометрискиот шаблон, валидација на отисокот од прст и враќање на картичката на сопственикот. Читачот на податоци, кој ги отфрла сите невалидни картички, ги чита и верификува податоците од сигурната партиција - INS, или запишува нови податоци (како што се информации за влез/ излез од земјата), но не може да брише податоци.

□

5. ИНФРАСТРУКТУРА СО ЈАВЕН КЛУЧ (PKI)

5.1 КОРИСТЕЊЕ НА PUBLIC KEY INFRASTRUCTURE (PKI)

Public Key Infrastructure (PKI) е прв чекор за да се овозможат сите безбедносни потреби на пораките и трансакциите за кои претходно дискутиравме. Потребата за универзален систем кој ќе ја поддржува електронската комерција, безбедните трансакции, и приватноста на информациите довела до имплементација на системот PKI. PKI е асиметричен систем со два клуча. Пораките се енкриптираат со јавен клуч, а се декриптираат со приватен. Како пример, еве го следново сценарио:

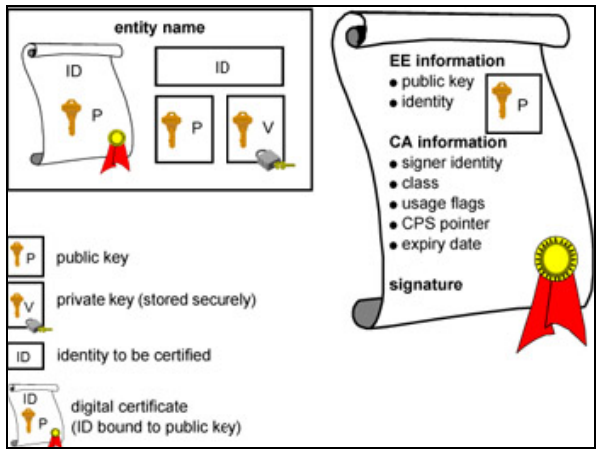
1. Сакате да пратите енкриптирана порка до Јордан, па го барате неговиот јавен клуч.
2. Јордан ви одговара со испраќање на клучот.
3. Го користите пратениот клуч за енкриптирање на пораката.
4. Ја праќате пораката.
5. Јордан го користи својот приватен клуч за да ја декриптира пораката.

Главната цел на PKI е да се дефинира инфраструктура која ќе работи со повеќе производители, системи и мрежи. Важно е да се нагласи дека PKI е рамка, а не специфична технологија. Имплементацијата на PKI зависи од перспективата на софтверските производители кои ја имплементираат. Ова е главниот проблем на PKI: секој добавувач може да ги интерпретира документите за инфраструктурата и да ги имплементира на свој начин. Многу од постоечките PKI имплементации не се компатибилни меѓу себе; сепак, оваа ситуација треба да се смени за некоја година, бидејќи клиентите бараат компатибилност.

Забелешка: Повеќето организации имаат PKI документација која го објаснува електронското потпишување како технологија. Релевантните документи кои спаѓаат во таа категорија често вклучуваат и Confidentiality Certificate Protocol Document и Digital Signature Certificate Policy Document.

Дигиталниот сертификат издаден од властите за сертификати (CA), со користење на инфраструктура со јавен клуч (Public Key Infrastructure – PKI), може да се користи за автентификација на идентитетот на праќачот, и за спонтани контакти со непознати. Дигиталните сертификати обезбедуваат високо ниво на доверба за идентитетот на индивидуата, т.е. ентитетот со кој комуницираме. Дигиталниот сертификат е средство за автентификација на идентитетот. Сертификатот е обично издаден од доверлива/ позната трета страна (CA) која поврзува индивидуа (или ентитет) - со јавен клуч. Дигиталниот сертификат е дигитално потпишан од CA со тајниот клуч на CA. Ова обезбедува независна потврда дека индивидуата или ентитетот се навистина оние кои се претставуваат. CA издава сертификати кои гарантираат за идентитеот на оној на кого му е издаден. CA и неговиот јавен клуч мора да се широко познати, за да нема потреба од автентификација на дигиталниот потпис на CA. Всушност, ние се ослонуваме на дигиталниот потпис на CA - за автентификација на идентитетот на сопственикот на сертификатот и за поврзување на тој идентитет со неговиот јавен клуч.

Сертификатот издаден од CA спојува (лепи) посебен јавен клуч со името на ентитетот кој сертификатот го идентификува (како што е име на вработен или на сервер). Сертификатите помагаат да се спречи користење на лажен јавен клуч за имперсонација. Само јавниот клуч сертифициран од сертификатот ќе работи со одговарачкиот приватен клуч, поседуван од ентитетот идентификуван од сертификатот. Во дополнување на јавниот клуч, сертификатот секогаш го вклучува името на ентитетот што го идентификува, датата на траење, името на CA што го издала сертификатот, сериски број, и други информации. Најважно од сè, сертификатот секогаш вклучува дигитален потпис на CA што го издала.



Сл. 5.1: Стандардна содржина на дигитален сертификат

Фундаменталниот проблем се наоѓа во методот за автентикација со јавен клуч. Ако земеме јавен клуч од нечија веб страна или го добиеме на email, како ќе знаеме дека припаѓа на личноста што мислиме дека и припаѓа? Што го спречува Јанко да ни прати јавен клуч користејќи го името на Игор, па така да помислиме дека е од него? Кога мислиме дека праќаме порака што може да биде прочитана само од Игор, всушност ќе пратиме порака што може да биде прочитана само од Јанко. Никогаш не треба да користиме јавен клуч ако не сме сигурни дека припаѓа на личноста со која се обидуваме да комуницираме. За да се избегне овој проблем, мора навистина да сме сигурни дека јавниот клуч што го користиме припаѓа на примателот на кого му стигнува пораката. Ако го добиеме клучот директно од него, во ред. Ако го добиваме од трета страна, таа трета страна мора да биде една од оние на кои им веруваме.

За широка употреба на јавните клучеви помеѓу странци, како и што е потребно во e-commerce-от, ќе ни треба online пристап до доверливи трети страни кои ќе одржуваат бази на податоци од јавни клучеви во форма наречена сертификат, што ќе биде внесен во базата по внимателно автентикување на неговите застапници. Ваква доверлива страна се Certificate Authority - CA за кои споменавме погоре. За да видиме како работи целата оваа шема, да претпоставиме дека Игор сака да му прати на Цобе, неговиот брокер, нарачка. Тој ја составил пораката: "Купи 100

акции од Тутунска Банка по цена од 2000 денари по акција". Тој го користи неговиот приватен клуч за шифрирање на пораката, така да Цобе биде сигурен дека пораката е навистина од него. Тогаш тој побарува од неговата CA да му го пратат јавниот клуч од сертификатот на Цобе. Ако Цобе ја користи истата CA, неговиот јавен клуч (сертификат) се зема од базата, дигитално се потпишува со приватниот клуч на CA, и се враќа на Игор. Игор знае дека стигнало од CA, бидејќи е дигитално потпишано и може да го дешифрира користејќи го јавниот клуч на CA. Повеќе од тоа, тој им верува на CA дека го автентицирале клучот кога Цобе го испратил до CA, па така тој знае дека навистина припаѓа на Цобе. Игор го користи јавниот клуч на Цобе да ја шифрира пораката со нарачка; дигитално го потпишува неговиот приватен клуч и праќа шифриран текст кон Цобе. Цобе ја дешифрира пораката со неговиот приватен клуч. Цобе го бара од CA јавниот клуч на Игор и го користи да го дешифрира неговиот дигитално потпишан текст, кој знае дека само тој можел да го прати. Ако му испрати потврда за пораката, дигитално потпишана со свој приватен клуч, тој знае, а може и да докаже, дека тој ја добил пораката. Датуми и времиња можат да се внесат во било која од пораките (ако е потребно), или пораката може да помине низ CA која става временски печат - дигитално потпишан од CA, користејќи нивен приватен клуч.

Следните секции ги објаснуваат главните функции и компоненти на PKI инфраструктурата и кажуваат како тие работат во релација со целиот модел.

Внимавајте: Под никакви услови не го давајте или праќајте вашиот приватен клуч. Со тоа ја загрозувате вашата гаранција дека само вие можете да работите со податоците и со тоа ќе ја оштетите вашата сигурност.

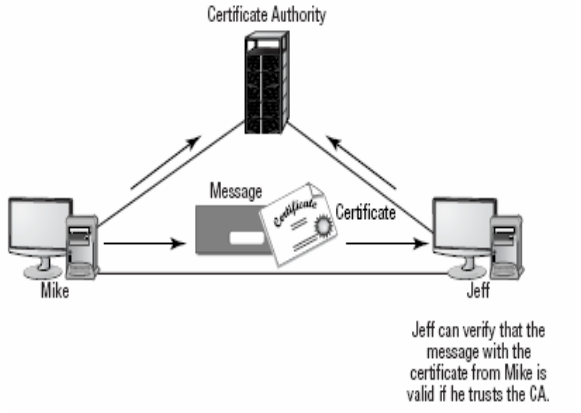
5.1.1 Користење на Certificate Authority

Certificate authority (CA) е организација која е одговорна за издавање, реиздавање и дистрибуција на сертификати. Сертификат не е ништо друго, туку механизам со кој се поврзува јавниот клуч со индивидуата. Содржи голем дел на информации за корисникот. Секој корисник на PKI системот има сертификат кој може да се искористи за потврдување на автентичноста на корисникот.

На пример, ако Mike сака на Jeff да му испрати приватна порака, мора да постои механизам кој на Jeff ќе му потврди дека пораката примена од Mike е навистина од него. Ако трета страна гарантира за Mike, и Jeff и верува на таа трета страна, Jeff може да претпостави дека пораката е автентична поради тоа што третата страна тоа го тврди. Сликата 5.2 го покажува тој процес во комуникација помеѓу Mike и Jeff; стрелките во оваа слика ја покажуваат патеката помеѓу CA и личноста која користи CA - за процес на верификација.

CA може да биде приватен или јавен. Многу оперативни системи можат да бидат конфигурирани како CA системи. Овие CA системи можат да се користат за генерирање на интерни сертификати кои ќе се користат во рамките на самата компанија. Процесот на доделување на сертификати на корисниците, иако ефективен за осигурување на безбедноста - бара сервер. Со тек на време - серверот може да стане претоварен и да има потреба од помош. Додатна компонента,

Registration Authority (RA) постои за да помогне и да превземе дел од работата на CA. RA ќе го дискутираме во следното поглавје.



Сл. 5.2: CA процес

Како што наведовме порано, CA е тело, јавно или тајно, кое се стреми да ја задоволи потребата од трето доверливо тело во е–бизнисот. CA издава дигитални сертификати кои гарантираат за идентитетот на тие на кои им е издаден. За овој процес да биде сигурен, јавниот клуч на CA мора да биде добро познат и достоен на нашата доверба. Кога велиме достоен на нашата доверба, се мисли на репутацијата и доверливоста на CA како ентитет. Дигитален сертификат издаден од "Sam's Digital Certificates and Deli" не би бил многу доверлив на Интернет. CA исто така, мора да ја исполни потребната доза на испитување на идентитетот на индивидуите и ентитетите, пред да издаде дигитален сертификат на некого. Јавниот клуч на CA мора да биде широко познат за да биде ефективен. Дигитален сертификат издаден од CA е безвреден доколку не го знаеме јавниот клуч на CA, или ако немаме независни средства да верификуваме дека доставениот јавен клуч е поврзан со CA. Од таа причина, јавните клучеви на CA мора да бидат лесно достапни и можат да се верификуваат. CA има голем број на ентитети кои издаваат дигитални сертификати. VeriSign, Inc, кој беше формиран од RSA Data Security и неколку други големи корпорации, се главните издавачи. Други компании кои издаваат дегитални сертификати се GTE, AT&T, и Microsoft. Покрај нив постојат и многу други. Процесот на добивање на дигитален сертификат е релативно едноставен за секој легитимна индивидуа или ентитет.

Уште еднаш во примерот со Игор и Предраг, Игор генерира сопствен пар на клучеви од својот X.509 софтвер или уред. Тогаш му го праќа својот јавен клуч на CA со доказ кој и што е. Ако дигиталниот сертификат е за неговата компанија, CA може да побара и копија од прописите на корпорацијата, копии од финасиската состојба, и други докази дека компанијата е навистина она што тврди дека е - и дека е во добра состојба. Ако сертификатот е лично за него, CA може да побара и извод од матично, а може и отисок од прст. Кога поминал процесот на проверка и CA е уверен дека Игор е навистина она за што се претставува, CA му праќа дигитален сетификат за да ја вчита во неговиот софтвер или уред. Овој сертификат е потпишан од CA со нејзиниот таен клуч. Дигиталниот сертификат ќе го потврди

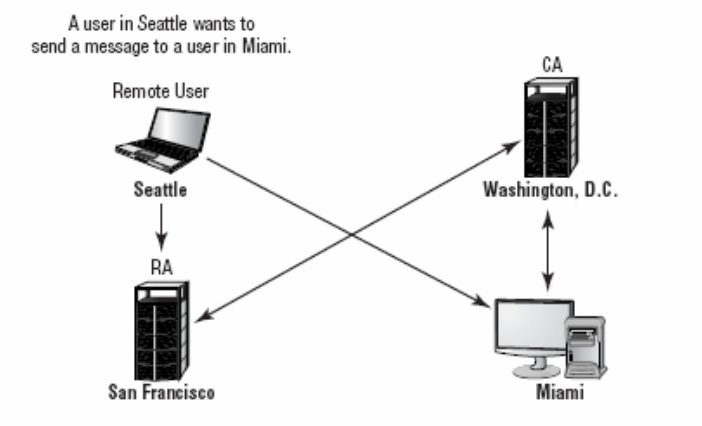
фактот дека CA потврдува дека Игор е навистина она за што се претставува и го поврзува Игор со неговиот јавен клуч. Сега Игор може да го презентира сертификатот на Предраг за да се автентификува себе си и својот јавен клуч. Кога Предраг ќе ја прими потпишаната порака од Игор, ќе му треба јавниот клуч на Игор за да го верификува дигиталниот потпис на Игор и да се осигура дека пораката пристигнала неотворена. Бидејќи веќе го знае јавниот клуч на CA (ќе биде насекаде објавен), може да го декриптира дигиталниот сертификат, да потврди дека дигиталниот сертификат е потпишан од CA, да го верификува интегритетот на сертификатот, и да го добие јавниот клуч на Игор, и тогаш да ја декриптира потпишаната порака.

Потребата од CA е јасна, но обврските и одговорностите на CA не се јасно дефинирани. Треба да се дефинираат уште многу прашања во врска со CA. Многу од нив се од законска, а не од техничка природа: Кои се обврските на CA кога издава дигитални сертификати? Што ако CA направи грешка и издаде сертификат на погрешна индивидуа или ентитет? CA може да сноси огромна одговорност ако таа грешка доведе до измама или финансиска загуба. Бидејќи се движиме кон без–хартиен бизнис и без – хартиено општество, концептот на CA станува сè поважен. Тие ќе имаат огромно влијание на иднината на е–бизнисот. Ова влијание ќе се одрази на секојдневниот живот: тоа значи развој на сосема ново множество на бизнис релации кои ќе бидат неопходни за секојдневна функционалност. Можеби, еден ден, без дигитален сертификат не ќе можеме да купиме ни млеко во продавница.

5.1.2 Работа со Registration Authorities и Local Registration Authorities

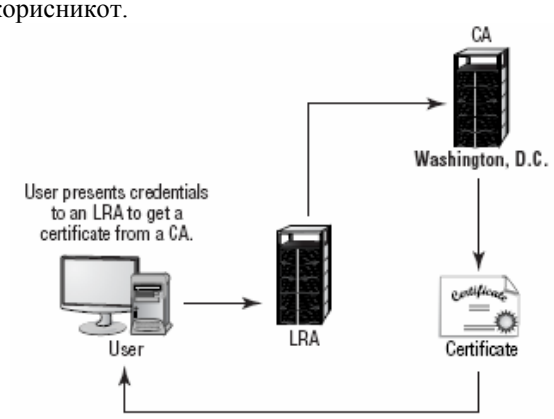
RA превзема дел од работата на CA. RA системот оперира како посредник во процесот: дистрибуира клучеви, прифаќа регистрации за CA и ги валидизира идентитетите. RA не издава сертификати; таа одговорност останува кај CA. Сликата 5.3 покажува RA кој работи во Сан Франциско, додека CA е лоциран во Вашингтон Д.Ц.. Корисникот од Сиетл добива авторизација за сесијата од RA во Сан Франциско. Корисникот од Сиетл може да го искористи RA од Сан Франциско за да ја провери валидноста на сертификатот на корисникот од Мајами. Стрелките помеѓу корисникот од Сиетл и RA серверот претставуваат барање за сертификат од оддалечен корисник. RA има комуникациска врска со CA во Вашингтон. Бидејќи CA во Вашингтон е поблиску, корисникот од Мајами ќе го користи него за верификација на сертификатот. Local registration Authority (LRA) го носи процесот еден чекор подалеку. Може да се користи да го идентификува идентитетот на индивидуа за издавање на сертификат. Ако корисникот во Сиетл има потреба од нов сертификат, би било непрактично да лета назад во Вашингтон Д.Ц. за да земе друг. LRA може да се искористи да го верифицира и потврди идентитетот на индивидуата наместо CA. LRA може да ги препрати автентификациските документи на CA - за да се издаде сертификат.

Совет: Примарната разлика помеѓу RA и LRA е таа што вториот може да биде искористен за идентификација или за поставување на идентитет на индивидуата.



Сл. 5.3: RA превзема дел од работите на CA

Сликата 5.4 го покажува процесот кој се одвива помеѓу LRA и CA. LRA инволвира индивидуа или процес за да го верификува идентитетот на личноста која има потреба од сертификат. Стрелките во сликата 5.4 покажуваат по која патека се оди од корисникот кој бара сертификат (преку LRA) - до CA кој го издава сертификатот. Стрелките го покажуваат патот по кој CA го испраќа новиот сертификат до корисникот.



Сл. 5.4: LRA верификува идентитет наместо CA

Забелешка: LRA инволвира физичка идентификација на личноста која бара сертификат.

Следната секција дава повеќе детали за сертификатите и нивните корисници, вклучувајќи ја валидацијата на корисниците, системите и уредите. Сертификатот исто така има одредени карактеристики кои треба накратко да ги објасниме.

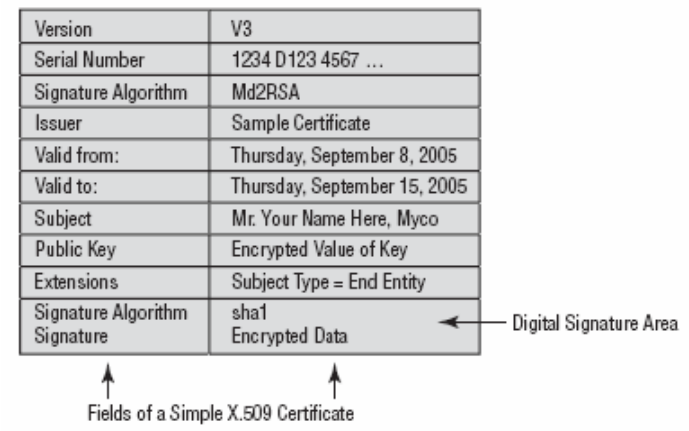
5.1.3 Имплементација на сертификати – X.509 стандард

Сертификатите, како што можеби се сеќавате, овозможуваат примарна метода за идентификација на валидноста на корисникот. Сертификатите исто така

се користат за чување на авторизациски информации. Друг важен фактор е верифицирањето или сертифицирањето на системот дали тој користи коректен софтвер и процеси за комуникација. Што добро ни носи сертификатот, ако системот користи постар систем за криптографија кој има безбедносен проблем? Следните неколку дела ја опишуваат X.509 структурата на сертификати и некои попознати употреби на сертификатите.

X.509

Најпознатиот сертификат кој се користи е X.509 верзија 3. X.509 е стандарден формат на сертификат поддржан од International Telecommunications Union (ITU) и други организации за стандардизација. Усвојувањето на стандард за сертификат е важен чекор за системите, за да може да се осигура интероперабилноста во околина што користи сертификати. Пример за форматот и содржината на сертификат е покажан на слика 5.5.



Сл. 5.5: Сертификат и дел од информациите кои тој ги носи

Забележете дека сертификатот содржи идентификатори од два различни алгоритми користени во процесот. Во овој случај, алгоритмот за потпис е Md2RSA, а дигиталниот потпис е со алгоритам SHA1. Овој сертификат исто така има единствен сериски број даден од CA.

Забелешка: X.509 сертификатот има повеќе полиња од тој на сликата; овој пример е само наменет да ви даде преглед за тоа како изгледа сертификат.

X.509 е широко употребуван формат на сертификат. Сите X.509 сертификати се во согласност со ITU-T X.509 стандардот; затоа (теоретски) X.509 сертификатите креирани за една апликација можат да бидат употребени од било која друга апликација која е во согласност со X.509. Во пракса, различни компании си имаат креирано нивни екстензии на X.509 сертификатот. Сертификатот побарува некој да потврди дека јавниот клуч и името на сопственикот на клучот одат заедно. Со PGP сертификатите, секој може да ја има улогата на валидатор. Со X.509 сертификатите, валидатор е секогаш авторитетот за сертифицирање, или некој кој е назначен од CA.

X.509 сертификатот е колекција на стандардно множество на полиња кои содржат информации за корисникот или уредот и нивниот соодветен јавен клуч. X.509 стандардот дефинира кои информации ќе бидат внесени во сертификатот, и опишува како да бидат енкриптирани. Сите X.509 сертификати ги имаат следниве податоци:

- **X.509 број на верзија** - кажува која верзија на X.509 стандардот се нанесува на сертификатот, што влијае и врз информациите кои можат да се наведат во него. Најчесто е верзија 3.
- **Јавниот клуч на сопственикот на сертификатот** - јавниот клуч на сопственикот на сертификатот, заедно со идентификувачки алгоритам кој опишува на кој крипто-систем припаѓа клучот и соодветните параметри на клучот.
- **Сериски број на сертификатот**- ентитетот (апликација или личност) кој го креирал сертификатот е одговорен за доделување на уникатен сериски број за да го разликува од другите сертификати кои ги издава. Оваа информација е употребена на различни начини, на пример кога сертификатот се поништува, неговиот сериски број се става во *Certificate Revocation List* или *CRL.*
- **Уникатен идентификатор на сопственикот на сертификатот -** (или DN - *distinguished name*). Ова име е предвидено да биде уникатно низ целиот Интернет. DN се состои од неколку подсекции и наликува на ова:

  CN=Bob Allen, OU=Total Network Security Division, O=Network Associates, Inc., C=US
- **Период на валидност на сертификатот -** ја содржи датата на издававање на сертификатот и датата на истекување на важноста, индицира кога сертификатот ќе истече.
- **Уникатно име име на издавачот на сертификатот -** уникатното име на ентитетот кој го потпишал сертификатот. Ова обично е CA. Со употреба на сертификатот се подразбира доверба кон ентитетот кој го потпишува сертификатот.
- **Дигитален потпис на издавачот** - потпис со употреба на приватниот клуч на ентитетот кој го издава сертификатот.
- **Идентификатор на алгоритмот на потписот -** го идентификува алгоритмот употребен од CA за потпишување на сертификатот

Има многу разлики помеѓу X.509 сертификатот и PGP сертификатот, но најистакнати се следниве:

- Можеме да креираме сопствен PGP сертификат; мора да побараме да ни издадат X.509 сертификат од Авторитетот за Сертификати (CA).
- X.509 сертификатите оригинално поддржуваат само единично име за сопственикот на клучот.
- X.509 сертификатите поддржуваат само еден дигитален потпис за атест на валидноста на клучот.

За да добиете X.509 сертификат, мора да побарате од CA да ви издаде еден. Вие го понудувате вашиот јавен клуч, како доказ дека го поседувате соодветниот приватен клуч, и некои специфични информации за вас. Вие тогаш дигитално ги потпишувате информациите и го пракате целиот пакет – побарување за сертификат - до CA. CA тогаш проверува дали информациите што се пратени се коректни, и ако е во ред, го генерира сертификатот и го праќа.
Можеби X.509 ни наликува на стандарден книжен сертификат со јавен клуч втиснат на него. Го има вашето име и некои информации за вас, плус потписот на личноста која ви го издала сертификатот.

Сл. 5.6: X.509 сертификат

Најраспространета примена на X.509 сертификатите имаме во WEB пребарувачите.

5.1.4 Политики на сертификати

Политиките на сертификатите дефинираат за што можат да се користат сертификатите. CA може да издаде повеќе различни типови на сертификати, еден за e-mail, еден за e-commerce, и еден за финансиски трансакции. Политиката може да индицира дека сертификатот не е наменет за потпишување на договори или купување на опрема. Политиките на сертификатите влијаат врз тоа како сертификатите се издаваат и како се користат. CA има политики за интероперабилност, или сертификацијата на други CA сајтови; процесот на интероперабилност се вика cross certification. Организациите кои користат сертификати исто така имаат право да одлучат кои типови на сертификати ќе ги користат и за која цел. Ова е доброволен процес во кој секоја организација што е инволвирана, може да одлучи што и како да дозволи сертификатот. Организацијата - примател може да ја користи таа политика за да одреди дали тој сертификат доаѓа од легитимен извор. Замислете го тоа на следниов начин: PKI сертификат може да биде генериран на многу начини од многу сервери. Политиката индицира кои сертификати ќе бидат прифатени во дадена апликација.

Certificate Practice Statements

CPS е изјава што ја користи CA за да издаде сертификат и да ја имплементира политиката на CA. Ова е детален документ кој се користи да ја стави во сила политиката на CA. CA ја дава оваа информација на корисниците на своите сервиси. Овие изјави кажуваат како се издаваат сертификатите, кои мерки се превземаат за нивна заштита, и правилата кои CA корисниците мораат да ги следат за да ја одржат трајноста на нивните сертификати. Овие политики треба да им се достапни на CA корисниците.
Ако CA не сака да им ги овозможи овие информации на корисниците, CA самата по себе може да биде недоверлива, па и доверливоста на самите корисници се доведува во прашање.

Забелешка: Запаметете дека CPS е детален документ кој се користи за ставање во сила на политиката на CA; политиката на сертификатот не се однесува на CA, туку на самиот сертификат.

5.1.5 Отповикување на сертификатот

Отповикувањето на сертификатот е процес на негово отповикување пред тој да истече. Сертификатот може да треба да се отповика затоа што е украден, работникот оди во нова компанија, или некој го отповикал пристапот. Отповикувањето на сертификатот се прави преку Certificate Revocation List (CRL), или со користење на Online Certificate Status Protocol (OCSP). Складиштето е едноставно база на податоци, или сервер каде што се чуваат сертификатите.

Процесот на отповикување на сертификатот почнува кога CA е нотификувана дека одреден сертификат треба да биде отповикан. Ова мора да се направи штом приватниот клуч стане познат. Сопственикот на сертификатот може да бара отповикување во било кое време, или барањето може да биде направено од страна на администраторот. CA го обележува сертификатот како отповикан. Оваа информација се публикува во CRL и станува достапна преку OCSP протоколот. Процесот на отповикување обично е многу брз; времето се базира на интервалот на публикување на CRL – от. Проследувањето на информацијата за отповикувањето - до корисниците може да трае подолго. Штом сертификатот е отповикан - тој може да се употребува и да биде доверлив повторно.

CA го публикува CRL регуларно, обично секој час или секој ден. CA испраќа или ја публикува листата кон организациите кои избрале да ја примаат; овој процес е автоматски во случај на користење на PKI. Времето помеѓу издавањето на CRL–от и пристигнувањето до корисниците може да биде долго за некои апликации. Оваа временска празнина се нарекува латенција. OCSP го решава проблемот на латенцијата: ако примачот користи OCSP за верификација, одговорот е достапен веднаш. Во моментов овој протокол е под евалуација и може да биде заменет во иднина. Кога клучот е компромитиран, барањето за отповикување треба веднаш да се прати до CA. Може да потрае ден или два за CRL–от да биде поделен на сите што го користат тој CA.

5.2 ИМПЛЕМЕНТИРАЊЕ НА МОДЕЛИ ЗА ДОВЕРБА

За да може PKI да работи, можностите на CA мора да се достапни на сите корисници. Моделот кој е прикажан е едноставен модел на доверба. Но, колку и да е едноставен, овој модел може да не работи, ако PKI имплементацијата расте. Концептуално секој корисник на компјутер во светот би имал сертификат. Но постигнувањето на тоа би било екстремно комплексно и би креирало проблеми. Постојат четири главни типови на модели за доверба кои се користат со PKI:

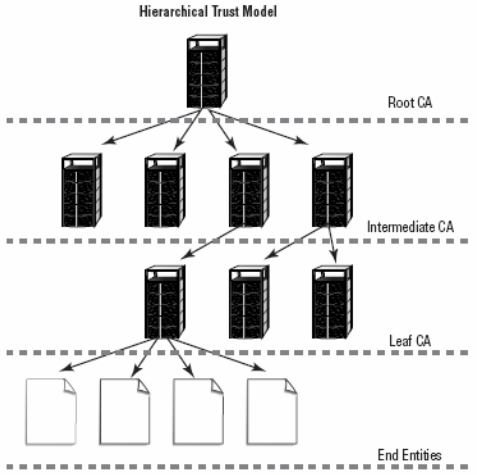
- Хиерархиски модел
- Модел на мост
- Mesh модел
- Хибриден модел

PKI е дизајниран да дозволи креирање на повеќе модели на доверба. Овие модели можат да бидат доста грануларни од перспектива на контрола. Грануларноста се однесува на можноста да се менацираат индивидуални извори во CA мрежата. Во продолжение, ќе ги прегледаме сите овие модели. Детално ќе покажеме како овие модели работат и ќе дискутираме за предностите и маните.

5.2.1 Хиерархиски модел на доверба

Овој модел уште се нарекува и дрво, коренот CA е на врвот и ги овозможува сите информации. Средните CA се следни во хиерархијата и тие само веруваат на информацијата дадена од коренот CA. Коренот CA исто така им верува на средните CA кои се во неговата хиерархија, а на други CA не им верува. Овој договор дозволува повисоко ниво на контрола на сите нивоа на хиерархијата. Ова е можеби најраспространетиот модел во големите организации кои сакаат да воспостават свој процес на сертификати. Хиерархиските модели дозволуваат силна контрола врз активностите.

Сликата 5.7 ја илустрира оваа структура. Во оваа ситуација, средните CA веруваат само на CA кое е директно над нив или под нив. CA кореите можат да имаат доверба меѓу нив, како и помеѓу средните и CA листовите. CA-лист е било кој CA кој се наоѓа на крајот на CA мрежата или ланецот. Оваа структура ви дозволува да бидете креативни и ефикасни кога креирате хибриден систем.



Сл. 5.7: Хиерархиски модел на доверба

5.2.2 Модел на доверба - Мост

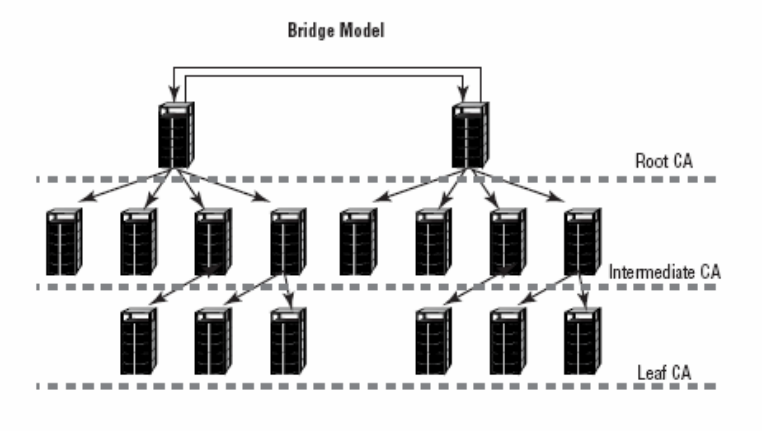
Кај овој модел постојат peer-to-peer релации помеѓу CA корените. CA-корените можат да комуницираат меѓусебе, дозволувајќи крос-сертификација. Овој договор дозволува процесот на сертификација да се постави помеѓу организации или оддели. Секој среден CA верува само на CA кој се наоѓа под или над него, но CA структурата може да се прошири без креирање на додатни CA слоеви.

Додатната флексибилност и интероперабилност помеѓу организациите, се примарна предност на моделот мост. Недостаток на доверба во коренот-CA може да биде голема маана. Ако еден од корените CA не одржува висока интерна безбедност за своите сертификати, може да дојде до безбедносен проблем. Нелегитимен сертификат може да биде достапен за сите корисници во моделот.

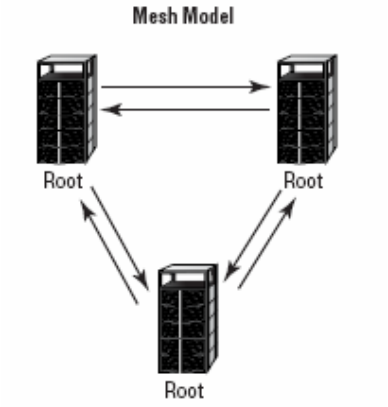
Овој модел може да биде корисен ако имате голема и географски дисперзна организација, или имате две организации кои работат заедно. Голема, географски дисперзна организација може да има CA-корен на секоја оддалечена локација; CA -корените ќе имаат своја интерна хиерархија и корисниците ќе можат да пристапат до сертификатите од било кое место во CA структурата. Сликата 5.8 илустрира структура мост. Во овој пример средните CA комуницираат само со нивниот CA-корен. Секоја крос-сертификација се прави помеѓу двата корени.

5.2.3 Mesh модел на доверба

Овој модел ги проширува концептите на моделот мост со поддршка за повеќе патеки и повеќе CA корени. Секој од корените е прикажан на сликата 5.9 и може да крос-сертифицира со другиот корен-CA. Ова уште се нарекува и web структура. Иако не е покажано на сликата, секој од корените може да комуницира и со средните CA во своите хиерархии.



Сл. 5.8: Мост модел на доверба



Сл. 5.9: Mesh модел на доверба

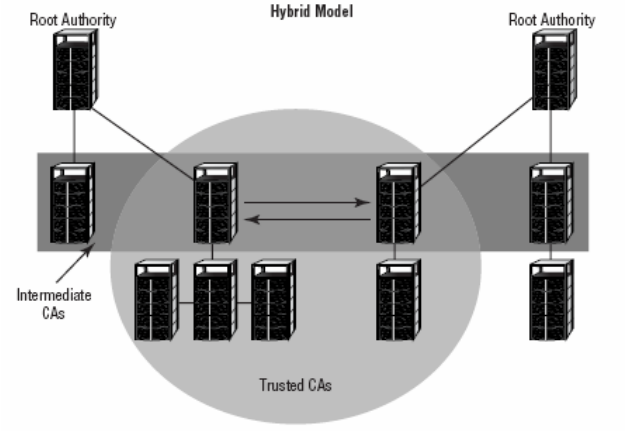
Оваа структура може да биде корисна во ситуација кога повеќе организации мораат да прават крос-сертифицирање. Предноста е дека имате повеќе флексибилност кога ја конфигурирате CA структурата. Главната маана на овој модел е тоа што секој CA корен мора да биде доверлив за да ја оддржи безбедноста.

5.2.4 Хибриден модел на доверба

Хибридната структура може да користи можности од сите структури кои се објаснети погоре. Можете да бидете екстермно флексибилни кога ја градите оваа структура. Флексибилноста на овој модел исто така дозволува креирање на хибридна околина. Сликата 5.10 илустрира таква структура. Забележете дека во оваа структура, средниот CA сервер на десната страна од сликата е единствениот сервер кој е познат од страна на CA што се под него. Подредените на средина одлево CA, се поврзани со два CA на нивните страни. Овие два CA не знаат за други CA, затоа што се поврзани само со CA кој им дава конекција. Овие два

средни сервери и нивните подредени си веруваат меѓу себе; не им веруваат на другите кои не се во линкот.

Главниот проблем на овој модел е што тој може да стане комплициран и збунувачки. Корисникот може ненамерно да добие доверба која не требал да ја добие. Во нашиот пример, корисникот може случајно да биде доделен на CA кој се наоѓа во среднот круг. Како член на тој круг, корисникот може да пристапи до информација што треба да е достапна само на CA коренот. Како додаток, релацијата помеѓу CA може да продолжи и по нивното користење; доколку некој не е свесен за нив, овие релации можат да постојат дури и по терминирањето на врските помеѓу горните организации.

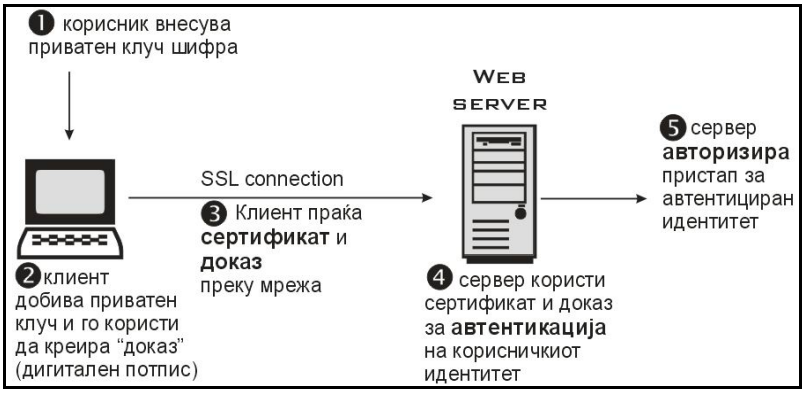


Сл. 5.10: Хибриден модел на доверба

5.3 АВТЕНТИФИКАЦИЈА СО СЕРТИФИКАТИ

Клиентската автентикација базирана на сертификати е дел од SSL (Secure Socket Layer) протоколот. Серверот користи техника на криптографија со јавен клуч за да го потврди потписот и да ја потврди валидноста на сертификатот. Слика 5.10 покажува како клиентската автентикација работи користејќи сертификати и SSL протокол. За да се автентицира - корисникот на сервер (клиентот) дигитално потпишува случајно генерирано парче на податок и ги праќа и сертификатот и потпишаниот податок преку мрежата. За целта на оваа дискусија, дигиталниот потпис поврзан со некои податоци - може да се сфати како доказ доставен од клиентот за серверот. Серверот го автентицира корисничкиот идентитет врз база на овој доказ.

На слика 5.11 се претпоставува дека корисникот веќе решил да му верува на серверот и побарал ресурс, а серверот побарал клиентска автентикација во процесот на проценување - дали да му се дозволи пристап до бараниот ресурс.



Сл. 5.11: Процес на автентификација со дигитален сертификат

Процесите прикажани на слика 5.11 бараат користење на SSL. Слика 5.10 исто така претпоставува дека клиентот има валиден сертификат што може да се користи за идентификација на клиентот кај серверот. Автентикацијата базирана на сертификати општо е поприфатена од автентикацијата базирана на шифра, бидејќи е базирана на тоа што корисникот има (јавниот клуч), но и што корисникот знае (шифрата што го штити приватниот клуч). Важно е да се напомене дека овие две претпоставки се точни, само ако неовластен персонал нема добиено пристап до корисничката машина или шифра, т.е. ставена е шифра за базата на податоци на приватниот клуч на клиентскиот софтвер, а софтверот е поставен да побарува шифра во разумни фреквентни интервали.

- **Важно:** Ниту автентикација базирана на шифри, ниту автентикација базирана на сертификати не адресираат (решаваат) сигурносни проблеми поврзани со физичкиот пристап до индивидуални машини или шифри. Криптографијата со јавен клуч може само да верификува дека е користен приватен клуч за потпис на некои податоци, во кореспонденција со јавниот клуч во сертификатот. Корисникот има одговорност да ја заштити физичката сигурност на машината и да го држи во тајност приватниот клуч.

Ова се чекорите покажани на слика 5.11:

1. Клиентскиот софтвер, како што е Communicator, одржува база на податоци со приватни клучеви што одговараат на јавниот клуч издаден со било кој сертификат за тој клиент. Клиентот ја бара шифрата за оваа база првиот пат кога клиентот и пристапува во текот на дадена сесија, на пример, првиот пат кога корисникот ќе проба да пристапи до SSL-овозможен сервер, кој бара автентикација базирана на сертификат. По внесувањето на шифрата еднаш, корисникот не мора да ја внесува повторно до крајот на сесијата, дури и да пристапува кон други SSL-овозможени сервери.

2. Клиентот ја отклучува базата на приватни клучеви, го повлекува приватниот клуч за корисничкиот сертификат, и го користи приватниот клуч за дигитално потпишување на некој податок што е случајно

генериран за оваа употреба (врз база на влез и од клиентот и од серверот). Овој податок и дигиталниот потпис формираат "доказ" за валидноста на приватниот клуч. Дигиталниот потпис може да биде креиран само со тој приватен клуч и може да биде потврден со одговарачкиот јавен клуч против потпишаниот податок, кој е уникатен за SSL сесијата.

3. Клиентот ги праќа - и корисничкиот сертификат и доказот преку мрежата.

4. Серверот го користи сертификатот и доказот за да го автентицира идентитетот на корисникот.

5. Во оваа точка, серверот може опционо да изведува други автентикациони задачи. Серверот тогаш продолжува да евалуира дали на идентификуваниот корисник му е дозволено да пристапи на бараниот ресурс. Овој евалуационен процес може да вклучи множество од стандарни автентикациски механизми, потенцијално користејќи дополнителна информација од LDAP директориум, база на податоци на компанијата, итн. Ако резултатот од проценувањето е позитивен, серверот дозволува пристап на клиентот до бараниот ресурс.

Како што може да видиме од сликата 5.11, сертификатите го заменуваат автентикацскиот дел од интеракцијата помеѓу клиентот и серверот. Наместо да се бара од корисникот да праќа шифри преку мрежата преку целиот ден, потребно е едно најавување од корисникот за да ја внесе шифрата од базата на податоци со приватни клучеви (без да го праќа преку мрежа). До крајот на сесијата, клиентот го презентира корисничкиот сертификат за да го автентицира корисникот на секој нов сервер на кој ке наиде. Постоечките механизми за автентикација базирани на автентицираниот кориснички идентитет - не се афектирани.

5.4 ОГРАНИЧУВАЊА НА ДИГИТАЛНИТЕ СЕРТИФИКАТИ

Сеуште има голем број на прашања кои мора да се одговорат, како на пример како да се справиме со истечени сертификати; сеуште постои ризикот дека документ со голем век на користење ќе биде потпишан со сертификат со траење од две години. Која е легалноста на документот откако дигиталниот сертификат ќе истече? Друго прашање кое треба да се разгледа е - како да се справиме со отповикувањето на сертификати?

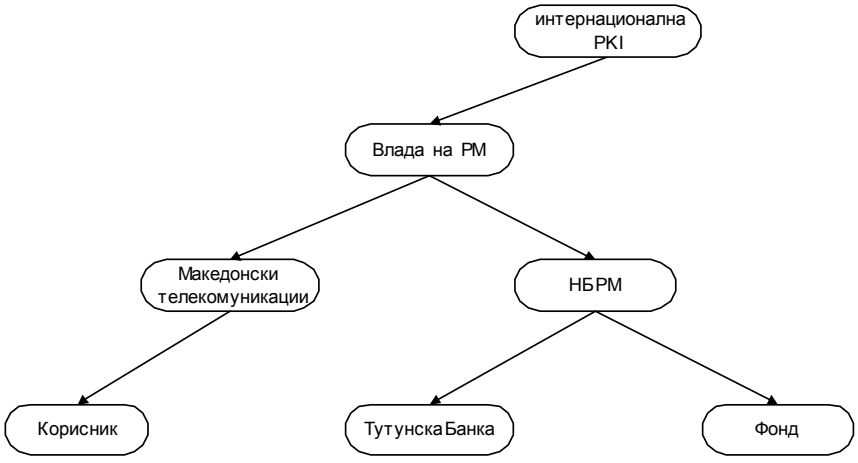
Отповикувањето на сертификатите е опширен процес. Како да отповикаме сертификат кога веќе е издаден? Еднаш издаден, сертификатот е валиден сè додека не истече. Најчесто тоа е најмалку една недела. Не постои процес за моментално отповикување на сертификат, без разлика дали е компромитиран или пак CA ќе сака да го повлече. CA ќе мора периодично да издава листа на ревокација на сертификати (CRL). Сите учесници кои користат PKI ќе треба да да поседуваат ажурна CRL. Но, по некое време CRL ќе стане многу голема. Исто така, постојат и голем број на прашања во врска со одговорностите и обврските на CA околу издавањето на сертификати кои мораат да се дефинираат. Најважно за успехот на

дигитални сертификати е улогата на CA. Со CA, довербата не се заснова на потписот на индивидуа или ентитет. Наместо тоа, довербата е префрлена на CA.

5.5 PUBLIC KEY INFRASTRUCTURE ВО ПРАКСА

Како дел од идната имплементација на дигитални сертификати, постои движење за развој на PKI. Инфраструктурата ќе биде неопходна за автентификацијата со дигитални сертификати и CA. PKI е хиерархиска мрежа на CA. Root certificate авторитетот ги сертифицира подредените CA. Хиерархијата се препознава како доверлива од сите ентитети кои им веруваат на хиерархиските CA. Не треба секој ентитет да му верува на другиот, само на хиерархијата. Некои планови предвидуваат хиерархија на CA, каде што еден CA го сертифицира идентитетот на претходниот. Најгорниот - root CA на РМ треба да биде Владата.

Други предвидуваат похоризонтална шема на cross - сертификација со само неколку нивоа. Во било кој од случаите - процесот за остварување на доверливи релации може да се обезбеди преку сертификат-базиран PKI. Слика 5.12 покажува како би можела да изгледа структурата на PKI, теоретски.



Сл. 5.12: Структура на PKI

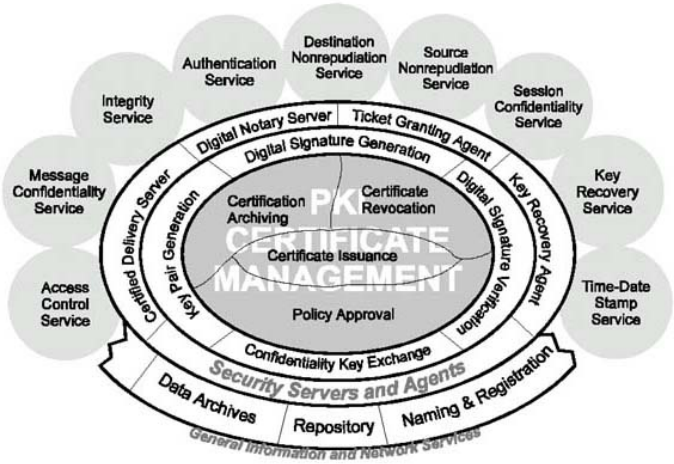
Тешкиот дел би бил развивање на стандарди и инфраструктура за сертифицирање на дигитални потписи и сертификати помеѓу организации кои користат различни шеми. И додека во САД се прават напори за национална PKI, најпредизвикувачка задача е да се направи глобална инфраструктура.

Сценарио од вистинскиот живот - дизајнирање на CA структура во вашата организација
Треба да имплементирате CA структура во вашата организација. Вашата организација има неколку големи национални фабрики и мали оддалечени

делови низ земјата. Некои од тие делови имаат брзи мрежи; другите имаат бавни dial-up мрежи. Вашиот менаџмент вели дека мрежниот сообраќај е многу висок, и не сакаат да ја преоптоварат мрежата со CA сообраќај. Како ќе постапите?
Треба да инсталирате CA систем на секоја голема локација низ земјата. Додатно - треба да инсталирате CA на секоја географска локација каде што се потребни сертификати. Треба да воспоставите процедура која ќе дозволи сертификатите да се издаваат на оддалечените локации, и треба да имплементирате RA процес во поголемите локации. Оддалечените корисници може да ги примаат сертификатите по мејл или со друга метода, ако немаат мрежа.

5.5.1 „PKI - свесни“ апликации

Овој израз се однесува на апликации што имаат одреден CA софтверски додаток, додаден од страна на добавувачот, така што се во можност да ги користат добавувачкиот CA и сертификатите, за да ги имплементираат функциите на PKI. Овој израз не значи дека апликациите поседуваат некакво вградено “знаење“ во нив за тоа што претставуваат сигурносните мерки, или пак кои PKI сервиси се релевантни за нив. На слика 5.13 е прикажан еден централен поглед на сигурносните сервиси на една PKI.



Сл. 5.13: Централен поглед на сигурносни сервиси на PKI

Прикажан е „PKI - центричен“ поглед на сигурносни сервиси базирани на сертификати. Сигурносните сервиси овозможени од PKI се прикажани како кругови околу периферијата на PKI, а серверите што ги подржуваат се прикажани под нив. Во центарот е основната PKI која што се бави со издавање и менаџмент на сертификатите. Првиот прстен ги претставуваат клиентите на PKI кои ги користат сертификатите, а следниот прстен прикажува различни специфични сигурносни сервери и агенти кои што овозможуваат различни сигурносни сервиси.

Некомплетниот надворешен прстен од генерални информации и комуникациски сервиси е прикажан на дното, за да означи некои генерални сервиси кои иако не се поврзани со сигурноста, имаат значење за сигурносните сервиси. Најнадворешниот прстен од „балончиња“ ги репрезентира сервисите кои што може да бидат реализирани преку основната PKI, клиентите, агентите и серверите.

5.5.2 Карактеристики на успешна PKI

Прифаќањето на технологијата на PKI е сеуште во зачеток и претставува новина за многу компании и организации. Од голема важност е да следните карактеристики да бидат земени во предвид при правење на анализа за имплементација на PKI.

- Флексибилност:

Од особена важност е да сите компоненти на PKI бидат интер-операбилни помеѓу себе, бидејќи сигурно тие нема да бидат од еден ист добавувач. На пример, CA можеби ќе треба да работи со постоечките системи, како што се директориумските сервери кои се однапред инсталирани во организацијата. Во PKI треба да се користат отворени, стандардни интерфејси како што се: LDAP и X.500 (DAP) со што се осигурува дека таа е во можност да работи со сите стандардни директориумски сервери. Покрај тоа, многу организации ги преферираат добавувачите на „smart“ картички и хардверски сигурносни модули (HSM). Повторно, со користење на стандардни интерфејси како што е PKCS#11 (Criptoki), PKI има флексибилност да работи со широк спектар од сигурносни токени. Во многу PKI системи, за да се обезбеди потребното ниво на доверба - потребна е лице во лице регистрација. Сепак, ова не секогаш е најсоодветно, така што можеби ќе биде потребна регистрација од далечина. PKI треба да им овозможи на корисниците да ги бараат сертификатите преку e-mail, користејќи стандарден Web пребарувач, или автоматски преку мрежни комуникациски уреди за VPN. За некои поопширни имплементации, сертификатите треба автоматски да се креираат во “бечови“ - на пример кредитните картички или личните карти. Во таков случај, PKI има потреба од флексибилност на автоматски RA процес поврзан со базата на податоци за картичките.

- Лесна за употреба:

Иако принципите врз кои еден PKI систем работи може да бидат комплицирани, нивниот менаџмент не треба да биде. Мора да се овозможи да PKI биде воден од нетехнички персонал, како на пример бизнис администраторите. Тие не треба да се занимаваат со проблемите на криптографските алгоритми, клучеви и потписи. Треба да биде лесно и да се сведе на ниво на кликнување на икони и да се остави остатокот да го прават софтверските апликации. Интерфејсот треба да биде графички и интуитивен, наместо да биде натрупан со комплексни записи од бази на податоци. Флексибилноста и леснотијата за работа сериозно ќе се одразат на повратокот на средствата од инвестирањето во PKI систем, бидејќи тие имаат влијание врз процесите како што се: тренинг, одржување, конфигурирање на системот, интеграција и секако иден растеж на бројот на корисници. Овие работи можат да ја зголемат цената на еден PKI систем и треба да бидат разгледани уште во еволутивната фаза.

- Скалабилност:

Ако во една организација се зголемува употребата и зависноста на PKI, од голема важност е PKI системот да може да го прати тој растеж. На почетокот - PKI може да подржува само една апликација, но треба да биде доволно многустран за да може да подржува и идни апликциаи кои би доаѓале во реално време. Треба да биде возможно да се додаваат дополнителни CA и RA компоненти за поддршка на зголемениот број на сертификати, како што расте PKI. Исто така, може да има потреба од различни типови на сертифиакти и механизми за регистрација, ако делокругот на PKI се прошири за да вклучи нови сервиси.

- Интероперабилност:

PKI технологијата сеуште е во развојна фаза и тешко е да се предвиди со сигурност идната употреба и услови за PKI системите. Стандардите за PKI сеуште еволуираат. Поради тоа, со цел да се заштитат тековните инвестиции и да се избегнат главоболки заради интероперабилноста, од витално значење е да се направи PKI - комплетно отворена и да се вгради во најчестите и најнапредните комерцијални стандарди.

- Сигурност на CA/RA:

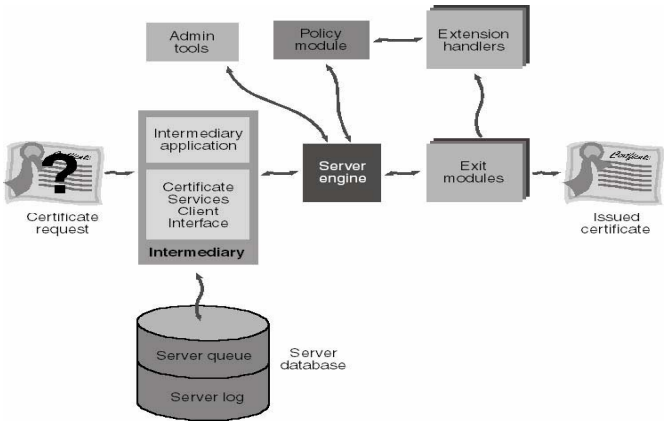
Системите за CA/RA се срцето на секоја PKI. Нивната сигурност е од примарна важност и со нивно загрозување - целото решение за PKI може да се доведе во опасност. Конкретно - PKI треба да го обезбеди следново: приватните клучеви на CA треба да се чуваат во посебни сигурносни модули. Пристапот до CA и RA треба да е строго контролиран, на пример со „smart“ картички со што се овозможува јака автентикација на корисниците. Треба да се конфигурира процесот за менаџмент со сертификатите, така што да биде потребно повеќе од еден оператор за авторизација на барање за сертификат. Сите барања за сертификати треба да бидат дигитално потпишани со строга криптографска автентикација, за да се детектираат и избегнат хакерите кои може да генерираат поинакви сертификати. Сите значајни настани извршени од CA/RA систем треба да бидат снимени на сигурен начин, каде што секој настан е означен и потпишан со време и датум на извршување, со што се оневозможува фалсификување.

5.6 КОРИСТЕЊЕ НА СОФТВЕРСКИ ИЗДАДЕНИ СЕРТИФИКАТИ

Microsoft Certificate Services и овозможува на организацијата издавање, обновување и прекинување на дигитални сертификати, без да се повикуваат на надворешен авторитет за сертификати. Освен тоа, ***Certificate Services*** (*CS*) и овозможува на организацијата целосна контрола над политиките на издавање, управување и прекинување на сертификатите. CS ги евидентира сите трансакции, па им овозможува на администраторите да ги најдат, пратат и управуваат со барањата за издавање на сертификати.

Сервисот Certificate Services може да бара и дистрибуира сертификати со било кој механизам на пренос т.е. може да прифаќа барања од поднесувачи и да праќа сертификати со помош на ***HTTP*** (*HyperText Transfer Protocol*), со помош на **далечинско повикување на процедури** (*Remote Procedure Call, RPC*), или со прилагоден пренос.

Елементите на архитектурата на сервисот Certificate Services вклучуваат **серверска машина** која ги обработува барањата за издавање на сертификати и други модули кои ги вршат работите при комуницирањето со серверската машина. На слика 5.14 е прикажано како компонентите комуницираат со серверската машина.



Сл. 5.14: Серверска машина и други компоненти на сервисот Certificate Services

Серверската машина (*server engine*) е централната компонента на сервисот Certificate Services. Машината делува како посредник за сите барања кои ги прима од влезните модули и го насочува протокот на информации помеѓу компонентите при обработката и издавањето на сертификати. Во секоја фаза на обработката, машината соработува со различни модули и обезбедува преземање на соодветни активности во зависност од статусот на барањето.

Посредникот (*intermediary*) е елемент од архитектурата кој од клиентот ги прифаќа новите барања за издавање на сертификати и ги проследува до серверската машина. Тој се состои од два дела: **посреднички апликации**, кои ги вршат задачите на сметка на клиентот и **клиентски интерфејс** за сервисот Certificate Services, кој ја врши комуникацијата помеѓу посредничките апликации и серверската машина.

Посредничките апликации може да се прават на барање за издавање на сертификати на различни видови на клиенти, преку различни видови на пренос, или во зависност од критериумите на политиките. Микрософтовиот ***IIS*** (*Internet Information Services*) е посредничка апликација која дава поддршка на клиентите преку HTTP. Овие апликации може да ја проверуваат и претходната состојба на поднесеното барање и да ги земаат информациите за конфигурирање на сервисот Certificate Services.

Серверската база на податоци (*server database*) служи за чување на информации за состојбата и датотеките на дневниците за сите издадени сертификати, како и *листи на невалидни сертификати* (*Certificate Revocation List, CRL*). Базата на податоци се состои од два дела: *серверски евиденции и серверски ред*.

Во **серверската евиденција** (*server log*) се чуваат сите сертификати и CRL кои се издадени од тој сервер, така да администраторите можат да ја следат, испитуваат и архивираат активноста на тој сервер. Освен тоа, серверска евиденција користи и серверската машина за да во неа ги чува потенцијалните отфрлања пред нивното објавување во CRL.

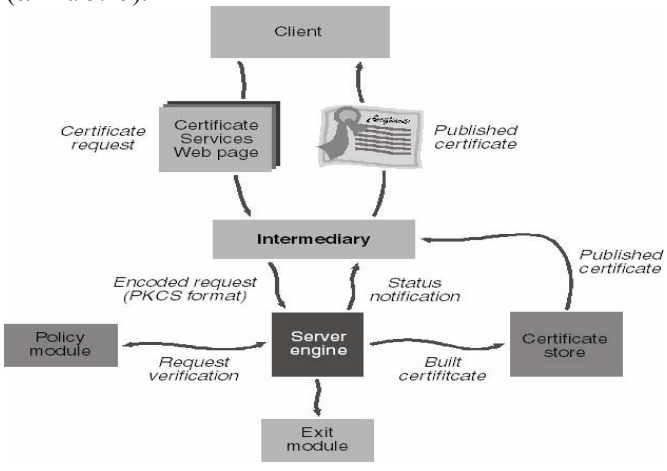
Во **серверскиот ред** (*server queue*) се одржуваат информациите за статусот (примањето, формалната анализа, авторизацијата, потпишувањето, испраќањето) за време на обработката за издавање на сертификати.

Модулот на политики (*policy module*) содржи множество на правила кои важат за издавањето, обновувањето и укинувањето на сертификати. Сите барања кои ги прима серверската машина мораат да поминат низ овој модул заради проверка. Модулот на политика се користи и за анализа на дополнителни информации кои се содржат во барањето, за да се постават својствата на сертификатот според нив.

Обработката на проширувањата (*extension handler*) се прави во соработка со модулот на политики за да им се одреди одредено проширување на сертификатите. Обработката на проширувањето користи шаблони на прилагодени проширувања кои треба да се појават во сертификатот. Модулот на политики по потреба го вчитува соодветниот шаблон.

Излезните модули (***exit modules***) ги објавуваат готовите сертификати и CRL листите со било кој протокол. Се подразбира дека серверот при објавување на секој сертификат или CRL листа, ги известува сите инсталирани излезни модули.

Сервисот Sertificate Services нуди ***COM*** (*Component Object Model*) интерфејс за пишување на прилагодени излезни модули за различни преноси и протоколи, или за прилагодени опции за испорака. Certificate Services содржи сервиси за обработка на барањата за издавање на сертификати и за издавање на дигитални сертификати (слика 5.15).



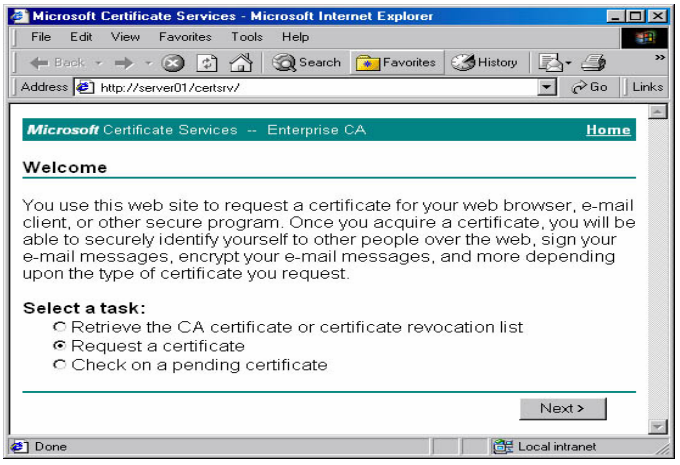
Сл. 5.15: Обработка на барање за издавање на сертификат

Certificate Services, при обработката на барањето за издавање на сертификати, ги поминува следните чекори:

1. Клиентот праќа на посредничката апликација барање за издавање на сертификат. Посредничката апликација го форматира барањето со PKCS#10 и го поднесува на серверската машина.
2. Серверската машина го повикува модулот на политика, кој ги испитува својствата на барањето, одлучува дали барањето ќе се прифати и ги подесува незадолжителните својства на сертификатот.
3. Ако барањето се прифати, серверската машина го презема барањето и го комплетира сертификатот.
4. Серверската машина го чува целиот сертификат во местото за сертификати и ја известува серверската апликација за статусот на барањето. Ако излезниот модул тоа го бара, серверската машина го известува за издавањето на сертификатот. На овој начин, излезниот модул може да изврши дополнителна обработка, пр: објавување на сертификатот во сервисот на директориуми.
5. Посредникот го добива објавениот сертификат од местото за сертификати и го проследува до клиентот.

Постапката на добивање на дигитален сертификат е т.н. **регистрирање на сертификати** (*certificate enrollment*). Постапката почнува со тоа што клиентот поднесува барање за издавање на сертификат, а завршува со инсталирање на издадениот сертификат во клиентската апликација.

Контролата на регистрирање и обрасците на пристап се преку страната Certificate Services Enrollment Page. Таа страна се наоѓа на веб страната Certificate Services која е на адреса http://ime_na_serverot/certsrv/, пр: http://server01/certsrv/. Ова е дадено на слика 5.16.



Сл. 5.16: Образец за контрола на регистрирањето за Сервер01, како CA корпорација

Во постапката на издавање на дигитални сертификати, CA организацијата го проверува идентитетот на корисникот кој бара сертификат и потоа го потпишува со сопствениот приватен клуч. Клиентската апликација како што е Microsotf Internet Explorer, го проверува CA потписот пред прифаќање на сертификатот. Ако CA потписот не е валиден или ако доаѓа од непознат извор, Internet Explorer-от го известува корисникот со прикажување на безбедносни пораки и може дури и да го спречи корисникот да го прифати сертификатот.

CA сертификатот е сертификат со потпис кој содржи јавен клуч, кој се користи за проверка на дигитални потписи. Тој ја идентификува CA организацијата која ги издава сертификатите на автентичност на серверите и клиентите кои ги бараат. Клиентите користат CA сертификат на CA авторитет кој има издадено серверски сертификат - за да го проверат. Серверите користат CA сертификат на CA авторитет кој има издадено клиентски сертификат - за проверка на клиентскиот сертификат.

CA-сертификатот со сопствен потпис (*self-signed CA certificate*) е т.н. основен сертификат, бидејќи тоа е сертификат на основниот CA авторитет. Основниот CA мора да го потпише сопствениот CA сертификат, бидејќи по дефиниција не постојат други авторитети кои би го потпишале неговиот сопствен CA сертификат.

CA-сертификатите не се бараат, ниту издаваат, на ист начин како серверските или клиентските сертификати на автентичност. Серверските и клиентските сертификати на автентичност се единствени за секој клиент и сервер, не се делат и мораат (на барање) да се направат и издадат во CA авторитет. За разлика од нив, CA сертификатот не мора да се издаде на барање, бидејќи се прави еднаш и потоа може да го користат сите сервери и клиенти кои бараат сертификат од CA авторитет. Вообичаен начин на дистрибуција на CA сертификат е тој да се постави на локација која е позната и достапна на секој што бара сертификат од CA авторитет.

Сервисот Certificate Services се инсталира со помошниот програм Add/Remove Programs од Control Panel-от или како опција при инсталирање на Windows 2000 Server-от. Администраторите кои се запознаени со правење на CA авторитет, може да изберат прилагодено подесување со напредните (Advanced) опции, кои се нудат при инсталирање на сервисот.

Со видот на CA се одредува како ќе се користи CA-авторитетот во CA-хиерархијата и дали CA ќе се потпира на сервисот Active Directory. Има четири видови на CA авторитети:

- **Основен CA-авторитет на претпријатие** (*Enterprise Root CA*) – Овој CA авторитет е основа на хиерархијата и мора да го користи сервисот Active Directory.
- **Подреден CA-авторитет на претпријатие** (*Enterprise Subordinate CA*) – Овој CA-авторитет станува подреден на основниот CA-авторитет на претпријатието. Мора да го користи сервисот Active

Directory. Потребен му е и сертификат од основниот CA-авторитет на претпријатието.

- **Самостоен основен CA-авторитет** (*Stand-alone Root CA*) – Овој CA-авторитет станува основа на хиерархијата, но сервисот Active Directory не му е потребен.
- **Самостоен подреден CA-авторитет** (*Stand-alone Subordinate CA*) – Овој CA-авторитет ќе биде подреден на самостојниот основен CA авторитет. Не му е потребен сервисот Active Directory, но потребен му е сертификат од самостојниот основен CA-авторитет.

Главна алатка за администрирање на сервисот Certificate Services е дополнителниот модул Certification Authority (слика 5.17).

Сл. 5.17: Дополнителеи модул Certification Authority за CA претпријатие (Enterprise)

Со дополнителниот модул може да се извршуваат различни административни работи:

- Да се стартува и прекине CA-авторитет.
- Да се подесат безбедносни дозволи и делегира контрола над CA-авторитет.
- Да се прегледа CA-сертификатот.
- Да се направи резервна копија на CA-авторитетот.
- Да се врати претходната состојба на CA-авторитетот од резервната копија.
- Да се обнови основниот или подредениот CA-авторитет.
- Да се управува со прекинувањето на сертификатите.
- Да се управува со барањата за издавање на сертификати.
- Да се управува со шаблоните за сертификати.
- Да се менуваат параметрите на политики, Policy Module или Exit Module.
- Да се мапираат сертификатите на корисничките налози.

Дополнителниот модул Certification Authority може да се користи за администрирање на сервисот за издавање на сертификати на локалниот или друг

компјутер. Овој модул се инсталира при инсталирањето на сервисот Certificate Services, или при инсталирањето на Administration Pack (Adminpak.msi).

□

6. БЕЗБЕДНОСТ НА ОПЕРАТИВЕН СИСТЕМ И АПЛИКАЦИИ

6.1 ИЗВОРОТ НА СИТЕ МРЕЖНИ ПРОБЛЕМИ

Без сомнеж, корпоративната мрежа може да биде една од најкомплексните технолошки средини, што треба да се одржува. Ваша работа, како обучен мрежен инженер или систем администратор, е да се осигурите дека вашата мрежа е оптимално конфигурирана така што сѐ да функционира во најдобар ред. Секој „искусен“ мрежен администратор ќе ви каже, кога ќе добиете извештај за проблем во мрежата, постои само едно што треба веднаш да го направите: ОГК – обвини го корисникот (BTU – Blame The User). Деведесет проценти од сите претпоставени проблеми во мрежата се резултат на корисници кои прават нешто што не смеат да го прават, како на пример инсталирање на несоодветен и несертифициран софтвер и хардвер, чепкање во поставките на регистрите, виткање или влечење на кабелот CAT5 што работи на нивниот NIC, и други фрустрирачки пакости. Ова посебно се случува кога неколку работни станици се погодени од мистериозна мрежна болест. И додека ние би сакале да ги казниме тие корисници, политиката ОГК е одличен начин за одржување на мрежата во исправна состојба, и за одговарање на проблемите на корисниците на благовремен и ефикасен начин.

Во секој случај, се подразбира дека ОГК нема да ви биде многу напомош, освен ако не се придржувате на неколку важни трикови. Прво, *никогаш* не дозволувајте корисникот да дознае за системот ОГК – најверојатно е дека ќе збесне. Второ, запомнете дека скоро сите проблеми поврзани со ОГК се поправаат или барем идентификуваат во првите 10 минути, откако ќе одговорите на повикот за помош. Ако, по првите 10 или 15 минути, ниту вие, ниту корисникот не можете да дојдете дури ни до идеја зошто мрежата се глупира – или ако се заглавени повеќе од неколку машини – можеби е време да се прегрупирате и да барате некоја пореална причина некаде на вашиот сервер, или во мрежата од хабови (јазли), рутери, и кабли.

6.1.1 Слушајте ги вашите корисници

Како ваша прва одбранбена линија против мрежните проблеми, задолжително слушајте ги корисниците. Крајните корисниците, се најверојатно поосетливи на мрежни проблеми отколку, да речеме, системските администратори, програмери, или мрежни инженери, и тие скоро сигурно ќе започнат да викаат на првиот знак за проблем. Ова се случува поради тоа што мрежните администратори и други сродни технички типови, најверојатно најголемиот дел од нивното време го поминуваат директно пред серверската конзола, а не на оддалечена работна станица на другиот крај од зградата, кајшто проблемите тежнеат да бидат многу поизразени. Имајте предвид дека, кога корисниците се жалат за наизглед беззначајни проблеми, сепак вреди да се потрошат неколку минути од вашето време за да се испита проблемот. Наспроти ОГК, секогаш во еден период корисникот забележува нешто што е индикативно за започнување на катастрофа, а вие ќе бидете благодарни ако го уочите проблемот.

6.1.2 Слушајте го вашиот мрежен оперативен систем

Како што е важно да се слушаат барањата, жалбите и распрашувањата на корисниците, подеднакво е важно да се слуша што има да каже и вашиот(е) **М**режен(и) **О**перативен(и) **С**истем(и) (МОС / NOS Network Operating Sistem) за неговите импресии околу перформансите на мрежата. Веројатно си мислите, - како може мојот оперативен систем да ми зборува? Само два збора: серверскиот белешки (серверски log фајлови). Збунувачки, како што често знаат да бидат, серверските белешки, во суштина се ваши пријатели. Во зависност од вашиот оперативен систем, ќе имате сè, од грст сервиси што наизменично соопштуваат за нивниот статус, до административни сервиси за целосно следење, што ја регистрираат секоја грешка, предупредување, или информативни атрибути (flag) поставени од многуте апликации, сервиси, и хардвер што ја сочинуваат вашата мрежа. Клучот во овој случај е не само да се знае каде да се бара, туку и **што** да се бара, и **како** да се одговори на специфичните предупредувања. Ова е доволно комплексна тема, што бара пишување на посебна книга. Тоа што, (да се надеваме) ќе ве спаси, е вашето разбирање на разновидните компоненти од вашата мрежа, како тие меѓусебно соработуваат (се однесуваат), и зависностите помеѓу секој сервис и помеѓу одредени сервиси и специфичен хардвер. И повторно, тоа е искуството стекнато преку читање на книги од областа, и практично надгледување на мрежата преку белешки (logs).

Локацијата и содржината на белешките се разликува во зависност од МОС, и зависи од самиот оперативен систем, како и од конфигурациските приоритети (подесувања) дефинирани од администраторот (најчесто специфицирани при самата инсталација). На сервери што работат на UNIX-базирани оперативни системи, ќе најдете белешки растурени низ целата структура на директориумите, кои што известуваат за сè, од сервиси за електронска пошта и WEB сообраќај, до статус на дискот/партицијата и безбедносни информации. Windows мрежите, од друга страна, нудат една од најразбирливите и лесни-за-употреба алатки за создавање на белешки, која што се добива бесплатно, како дел од самиот оперативен систем. *Windows Event Viewer* врши мониторинг и ги запишува пораките за статусот на сите мрежни сервиси, податоци за безбедноста, и други апликации, обезбедувајќи консолидиран прегледник на белешките (logs).

6.1.3 Застареност внимавај!

Трета главна одбрана што треба да се поседува против мрежните проблеми е закрпата (patch). Благодарејќи на ажурноста на корисниците и администраторите од целиот свет, не поминува долго време пред недостатоците и пропустите на оперативните системи, да се идентификуваат и да се публицираат. Ова вклучува цела гама на додатоци на оперативните системи, од безбедносни карактеристики преку закрпи на фајловите системи, па сè до графички потсистеми гладни за ресурси. Така, за да нивните продукти продолжат да функционираат, многу продавачи, вклучувајќи ги *Microsoft, Novell, Sun Microsystems* и други, често нудат закрпи (надградби) за нивните оперативни системи, за да ги поправат овие приметливи и понекогаш непознати грешки (bugs). Овие закрпи воглавно се достапни на Web страницата на производителот на конкретниот МОС, и воедно се

или бесплатни или ефтини. Исто така морате да бидете во тек со најновите ревизии на овие производи, со следење на разните Usenet групи за дискусија на новитетите, кои се релевантни за конкретниот хардвер и софтвер што го употребувате.

6.1.4 Употребувајте ги дијагностичките алатки на вашиот оперативен систем

Многу честа грешка што ја прават мрежните администратори, е отфрлањето на дијагностичките алатки што се интегрирани во МОС, или како додаток на мрежните оперативни системи. Ова често се случува со администратори што управуваат со Windows, кои се воглавно малку импресионирани од изгледот на PerfMon, бесплатната Windows дијагностичка алатка.

Во суштина, реалноста за *Windows performance monitor* е сосема поинаква. Додека некои пакети од „трети лица“ вклучуваат поатрактивен изглед или некои шарени волшебници за надгледување, *performance monitor* ви дозволува да го следите било кој сервис (услуга/процес), апликација, и дури секој бајт на податоци што поминува низ, или покрај вашата мрежа. Ако потрошите малку време учејќи како *PerfMon* работи, ќе откриете дека тоа е одлична алатка што може да се снајде во можеби 80 проценти (некогаш и повеќе) од потребите за мониторинг на вашата мрежа. На пример, повеќето алатки за мониторинг на Windows се *full-screen* апликации што користат Windows GUI (графички кориснички интерфејс), додека алатките на UNIX се воглавно алатки од командна линија, што вршат запис на стандардниот излез или преку стандардните грешки. Подолу ќе дискутираме за примарните алатки за мониторинг и подесување, и за Windows и за UNIX оперативните системи.

UNIX исто така обезбедува големо множество на алатки дизајнирани за да ви овозможат мониторинг на вашата мрежа. Додека дијагностиката на UNIX можеби не е секогаш атрактивна или ориентирана кон корисникот како што би сакале, ќе имате проблем да најдете надворешни алатки, што можат да конкурираат на количеството информации што ни го обезбедат мониторинг-алатките на UNIX. Ако имате желба, можете да прескокнете директно на делот за UNIX, и да прочитате за некои поспецифични информации, поврзани со мониторингот на UNIX.

6.2 ЗАШТИТА НА OS И NOS

Секоја мрежа е онолку силна колку што е силна нејзината најслаба компонента. Понекогаш, најзабележливите слабости се занемаруваат, и ваша улога како администратор за безбедност е тоа да не се случи. Мора да бидете сигурни дека оперативните системи кои се поставени на работните станици и на мрежните сервери се максимално безбедни.

Заштитата на оперативниот систем (OS) или на мрежниот оперативен систем (NOS) се однесува на процесот на правењето на околината побезбедна од нападите и од натрапниците. Оваа секција ги дискутира заштитата на OS и методите за

сочувување на таа сигурност, иако секојдневно се појавуваат стотици нови закани. Оваа секција исто така ќе ги дискутира и пропустите кај популарните оперативни системи и што може да се направи за да се заштитат тие оперативни системи

Забелешка: Оваа книга не ги тестира спецификите на заштитата на оперативните системи. Но треба да ги знаете и да ги разберете генералните принципи на заштитата. Секој продукт има различен сет на процедури и методи за да тоа се постигне. Прегледајте ги Интернет страниците посветени на вашиот софтвер и хардвер, литературата и документите за инсталација, за да можете потполно да ги разберете овие процедури.

6.2.1 Конфигурирање на мрежните протоколи

Конфигурирањето на мрежните протоколи кај оперативниот систем е голем фактор кај заштитата. Компјутерските системи користат три примарни мрежни протоколи:

- NetBEUI
- TCP/IP
- IPX/SPX

Секој од овие протоколи може да го транспортира мрежниот протокол на Microsoft NetBIOS низ мрежата. NetBIOS системите периодично објавуваат имиња, типови на сервиси и други информации преку мрежата која им е достапна. NetBIOS исто така се користи за програмирање на меѓуврски и за други цели. Веќе неколку години Microsoft предлага протоколот TCP/IP да биде примарен мрежен протокол кој би се користел во мрежите. Компанијата концентрира многу напори за да го направи овој протокол безбеден.

Апликациите како Netscape, Internet Explorer, и Office се подложни на напади на искористување. Бидете сигурни дека вашите апликации се подигнати на највисокото можно ниво со нови закрпи и безбедносни поправки. Во следните секции ќе погледнеме како мрежните протоколи се конфигурираат, како се инсталираат и како работат во компјутерска околина.

6.2.2 Мрежно поврзување

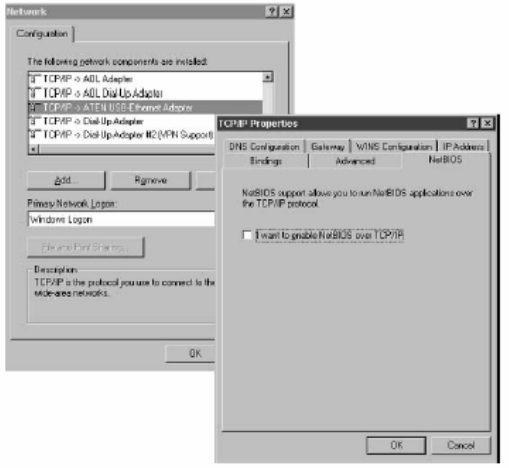
Поврзувањето е процес на врзување на мрежен протокол со друг мрежен протокол или со мрежна каричка (NIC – Network Interface Card). Во мрежата на Microsoft, NetBIOS може да се поврзе со било кој од трите горе спомнати протоколи. На пример, поврзувањето на NetBIOS со TCP/IP ги енкапсулира NetBIOS пораките во TCP/IP пакети. TCP/IP потоа се користи за испраќање на NetBIOS сообраќај низ мрежата. Овој процес на поврзување е токму местото каде ќе ја најдете вашата безбедносна дупка. Проблемот лежи во фактот дека NetBIOS информацијата се енкапсулира во TCP/IP пакет кој е ранлив на пресретнување (sniffing). Сликата 6.1 го илустрира процесот на мрежно поврзување - ако TCP/IP пакетот е пресретнат, критични системски информации, вклучувајки и лозинки, можат да бидат откриени.

Осигурете се дека вашите мрежни протоколи и мрежни адаптери имаат правилни конфигурации. Не го поврзувајте NetBIOS протоколот доколку не е апсолутно потребно. Сликата 6.2 го покажува мрежното поврзување кај типичен Windows 98 систем. Забележете дека NetBIOS протоколот не е поврзан со TCP/IP протоколот и мрежниот контролер. Кога два компјутера, како што се сервер и клиент, пробаат да комуницираат меѓусебе, тие мораат да најдат заеднички јазик. Тоа го прават така што пробуваат различни протоколи базирани според редот на поврзување. Од таа причина, протоколите кои најчесто се користат за сервер/клиент комуникација, треба да бидат на врвот на листата за поврзување.

6.2.3 NetBEUI

NetBEUI е сопствен протокол на Microsoft наменет за Windows мрежите. Доколку вашата цела мрежа е конфигурирана за NetBEUI, таа ќе биде скоро невозможно да се нападне од надвор. Ова е заради тоа што NetBEUI не е рутирачки протокол, па така не можете да се поврзете на надворешна мрежа преку рутер.

Сл. 6.1: NetBIOS поврзување со TCP/IP протокол



Сл. 6.2: Мрежно поврзување во Windows 98 систем

Алатките како што се Network Neighborhood, Explorer и делењето на документи користат NetBIOS за комуникација. Виртуелно сите внатрешни мрежни функции ќе оперираат безпрекорно, ако NetBEUI се користи за интерно вмрежување.

NetBEUI не е дизајниран да овозможи безбедносни опции, и неговите пакети обелоденуваат многу за системската конфигурација, сервисите кои работат и други информации кои можат да бидат искористени за да се идентификуваат слабостите на системот. NetBEUI, сепак не е замислен за големи мрежи и е помалку ефикасен од IPX/SPX или TCP/IP во таква околина.

6.2.4 TCP/IP

TCP/IP е ранлив на сите закани кои се дискутирани во Поглавјето 1 "Идентификување на Потенцијалните Ризици''. Ако вашиот систем е поврзан со Интернет или некоја друга голема мрежа, безбедноста на системот е врзана со ранливоста на TCP/IP мрежниот протокол. Сегашната имплементација на TCP/IP е релативно сигурна. Поранешните верзии на TCP/IP кои се имплементираа од страна на Microsoft, Novell, Apple и други продавачи, имаа голем број на технички проблеми и безбедносни дупки. Безбедноста на мрежата, независно од производителот е добра онолку колку што е добра имплементацијата која производителот ќе ја постигне.

Забелешка: Не брзајте со заклучоците од типот, сите Интернет дупки се слабости во TCP/IP. По толку многу години на развој и имплементација, протоколот е сега релативно сигурен. Многу од новите дупки се во оперативните системи и апликациите што го користат TCP/IP како транспорт.

6.2.5 IPX/SPX

IPS/SPX е многу ефикасен, рутирачки протокол кој оригинално е дизајниран за користење кај Novell NetWare системите. Рутерите кои се користат денеска генрално не рутираат IPX/SPX, доколку не се специјално конфигурирани да го прават тоа. NetBIOS може да се поврзе со IPX/SPX, и нема да биде ранлив кон надворешните напади освен ако овој протокол е рутиран.

6.3 ЗАШТИТА НА MICROSOFT WINDOWS

Работната околина на Windows е, без многу двоумење една од најуспешните оперативни системи превземени од било која компанија. Windows продолжува да биде еден од најпопуларните оперативни системи некогаш направени. Windows 98 беше инсталиран на буквално секој персонален компјутер произведен неколку години наназад, и претставува еден од најпопуларните оперативни системи што било кога се продавани. Windows ME беше мало подобрување на Windows 98, се испорачуваше неколку години пред да биде комплетно замент со Windows XP. Windows 9x продуктите не беа правени за да бидат безбедни, и тие имаат малку сигурносни механизми дизајнирани во нив.

Забелешка: Можете да направите неколку ефектни работи за да ја подобрите безбедноста на овој тип системи. Процесот инволвира мрежна конфигурација, работење со сервиси, делење на документи и чување на апликациите на највисок степен на развој. Како додаток, можете Windows 9x системите да ги направите посигурни со користење на Системските Политики за да спречите трајни

промени во регистерот. Регистер претставува база на податоци на конфигурациски подесувања. Системските Политики се лоцирани на сервер и се превземаат од страна на клиентот со секое поврзување.

6.3.1 Заштита на Microsoft Windows NT 4

Windows NT 4 се користеше како оперативен систем за сервер и работна станица уште од средината на 1990-те. Од страна на многумина се сметаше како еден од најсигурните продукти на Microsoft. Имаше шест големи надградби или сервис пакети кои се аплицираа, и работеше многу сигурно. Windows NT 4 исто така докажано работеше ефективно на EAL3 нивото.

Забелешка: Windows NT 4 го постигна TCSEC C2 сертификатот во 1999-та. Претходно, Windows NT 3.5, и Windows NT 3.51 исто така го постигнаа овој сертификат кој е еквивалентен на EAL3 сертификатот. Тие се единствените оперативни системи понудени од Microsoft кои го потврдуваат тоа тврдење до денес.

Windows NT4 е добра, солидна серверска платформа. Голема разлика се апликациите кои се испорачуваат со него. Windows NT овозможува RAS (Remote Access Services), web services, FTP, и делење на документи. Осигурете се дека сите тие продукти се со најнови надградби или сигурносни ревизии. Последната надградба за Windows NT4 е претставена како Service Pack (SP) 6; и ги решава повеќето познати безбедносни проблеми. Microsoft вели дека SP6a е последната надградба која ќе ја овозможи за Windows NT 4.

Забелешка: Иако нема да има повеќе надградби Microsoft ќе нуди безбедносни закрпи.

Осигурете се дека сите сервиси кои не ви се потребни се изгаснати. За да го направите ова морате да го користите Control Panel. Друга област која загрижува ги инволвира политиките на пристапните профили; осигурете се дека политиките за лозинките се подесени во политиките на пристапните профили и ги рефлектираат компаниските стандарди. Windows NT4 вклучува широки можности за запишување на грешки, запишување на системски промени и други алатки кои го прават работењето полесно. Ги поддржува безбедносните и групите за пристап, како и индивидуалниот пристап кон податоците и дозволите на корисниците.

6.3.2 Заштита на Microsoft Windows 2000

Windows 2000 излезе на пазарот со стартот на новиот милениум. Вклучува верзија за работна станица, како и неколку серверски верзии. Пазарот го прифати овој оперативен систем, и тој нуди релативно добро ниво на безбедност, ако е донесен до последното ниво на надградба. Windows 2000 овозможува Windows Update икона во старт менито, оваа икона овозможува поврзување со Интернет страната на Microsoft и автоматско превземање и инсталирање на надградбите. Голем број на безбедносни надградби се достапни за Windows 2000 – осигурете се дека тие се аплицирани.

Забелешка: Во Windows околината, Сервис менаџерот или аплетот е еден од примарните методи (заедно до полотиките) кои се користат за онеспособување на сервисот.

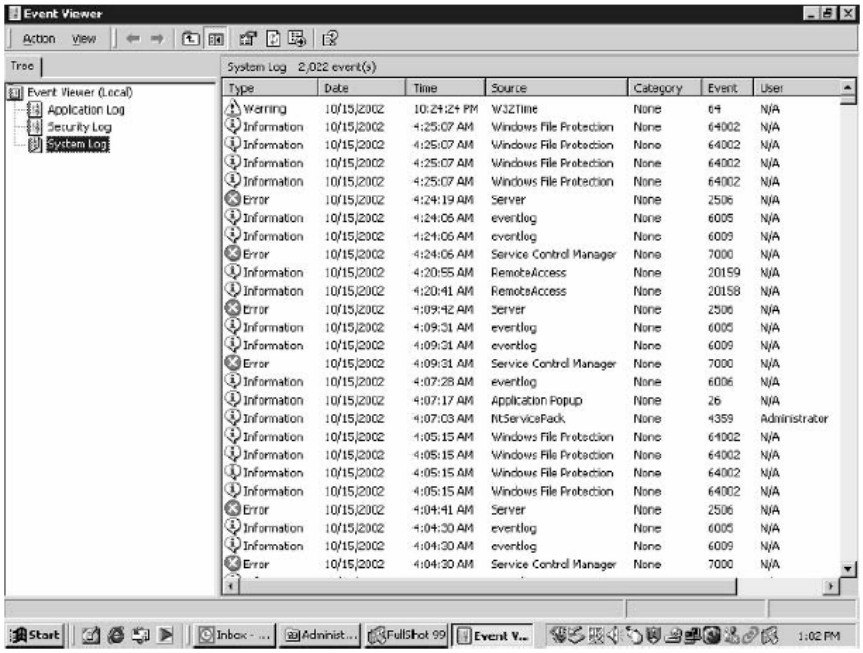
Продуктите за работните станици и серверите работат слично како и Windows NT 4. Овие продукти ги имаат истите безбедносни проблеми кога се користат заедно со продуктите што Microsoft ги дава заедно со оперативните системи. Некои од апликациите кои се подложни на напади ги вклучуваат IIS, FTP и други познати веб технологии. Повторно осигурете се дека продуктите се оневозможени доколку не ви се потребни, и оддржувајте ги со последните надградби. Многу сигурносни надградби се издадени за Windows 2000. Microsoft TechNet и безбедносните Интернет страници овозможуваат алатки, бели страници, и материјали кои помагаат да се осигура Windows 2000 системот.

Забелешка: Можете да ја најдете Microsoft TechNet Интернет страната на http://www.microsoft.com/technet/default.mspx и Microsoft страната за безбедност http://www.microsoft.com/secuity/.

Windows 2000 вклучува широки можности за запишување на системски промени, алатки за репортирање и мониторирање. Овие алатки помагаат работата за мониторирање на безбедноста да биде полесна отколку кај Windows 9x клиентите. Како додаток - Windows 2000 овозможува голема флексибилност во работењето со групи на корисници, безбедносни атрибути, и контрола на пристап во самата околина.

Event Viewer-от е главна алатка за прегледување на записите кај Windows 2000. Сликата 6.3 покажува пример за Event Viewer. Голем број на различни типови на настани можат за се запишат со користење да Event Viewer, и администраторите можат да го конфигурираат нивото на записи. Друга многу битна безбедносна алатка е Performance Monitor-от. Како администратор на Windows 2000 мрежа, вие морате да знаете како да го користите Performance Monitor. Оваа алатка може да биде од животна вредност кога поправате проблеми и решавате различни проблеми, како што ќе видите подолу.

Windows 2000 серверите работат со технологијата наречена Active Directory (AD) која ви дозволува да ги контролирате безбедносните конфигурациски опции за Windows 2000 системите во мрежа. За жал, вистинската сила на AD не се покажува доколку сите системи во мрежата работат на Windows 2000 или повисока. Ние ќе го опишеме Performance Monitor-от на Windows 2000 за да подобро се запознаете со неговите операции. Performance Monitor-от има свои објекти и бројачи кои се многу специфични. Можете да го користите Performance Monitor-от како главен пронаоѓач на грешки, како и за безбедносни пропусти. На пример, можете да видите каде ресурсите се искористени и од каде доаѓа нивната активност.



Сл. 6.3: Запис на Event Viewer во Windows 2000 систем.

6.3.3 Работење со Performance Monitor-от

Во оваа вежба, ќе го користите Performance Monitor-от за да се запознаете подобро со неговата функционалност:

1. Одете на Start > Settings > Control Panel > Administrative Tools, па бирајте Performance.
2. Кликнете на Add Counters копчето, и изберете го објектот кој ги мери перформансите на процесорот.
3. Додадете %Processor временскиот бројач, па потоа затворете.
4. Одберете Start > Search > For Files and Folders и изберете го Search Now копчето, без да специфицирате што да се бара. Потоа брзо префрлете се во Performance Monitor-от и гледајте каков е ударот на ова пребарување врз процесорот. Оваа акција си бара време, па така ќе ви овозможи да ги забележите промените во Performance Monitor-от.
5. Стартувајте ја истата операција уште еднаш, но овој пат сменете ја можноста за преглед во Performance Monitor-от во "histogram" (две копчиња налево од + знакот).
6. Стартувајте ја истата операција уште еднаш, но овој пат сменете ја можноста за преглед во Performance Monitor-от во "report" (копчето прво од лево до + знакот).
7. Излезете од Performance Monitor-от.

Performance Monitor-от ви дозволува да гледате што се случува во системот од гледна точка на ресурси. Оваа вежба покажува три погледи кои можете да ги користите за да го гледате истиот процес. Објектите што ќе ги изберете да ги

гледате, се лимитирани само по сервисите инсталирани на серверот/мрежата. Треба да ја знаете добро оваа алатка за да бидете ефикасен администратор на Windows 2000.

6.3.4 Заштита на Microsoft Windows XP

Windows XP е најновиот клиентски оперативен систем на Microsoft. Според функциите, тој е замена и за Windows 9x фамилијата и за Windows 2000 Professional. Во моментов постојат две верзии на Windows XP, Home и Professional. Windows XP Home едицијата е наменета директно да ги замени Windows 9x клиентите. Windows XP Home може да се инсталира или како надградба врз Windows 9x или како чиста инсталација на нов систем. Windows XP Professional е наменет како надградба за Windows 98 и Windows 2000 Professional во корпоративна околина.

Windows 98 системот не може да ги искорити безбедносните можности на Windows NT или 2000 базираната мрежа. Многу луге користат Windows 98 дома, и сакаат да ги имаат истите можности во канцеларија. Windows XP го овозможува тоа во стандарден формат - и за домашни и корпоративни корисници. Windows XP Professional исто така ги користи предностите на Windows 2000 Серверите кои користат Active Directory.

Забелешка: Microsoft препорачува да имате инсталирано анти-вирус софтвер кој работи во позадина пред да ја почнете надградбата од Windows 9x или 2000 на Windows XP. За време на надградбата, системот ќе треба да се поврзе директно со Microsoft. Оваа конекција може да му донесе безбедносни пропусти на системот.

6.3.5 Заштита на Microsoft Windows Server 2003

Надградбата на Windows 2000 Server линијата на продукти е Windows 2003 Server кој е достапен во четири варијанти:

- Web edition
- Standard edition
- Enterprise edition
- Datacentar edition

Овој продукт ги носи следниве особини во Microsoft server линијата:

- Internet Connection Firewall
- Secure Authentication (локално или од далеку)
- Secure wireless connection
- Software restriction policies
- Secure Web Server (IIS 6)
- Encryption and cryptography enhancements
- Improved security in VPN connection

- PKI and X.509 поддршка на сертификати

Накратко кажано, целта е да се направи продуктот безбеден и флексибилен, а Windows 2003 Server е навистина безбеден, доколку правилно се конфигурира.

6.4 ЗАШТИТА НА ДРУГИТЕ ОС

6.4.1 Заштита на UNIX/LINUX

Работната околина на UNIX и на неговите деривати се едни од најинсталираните серверски продукти во историјата на компјутерската индустрија. Многу различни верзии на Unix се достапни, најпопуларната и бесплатна верзија е наречена Linux. Unix–от е креиран во 1970-та. Дизајнерите на овој продукт го земале пристапот на отворен изворен код, што значи дека комплетниот изворен код на оперативниот систем е достапен за повеќето верзии. Оваа филозофија на отворен изворен код им овозможи на илјадници програмери, компјутерски научници и развивачи на системи - да го подобрат самиот продукт.

Забелешка: Во Јуни 2002-ра, Националната Безбедносна Агенција (NSA) претстави група од подобрувања за да овозможи додатна сигурност за Linux системите. Овие подобрувања беа групирани во сет од алатки наречени Security Enhanced Linux (SELinux). SELinux користи мандаторни контроли на пристап, како дел од механизимите за подобра безбедност.

Linux и Unix кога се добро конфигурирани, овозможуваат високо ниво на безбедност. Главниот предизвик кај Unix е токму да се конфигурира добро. Unix вклучува капацитети кои можат да работат со скоро секој протокол и сервис. Би требало да ги исклучите повеќето сервиси доколку не ви се потребни, тоа се прави со стартување на скрипта за време на стартот на системот. Скриптата ќе ги конфигурира протоколите и ќе ги одреди сите сервиси кои се стартувани.

Целата безбедбност на Unix е поставена на нивото на документите. Документите и директориумите мора да се постават во потребниот редослед, за да се постават точните дозволи за пристап. Структурата на документите е хиерархиска по природа и кога ќе се подесат дозволите за пристап кај датотеките - тие автоматски се пренесуваат на датотеките и документите кои се наоѓаат внатре. Сите овие привилегии се подесуваат од страна на администраторот или од корисникот (ако знае како да ги подеси привилегиите). Оддржувањето на закрпите и надградбите на најново ниво е од есенцијална важност за Unix околината. Ова може да го постигнете со редовно посетување на Интернет страниците на производителите и редовно да ги превземате последните поправки. Linux–от исто така овозможува голем број на записи на активност. Овие записи се од голема важност доколку сакаме да го утврдиме моделот на нападот.

Како додатен метод за безбедност на Linux системите е постигнат со додавање на TCP wrappers, кои се записи на ниско ниво - дизајнирани за Unix системите. Wrappers овозможуваат додатно и подетално запишување на активностите со користење на специфичен протокол. Секој протокол или порта мора да има

wrapper инсталиран за неа. Wrapper-те тогаш ги снимаат активностите и го оневозможуваат пристапот кон сервисот или серверот.

Забелешка: Linux се смета за програма со отворен изворен код. Ова значи дека комплетниот изворен код е достапен за преглед и модификација. Ова бара високо ниво на програмерски вештини. Многу продавачи Sun, IBM и HP ги имплементираа Unix – базираните системи за да ги олеснат процесите. Во повеќето случаи тие самите ги прават модификациите барани од купувачите.

Како администратор на Unix или Linux мрежата, ќе се среќавате со голем број на конфигурациски фајлови и променливи со кои морате да работите за да ги оддржувате сите хостови во комуникација. Во следната вежба ќе видите еден куп на фајлови во Unix/Linux околината, за да утврдите некои главни конфигурациски вредности.

6.4.2 Работење со Unix/Linux мрежите

Во оваа вежба ќе работите од командната линија и ќе ги гледате вредностите на некои клучни променливи:

1. Од командниот промпт, појдете во /etc directory.
2. Погледнете ја содржината на HOSTNAME фајлот со испишување на следното во командниот промпт: cat HOSTNAME. Покажаната вредност го содржи името на хостот и доменот прикажани во една линија (во некои имплементации, името на фајлот е со мали букви наместо со големи).
3. Погледнете ја содржината на хостовите со испишување cat hosts. Ова е ASCII фајл кој се користи за испишување на IP адресите и текстуалните имиња на познатите хостови. Користењето на овој фајл е претходница на DNS-от. Може да се користи наместо DNS кај малите мрежи.
4. Погледнете ја содржината на мрежниот фајл со испишување на cat networks. Овој фајл ги покаува познатите мрежи со кои хостот може да комуницира.
5. Излезете од командната линија.

Овие фајлови ги содржат конфигурациските вредности кои се користат за да се подесат мрежните параметри. Треба да ги познавате овие фајлови како и нивната примена.

6.4.3 Заштита на Novel NetWare

Novel беше една од првите компании кои нè запознаа со концептот на мрежни оперативни системи (NOS) за десктоп компјутери, наречен NetWare. Првите верзии на NetWare овозможуваа поврзување во примитивни, но ефективни мрежи (LAN-ови). Последната верзија на NetWare, верзијата 6.5, вклучува делење на печатачи, подршка за повеќе клиенти, и доста застапена безбедност. NetWare функционира како серверски продукт. Серверот има свој NOS. NetWare софтверот исто така содржи и клиентски апликации за неколку различни типови на системи, вклучувајќи Macintosh и PC. Можете да ги раширите серверските сервиси со

додавање на NetWare Loadable Modules (NLM) на самиот сервер. Овие модули дозволуваат извршниот код да биде пачуван или вметнат во самиот ОС. NetWare верзијата 6.x примарно е ранлива на DoS (Denial of Service) напади, како спротивност на нападите на искористување. NetWare безбедноста е постигната низ комбинации на контрола на пристап, кориснички права и автентификација.

Забелешка: Срцето на Netware безбедноста е во NetWare Directory Service (NDS) или eDirectory (за поновите Novell имплементации). NDS и eDirectory ја содржат информацијата за правата, пристапот и користењето на NetWare базираните мрежи.

Неколкуте додатни можности го прават NetWare - продукт кој вреди да се земе во предвид за користење. Ова ги вклучува e-commerce продуктите, повлекување на документите и подобреното мрежно печатење.

Забелешка: Пред верзијата 5, NetWare беше предефиниран на сопственото решение IPX/SPX-протоколот за вмрежување. Сите понови верзии на NetWare го користат TCP/IP.

6.4.4 Заштита на Apple Macintosh

Macintosh системите изгледа дека се најранливи на физичкиот пристап таргетиран преку конзолата. Мрежната имплементација е сигурна како и кај другите системи за кои дискутиравме во ова поглавје. Macintosh безбедноста се спушта на ниво на контрола на пристап и автентикација на системите. Macintosh користи едноставна 32-битна енкрипција на лозинките која е релативно лесна да се пробие. Фајлот со лозинките се наоѓа во Preference датотеката; доколу овој фајл се дели или е дел од мрежен делив диск - може да биде ранлив на декрипција. Macintosh системите исто така имаат неколку свои мрежни протоколи кои не се наменети за рутирање. Во последно време, Macintosh системите имплементираат TCP/IP вмрежување како интегрален дел на оперативниот систем.

6.5 ЗАШТИТА НА ПОДАТОЧНИТЕ СИСТЕМИ

Неколку податочни системи се инволвирани во оперативните системи за кои дискутиравме, и тие имаат високо ниво на интероперабилност помеѓу себе – од мрежна гледна точка. Низ годините, различни продавачи имплементирале нивни сетови на податочни стандарди. Некои од попознатите податочни системи вклучуваат:

Microsoft FAT
Ова е првиот податочен систем на Microsoft со име File Allocation Table (FAT). FAT е дизајниран за релативно мали дискови. Изграден е прво како FAT-16 и финално на FAT-32. FAT-32 дозволува големи дисковни системи да бидат користени во Windows системите. FAT дозволува само два типа на заштита: делливо ниво и корисничко ниво на привилегии за пристап. Ако корисникот има пристап за пишување или промена на дискот или директориумот, тој ќе има пристап кон било која датотека во тој директориум. Ова е многу несигурно во Интернет околината.

Microsoft NTFS
New Technology File System (NTFS) е воведен во Windows NT за да ги среди безбедносните проблеми. Пред Windows NT да биде претставен, на Microsoft му стана јасно дека е потребен нов податочен систем за да ги поддржува растечките големини на дисковите, безбедносните забелешки и потребата за стабилност. Токму заради овие причини е направен NTFS.

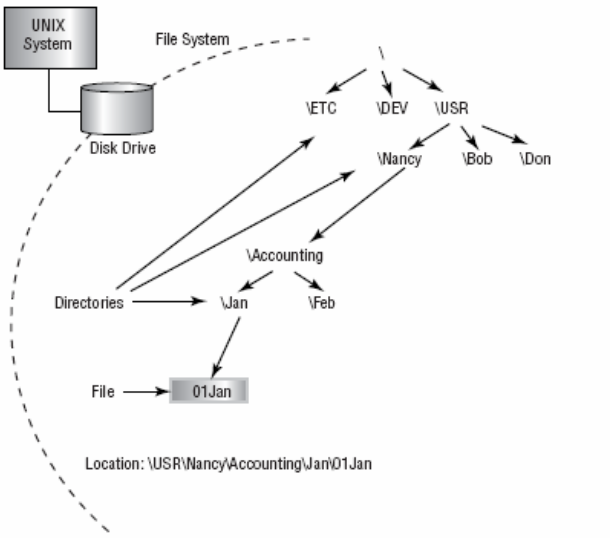
Иако FAT беше релативно стабилен доколку системите го контролираа, - тој податочен систем не беше толку сјаен кога ќе снемаше струја или кога системот ќе се срушеше ненадејно. Едно од подобрувањата кај NTFS е системот за следење на трансакциите, кој овозможува Windows NT да се врати назад за секоја дисковна операција која била во прогрес кога Windows NT паднал или снемало струја. Со NTFS, датотеките и директориумите можат да ја градат безбедноста на свое основно ниво. Безбедноста на NTFS е флексибилна и вградена. Не само што NTFS ја следи безбедноста на листите за контрола на пристап (Access Control List – ACL), кои можат да ги држат дозволите за локалните корисници и групи, туку секој влез во листите за контрола за пристап може да го специфицира типот на пристап кој е даден – како што е право само за читање, право на промена или целосна контрола. Ова дозволува голема флексибилност во поставувањето на мрежата. Како додаток, специјалните програми за датотечна енкрипција се развиени за да ги енкриптираат податоците додека тие се чуваат на дискот. Microsoft силно препорачува сите мрежно делени дискови - да користат NTFS.

Novell NetWare сервиси за чување на податоци
Novell како и Microsoft имплементираше своја податочна структура наречена Novell NetWare File System. Овој систем дозволува комплетна контрола врз секој податочен извор на NetWare сервер. NetWare File System–от беше надграден на NetWare Storage Service (NSS) во верзијата 6. NSS овозможува подобри перформанси и поголеми капацитети за складирање од NetWare File System. NSS како и својот претходник користи NDS или eDirectory за да овозможи автентикација за пристап.

Unix Filesystem
Unix податочниот систем е комплетно хиерархиски податочен систем. Секоја датотека, податочен систем или под директориум има комплетна гранулација на контролата на пристап. Трите примарни атрибути во Unix датотеката или директориумот се Читање, Пишување или Извршување. Можноста индивидуално да се креираат овие опции, исто како и да се постави наследност на поддиректориумите, му дава на Unix највисоко ниво на безбедност (возможно за комерцијален систем). Главната потешкотија со Unix е дека поставувањето на овие контроли на пристап може да биде доста долго кога системот е иницијално конфигуриран. Сликата 6.4 ја покажуваа таа хирархија. Повеќето сегашни оперативни системи ја прифатија оваа метода за своја организација.

Unix Network Filesystem
Network File System (NFS) е Unix протокол кој дозволува системите да подесуваат податочни системи од оддалечените локации. Оваа можност дозволува

клиентскиот систем да го гледа серверот или оддалечената десктоп лоакција како дел од локален клиент. NFS кога функционира, е тешко да се обезбеди. Дискусијата за овој процес е надвор од границите на оваа книга, главната тема лежи во наследните линии на верување кај процесот на автентикација. NFS оригинално беше имплементиран од Sun Microsystems и стана стандарден протокол во Unix околините.



Сл. 6.4: Хиерархиска податочна структура која се користи во Unix OS

Забелешка: Не го мешајте NetWare File Systems со Network File Systems, тоа се две потполно различни технологии.

Apple File Sharing
AFS беше наменет за да овозможи едноставно вмрежување на Apple Macintosh системите. Овој систем користеше свој сопствен мрежен протокол наречен AppleTalk. AppleTalk мрежата не се рутира преку Интернет и се смета за безбедна. AFS дозволува сопственикот да постави лозинка и привилегии за пристап. Овој пристап е сличен со Unix податочниот систем. OS X, најновата верзија на Macintosh оперативниот систем, има целосно имплементиран Unix базиран податочен систем. Генерално Apple Networking се смета за безбедно, онолку колку што се безбедни другите имплементации за кои дискутиравме во овој дел. Главната слабост на оперативниот систем ја инволвира физичката контрола на системите.

Секоја од овие имплементации на податочни системи бара внимателно разгледување кога се имплементира во мрежа. Морате да ги процените нивните индивидуални можности, лимитации, и ранливости кога бирате кои протоколи или системи ќе ги имплементирате. Повеќето снабдувачи на оперативните системи поддржуваат повеќе протоколи и методи. Исклучете ги протоколите што не ви се потребни, поради тоа што секој протокол или податочен систем кој работи на

работна станица или сервер - ја зголемува вашата ранливост и отвореност на напади, губење на податоци, или DoS напади.

Забелешка: Доколку е можно, не ги споделувајте root директориумите на дисковите. Ако го направите тоа - дозволувате пристап кон системските датотеки, лозинките, и другите осетливи информации. Споделете делови од хард дисковите кои не содржат системски датотеки.

Периодично проверувајте ги Интернет страниците за поддршка на производителите или другите извори на поддршка, тие ќе ви овозможат да ги аплицирате моменталните надградби, и сигурносни закрпи во вашиот систем. Со правење на ова регуларно - ќе го намалите вашето изложување на безбедносни ризици.

6.6 НАДГРАДБА НА ВАШИОТ ОПЕРАТИВЕН СИСТЕМ

Производителите на оперативните системи вообичаено овозможуваат надградби на продуктите. На пример, Microsoft овозможува серија на регуларни надградби за Windows 2000 (сопствен систем) и за другите апликации. Сепак, во случај на јавните системи (Linux), надградбите можат да се појават на групите за новости, кај производителот или во корисничките заедници. Во двата случаи, јавни и приватни, надградбите помагаат да се одржат оперативните системи на највисоко можно ниво на ревизија. Истражувањето на надградбите е важно, и ако имате можност добро е да побарате совети од други корисници пред да ја инсталирате надградбата. Во многу случаи, сервисниот пакет или надградбата го остават системот неупотреблив. Направете резервна копија пред да ја инсталирате надградбата.

Забелешка: Windows NT 4 Service Pack 3 го менува податочниот систем и структурата на регистерот на Windows NT. Оваа надградба во почетокот имаше проблеми кои беа причина многу сервери да паднат. Промените, за жал, се толку големи што присилиле голем број на администратори да ги реинсталираат и конфигурираат оперативните системи и апликациите. Осигурете се прво со тестирање на надградбите на тест системи, пред да ги имплементирате во продукциските системи.

Три различни типови на надградби се дискутираат тука: брзи поправки, сервисни пакети, и закрпи.

Брзи поправки

Брзите поправки се користат за поправање на системот за време на нормална работа, иако некои од нив може да бараат рестартирање на системот. Брзата поправка може да премести податоци од лоша точка на дискот и да пре-мапира податоци во нов сектор. Со ова се спречува губење на податоци и губење на сервиси. Овој тип на поправки може исто така да опфати релокација на блок на меморија ако се појави мемориски проблем. Ова дозволува системот да продолжи со нормалните операции сè додека перманентна поправка не се направи. Microsoft

се референра на поправка на баг како брза поправка. Ова инволвира замена на датотеки со преземената верзија.

Севисни пакети
Сервисен пакет е опсежен сет на поправки кои се консолидирани во еден продукт. Сервисниот пакет може да се користи за корекција на голем број на проблеми или да внесе новини и нови можности во оперативниот систем. Кога се инсталира сервисниот пакет, обично со себе носи голем број замени за одредени датотеки. Секогаш проверувајте ги Интернет страниците кои се поврзани со производителите на вашиот софтвер, за да се осигурате дека сервисниот пакет работи како што треба. Понекогаш производителот ќе објави сервисен пакет пред истиот да биде темелно тестиран. Нетестиран сервисен пакет може да доведе до екстремна нестабилност на системот, па дури и до неупотребливост.

Забелешка: Еден голем производител на оперативни системи претстави сервисен пакет за популарен серверски продукт три пати, пред да го претстави сервисниот пакет кој е исправен. Кога ќе се инсталираше, овој сервисен пакет - многу системи стануваа неоперативни. Овој сервисен пакет сруши цела серверска фарма на голем Интернет сервис провајдер. Многу корисници ги изгубија своите сервери за неколку дена, додека сè не се среди и поправи.

Закрпи
Закрпа е привремена или брза поправка на програма. Закрпите се користат за привремено да ги заобиколат сетовите на инструкции кои не функционираат како што треба. Неколку производители на оперативни ситеми или апликациски продукти, издаваат закрпи кои можат рачно да се аплицираат или да се аплицираат со помош на дискета - за да се поправи програмата. Кога работите со корисничка поддршка на технички проблем кај оперативен систем или апликација, корисничкиот сервис можеби ќе треба да навлезе во кодот и да ги направи измените на ниво на бинарните датотеки кои работат во вашиот систем. Двојно проверете ја секоја промена за да спречите катастрофални проблеми поради неправилно внесен код.

Забелешка: Закрпите решаваат проблеми, но тие исто додаваат потенцијални нови проблеми. Повеќето производители попрво би претставиле нова програма отколку да ја закрпат постоечката. Новата верзија може да поправи повеќе проблеми.

Кога има повеќе познати податоци за проблемот, сервисен пакет или брза поправка можат да бидат издадени за да го поправат проблемот на повисоко ниво. Закрпувањето се повеќе се одбегнува, поради тоа што производителите на оперативните системи попрво би пуштиле нова верзија на кодот, отколку да го крпат истиот.

6.7 ЗАШТИТА НА МРЕЖНИТЕ УРЕДИ

Досегашните дискусии зборуваа како да се постават основите на безбедноста и надградбата на оперативните системи. Исто така на кратко се свртевме кон податочните системи. Овој дел зборува за чувањето на вашите

мрежни уреди на надградено ниво. Рутерите, гејтвеите, заштитните ѕидови, и другите уреди кои постојат во мрежата - се исто така подложни на напади. Во следниве секции, ќе погледнеме како да се конфигурираат и доведат до безбедно ниво, вашите мрежни уреди. Фокусот ќе биде на апликациите и рутерите, со покривање и на уредите кои влегуваат во оваа тема.

6.7.1 Надградби на мрежните уреди

Како администратор за безбедност, треба да бидете сигурни дека софверот кој го користат уредите, како што се рутерите и преклопниците - е секогаш со последна можна верзија. Овие уреди обично користат ROM базирани (Read Only) оперативни системи и апликации. Тие исто така можеби имаат дискетни единици или CD драјвови кои се користат за надградба на нивниот софтвер.

Забелешка: Внимавајте секогаш да ги посетувате Интернет страниците на производителите на уредите во вашата мрежа и периодично да ги аплицирате надградбите кои тие ги публикуваат.

Рутерите се вашата прва линија на одбрана од надворешните напади. Нови методи за експлоатација и напад на мрежните уреди, се пронаоѓаат со иста брзина како и новите опции. За среќа повеќето мрежни уреди имаат лимитиран опсег на функции, за разлика од серверите кои се за генерална употреба. Овој тесен опсег им дозволува на производителите да ја подобрат безбедноста на мрежните уреди доволно брзо.

Поголем дел од овие уреди користат сопствени оперативни системи кои ги менаџираат функциите во рутерот. Уредите како што се хабовите и свичевите генерално се однапред конфигурирани и се спремни за работа штом ги извадите од кутија, иако повеќето уреди од висока класа дозволуваат промена на конфигурацијата. Заштитните ѕидови, од друга страна, овозможуваат примарен преглед на мрежниот сообраќај штом податоците ќе поминат низ рутерот. Заштитните ѕидови константно се надградуваат за да овозможат зголемена софистицираност и зголемени можности. Рутерите станаа значително комплексни, исто како и заштитните ѕидови и другите уреди во вашата мрежа. Доколку тие не се чуваат со инсталирани последни надградби, тие можат да станат ранливи на нови напади или експлоатации.

Многу од поновите рутери исто така дозволуваат да се додадат и додатни функции. Некои од овие функции се грижат за безбедноста и за пристапот. Треба да сте сигурни дека ваштата мрежа во секое време е надградена со последните надградби кои ви се достапни. Кај мрежните уреди производителите ги надградуваат функционалностите на нивната опрема, во обид да се справи со нови напади и протоколи во регуларно време, (овие надградби понекогаш се бесплатни). Кога нова опција е претставена, комплетна надградба на фирмверот е потребна. Доколку ваква надградба е потребна, во повеќето случаи ќе ви биде наплатено за истата. Многу производители на рутери овозможуваат сервис за своите уреди, на база дел по дел. Овие производители му дозволуваат на купувачот самиот да ги меша специфичните протоколи, можности, и

функционалности, за да одговараат на околината во која се наоѓаат. Во некои случаи основен рутер може да чини само 1000 долари, но надградбите и додатните пакети кои додаваат екстра функции, може да чинат повеќе илјади. Предноста е што клиентите можат да ја конфигурираат опремата само со тие опции кои им требаат, а можат да надградуваат подоцна, кога ќе имаат потреба.

6.7.2 Кофигурирање на рутери и заштитни зидови

Многу Интернет сервис провајдери (ISP) и други провајдери ќе работат заедно со вас за да ги инсталираат и конфигурираат карактеристиките кои се потребни за вашата мрежа. Овие карактреистики обично можат да бидат имплементирани со користење или на web базиран интерфејс, или интерфејс базиран на терминалски прозорец. Правилната конфигурација на овие уреди е есенцијална за да се осигураме дека вашата мрежа работи глатко и ефикасно. Рутерите, всушност имаат голем број на конфигурациски можности, вклучувајки ја и базичната поддршка за заштитен sид и безбедност. Неколку производители на мрежна опрема, како што е CISCO, нудат сертификација и тренинг програми.

CISCO Certified Internetwork Expert (CCIE) сертификацијата се смета за една од најтешките сертификати во индустријата. Не само што од кандидатите се бара да изработат тестови базирани на multiple-choice одговори слични на Security+ испитот, но тие исто треба да демонстрираат решавање на проблеми во лабараторија.

Неколку производители на мрежна опрема нудат веќе - конфигурирани заштитни sидови на клиентите. Овие заштитни sидови се наречени аплајанси (appliances). Овие аплајанси, како и секој друг компјутерски систем, бараат надградби и одржување. Оваа технологија ветува дека ќе ги направи мрежите полесни за чување. Ќе бидете во можност да купите заштитен зид како аплајанс кој само ќе се вклучи и запали. Ова ќе овозможи системите на заштитните sидови кои се комплексни, да бидат едноставни за инсталација и одржување во помали мрежи. Двата најбитни оперативни аспекти на заштитата на мрежните уреди се осигурувањето дека вашите мрежни уреди работат само на потребните протоколи, сервиси и листи за пристап. Следните две секции ги опишуваат овие можности од перспектива на безбедност.

6.7.3 Оспособување и онеспособување на Сервиси и Протоколи

Многу рутери ја нудат можноста да овозможат DHCP, филтрирање на пакети, конфигурирање на сервисни протоколи, и други сервиси за користење во мрежата. Осигурете се дека вашиот рутер е конфигуриран да ги дозволи само протоколите и сервисите кои ви се потребни за вашата мрежа. Оставањето на додатни мрежни сервиси активирани, може да предизвика потешкотии и да креира ранливости во вашата мрежа. Конфигурирајте ги вашите мрежни уреди, колку што е можно порестриктивно. Овој додатен слој на безбедност не ве чини ништо, а од друга страна му отежнува на натрапникот да влезе во вашиот систем.

6.7.4 Работење со листи за дозволување на пристап

Листите за контрола на пристап овозможуваат да се игнорираатбарањата од специфицирани корисници или системи, или да им се дозволат одредени мрежни привилегии. Можете да откриете дека некоја IP адреса константо ја скенира вашата мрежа, па така можете да ја блокирате таа IP адреса, и таа нема да има пристап кон вашата мрежа. Доколку ја блокирате на самиот рутер, IP адресата автоматски ќе биде одбивана секогаш кога ќе проба да пристапи кон вашата мрежа. Листите за контрола на пристап дозволуваат - посилни сетови на контрола на пристап да се постават во вашата мрежа. Базичниот процес на листите за контрола на пристап му дозволува на администраторот да ја дизајнира и адаптира мрежата, така да таа може да се бори со специфични безбедносни закани.

6.8 ЗАШТИТА НА АПЛИКАЦИИТЕ

Како што објаснивме, добар почеток за обезбедување на мрежата е да се биде сигурен дека секој систем во мрежата е со последната возможна надградба и да провериме дека само протоколите кои ни се потребни се оспособени. За жал, овие чекори не се доволни. Вашите сервери и работни станици исто така работат со сервиси и апликации. Серверите (посебно web, серверите за електронска пошта и медиумските сервери) се посебно подложни на искористување и напад. Тие апликации мора исто така да се заштитат за да се направат тешки за искористување колку што е можно повеќе. Овој дел ги објаснува заштитата на апликациите, на работната станица и на серверот - за да се постигне максимална безбедност.

6.8.1 Заштита на web серверите

Web серверите се една од омилените области за напаѓачите. Internet Information Server (IIS), широко распространет web сервер, константно успева да се најде во вестите. IIS-от како повеќето web сервери овозможува конекција за web пребарувачите. Web серверите оригинално беа едноставни и примарно се користеа за да овозможат HTML текст и графички содржини. Модерните web сервери овозможуваат пристап кон базите на податоци, мултимедијални содржини, и буквално секаков друг тип на сервиси кои можат да бидат замислени. Ова откритие им дава можност на web страниците - да им овозможат на сурферите богати и комплексни можности.

Сите сервиси и можности поддржани на web страниците, се потенцијална цел за експлоатација. Осигурете се дека ги одржувате последните софтверски стандарди. Исто така, морате да бидете сигурни дека на корисниците им обезбедувате минимални привилегии кои се доволни за тие да ги исполнат своите задачи. Ако корисниците пристапуваат до вашиот сервер преку anonymous корисничкиот профил, тогаш здравиот разум ви налага anonymous корисничкиот профил да има дозвола само да ја гледа web страната и ништо повеќе. Две битни области на интерес кај web серверите се филтрите и контролирањето на пристапот кон

извршните скрипти. Филтрите дозволуваат да го лимитирате сообраќајот. Лимитирањето на сообраќајот на ниво само на тоа што е потребно да го нудите - ќе ви помогне да се чувате од напади.

Забелешка: Добар сет на филтри може исто така да се аплицира на вашата мрежа, за да ги стопира корисниците при пристапување на страници кои не се бизнис поврзани. Не само што ова ќе ја зголеми продуктивноста, туку во исто време ќе ја намали можноста за превземање на вируси од сомнителни Интернет страници.

Извршните скрипти, (како оние што се пишувани во CGI), често се стартуваат на повисоки нивоа. Во повеќето услови, тоа не е проблем, бидејќи корисниците се враќаат на нивното вообичаено ниво на привилегии, кога ќе се заврши извршувањето. Проблемите се појавуваат кога корисникот ќе излезе од скриптата, додека е на повисокото ниво. Од администраторска гледна точка - најдобра акција која треба да се превземе, е да се потврди дека сите скрипти на вашиот сервер се темелно тестирани, ослободени од проблеми и потврдени за употреба.

Забелешка: IUSR_computer_name профилот е креиран кога сервисите се инсталирани на IIS и се користат да го претставуваат anonymous корисникот. Правата доделени на овој профил се доделуваат на сите anonymous web корисници.

6.8.2 Заштита на серверите за електронска пошта

Серверите за електронска пошта претставуваат комункациска кичма кај многу бизниси. Овие сервери типично работат како додатни сервиси на веќе постоечки сервер или дедициран систем. Ставањето на активен вирус-скенер на серверот за електронска пошта може да го намали бројот на вируси во вашата мрежа; исто така може да спречи ширење на вируси од страна на вашиот сервер за електронска пошта. Скенерот ги филтрира сомнителните пораки кои пристигаат и ги информира корисниците на електронската пошта за потенцијалниот проблем во системот. Оваа карактеристика ќе стане стандард во повеќето сервери за електронска пошта во блиска иднина. Многу е ефективна во спречувањето на ширење на вирусите преку електронска пошта. Неколку сервери користат складови на податоци, или сторици, за да овозможат колаборација, закажување на состаноци, конфереции, и други функции. Функционалноста и можностите на овие сервери се зголемува регуларно. Држете ги на најново можно ниво.

Сценарио од вистинскиот живот - користење на листи за контрола на пристап за борба против спам-от
Сведок сте на повторувачки обиди - некој да се конектира на вашиот сервер за електронска пошта, преку TCP/IP адреса. Овие пропаднати обиди се појавуваат во вашите системски записи. Континуирано се бара пристап преку портата 25. Серверите за електронска пошта се поплавуваат од страна на автоматизирани системи, кои се обидуваат да ги користат за праќање на електронски ѓубре пораки,

наречени спам. Повеќето нови e-mail сервери имаат имплементирани мерки за спречување на ова. Но сепак, заканите стануваат се пософистицирани. Вие можеби ќе успеете да ги намалите овие обиди за пристап кон вашиот систем, ако ги внесете TCP/IP адресите во листите за контрола на пристап кај вашиот рутер и ги забраните тие адреси. Со тоа вашиот рутер ќе ги игнорира барањата за конекција од тие IP адреси, ефективно подобрувајки ја вашата сигурност.

6.8.3 Заштита на серверите за трансфер на податоци (FTP)

File Transfer Protocol (FTP) серверите не се наменети за високо - безбедни апликации поради нивната наследена слабост. Повеќето FTP сервери дозволуваат креирање на податочни околини на било кој дел од системот. Треба да креирате посебен дел или под-директориум во системот и таму да дозволите трансфер на податоци. Доколку е возможно, користете виртуелни приватни мрежи (VPN) или Secure Shell (SSH) конекции за FTP активности. FTP не е познат по сигурност, и многу FTP системи испраќаат некриптирани лозинки и кориснички имиња низ мрежата. FTP е една од алатките која често се користи за експлоатирање на системите.

Гледано од страна на оперативната безбедност, би требало да користите посебни профили за пријавување и посебни лозинки за FTP пристап. Со ова ќе спречите системските профили да бидат прикажани на неавторизирани индивидуи. Исто така, осигурете се дека сите податоци на FTP серверот се скенирани за вируси. На крај, **секогаш** оневозможете го anonymous профилот. За да го направат користењето на FTP полесно, повеќето сервери доделуваат пристап на анонимните кориснички профили. Но од сигурносна гледна точка, ова е последна работа што би требало да ја дозволите (анонимните корисници да ги копираат и користат податоците од вашите сервери). Со оневозможување на anonymous профилот, вие барате корисникот да ви биде познат - автентициран корисник, кој има право да пристапи кон FTP серверот.

Забелешка: Како што напоменавме - web пристапот, со различни верзии на IIS, IUSR_computer_name профилот се креира кога сервисите се инсталираат и се користи да го претставува анонимниот корисник. Правата доделени на овој профил се доделуваат на сите anonymous web корисници.

6.8.4 Заштита на DNS серверите

Domain Name Service (DNS) серверите ги преведуваат имињата на хостовите во IP адреси. Овој сервис овозможува името на Интернет страницата како што е www.sybex.com - да се преведе во IP адреса како што е 192.168.1.110.

Забелешка: Регистрирана компанија раководи со вашето име на доменот. Повеќето регистратори бараат годишна претплата. Доколку таа претплата не се плаќа, друга компанија може да ви го превземе името на доменот. Ваквото превземање е срамно за многу компании.

DNS серверите можат да се користат внатрешно за приватни функции, но исто така можат да се користат надворешно за јавни барања. DNS – поврзаните напади не се чести, но генерално доаѓаат во три типа:

DNS DoS напад
DoS нападите примарно ги напаѓаат DNS серверите. Намерата е да се наруши работата на серверот, и со тоа системот е бескорисен. За да внимавате на тие напади, осигурете се дека вашиот DNS сервер и оперативен систем се надградени на највисоко можно ниво. Со тоа ги минимизирате можностите за DoS напади

Network Footprinting
Footprinting претставува собирање на податоци за вашата мрежа, за да се најде некоја слаба точка која може да се искористи. Кога користите footprint, вие барате ранливости и секакви можности за влез. Голем дел од информациите за вашата мрежа се чуваат во DNS серверите. Со користење на обична DNS наредба, како што е NSLOOKUP, напаѓачот може да открие многу за вашата мрежна конфигурација. DNS податоците типично имаат информација која се однесува на доменските имиња, електронската пошта, web-от, комерцијата и другите сервери на вашата мрежа. Чувајте што е можно помалку информации во вашите надворешни DNS сервери.

Compromising Record Integrity
DNS пребарувањата на системите обично ги инволвираат или примарните, или примарните и секундарните DNS сервери. Ако направите промена во примарниот или секундарниот сервер, промената се пропагира кон другите DNS сервери на кои им се верува. Ако проблематичен или лажен запис се внесе во DNS, записот ќе покажува на локацијата на напаѓачот, наместо таму када што треба. Замислете го срамот за корпорацијата кога посетителите на нејзиниот Интернет сајт се редиректираат на сајтот на конкурентот, или уште полошо, кон порно сајт. Бидете сигурни дека сите DNS сервери бараат автентикација пред да се направат или пропагираат надградбите. Со ова ќе се осигурате дека неавторизираните записи - не се вметнуваат во вашите сервери.

Забелешка: Нападот на DNS кешот беше проблем кој постоеше во почетните имплементации на DNS. Веќе подолго време тоа не е проблем, но сепак треба да знаете дека постои. Со отворањето на DNS кешот, демонските DNS пакети понекогаш ќе содржат други информации (податоци кои можат да помогнат за други типови на напади).

6.8.5 Заштита на NNTP серверите

Network News Transfer Protocol (NNTP) серверите овозможуваат испорака на пораки со вести од мрежата. NNTP серверите исто така се користат заа интерна комуникација во компанијата. Овие сервери треба да бараат автентикација пред прифаќање на запис, или при дозвола за правење на конекција.

Забелешка: NNTP серверите во многу јавни поставки станаа преполни со пораки кои содржат небитни информации. Модераторите, како и автоматските

алатки наречени роботи, се користат за преглед на овие небитни пораки и нивна елиминација. Групите кои немаат ваков тип на приод - станаа практично неупотребливи.

NNTP серверите можат да се преполнат со спам или DoS напади. Многу user групи почнале како мали групи на корисници, кои имале ист интерес. Типично групите имаат модератор за да бидат сигурни дека нема пропагирање на спам пораки. Сепак, некои групи пораснале, па вклучуваат десетици илјади членови од целиот свет, и количеството на транспорт (пораки) на овие сервери, одамна го надминало количетвото на пораки кои модераторите можат да ги проверуваат.

Забелешка: Внимавајте кога се зачленувате во групите со вашата вистинска адреса за електронска пошта. Многу спамери ја користат таа информација за да испраќаат непотребни пораки, па така одеднаш можете да станете жртва на голем број спам пораки.

Неколку програми за скенирање се достапни за да помогнат да се намали количетвото на непотребни пораки. Секако, колку и да се добри контрамерките, секогаш се наоѓа некој да ја неутрализира нивната ефективност.

6.8.6 Заштита на податочните и принт серверите

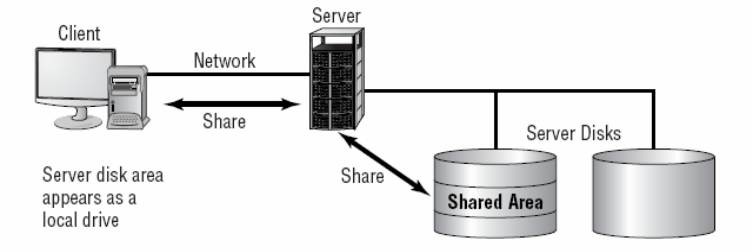
Податочните и принт серверите примарно стравуваат од DoS напади и напади со неавторизиран пристап. DoS нападите можат да имаат цел во специфичните протоколи, или да оптоварат некоја порта со нивната активност. Овие сервери треба да ги стартуваат само протоколите кои се потребни за поддршка на мрежата. Во мрежата која има само PC базирани системи, NetBIOS сервисите се оневозможени на серверите, или ако заштитен sид е поставен помеѓу серверот и Интернет. Многу од популарните напади кои се појавуваат кај системите денес - се прават преку NetBIOS сервисите, преку портите 135, 137, 138 и 139. Кај UNIX системите затворете ја портата 111, односно Remote Procedure Call (RPC).

Забелешка: RPC е програмерски интерфејс кој дозволува оддалечен компјутер да стартува програми на локална машина. Тоа прави сериозни пропусти во системите каде е дозволен RPC.

Делењето на директориумите треба да биде лимитирано само на есенцијално ниво, (само најбитните функции да работат). Сите основни директориуми треба да бидат скриени за пребарување. Подобро е да дедицирате под-директориум и тој да го делите. Сликата 6.5 покажува делива мрежна конекција. Забележете дека кога корисникот се поврзува на мрежно делив директориум, тој воопшто не е свесен каде се наоѓа овој директориум во хиерархијата на системот.

Забелешка: Секогаш имајте најрестриктивни пристапни правила за деливите директориуми.

Забелешка: Никогаш не делете го (share) основниот директориум (root) на системот. Со ова креирате ранливост кај секоја датотека во системот. Намето ова, делете поддиректориуми.



Сл. 6.5: Деливост на директориумите

Ако напаѓачот влезе во основниот директориум, сите поддиректориуми кои се во тој директориум се ранливи. Ако се влезе во поддиректориумот - само тоа што е во него е ранливо.

6.8.7 Заштита на DHCP серверите

Dynamic Host Configuration Protocol (DHCP) се користи во многу мрежи за да го автоматизира делењето на IP адресите на работните станици. DHCP сервисите можат да се нудат од страна на многу различни типови на уреди, вклучувајќи рутери, свичеви и сервери. DHCP процесот инволвира издавање на TCP/IP адреса на работната станица на одредено време. DHCP исто така овозможува други мрежни конфигурациски опции на една работна станица. Во дадена мрежа или сегмент, само еден DHCP сервер може да работи. Ако работат повеќе, тие ќе се судрат меѓусебе во процесот на давање на адреси. Ова ќе доведе до дуплирање на адресите и води кон конфликти. Клиентите кај кои е овозможен DHCP - можат да бидат опслужени од страна на Network Address Translation (NAT) серверите. (Во Глава 2, "Мрежна безбедност", постои дискусија за NAT серверите). Користењето на DHCP треба да е лимитирано само на работните станици.

Сценарио од вистинскиот живот - од каде се сите овие IP адреси?

Некои од вашите корисници одеднаш ви се јавуваат да пријават дека по рестартувањето на нивните системи, тие не можат да пристапат кон сервисите на мрежа или на Интернет. Откога ја истраживте ситуацијата, откривате дека IP адресите кои тие ги користат се погрешни за вашата мрежа. IP адресите се валидни, но не се дел од вашата мрежа. Го прегледавте вашиот DHCP сервер и не можете да најдете причина за ова. Што треба да истражите следно?

Најверојатно, некој конфигурирал друг сервер или уред во вашата мрежа како активен DHCP сервер. Овој сервер сега издава адреси на тие корисници наместо вашиот сервер, или нивните системи не можат да го видат DHCP серверот, па добиваат Automatic Private IP Addressing (APIPA) адреси.

Ова се случува кога администраторите или програмерите тестираат пилот системи. Сите тест системи треба да се изолирани од вашата продукциска мрежа, или со рутер или со некој друг механизам. Овие сервери се наречени rogue сервери и можат да направат голема забуна во DHCP околината.

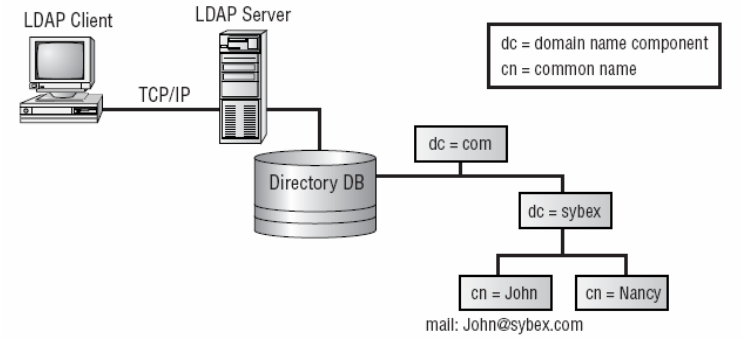
6.9 РАБОТА СО ПОДАТОЧНИ СКЛАДОВИ

Многу од компјутерите кои се користат во мрежите денес, најмногу се употребуваат за чување на податоци. Овие податоци обично се чуваат на сервери кои овозможуваат директориумски сервиси и сервиси за бази на податоци. Овие системи се наречени податочни складови. Оваа секција ги опишува некои од најкористените податочни складови. Повеќето податочни складови се овозможени со некоја форма на база на податоци.

6.9.1 Датотечни сервиси

Датотечните сервиси се алатки кои овозможуваат организирање и одржување на комплексни мрежи. Датотечните сервиси дозволуваат податоците, апликациите и другите информации брзо и лесно да бидат реалоцирани во самата мрежа. Ова во голема мерка ја олеснува администраторската работа, и дозволува програмерите и луѓето кои работат на развој на апликациите - подобро да ја искористат мрежата и нејзините ресурси. Повеќето сегашни методи ги третираат податоците и другите мрежни ресурси како објекти. Овој објектно-ориентиран пристап дозволува информацијата да биде зачувана и да биде пристапувана преку одредени карактеристики или атрибути.

Како додаток, покрај креирањето и чувањето податоци, датотечните сервиси исто така мораат да публикуваат коректни податоци за корисниците. Можеби најдобриот начин за визуелизација на оваа функција е да ја замислиме како жолти и бели страници на одреден телефонски именик. Бизнисот сака своите имиња да ги прикаже во азбучен ред. Исто така потребно е имињата да се прикажат по категории во директориумот. Ако сте компјутерски консултант, можеби ќе сакавте вашето име и телефонски број да биде прикажано под компјутерски консултанти, компјутерски тренери, и други области. Ова е тоа што го овозможуваат податотчните сервиси. Повеќето податочни сервиси имаат имплементирано хиерархиски модел, сличен на оној од сликата 6.6. Оваа хиерархија дозволува објектот единствено да биде идентификуван од корисниците на директориумот.



Сл. 6.6: Структура на директориумот која покажува единствена идетификација на корисникот

Безбедноста за овие сервиси е критична, типично се постигнува ско користење автентификација и контрола на пристап. Не би сакале вашиот влез кон директориумот да се гледа од секаде, зарем не? Следната секција на кратко опишува некои од директориумските сервиси кои се користат во мрежите денеска. LDAP, Active Directory и eDirectory се почесто стануваат цел на напади.

6.9.2 LDAP

Light-weight Directory Access Protocols (LDAP) е стандарден протокол за пристап кон директориуми, кој дозволува да им бидат упатувани прашања на директориумите (посебно кај парираните, X.500 базирани директориуми). Ако директориумскиот сервис поддржува LDAP, можете да го прашувате со LDAP клиент, но во суштина LDAP протоколот е тој што се користи многу во онлајн белите и жолти страници. LDAP е главниот протокол за пристап, користен од страна на Active Directory (следно за дискусија). Предефинирано работи на портата 389. Синтаксата на LDAP користи запирки помеѓу имињата.

6.9.3 Active Directory

Microsoft го имплементираше директориумскиот сервис наречен Active Directory (AD) во Windows 2000. За продуктите на Microsoft, AD е кичмата за сите безбедносни, пристапни и мрежни имплементации. AD им дава на администраторите комплетна контрола на ресурсите. Тоа е сопствено решение што овозможува сервиси за други директориумски сервиси како LDAP. Еден или повеќе сервери ги оддржуваат AD функциите; овие сервери се поврзани во дрво-структура која дозволува информацијата да биде делена или контролирана низ целата AD-структура. Во конјункција со AD, LDAP користи четири различни типови на имиња:

Distinguished Name
(DN) дедицирано име - постои за секој објект во AD. Овие вредности не можат да се дуплираат и мора да се единствени. Ова е комплетната патека до објектот, вклучувајки ги сите контејнери.

Relative Distinguished Name
(RDN) релативно дедицирано име - не мора да има единствена вредност, сè додека нема дупликати во Организациската единица (OU). Како на пример, RDN е дел од името кое е единствено во рамките на својот контејнер.

User Principal Name
(UPN) уште се нарекува и пријателско име. Се состои од профилот на корисникот и доменот на корисникот и се користи за идентификација на корисникот (замислете адреса за електронска пошта).

Canonical Name
(CN) е во суштина DN дадено во конотација одозгора – надолу.

X.500
International Telecommunications Union (ITU) е интернационална група за стандардизација за директориумските сервиси; во доцните 1980-ти, го имплементираше X.500 стандардот, кој беше база за подоцнежните модели како LDAP. Главниот проблем во индустријата при имплементација на X.500 беше комплексноста на самата имплементација. Novell беше еден од првите производители кој го имплементираше X.500 во неговиот NetWare NDS продукт.

eDirectory
Е кичма на новите Novell мрежи. Ги чува сите информации за системските ресурси, корисници, и другите битни информации за системите врзани со NetWare серверот. Тоа е надградба и замена за NDS, и е широко прифатен во заедницата.

6.9.4 Бази на податоци

Главната причина за инсталација на самите компјутери е нивната можност за чување, пристап и промена на податоците. Примарната алатка за контрола на податоците е базата на податоци. Базите на податоци станаа пософистицирани и нивните можности драматично нараснаа во изминативе 10 години. Овој развој креираше многу можности за преглед на податоците на нови начини. Исто така креираше проблеми за дизајнерите и за корисниците на овие продукти. Овој дел на кратко дискутира за технологиите развиени за базите на податоци и некои од заедничките теми поврзани со ранливоста на базите на податоци.

Технологии на базите на податоци

Релационите бази на податоци станаа најкористениот пристап кон имплементацијата на базите на податоци. Оваа технологија дозволува податоците да се прегледуваат на динамичен начин, базиран на потребите на корисникот или на администраторот. Најчестиот јазик за комуникација со базите на податоци е наречен Structured Query Language (SQL). SQL-от дозволува прашањата да се конфигурираат во реално време, и да се праќаат на серверите со бази на податоци. Оваа флексибилност претставува голема ранливост кога не е имплементирана безбедно.

Забелешка: Не го мешајте терминот SQL со базата на податоци на Microsoft SQL Server. SQL сервер го имплементира SQL јазикот, како и повеќето други бази на податоци.

На пример, ќе сакате да ги имате сите телефонски броеви на сите ваши клиенти кои живеат во одредена географска област и купиле продукти од вас во изминатите две години. Во рачен систем, прво треба да одредите кои клиенти живеат во таа област. Рачно ќе барате во досиеата на клиентите, па потоа ќе ги идентификувате клиентите кои купиле нешто. Овој процес е доста заморен и бара многу време. При користење на релациона база на податоци, можете да пратите прашалник до базата на податоци да ги најде сите досиеа кои ги задоволуваат вашите услови и да се испечати листата. Командата за да се направи ова може да

биде една линија код, или може да бара илјадници инструкции. Очигледно, се доаѓа до зголемена продуктивност и оправдување на инвестицијата.

Корпоративните или организациските податоци се едни од највредните работи кои ги има организацијата. Обично се чуваат или на десктоп системи или на централизирани сервери за бази на податоци. Овие информации ги прават серверите примамливи цели за индустриска шпионажа и оштетување. Серверите за бази на податоци патат од истите ранливости за кои зборувавме досега. Додатно, базите на податоци сами по себе се комплексни сетови на програми кои работат во спрега, за да овозможат пристап до податоците. Првите системи на бази на податоци се поврзуваа со крајните корисници директно преку апликациите. Овие програми беа со намера да овозможат лесен пристап до податоците и да дозволат трансакциите да се изведуваат врз базите на податоци. Во приватна мрежа, физичката сигурност беше единственото нешто на кое се обрнуваше внимание.

Како што растеше Интернет, бизнисите им дозволуваа на клиентите пристап до податоците, како на пример до каталозите, статусот на нарачките, нарачки преку Интернет, и буквално секоја можност што клиентот ќе ја побараше. Ова ја зголеми интероперабилноста, додаде повеќе кодирање, повеќе софтвер и ја зголеми комплексноста на темите врзани со базите на податоци. Производителите на софтвер работат напорно за да ги исполнат барањата на клиентите. За жал, брзото издавање на софтвер е отскочна даска за безбедносните проблеми. Зголемувањето на потребите за системи ориентирани кон базите на податоци (и безбедносните проблеми кои се откриваат од страна на развивачите на софтвер и производителите) се најголемата ранливост кај серверите за бази на податоци.

Забелешка: Базите на податоци бараат крпење, како и секоја друга апликација. Тие можат и требаат да користат контроли на пристап и да овозможат сопствени нивоа на безбедност.

За да ги подобрат перформансите на системот, како и да се подобри безбедноста на базите на податоци, компаниите имплементираа модел на столбови. Три различни модели се опишани овде:

Модел на еден столб: Во овој модел, базата на податоци и апликацијата постојат во еден систем. Ова е заедничко за десктоп системите кои работат на единечна база на податоци. Раните Unix имплементации исто така работеа по овој терк. Секој корисник ќе се најавеше на терминал и стартуваше дедицирана апликација која им пристапуваше на податоците.

Модел на два столба: Во овој модел клиентскиот компјутер или систем стартува апликација која комуницира со базата на податоци, која работи на различен сервер. Ова е честа имплементација, и работи добро за многу апликации.

Модел на три столба: Овој модел ефективно го изолира крајниот корисник од базата на податоци со поставување на сервер во средината. Овој сервер ги прима барањата од клиентите, ги евалуира, и потоа ги испраќа до серверот на кој е базата на податоци за процесирање. Серверот со базата на податоци ги испраќа податоците назад кон средниот сервер, кој потоа ги испраќа до клиентскиот

систем. Овој пристап станува сè по распространет во денешно време. Средниот сервер исто така може да го контролира пристапот до базата на податоци и да овозможи додатна безбедност.

Трите модели овозможуваат зголемување на можностите и комплексноста. Секој систем кој е инволвиран, мора да биде индивидуално оддржуван и регуларно надградуван за да овозможи безбедност.

6.9.5 Бекап на податоците

Кога зборуваме за базите на податоци - неизоставно мора да се нагласи бекапот на податоци - како мерка за заштита на базата. Секоја организација што има database сервер - мора да има јасно дефинирани процедури за бекап на базата. Постојат различни медиуми за бекап - но најчесто се користат магнетни ленти, оптички дискови и други уреди со голем капацитет. Битно е да се нагласи да бекап-лентите треба да се чуваат во друга просторија (не каде што е податочниот сервер), а по можност и во друга зграда. Ова се прави како мерка за превенција - ако се оштети серверот заради некоја хаварија - да можат да се спасат податоците. Трите најосновни вообичаени методи се следниве:

1. *Целосна бекап метода.* Оваа бекап метода прави целосен бекап на секој фајл на серверот секој пат кога тој работи. Таа метода првенствено се применува тогаш кога тоа го дозволуваат времето и просторот на траката, и се користи за системската архива или за сетирани траки.
2. *Растечка бекап метода.* Оваа бекап метода ги копира само оние фајлови што неодамна се додадени или изменети (истиот ден) и го игнорира секој друг бекап сет. Обично се постигнува така што се ресетира архивскиот бит на фајловите откако за нив е направен бекап. Оваа метода се применува ако времето и просторот на траката се во крајно поволна состојба. Меѓутоа, оваа метода има некои слабости својствени за неа за кои ќе зборуваме подоцна.
3. *Диференцијална бекап метода.* Оваа бекап метода ги копира само оние фајлови што се изменети откако последен пат бил направен целосен бекап. Овој вид на бекап е зголемувачки бидејќи времето и просторот на траката што се потребни за бекапот за секоја ноќ се зголемува во текот на неделата бидејќи ги копира изменетите фајлови од тој ден и од претходниот ден се до последниот целосен бекап. Во ова сценарио архивскиот бит на секој фајл не се ресетира се до следниот целосен бекап.

Според времето на креирање - бекапот може да биде дневен (ги опфаќа сите дневни промени/ трансакции на базата), неделен, месечен и годишен бекап. Битно е да се обучат операторите за ефикасно спроведување на методите за restore, т.е. враќање на базата во конзистентна состојба, после одредена загуба на податоци.

6.10 ПРИВИЛЕГИИ (PERMISSIONS)

Повеќето компјутерски и мрежни оперативни системи го применуваат концептот на "привилегии" за контрола на пристапот. Привилегиите специфицираат

кои операции можат различни корисници да ги применуваат врз одредени фајлови и директориуми. На секој корисник му е доделено ниво на пристап за секој директориум и фајл. Секој корисник и фајл се доделени на група. Групите можат да бидат специфицирани во ACL. Наместо да има посебни правила за секоја индивидуа или група, правило за одредена група во ACL може да специфицира привилегии за сите индивидуи во таа група. За повеќето системи, постојат барем три или 4 нивоа на привилегии:

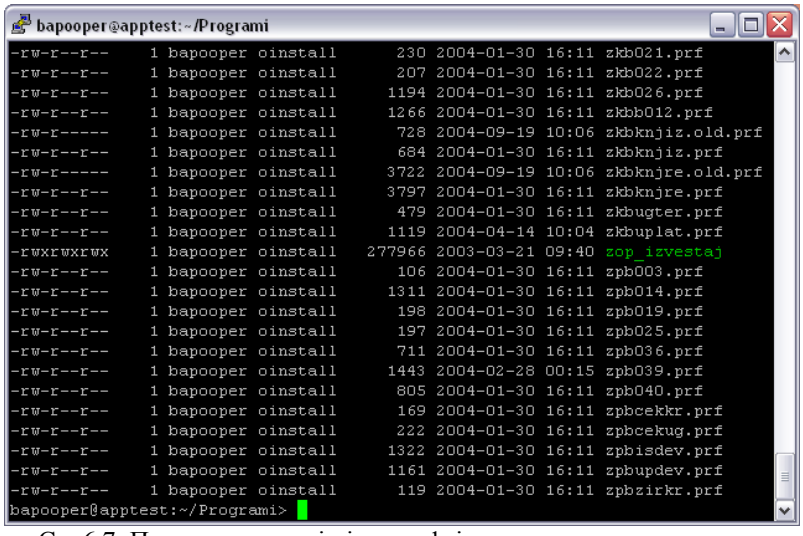
- *Read:* корисник со ова нови на пристап, дали е за фајл или директориум, ја има можноста да чита и гледа содржина и особини.
- *Write:* корисник со ова ниво на пристап, дали за фајл или директориум, има можност да запишува или да менува фајл, или да креира фајлови во директориум, а во некои случаи и да менува привилегии за пристап до директориум или фајл во директориумот.
- *Execute:* оваа привилегија, кога е дозволена, му дозволува на корисникот да извршува програми во даден директориум.
- *Delete:* ова право на пристап му дозволува на корисникот да избрише фајл, директориум, или фајлови во директориум.

Кај повеќето компјутерски и мрежни оперативни системи пристапот до фајл е поделен на три нивоа, кои зависат од групата на која и припаѓа корисникот: owner, group, и public или world. На секоја група и се доделени нивоа на пристап да одреден расурс. Овие нивоа се опишани подолу:

- *Owner:* оваа група се однесува на сопственикот на фајл или ресурс. Сопственикот - или го креирал ресурсот, или пак му е дадена или одземена привилегија за сопственост на ресурсот. Сопственикот на одреден ресурс обично може да чита, запишува, извршува, и да брише во ресурсот, но тоа не е секогаш така. Не е невообичаено за сопственикот на ресурсот по грешка да ги отстрани своите привилегии. Ова се прави со отстранување на сите привилегии на фајлот, или пак со префрлање на сопственоста на фајлот на некој друг. Обично, кога ќе се случи ова - корисникот не може да ги поврати привилегиите без помош од систем администраторот.
- *Group:* оваа група се однесува на корисници кои имаат меѓусебна врска, на пример ако работат во ист сектор. На корисниците во даден сектор може да им се додели привилегија за читање, запишување, извршување или бришење на некој фајл. Сите останати групи ќе бидат ограничени во пристап до овој ресурс или пак ќе имаат само привилегија за читање.
- *World or public:* оваа група се однесува на нивото на пристап на одреден фајл кое го поседуваат сите. Во Windows оваа група се нарекува Everyone. На оваа група може да и се одели привилегија за читање, запишување, извршување или бришење на одреден ресурс, но најчесто има ограничени привилегии, само за читање. Многу често, мрежни ресурси како печатари или делени директориуми кои се достапни на сите корисници, ќе имаат ограничени привилегии на пристап за групата public. Печатарите бараат одредено ниво на пристап, за да може да се печати на нив од одалечена дестинација.

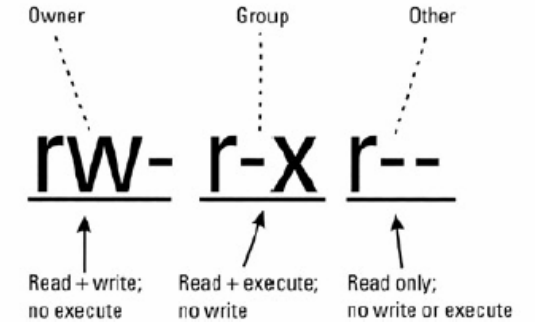
6.10.1 Привилегии кај UNIX OS

UNIX користи само три permissions. Тоа се read, write, и execute. Сликата ги прикажува доделените permissions за фајл кај UNIX фајл систем.



Сл. 6.7: Преглед на permissions за фајлови во еден директориум

На слика 6.7 привилегиите во левата колона се состојат од 10 букви или цртки. Првиот знак во колоната е колоната за типот на фајлот. Ако линијата започнува со “d“ тогаш станува збор за директориум, додека " l" претставува врска – линк. Ако линијата започнува со “a“, тогаш станува збор за стандарден фајл. Наредните 9 карактери ги даваат правата на пристап за трите категории или групи на сопственици, група, или останати. (Останати во UNIX е исто со world or public). Првите три знаци ги даваат правата на пристап за категоријата сопственик. На сликата, првата линија покажува дека има привилегии на пристап "- r w - r - x r - - ". Овие 9 знаци се правата на пристап доделени на групите owner, group, и other. Како што може да се забележи, првите три карактери ги специфицираат правата на пристап за корисници од групата owner. Во случајов имаат привилегии за читање и запишување. Следните три карактери ги прикажуваат правата на пристап на корисници од групата group. Во примеров, тие имаат привилегија за читање и извршување. Последните три знаци од низата се прават на корисници од групата other. на нив им е дозволена само привилегија за читање на фајлот или директориумот.



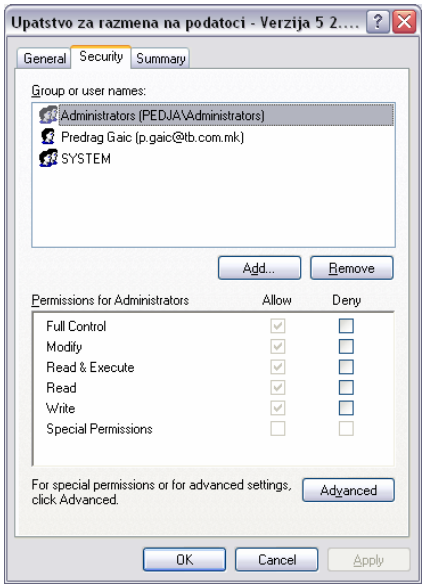
Промената на правата на пристап за некој директориум или фајл, кај оперативниот систем Unix е едноставна и се врши со наредбата:
chmod 777 ime_na_fajl

6.10.2 Привилегии кај Windows 2000

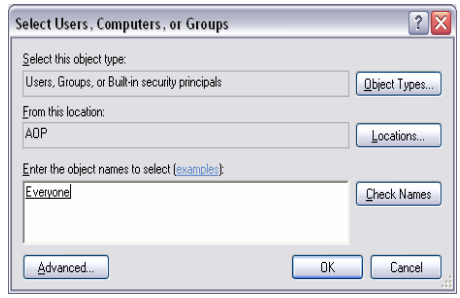
Microsoft's Windows 2000 исто го применува ACL и концептот на групи. Графичкиот кориснички интерфејс овозможува лесна и едноставна администрација со ACL. Како што и наведовме во досегашното излагање, секој корисник кој се најавил на domain преку својот user account располага со системските ресурси за кои има привилегии на пристап. Во една организациска мрежна структура, корисниците најчесто имаат потреба од пристап до различни типови на фајлови. За секој фајл и директориум во Windows фајл структурата, постои листа за контрола на пристап ACL, со чие едитирање им се доделуваат и одземаат привилегии за користење на тој фајл - на одреден корисник или група на корисници. Типичен изглед на ACL е даден на сликата 6.8. Како што може да се забележи од слика 6.8, во Windows има неколку permissions:

- Read
- Write
- Read&Execute
- Modify
- Full Control
- Special permissions

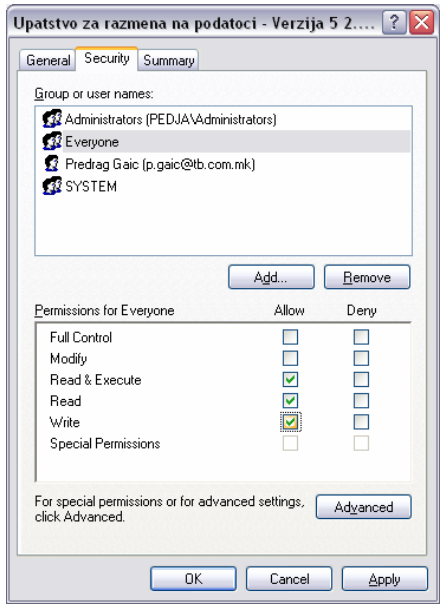
По default, за секој фајл, привилегии имаат корисници со account–и од групата на администратори и user account на корисникот кој се најавил на domain. За доделување на привилегии на корисник и/или група од корисници, се користи копчето Add, по чие притискање оперативниот систем ни дава можност да избереме - кој корисник или група од корисници ќе ги додадеме во ACL: на примерот од слика 6.9, сме ја додале групата Everyone, т.е. сакаме да подесиме права на пристап за сите корисници. Едитирањето на ACL се врши со едноставно обележување на привилегијата која сакаме да ја доделиме.



Сл. 6.8: ACL за фајл во Windows



Сл. 6.9: Додавање на група во ACL



Сл. 6.10: Додавање на привилегии за фајл, на одредена група на корисници

Контролата на пристап, т.е. привилегиите и групите се важен концепт за разбирање, бидејќи се важни алатки за контролирање на пристапот на

кориснуиците до системските ресурси. Кога се користат во комбинација со effective group assignment, правата на пристап можат да бидат ефективна безбедносна мерка. За жал, правата на пристап многу често се игнорирани или занемарени, и доделувањето на група се сведува на доделување на сите корисници на една груша. Како резултат на ова - правата за пристап до критичните системски фајлови - го прават системот ранлив и компромитлив.

6.11 ДОПОЛНИТЕЛНИ АЛАТКИ ЗА БЕЗБЕДНОСТ

Windows 2000 поседува множество од алатки за конфигурирање на безбедноста кои се проектирани за да ги намалат трошоците кои се поврзани со конфигурирањето и анализата на безбедноста на мрежите. Тоа се дополнителни MMC модули кои служат за подесување на безбедносните параметри кај Windows 2000 и за повремено анализирање на системот, со што се проверува дали конфигурирањето е непроменето и дали е потребно ново конфигурирање.

Во безбедносни параметри спаѓаат политиките на безбедност (локални и политиките на налози), контролата на пристап (сервиси, датотеки и базата Registry), евидентирање на настани, политиките на безбедност на IPSec и политиките на јавни клучеви. Алатките за конфигурирање на безбедноста се вклучени во три дополнителни модули: *Security Configuration and Analysis* (конфигурирање и анализа на безбедноста), *Security Templates* (шеми на безбедност) и *Group Policy* (политики на групи).

6.11.1 Дополнителен модул Security Configuration and Analysis

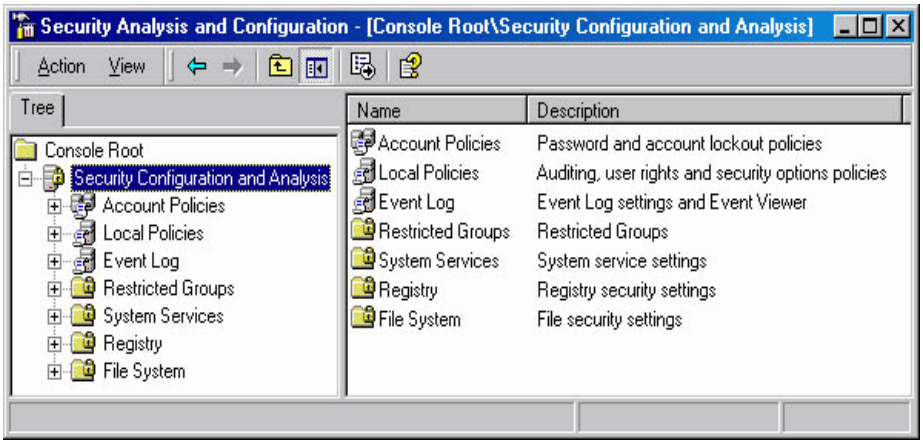
Со овој модул се конфигурира и анализира безбедноста на локалниот систем. Тој може да се користи за директно конфигурирање на безбедноста на локалниот систем. Може да се воведат безбедносни шеми кои се направени во модулот ***Security Templates*** и да се применат на **објекти на групни политики** (*Group Policy Objects, GPO*) за локален компјутер. На тој начин системот веднаш се конфигурира според нивоата кои се дефинирани во дадената шема.

Состојбата на оперативниот систем и апликациите на компјутерот се менува. Пр: понекогаш се случува да мора да се промени нивото на безбедност на системот за моментно да се решат некои проблеми на администрирање или проблеми на мрежата; често се случува овие промени да останат и по решавањето на проблемот. Ова значи дека компјутерот повеќе не ги задоволува безбедносните барања на претпријатието.

Со редовна анализа, администраторот го следи и одржува нивото на безбедност на секој компјутер. Анализите се многу темелни. Во резултатите се наоѓаат информации за сите аспекти на системот кои се однесуваат на безбедноста. Администраторот на овој начин може да го подесува нивото на безбедноста, и што е уште поважно, да ги открие безбедносните пропусти што можат да се јават во системот. Дополнителниот модул Security Configuration And Analysis дава брз преглед на резултатите од анализата на безбедноста на системот. Со моменталните вредности на параметрите се нудат и препораки, а се користат и икони и забелешки за да се укаже на областите каде моменталните вредности не го

задоволуваат зададеното ниво на безбедност. Со овој модул се решаваат и противречности кои анализата ги открила. На слика 6.11 е даден дополнителниот модул Security Configuration And Analysis. Овој модул ги овозможува следните работи:

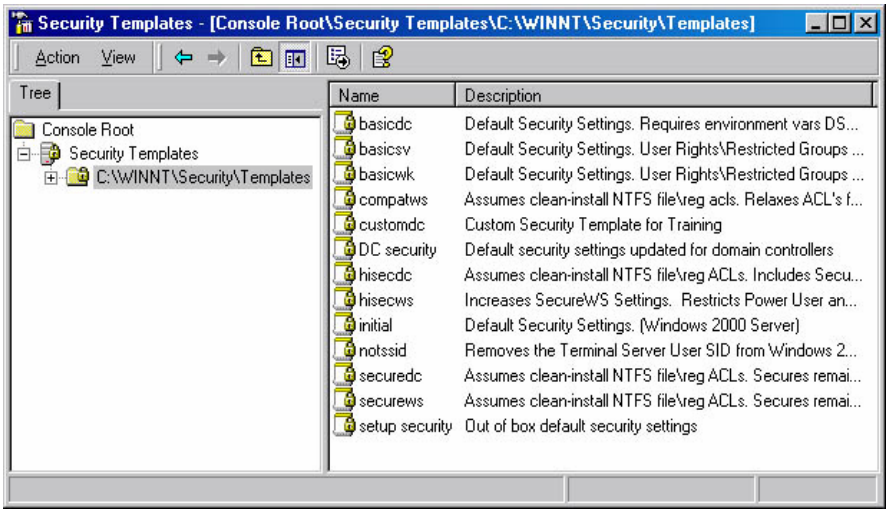
- Поставување на работните бази на податоци.
- Воведување на шемите за безбедност.
- Анализа на безбедноста на системот.
- Преглед на резултатите од анализата на безбедност.
- Конфигурирање на безбедноста на системот.
- Уредување на основната безбедносна конфигурација.
- Извезување на шемите за безбедност.



Сл. 6.11: Дополнителен модул Security Configuration And Analysis

6.11.2 Дополнителен модул Security Templates

Безбедносната шема (*security template*) е физичка репрезентација на безбедносната конфигурација: тоа е датотека во која се чува група од безбедносни параметри. Windows 2000 содржи множество на безбедносни шеми, од кои секоја се базира на некаква улога на компјутерот. Постојат различни шеми во опсегот - од клиенти во домен со ниско ниво на безбедност, па до многу безбедни контролери на домени. Шемите може да се користат такви какви што се, може да се менуваат, или да послужат како основа за правење на прилагодени безбедносни шеми. Дополнителниот модул Security Templates (слика 6.12) е алатка за правење и доделување на безбедносни шеми за еден или повеќе компјутери.



Сл. 6.12: Дополнителен модул Security Templates

Безбедносната шема е физичка датотека со слика на безбедносната конфигурација и може да се примени на локален компјутер, или да се воведе во некој **објект на групни политики** (*Group Policy Object, GPO*) во сервисот Active Directory. Кога ќе се воведе шема во GPO, Group Policy ја обработува шемата и ги спроведува соодветните промени на членовите на GPO (корисници или компјутери).

Дополнителниот модул Security Templates ги овозможува следните работи:

- Подесување на однапред дефинирани безбедносни шеми.
- Дефинирање на безбедносни шеми.
- Бришење на безбедносни шеми.
- Освежување на листата на безбедносни шеми.
- Подесување на описот на безбедносните шеми.

6.11.3 Дополнителен модул Group Policy

Безбедносните параметри го одредуваат однесувањето на системот во поглед на безбедноста. Со користење на ***GPO*** (*Group Policy Object*, објект на групни политики) од сервисот Active Directory, администраторите можат централизирано да ги применуваат нивоата на безбедност кои се потребни за заштита на системите.

Кога се одредуваат параметри за GPO во кои се наоѓаат повеќе компјутери, треба да се имаат во предвид организациските и функционалните карактеристики на дадената локација, доменот или организациската единица (ОУ). Пр: нивото на безбедност кое им е потребно на OU со компјутери во одделот ПРОДАЖБИ - се разликува од потребите на OU со компјутери во одделот ФИНАНСИИ.

Дополнителниот модул Group Policy овозможува централизирано конфигурирање на безбедноста во сервисот Active Directory. Фолдерот Security Settings се наоѓа во

јазолот Computer Configuration и во јазолот User Configuration. Со безбедносните политики администраторите може да го ограничат пристапот на корисниците до фолдерите и датотеките, да го подесат бројот на погрешно внесени лозинки кои корисникот може да ги употреби пред блокирање на компјутерот и да ги контролираат правата на корисникот како што е одредување на корисниците кои може да се пријават на доменот.

6.11.4 Event viewer (прегледник на настани)

Windows Event Viewer нема претрпено голема промена со години наназад. Овој тро-реден систем, запишува информации за системските, безбедносните и апликациските настани за подоцнежна анализа. Системските настани се случуваат кога откажува драјвер за време на извршување на операција, или кога не може да се вчита за време на подигање на системот. Безбедносните белешки, ги следат обидите за логирање (влез во системот) и други информации, поврзани со безбедноста, дозволувајќи ви да ги детектирате и да ги одбиете можните напади. Конечно, белешките за апликациските настани ќе ја фатат секоја информација од апликациите базирани на Windows, од WEB сервери, или пристапот од „трети лица“ кон базата на податоци, или кон комуникацискиот софтвер.

6.11.5 Network monitor (мрежен монитор)

Како една од највозбудливите алатки на Windows 2000, мрежниот монитор го овозможува она што порано беше единствено можно со посебни апликации, или како дел од скапите хардверски пакети на LAN анализатори. Мрежниот монитор претставува главен сервер за мрежната статистика, започнувајќи од детектираните пакети, пренос на податоци, или мултикаст, па сè до пренос на податоци специфични за конкретен адаптер. Имате можност да работите во нормален или во самостоен режим на работа, и исто така да ги зачувате податоците за подоцнежни анализи.

6.11.6 Монитор на перформансите (performance monitor)

Мониторот на перформанси е графичка алатка што ви овозможува да ги измерите перформансите на скоро сите аспекти од вашиот Windows мрежен оперативен систем, вклучувајќи го серверот и оддалечените работни станици. Мониторот на перформанси исто така обезбедува сервиси (услуги) за исцртување на графикони, креирање на извештаи, и активирање на аларми со цел да ве информира, дали и кога претходно дефинираните нивоа на перформансите се достигнати, како на пример % од процесорското време, број на пренесени пакети во секунда, и слично.

6.11.7 Администратор за оддалечен пристап

Ако користите Услуги за оддалечен пристап (RAS - УОП) во вашата мрежа и ве снајде неволја, вашата прва станица е Администраторот за оддалечен пристап (АОП). АОП ќе обезбеди брз преглед на севкупниот статус на УОП, вклучувајќи: достапни и зафатени порти, брзина на дојдовни и појдовни бајти и

пакети, CRC (Circle Redundancy Check), истекувања на времето, делење на рамки, хардвер, грешки во баферите, и идентификациски податоци за оддалечената работна станица.

6.11.8 Сервер менаџер

Windows Server Manager е ресурс што ќе ви овозможи да администрирате Windows домени, како и подесување на специфицирани компјутери. Можете да ја видите листата на корисници конектирани на извесни машини, да ги видите ресурсите специфични за одредена машина (делени или отворени), да вршите контрола на реплицирање на директориуми, да вршите конфигурирање на сервиси (услуги), и да пренесувате пораки за аларми на конектираните корисници. Дополнително, можете да управувате со примарните контролери на домени (ПКД – PDC), и да додадете или да отстраните машини од Windows доменот.

6.11.9 Вградени алатки за дијагностика

Вградениот комплет на алатки за дијагностика на Windows, т.н. Windows дијагностика, овозможува обемен (разбирлив) поглед на варијаблите за конфигурација и варијаблите за околина што вашиот Windows систем во моментот ги користи, во било која од деветте категории, вклучувајќи: Верзија, Систем, Дисплеј, Диск Уреди (драјвови), Меморија, Сервиси (Услуги), Ресурси, Околина, и Мрежа. Табулаторите по категории ќе ви ја овозможат следната информација:

- Version – верзија на ОС и кодот на градење (специфичен код кој покажува која тековна подверзија е користениот софтвер), 20-цифрени регистрациски броеви, и персонални податоци за регистрација.
- System – тип на HAL (Hardware Abstraction Layer – ниво за апстракција од хардверот), тип на BIOS (Basic Input Outpus System – основен систем за влез/излез) и негова верзија, и типови на процесор(и).
- Display – датум и тип на BIOS – от, моментални подесувања, меморија, тип на чип и DAC (Digital to Analog Converter), и податоци за конкретниот драјвер.
- Drives – пристап до секој уред и информација за сите уреди приклучени кон машината, (се мисли на уреди со дискови: хард дискови и CD ROM-ови).
- Memory – локација на фајлот за страничење (pagefile), физичка меморија и меморија на јадрото, манипулатори (handles), нишки (threads), процеси, вкупно количество на доделена меморија – Commit Charge Total
- Services – дава известување за сите инсталирани сервиси (услуги), нивната моментална состојба, (за сервиси што се активни, за исклучените и за паузираните).
- Resources – IRQ на ресурсите (Interrupt ReQuests), број и тип за сите уреди вклучени на серверот.
- Environment – тип на процесор, архитектура, ниво, ревизија; патека на Windows-от; оперативен систем.
- Network – се состои од четири категории на податоци: Општи (права на пристап, име на работна група/домен, LAN root), Транспорт (тип, адреси), Подесувања (вредности за истекување на времето, предвремено вчитување – read-ahead, бафери, и слично), и Статистика (примено/пратено количество на бајти, грешки во вчитување, и слично).

6.11.10 Менаџер за Интернет сервиси

Со скорешното додавање на *Microsoft Internet Information Server* како интегрален дел на Windows мрежниот оперативен систем, Microsoft го додаде *Internet Service Manager* (Менаџер за Интернет Сервиси – МИС) како алатка на првата линија за управување на Internet сервиси, базирани на Win 2000, што работат на локации било каде во вашата LAN. МИС ви дозволува да имате лесен пристап до било кој локален Windows сервер, овозможувајќи HTTP, FTP, или Gopher услуги, преглед на нивниот моментален статус (дали работи, дали е сопрен или паузиран), и реконфигурирање на својствата на специфични сервиси како реакција на тековниот или предвидениот мрежен проблем. Додека функциите за мониторинг на МИС се во голема мерка ограничени, тие кога се здружени, со способноста за далечинско вклучување, запирање, и конфигурирање на мрежните сервиси, можат да бидат божји дар за одржување на системите.

6.12 ПРОБЛЕМИ КАЈ WINDOWS И UNIX

6.12.1 Црни точки во користењето на Windows системите

Постојат многу потсистеми што работат усогласено за да обезбедат робустна околина за користење на мрежата, што ја знаеме како Windows 2000. Како и да е, секогаш кога се во прашање Windows мрежите, постои одреден број на важни карактеристики кои треба да ги познавате. Штом еднаш дознаете каде се наоѓаат, и што треба да барате, би требало да ви биде полесно да ги разрешите проблемите околу латентноста (доцнење) на мрежата, и другите тесни грла за перформансите на мрежата.

Надгледувањето (мониторингот) на црните точки на Windows секогаш од вас ќе бара да го користите Windows Performance Monitor (PerfMon). Иако вообичаено ќе завршите дополнувајќи ги анализите на perfMon со други алатки за мониторинг, PerfMon воглавно е најдобро место од кајшто треба да започнете со вашата истрага. Во зависност од сервисите и другите дополнителни делови, инсталирани со вашиот Windows сервер или работна станица, ќе имате избор за мониторинг на голем број PerfMon објекти, вклучувајќи прегледник (browser), кеш, FTP server, HTTP service, ICMP (Internet Control Message Protocol), IP (Internet Protocol), Меморија, NetBEUI/NetBEUI ресурси, Мрежен интерфејс/сегмент, Фајл за страничење, Физички диск, процес, Процесор, RAS port/TOTAL (Remote Access Service), Редиректор, Серверски/ Работни редови на чекање, Систем, TCP, Нишки, и UDP. Додека секој од овие фактори може да придонесе за испад на мрежата во даден момент, важно е да се обрати посебно внимание на минимум четири објекти. И додека овие четири објекти може да варираат во зависност од вашата специфична конфигурација, тие може да се категоризираат како: Мрежен Протокол по дефиниција, Хардвер за интерфејс, Меморија, и Сервер.

За брзо реагирање и отстранување на дефектите, би требало да запомните да го надледувате главниот мрежен протокол (мрежниот протокол по дефиниција) којшто ве поврзува со различни јазли. Во некои случаи ова може да се постигне

преку комбинација на TCP и IP објекти, или можеби како функција на NetBEUI објект. Колизиите, брзината на пакети и бајти, вредностите за истекување на времето, и други важни информации може да бидат испитани и оценети врз база на идеални и/или предвидени вредности на перформансите.

Хардверот за интерфејс се справува со состојбата на вашиот моментален адаптер на главната машина (host adapter), и неговите севкупни перформанси, во смисла на пратени и примени пакети, грешки, должина на ред за чекање, исл. Можете (и би требало) да се потпрете на овој објект со цел да ви помогне да одредите кога испадите на мрежата се резултат на неправилно конфигурирана NIC (Network Interface Card – Мрежна интерферјсна карта), испад на адаптерот, или дури лош кабел. Меморијата, многу едноставно, обезбедува податоци за перформансите, за моментално инсталираната системска меморија, вклучувајќи ги грешките при читање и запис *(read/write errors)*, пропусти – грешки поради физичка неисправност *(faults)*, копии, достапна меморија, исл. Може да го користите овој објект за да одредите дали мрежните сервиси (мрежни услуги) се деградирани поради меморија подложна на грешки (индицирано со голем број на грешки/пропусти), недоволно меморија (големи фајлови за страничење и чест пристап до дискот), или неправилно конфигуриран фајл за страничење. Објектот Сервер е последниот од централните објекти кон кој веднаш ќе се обратите ако има проблем во мрежата. Можете да одмерите сè, од дозволи и системски грешки - до дополнителни податоци за статусот на достапната физичка меморија. Исто така, вредноста Bytes Total/Sec (вкупен број на бајти/бајти во секунда) може да обезбеди непроценливи податоци за тоа колку е зафатена конкретна машина под различни услови (посебно е корисно за фајл – сервери), и може да биде од голема помош кога се обидувате да изведете пресметки за балансирање на оптоварувањето.

6.12.2 Проблеми кај Unix

Во најголем дел, отстранувањето на мрежните проблеми во светот на UNIX се фокусира на TCP/IP, кој претставува протокол за комуникација, и NFS, кој претставува мрежен фајл систем. Освен тоа, мора да сте постојано свесни за имплементацијата на остатокот од вашата мрежна инфраструктура, што е дополнителен извор на потенцијални проблеми. Секоја одлука што ја донесувате за градењето на вашата инфраструктура, ќе влијае на капацитетот и можностите на вашата мрежа.

Најголемиот дел од мрежите низ светот денес, што имаат применето UNIX системи се базирани на 10base-T, Ethernet технологии со парица. Иако за 10base-T често се мисли дека е 10Mbps медиум, вистинската брзина на мрежата што може да се оствари од страна на апликациите е значително помала. Штом реалните потреби започнат да го надминуваат капацитетот, сите корисници на мрежата тоа ќе го приметат, дури и ако работат со UNIX. Освен тоа, потребен е само еден систем на Ethernet мрежа за да ја доведе целата мрежа во застој. Постојан пренос (трансфер) на големи фајлови преку мрежата е само еден пример за активност што можат да ја извршат голем број на корисници и што може да има влијание на перформансите на мрежата. Запомнете, како и било кој друг ресурс во вашиот систем, мрежниот капацитет е ресурс што може да го снема (да се потроши).

Корисниците на UNIX, сепак, имаат дополнителна предност во светот на мониторинг на мрежите. Тие имаат многу моќни информативни алатки вградени во нивните оперативни системи. Со малку инструкции од ваша страна, корисниците можат многу лесно да ги детектираат проблемите поврзани со капацитетот. Едноставни команди со употреба на rsh (наредба во UNIX), може да дадат индиции дека вашата мрежа има проблеми.

Пред да кажеме за деталниот мониторинг на мрежата, да направиме краток тест за да провериме дали сме конектирани на мрежата. За да го сториме тоа, потребно е да го знаеме името или IP адресата на друга машина во мрежата. Ќе ја употребите наредбата ping за да испратите еден пакет до оддалечен систем и ќе го измерите времето што е потребно оддалеченият пакет да ви испрати еден пакет назад кон вас. Во наједноставната нејзина форма наредбата *ping* (прикажано на пример 6.1) прифаќа име на машина или IP адреса, како параметар во команден ред. Во примерот 6.1, хостот *dole* се чини дека нека не може да го пронајде хостот *whitehouse* – друг хост во мрежата.

Пример 6.1. Неуспешен *ping*.

```
dole % ping whitehouse
ping: whitehouse: Unknown host
```

Во случај кога препознавањето на вториот систем не успее со употреба на име, обидете се со употреба на IP адреса (види пример 6.2). Во овој случај *dole* го пронајде *whitehouse* со помош на користење на неговата IP адреса и испраќа и прима податоци 100% без грешка. *ping* ќе продолжи да испраќа податоци се додека не го прекинете кругот со притискање на Ctrl+C.

Пример 6.2. Успешен *ping.*

```
dole % ping 198.137.240.92
PING 198.137.240.92 (198.137.240.92): 56 data bytes
64 bytes from 152.163.41.3: icmp_seq=0 ttl=254 time=8 ms
64 bytes from 152.163.41.3: icmp_seq=1 ttl=254 time=2 ms
64 bytes from 152.163.41.3: icmp_seq=2 ttl=254 time=1 ms
64 bytes from 152.163.41.3: icmp_seq=3 ttl=254 time=2 ms
----198.137.240.92 PING Statistics----
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 1/3/8 ms
```

Мониторинг со користење на spray

Spray е UNIX наредба што се употребува за да испорача рафал од пакети со податоци на друга машина, т.е. дава известување колку пакети пристигнале успешно и колку време било потребно. Со слична природа како помалиот брат *ping*, *spray* може да се искористи уште поефикасно за мониторинг на перформансите отколку *ping,* бидејќи може да испрати повеќе податоци. Резултатите од наредбата, прикажани во пример 9.3 ќе ви дадат до знаење дали

другата машина била способна успешно да ги прими сите испратени пакети. Во примерот прикажан на пример 6.3, рафал од пакети со податоци се испраќа од машината извор (*dole*) до машината цел (*clinton*).

Пример 6.3. Употреба на *spray* за мониторинг на мрежата.

```
dole % spray clinton
sending 1162 packets of lnth 86 to clinton ...
      no packets dropped by clinton
5917 packets/sec, 508943 bytes/sec
```

Во примерот погоре, машината цел (dole) успешно ги врати сите податоци пратени кон неа од страна на машината извор (clinton). Доколку *clinton* беше под големо оптоварување, предизвикано од страна на претходен сообраќај низ мрежата, или некоја друга интензивна активност, некои од пакетите со податоци немаше да бидат вратени од страна на *clinton. spray* по дефиниција испраќа 1162, 86-бајтни пакети.

Пример 6.4. Преку употреба на променлив број на пакети, spray може да се користи за поблиска симулација на реален мрежен сообраќај.

```
dole % spray -c 1000 -d 20 -l 4096 clinton
sending 1000 packets of lnth 4096 to clinton ...
      no packets dropped by clinton
95 packets/sec, 392342 bytes/sec
```

Во случај кога вашите тестови со spray ќе резултираат со загуба на пакети, ваш наредeн чекор би бил правење на поглед одблиску на машината што се тестира. Прво, погледнете дали е вчитан некој тежок процес, дали има недостаток на меморија, или други проблеми со CPU. Во случај да не сте во можност да пронајдете ништо погрешно во вашиот систем за тестирање, што би можело да предизвика задоцнет одговор од страна на мрежата, испраќањето на сличен тест до вашата првобитна машина за тестирање, би можело да индицира дека постои поголем проблем во мрежата. Во тој момент, време е да се започне со проверка на вашиот хардвер за рутирање и на вашата инфраструктура за анализа на хардверот.

Мониторинг со Netstat

Наједноставниот начин да се провери оптоварувањето на мрежата на конкретен систем е да се употреби наредбата netstat. Кога се извршува без никаков параметар од команден ред, наредбата прикажува листа на активни сокети за секој протокол. Примерот 6.5 го покажува излезот добиен од netstat што работи на Silicon Graphics Indy работна станица. Во овој пример, хостот dole има повеќе отворени конекции. Единствен потенцијален проблематичен поим во листата е конекцијата од системот наречен dukakis. Сепак, со оглед дека тоа е конекција преку модем, длабочината на листата за испраќање се очекува да биде малку поголема.

Пример 6.5. Употреба на netstat за мониторинг на активните мрежни конекции

```
dole % netstat
Active Internet connections
Proto Recv-Q Send-Q  Local Address   Foreign Address   (state)
tcp   0     0  dole.telnet       reagan.431025       ESTABLISHED
tcp   0     0  dole.telnet       nixon.9031          ESTABLISHED
tcp   0     4  dole.telnet       dukakis.ppp.1036    ESTABLISHED
tcp   56    0  dole.1060         ftp.watergate.ftp   CLOSE_WAIT
tcp   52    0  dole.1799         news.washngtnpost.nntp CLOSE_WAIT
```

Во стандардниот извештај на netstat, единственото поле што е значајно за вашата операција на мониторинг е Send-Q, којшто известува за длабочината на испраќање, а тоа претставува количество на податоци во бајти што чекаат да бидат испратени (или да бидат примени, ако гледате во опашката за примање). Ако бројките во вашиот ред за испраќање низ конкретен мрежен сегмент се веќе големи и стануваат се поголеми, таа конкретна мрежа е веројатно преплавена со прекумерен сообраќај. Ако поединечни влезови се појавуваат со големи редови за испраќање, можно е да има проблем со некој конкретен хост.

Можеби најбрзиот начин да се утврди интегритетот на вашата мрежа – дали пакетите стигнуваат на целта најбрзо што можат – е со користење на netstat со –i параметар од командна линија. Сите системи приклучени на конкретен сегмент од вашата мрежа, го делат истиот. Кога повеќе од еден клиентски или серверски систем се обиде да ја искористи мрежата во исто време, настанува колизија во моментот кога пакетите од едната машина ќе се сретнат со пакетите од другата. Ова всушност не е необична состојба на повеќето мрежи; како и да е, кога бројот на колизии стане значаен процент од севкупниот мрежен сообраќај, ќе согледате значителна деградација на перформансите на мрежата. Освен колизиите предизвикани од истовремен пренос низ мрежата, и други услови може да предизвикаат грешки во преносот и приемот на податоците. Дефектни хабови, неисправни интерфејси, или дури и електромагнетни полиња од уреди што не се физички приклучени на мрежата (како на пр. мотори за лифтовите во зградите) може да да бидат виновници за високиот степен на колизии на пакетите. Како што бројот на колизии и други грешки во вашата мрежа расте, перформансите на мрежата се деградираат.

Табела 6.1. Информација вратена од страна на netstat.

Вредност	*Податоци*
Name	Име на мрежниот интерфејс (конвенциите за доделување на имиња се разликуваат кај UNIX)
MTU	Максимална големина на пакет од интерфејсот
Net/Dest	Мрежа кон која е сврзан интерфејсот
Address	Избрано Internet име за интерфејсот
Ipkts	Број на доаѓачки (влезни) пакети од последниот рестарт на системот

Ierrs	Број на грешки на доаѓачки пакети од последниот рестарт на системот
Opkts	Број на појдовни (излезни) пакети од последниот рестарт на системот
Oerrs	Број на грешки на појдовни пакети од последниот рестарт на системот
Collis	Број на детектирани колизии

Во претходниот пример, може да се види дека процентот на колизии детектирани во мрежата, е помал од 2.25% од вкупниот број на пратени пакети. Како што е нагласено претходно, ако колизиите се постојано изразени со двоцифрени бројки, вашата мрежа најверојатно страда од недостаток на капацитет. Исто така, во претходниот пример треба да се забележи односот на излезни и влезни грешки. И двете се многу ниски, што е друг индикатор дека мрежата на којашто е приклучен dole, функционира најнормално. Ако се сомневате дека проблемите во мрежата се виновник за деградираните перформанси на системот, оваа наредба треба да ја повторувате почесто. Активни, здрави системи ќе имаат број на влезни и излезни пакети што е во постојан пораст. Ако Ipkts се зголемува, а Opkts не, вашиот систем најверојатно не одговара на ниедно барање што го добива, што пак индицира дека вашиот систем можеби е преоптеретен или има некакви проблеми при преносот. Ако бројот на влезните пакети никогаш не се зголемува, вашиот систем не добива никакви податоци од мрежата. Кога се употребува параметарот –s од команден ред со наредбата netstat, се прикажува запис (белешка) со статистичка информација, асоцирана со секоја од поддржаните компоненти на TCP/IP.

Мониторинг со nfsstat –c

NFS е екстремно моќна алатка. Таа на корисниците им овозможува на лесен начин да ги делат фајловите помеѓу UNIX системи со монтирање на директориуми на оддалечени волумени како локални диск-уреди. Корисниците би требало да бидат обучени како правилно да ги користат NFS волумените. Важно е да се нагласи дека работите ќе бидат побавни, кога се пристапува кон фајловите преку мрежата користејќи NFS, посебно кога фајлот е голем. Пристапувањето кон фајлот директно на оддалечената машина со користење на оддалечен логин (влез во системот), ќе резултира со операција што ќе се изврши многу побрзо. Сепак, одредени функции како едитирање и копирање на фајлови што се со многу поразумна големина, се перфектно добри – тоа е причината поради која што NFS е создаден. Вашите корисници треба да бидат многу внимателни кога го користат NFS и треба да знаат како соодветно да го користат. Тоа е начинот на којшто вие најдобро можете да ги надгледувате прформансите на NFS на вашата мрежа.

6.12.3 Функции на мрежниот администратор

Задачите за администрирање на мрежа вклучуваат инсталирање и конфигурирање на мрежни работни станици, креирање и одржување на кориснички акаунти (сметки), создавање на архивни копии (бекап-и) од системот, дистрибуција на софтвер низ мрежните работни станици, и обезбедување на поддршка на крајните корисници. Секоја од овие задачи служи за специфична намена во администрирањето на мрежниот систем. Сепак, една задача може да има влијание на повеќе други задачи. Со цел да се добие увид во тоа како се

меѓусебно поврзани овие задачи, тие често се групирани во функционални области. Форумот за мрежи на ISO (Меѓународна организација за стандардизација), ги раздели задачите за администрирање и управување (менаџмент) со мрежите во пет основни функционални области: менаџмент на дефекти (Fault management), менаџмент на конфигурирањето (Configuration management), менаџмент на акаунти (Accounting management), менаџмент на перформанси (Performance management), и менаџмент на безбедност (Security management).

Менаџмент на дефекти е процес на лоцирање и поправање на мрежни проблеми. Дефект е дефиниран како било која аномалија што влијае неповолно на мрежните операции. Во чести дефекти се вбројуваат оштетени мрежни кабли, грешки на дисковите, и испади во меморијата (грешки). Процесот на менаџмент на дефектите започнува кога ќе се пријави сомнителен дефект. Откако ќе се идентификува и ќе се дефинира проблемот, главната причина за дефектот мора да се изолира за да се осигуриме дека ќе се преземе соодветна акција со поправно дејство. Менаџментот на дефекти е најважна задача во администрирање на мрежата. Со имплементирање на добри процедури за менаџмент со дефектите, мрежните администратори можат да го намалат времето изминато „во гаснење на пожарот“, со што се послободни да ги фокусираат нивните напори во подобрување на мрежните операции и перформанси.

Менаџмент на конфигурирањето е процес на собирање на информации од мрежата и употреба на податоците за менаџмент и оптимизација на мрежните уреди. Општите задачи на менаџментот на конфигурирањето вклучуваат доделување на мрежни адреси на мрежни уреди, и одржувување на актуелноста (модерноста-современоста) на инсталираниот софтвер во мрежата. Менаџментот на конфигурирањето е предуслов за менаџмент со перформансите.

Менаџмент со акаунти е процес на менаџмент и употреба на мрежните ресурси. Основните задачи на менаџментот со акаунти, вклучуваат креирање и одржување на кориснички акаунти и групи, како и доделување на права за пристап на корисниците и групите. Осигурувањето (водењето сметка) дека адекватни мрежни ресурси им се достапни на корисниците на мрежата и документирањето на употребата на таквите ресурси, е исто така функција на менаџментот со акаунти.

Активностите асоцирани со одржување и подобрување на брзината на мрежата, нејзиното реагирање, флексибилноста, и адаптибилноста колективно се познати како *менаџмент на перформансите*. Типичните задачи на менаџментот на перформанси вклучуваат подесување на системот, планирање на севкупниот капацитет, и отстранување на проблемите со перформансите. Системите поврзани во мрежи, дозволуваат на информацијата да биде рапидно дистрибуирана низ организацијата. Иако работењето со мрежата дозволува зголемување на продуктивноста и побрз пристап кон информациите, тоа креира можност за уништување или пристап од недозволени лица до чувствителните информации. Процесот на заштита од такви настани се нарекува *менаџмент на безбедноста*.

6.13 РЕЗИМЕ

Ова поглавје ве запозна со концептот на заштита на оперативните системи, мрежни уреди, и апликации. За да ја обезбедиме мрежата, секој од елементите во таа околина мора да биде индивидуално проценет. Запамтете, вашата мрежа е не повеќе сигурна отколку што е сигурен нејзиниот најслаб дел. Бизнисот со безбедност овозможува стандардизирани методи за проверка на безбедносните капацитети на одредени продукти. Никогаш не ги земајте во предвид оперативниот систем или апликацијата, односно нивната безбедност, за готови ако не се верификувани по EAL стандардите, кои овозможуваат седум нивоа на сигурност (најчест критериум кој го замени и TCSEC критериумот како примарен безбедносен сертификат). EAL 4 е ниво препорачано да овозможи нормална безбедност за корпоративните оперативни системи.

Бројот на ранливости рапидно расте. Порастот делумно се должи на фактот дека многу производители на системи не ги земаа темите од безбедноста сериозно во минатото. Овој став се менува, и многу од поголемите производители сега разбираат каква штета можат да донесат безбедностите пропусти на своите корисници. Процесот на правење на серверот или апликацијата - да биде отпорна на напади, се нарекува заштита. Еден од главните методи за заштита на оперативен систем е оневозможување на протоколите кои не се потребни од страна на системот. Одржување на системите на ниво на последна надградба, исто така помага во подобрување на безбедноста.

Заедничките протоколи кои се користат во PC-базирана мрежа се NetBEUI, IPX/SPX, и TCP/IP. Секој од овие протоколи креира единствени безбедносни предизвици кои мора да се одговорат. Протоколите кои не се користат треба да се оневозможат на сите уреди: секој протокол што се користи го зголемува потенцијалот за ранливост на вашата околина. ACL се имплементираат кај мрежните уреди и системи за да овозможат контрола на пристап до системите и корисниците. ACL дозволува самостојните системи, корисници или IP адреси да бидат игнорирани. Големите мрежи често користат Unix мрежи и додатни протоколи како NFS. NFS е тежок за обезбедување, и не треба да се користи во надворешни мрежи. Додатна безбедност е достапна преку користење на VPN конекции.

FAT датотечните системи овозможуваат безбедност на корисничко и деливо ниво. Како резултат на тоа, FAT не се препорачува како податочен систем во безбедни околини. NTFS овозможува безбедносни можности слични со Unix и дозволува контрола на индивидуални датотеки со користење на различни критериуми.

Производителите и продавачите овозможуваат надградби на продуктите за да ја подобрат безбедноста и да ги поправат грешките во продуктите кои тие ги поддржуваат. Трите примарни методи за надградба на системот се брзите поправки, сервисните пакети и закрпите. Брзите поправки се претежно привремени решенија, додека не се направи трајна поправка. Microsoft своите закрпи за багови ги вика брзи поправки. Сервисните пакети содржат повеќе поправки за еден систем. Закрпите се користат за привремено поправање на програмите, додека перманентна поправка не се најде. Производителите

претпочитаат замена на целите програми, отколку да крпат и поправаат постоечки. Кога инсталирате закрпа, првенствено следете ги упатствата збор до збор; неправилно инсталрана закрпа може да го дестабилизира целиот систем.

Мрежните уреди стануваат покомплицирани и тие бараат регуларна инсталација на надградби. Процесот на надградба вообичаено се постигнува со некоја терминално базирана или веб базирана апликација. Натрапниците сè повеќе ги земаат рутерите и другите уреди како цел на своите напади. И тие уреди треба да се чуваат на најново ниво на надградба. Заштитата на апликациите помага во минимизирање на ранливостите. Стартувајте ги само апликациите и сервисите кои се потребни за одржување на вашата околина. Напаѓачите ги таргетираат апликативните протоколи. Повеќето од новите системи нудат богати околини за крајните корисници, но секој протокол го зголемува ризикот.

Директориумските сервиси дозволуваат информацијата да се дели на структуиран начин со голем број на корисници. Овие сервиси мораат да бидат безбедни за да се спречи лажно претставување. Познати директориумски сервиси се LDAP, AD, X.500 и eDirectory. Технологиите врзани со базите на податоци се ранливи на напади поради флексибилноста која тие ја овозможуваат. Серверите за базите на податоци и апликациите исто така треба да се надградуваат редовно. За да се овозможи зголемена безбедност, многу околини имплементираат пристапи со повеќе столбови кон своите податоци.

□

7. БЕЗБЕДНОСТ НА WEB - IPSEC И SSL

Користењето на WWW во денешни услови е тесно поврзано со сигурностните техники. Не може да стане збор за е-бизнис и електронско банкарство без современата криптозаштита. Начинот на кој крипто-заштитата е имплементирана на web, дефинира протоколи за заштитена комуникација. Така, SSL se користи за безбеден HTTP-протокол, додека IPSec протоколот се имплементира кај VPN (Virtual Private Network).

7.1 SSL

Secure Socket Layer (SSL) се користи за да се постави безбедна комуникациска конекција помеѓу две TCP – базирани машини. Овој протокол го користи методот на ракување за да постигнат сесија. Бројот на чекори во ракувањето зависи од тоа дали чекорите се комбинирани и/или заедничка автентикација е потребна. Бројот на чекори секогаш е помеѓу четири и девет, базирано на тоа кој ја прави документацијата.

Забелешка: Netscape оригинално го разви SSL методот, кој доби широко прифаќање во индустријата.

И покрај различните имплементации, чекорите можат да се сумираат како на сликата 7.1. Кога барање за конекција се прави до серверот, серверот праќа порака назад до клиентот - велејќи дека е потребна безбедна конекција. Клиентот праќа до серверот сертификат, покажувајќи ги можностите на клиентот. Серверот потоа го проверува сертификатот и одговара со клуч за сесијата и со енкриптиран приватен клуч. Сесијата ќе остане отворена сè додека еден од краевите не даде наредба да се затвори сесијата. Командата се издава кога пребарувачот ќе се затвори или друг URL е побаран.

Сл. 7.1: Процес на SSL конекција

Secure Socket Layer, или општо познат како SSL претставува стандард за криптирана комуникација помеѓу два мрежни ентитети. Основната цел на SSL протоколот е да се обезбеди приватна и стабилна комуникација помеѓу два мрежни ентитети. Протоколот е составен од два слоеви, од кои на најниско ниво, веднаш над TCP мрежниот протокол, лежи SSL Record Protocol. Овој основен протокол е темел над кој е дефиниран SSL Handshake Protocol, кој овозможува клиентот и серверот да се автентицираат меѓусебно, да се договорат за

криптографски алгоритми кои ќе се користат, како и за определување на сесиски клучеви.

Најголема предност на SSL протоколот е во тоа што е апликативно независен протокол, така што над него може да се изградат други апликативни протоколи. Некои најпознати примери се:

- HTTPS, криптиран HTTP протокол (HTTP преку SSL)
- SSH, криптиран shell (telnet преку SSL)
- SFTP, криптиран трансфер на датотеки (FTP преку SSL)

7.1.1 SSL Record Protocol

Најниското ниво на SSL-протоколот дефинира неколку основни функционалности кои потоа се користат по метод на црна кутија во горните слоеви. На ниво на овој слој се дефинирани:

- *Фрагментација* - слојот на пакети (Record layer) ги фрагментира блоковите со податоци во SSL Plaintext пакети со големина од 2^{14} бајти или помалку. Големините на пораките од клиентот немаат значење во овој слој, што значи дека повеќе клиентски пораки може да се најдат во еден SSL Plaintext блок.
- *Компресија* - сите пакети се компресираат со помош на алгоритми за компресија дефинирани во тековната сесија. Алгоритмите за компресија ги преведуваат SSL Plaintext структурите во SSL Compressed стуктури.
- *Заштита на пакетите од промена (MAC) и енкрипција* - сите пакети кои се разменуваат на ниво на SSL Record слојот, мора да имаат Message Authentication Code на својата содржина. Откако ќе заврши инцијализацијата, двете страни веќе делат заеднички симетричен таен клуч со кој прво се пресметува MAC на пакетот, а потоа се криптира со договорениот симетричен криптографски метод.
- *CBC Block и Stream криптографски методи* - криптографските методи кои се користат за енкрипција и декрипција на пакетите можат да бидат на ниво на блокови или во форма текови (stream). SSL 3.0 подржува RC4 stream метод, и RC2 и DES block криптографски методи, кои се одредуваат во фазата на иницијализација.

7.1.2 SSL Handshake protocol

Криптографските параметри на една SSL сесија се воспоставуваат во фазата на иницијализација која е дефинирана со SSL Handshake Protocol-от, кој функционира врз SSL Record слојот. Кога SSL клиент и сервер ќе започнат да комуницираат меѓусебно, тие треба да се договорат за користењето на криптографски алгоритми, која верзија на протоколот ќе ја користат, да се автентицираат меѓусебно, и со помош на асиметричен криптографски метод да воспостават заеднички таен клуч.

Клиентот секогаш ја започнува комуникацијата со испраќање на **client hello** порака, на која што серверот мора да одговори со соодветна **server hello** порака, а во спротивно ќе резултира со неуспешен обид за поврзување. Овие две пораќи се

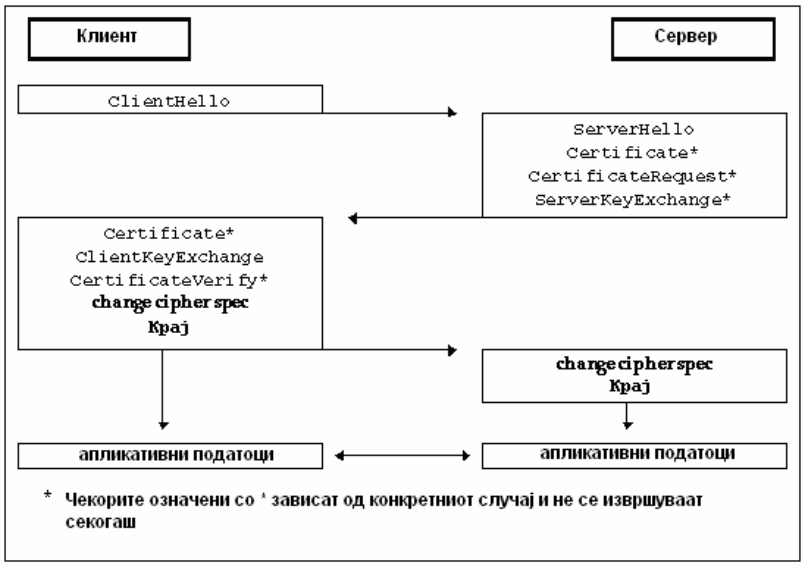
користат за да се воспостават основните безбедносни стандардни, т.е. клиентот и серверот да дознаат нешто повеќе за криптографските способности на другата страна. Пораките **client hello** и **server hello** ги воспоставуваат следните атрибути на една SSL сесија:

- Верзија на протоколот
- Идентификација на сесијата
- Пакет криптографски методи кои стојат на располагање
- Методи на компресија
- Дополнително се испраќаат два случајни броеви од страна клиентот и серверот: ClientHello.random и ServerHello.random.

Следејќи ги иницијалните hello пораките, серверот го испраќа својот дигитален сертификат, доколку треба да се автентицира неговиот идентитет. Дополнително се испраќа **server key exchange** порака, во случај кога серверот не поседува дигитален сертификат, или пак истиот е наменет исклучиво за дигитално потпишување. Ако серверот е автентициран од страна на клиентот, серверот може да побара дигитален сертификат од клиентот, во зависност од криптографските методи кои се користат.

Откако серверот ќе испрати **server hello done** порака до клиентот, означувајќи дека hello фазата од иницијализацијата е завршена. Серверот потоа влегува во фаза на чекање одговор од клиентот. Доколку серверот испрати **certificate request** порака, клиентот е задолжен да испрати **certificate message** која го содржи дигиталниот сертификат на клиентот. Во спротивен случај клиентот треба да испрати **no certificate** аларм. Во овој чекор истотата мора да биде испратена **client key exchange** порака чија содржина ќе зависи од асиметричниот криптографски алгоритам, кој е договорен со **client hello** и **server hello** пораките. Доколку клиентот испрати дигитален сертификат кој има можност за дигитално потпишување, експлицитно се испраќа **certificate verify** порака која е дигитално потпишана, за да се потврди сертификатот. Во следниот момент, клиентот испраќа **change cipher spec** порака, и клиентот го копира новиот блок Cipher Spec во својот тековен Cipher Spec блок.

На крајот клиентот испраќа **finished** порака криптирана под новиот алгоритам и новите клучеви. Како одгово на ова, серверот ќе испрати своја **change cipher spec** порака до клиентот, во кој што момент истотака ќе го копира новиот блок Cipher Spec во својот тековен Cipher Spec блок. Откако ќе го заврши ова, серверот испраќа **finished** порака криптирана под новиот алгоритам новите клучеви воспоставени со **change cipher spec** пораката. Во овој момент, иницијализацијата на SSL сесијата е завршена, а серверот и клиентот веќе имаат договорен симетричен криптографски алгоритам како и заеднични тајни клучеви и може да се премине на размена на вистинските апликативни податоци.



Сл. 7.2: SSL Handshake

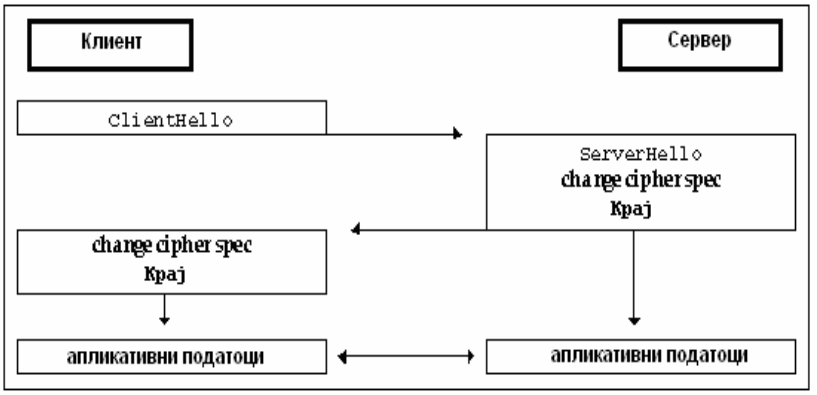
Во процесот кој го прикажавме на погорната слика, пораката ChangeCipherSpec не е дел од иницијализацијата на SSL протоколот, туку претставува посебна порака која може да се користи надвор од иницијализацискиот контекст. Оваа порака е издвоена за да може да се оптимизира самиот протокол во случај на повеќе кратки независни меѓу себе SSL-поврзувања, помеѓу ист клиент и сервер. Замислете си колку процесорски ресурси би се потрошиле, кога би требало да се извршува овој процес на иницијализација (SSL Handshake) - при секое HTTPS побарување од клиентот до серверот, а истите веќе споделуваат заеднички таен клуч.

За ваквите ситуации на повторно поврзување, или пак во случај на повеќе криптирани сесии во исто време, клиентот и серверот се договараат да го користат истиот клуч кој е договорен при првата иницијализација.

Самиот процес на разменување на пораките е прикажан на Слика 7.3 и се одвива на следниот начин:

- Клиентот испраќа **client hello** порака придружена со идентификациски број од сесијата која сака да се продолжи, или мултиплицира.
- Серверот проверува дали во својата база на опслужени сесии може да ја пронајде идентификацијата која ја праќа клиентот.
- Доколку серверот ја пронајде соодветната претходна сесија со клиентот во својата база, тој враќа **server hello** порака придружена со истата идентификација која е пратена од страна на клиентот.
- Потоа серверот испраќа **change cipher spec** со која означува барање за промена на криптографскиот метод според оној договорен во претходната сесија. Серверот потоа испраќа порака **finished** за да означи крај на договарањето на криптографски методи.

- Клиентот ја потврдува промената на криптографскиот метод со враќање на **change cipher spec** - порака проследена со **finished** за крај, што е проследена со почеток на размена на апликативните податоци.



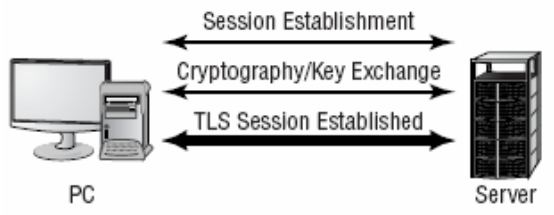
Сл. 7.3: SSL обновување на сесија

Секако дека останува опцијата серверот да го одбие продолжувањето на претходната сесија заради безбедносни причини (истечен временски рок на криптографски клучеви, грешен број за идентификација), што резултира со повторно целосно иницијализирање на SSL протоколот.

7.1.3 Transport Layer Security (TLS)

Transport Layer Security (TLS) е безбедносен протокол кој се проширува покрај SSL. Многу индустриски аналитичари предвидуваат дека TLS ќе го замени SSL во блиската иднина. Сликата 7.4 го покажува процесот на поврзување во TLS мрежата. TLS протоколот исто така се вика SSL 3.1, но и покрај името - не се однесува на SSL. TLS стандардот е поддржан со IETF.

Забелешка: Мислете за TLS како подобрена верзија на SSL. TLS се базира на SSL и треба да го наследи.



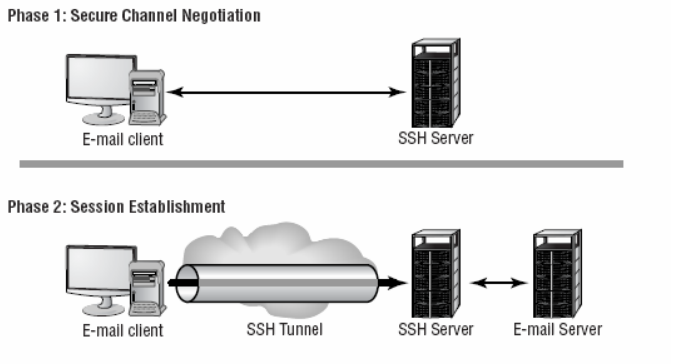
Сл. 7.4: Процес на TLS конекција

7.1.4 SSH

Secure Shell (SSH) е тунел протокол оригинално користен од страна на Unix системите. Сега е достапен за Unix и Windows околините. Процесот на

ракување помеѓу клиентот и серверот е сличен со процесот опишан во SSL. SSH примарно беше наменет за интерактивни терминални сесии.
Забелешка: SSH може да биде користен наместо постариот Remote Shell (RSH) кој беше стандард во светот на Unix. Може да се користи наместо rlogin и Telnet.

Сликата 7.5 го покажува SSH процесот на конектирање. Ќе приметите дека SSH конекцијата се постигнува во две фази: Првата фаза е безбеден канал за да се преговара конекцијата, и втората фаза е безбеден канал за да се постигне конекцијата.



Сл. 7.5: SSH конекција

Обезбедување на интерактивните корисници на Unix

Од вас се бара да го прегледате вашиот постоечки Unix систем и да го евалуирате за потенцијални безбедносни слабости. Неколку оддалечени корисници треба да пристапат кон Telnet и FTP можностите во вашата мрежа. Telnet и FTP конекциите ја праќаат информацијата без енкрипција. Како да го минимизирате ризикот за Telnet и FTP конекциите?
Имате неколку опции. Треба да размислите за користење на VPN конекции помеѓу оддалечените конекции и корпоративни системи. Едно решение би било да се овозможи SSH за вашите клиенти и инсталирање на вашите Unix сервери. Со тоа можете да дозволите FTP и Telnet конекција во безбедна околина.

7.1.5 HTTPS

Hypertext Transport Protocol Secure (HTTPS) е безбедна верзија на HTTP, јазикот на World Wide Web. HTTPS користи SSL за да го осигура каналот помеѓу клиентот и серверот. Многу е-бизнис системи користат HTTPS за безбедни трансакции. HTTPS сесијата се идентификува со HTTPS во URL-то и според клучот кој се покажува во веб пребарувачот.

Забелешка: HTTPS користи порта 443 предефинирано

7.1.6 S-HTTP

Secure Hypertext Transport Protocol (S-HTTP) претставува HTTP со гарантирана сигурност за пораките (додадена со користење на RSA или дигитален сертификат). HTTPS креира безбеден канал, S-HTTP креира безбедна порака. S-HTTP може да користи повеќе протоколи и механизми за заштита на пораката. Исто така овозможува интегритет на податоците и автентикација.
Забелешка: S-HTTP исто така го користи портот 443 предефинирано.

7.1.7 SSL подесувања во Windows Server 2003

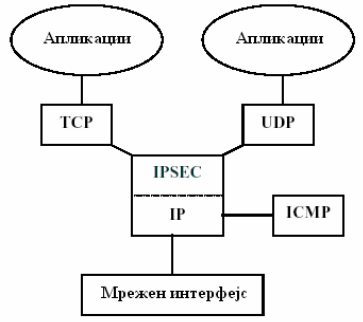
Оваа вежба бара тест машина (вон продукција) со Windows Server 2003. За да се конфигурира SSL порт, следете ги следниве чекори:

1. Отворете го Internet Services Manager со бирање Start > Administrative Tools > Internet Information Services (IIS) Manager.
2. Проширете го левиот панел сè додека вашиот веб сајт не стане опција. Десен клик на веб сајтот и изберете Properties од pop-up менито.
3. Изберете го табот за веб сајтот. Забележете го портот за SSL, ако не е напишан - внесете број.
4. Притиснете OK и излезете од Internet Information Services Manager.

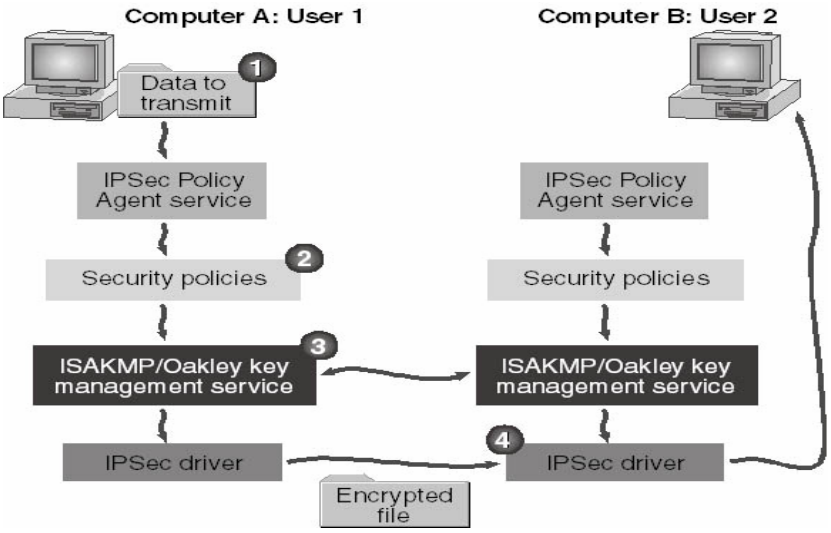
Ќе забележите дека полето за SSL портата е празно според предефинираните поставки, и било кој порт може да биде внесен тука – ова е разликата со некои претходни IIS верзии. Предефинираната вредност за SSL портата е 443; ако внесете друг број во тоа поле, клиентите мораат да го знаат тој број однапред, ако сакаат да се поврзат.

7.2 IPSEC

Бидејќи самата имплементација на SSL протоколот не е воопшто наивен и едноставен процес, направени се обиди, криптираната комуникација да се симне едно ниво подолу во мрежните слоеви, т.е. во транспортниот слој. Со имплементирањето на криптографски методи на ниво на транспорт, за апликативните протоколи е целосно транспарентна безбедноста на податоците кои се пренесуваат. За да се овозможи ова, дизајниран е нов протокол над IP протоколот, кој е наречен IPSec (IP Security, Слика 7.6).



Сл. 7.6: Местоположба на IPSec помеѓу мрежните протоколи

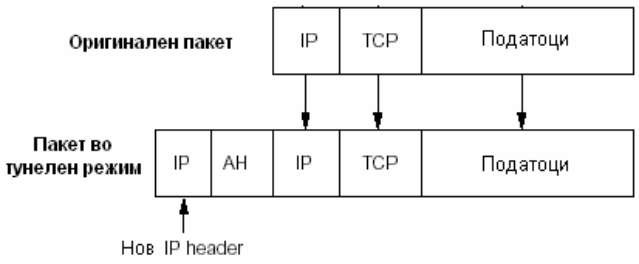


Сл. 7.7: Постапка на IPSec комуникација

Овој безбедносен протокол всушност требаше да биде само проширување на IPv6 протоколот, кој пак е проширување на постоечкиот IP протокол (IPv4). Бидејќи најголем дел Интернет инфраструктурата сеуште работи на IPv4, IPsec е портиран назад на стариот IP протокол. Идејата на IPsec е да се постигне автентикација, доверливост и интегритет на податоците на ниво на транспорт. Со тие цели, овој протокол нуди два режими на работа, тунелен и транспортен режим.

7.2.1 Тунелен режим на работа

Тунелниот режим на работа на IPsec протоколот претставува енкапсулирање на веќе постоечките IP пакети во нови пакети, врз кои се применети одредени криптографски методи.

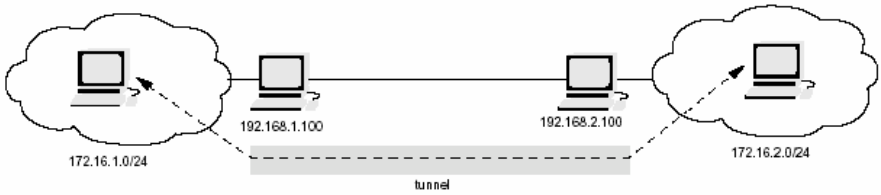


Сл. 7.8: Енкапсулирање на TCP/IP пакети во IPSec тунелен режим

Идејата позади тунелниот режим е да се воспостави криптирана транспарентна врска помеѓу два или повеќе рутери кои поврзуваат две различни мрежи. Значи при поврзувањето, криптирана врска се воспоставува само помеѓу влезно/ излезните точки во една мрежа, кои потоа ги енкапсулираат вистинските пакети во криптирани, кои потоа се транспортираат до другата мрежа каде што се

декриптираат. По декрипцијата пакетот изгледа сосем идентично како што би изгледал при нормален транспорт помеѓу двете мрежи.

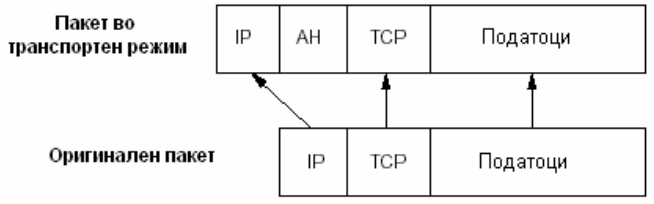
IPSec сепак не е толку совршен колку што изгледа на прв поглед. Криптираното тунелирање на транспортно ниво е одлична идеја, но сепак самата архитектура на IPSec-тунелирањето создава главоболки кога станува збор за преведување на мрежните пакети со помош на NAT.



Сл. 7.9: IPSec криптиран тунел помеѓу две мрежи

7.2.2 Транспортен режим на работа

Транспортниот режим од друга страна, ги штити само податоците во пакетот, и се применува врз оригиналниот пакет на кој само му се додава полето AH (Authentication Header), кое ќе го објасниме малку подоцна.



Сл. 7.10: TCP/IP пакет во IPSec транспортен режим

Транспортниот режим на работа е замислен како решение за криптиран транспорт помеѓу две фиксни точки. Значи транспортниот режим не е замислен да функционира транспарентно во систем од повеќе рутери, мрежи и огнени ѕидови, каде што сите заедно го контролираат однесувањето на криптираните мрежни пакети. Идејата во транспортниот режим е многу едноставна и практична - да се поврзат две работни станици криптирано.

Сл. 7.11: Поврзување на две работни станици во IPSec транспортен режим

IPSec протоколот, за заштита на интегритетот на IP пакетите, користи hash message authentication codes (HMAC). За секој пакет, како дел од AH заглавјето, IPSec пресметува HMAC, на основа на содржината на пакетот и симетричен таен клуч,

кои се влезните параметри на MD5 или SHA hash функциите. За да се заштити содржината на пакетотот, IPSec користи симетричен криптографски метод, најчесто DES, 3DES, AES.

За да се заштити протоколот од DoS (Denial of Service напади), IPSec користи метод наречен „Лизгачки прозорец“ што со други зборови значи, дека секвенцата на пакетите што пристигнуваат до еден IPSec уред - мора да биде во одреден круг на вредности, кои се нарекуваат „прозорец“. Прозорецот е лизгачки затоа што со секој нов пакет вредноста на прозорорец се поместува нагоре.

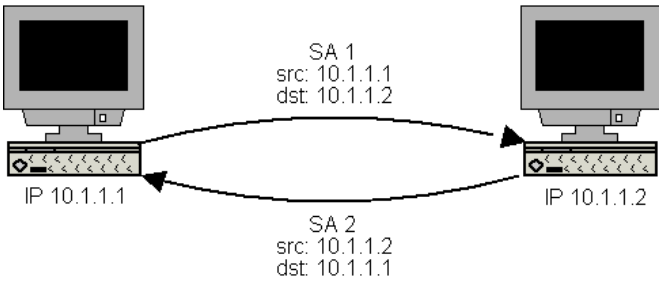
Криптираната комуникација помеѓу две точки се идентификува со помош на таканаречени безбедносни асоцијации (Security Association - SA), кои во себе ги содржат тајните клучеви, договорените криптографски алгоритми и IP адресите на точките на комуникација. Секоја поединечна IPSec SA во себе содржи:

- IP адреси на двете страни вклучени во комуникацијата. Се однесува на IP адресите на IPSec ниво, адресите на пакетите кои се тунелираат не се од интерес
- IPSec протокол на комуникација (AH, ESP, IPCOMP). IPSec користи свои под-протоколи за комуникација.
- Алгоритам и таен клуч, со кој се криптираат и декриптираат пакетите.
- Индексен број на SA (Security Parameter Index – SPI). SPI претставува 32-битен број кој единствено идентификува една SA.

Ова се само основните делови на една SA, кој единствено идентификува криптирана комуникација помеѓу две точки на IP ниво. Во зависност од имплементацијата на IPSec протоколот, SA структурите можат да содржат и дополнителни информации:

- IPSec режим на работа (тунелен, транспортен).
- Големина на „лизгачкиот прозорец“ за заштита од replay напади.
- Рок на траење на самата SA.

Секоја безбедносна асоцијација (SA), може да содржи само изворна и целна адреса на IP пакетите, со што сме ограничени на еднонасочна комуникација помеѓу двете точки. За да може да користиме целосно двонасочна комуникација, како на пример со TCP протоколот, тогаш мора да се послужиме со две безбедносни асоцијации од кои едната ќе служи за криптирање на излезните пакети, а другата за декриптирање на влезните.



Сл. 7.12: Двонасочна TCP комуникација со користење две SA

Бидејќи самите безбедносни асоцијации дефинираат само како да се заштити транспортот на податоци - за да може да одреди кој транспорт треба да се заштити - IPSec протоколот имплементира безбедносни полиси (Security Policy - SP), кои понатаму се чуваат во база да безбедносни полиси (Security Policy Database – SPD)

Секоја безбедносна полиса определува неколку основни параметри:

- Изворна и целна адреса на пакетите кои треба да се заштитат. Во транспортен мод ова се истите адреси од SA, но во тунелен мод може да се определи да се заштитат само дел од пакетите помеѓу двете мрежи, т.е. да се криптира комуникацијата само помеѓу одредени сметачи.
- Протокол (и порта) кои треба да се заштитат. Некои имплементации не дозволуваат фино гранулирање на нивоата на заштита, како на пример одредување на специфични протоколи или порти кои треба да се заштитат. Во општ случај, целата комуникација помеѓу две IP адреси е заштитена.
- Безбедносната асоцијација (SA) која ќе се користи за заштита на пакетите.

7.2.3 Барање на грешки во IPSec статистиките

Вежбата бара пристап кон сервер со Windows server 2003. За да го конфигурираме IPSec мониторингот треба да ги следиме следните чекори:

1. Отворете го System Monitor со бирање Start > Administrative Tools > Performance > System Monitor.
2. Кликнете на + иконата за да додадете бројачи.
3. За објект, изберете IPSec v 4 IKE.
4. Изберете го секој бројач кој ќе се појави во листата, потоа кликнете на Explain копчето за да дознаете што е можно да ви се покаже.
5. Додадете ги следниве бројачи: Total Authentication Failures и Total Negotiation Failures.
6. Притиснете Close.

Вие сега ги мониторирате грешките кои се јавуваат. На систем кој добро функционира, овој график треба да покажува дека нема активност. Секоја активност која се појавува индицира проблеми кај IPSec – от поради тоа што тој беше последен инсталиран, и тој треба да се прегледа темелно.

7.3 INTERNET KEY EXCHANGE (IKE) - IPSEC РАЗМЕНА НА КЛУЧ

Како и кај SSL протоколот, IPSec исто така има свој посебен протокол за иницијализирање на целиот крипто систем, размена на симетрични тајни клучеви и автентикација на потенцијалните комуникациски точки. Овој протокол се вика Internet Key Exchange (IKE) и е одговорен за создавање на соодветните Безбедносни Асоцијации (SA) кои понатаму ќе ја идентификуваат криптираната врска помеѓу инволвираните страни.

Самиот IKE протокол функционира во две фази:

1. Се воспоставува ISAKMP безбедносна асоцијација (*Association Key Management Security Association* (ISAKMP SA)).
2. ISAKMP SA од претходниот чекор се користи за воспоставување на вистинските IPSec безбедносни асоцијации.

Во првата фаза, кога се воспоставува ISAKMP SA, се врши и автентикација на двете страни. Процесот на автентикација на соговорниците може да се изврши по неколку различни стандарди:

- Предефинирани клучеви (Pre-shared Keys – PSK)
- Асиметрична автентикација – RSA, DHA
- X.509 сертификати
- Некои имплементации подржуваат и Kerberos

Фазата на формирање ISAKMP SA, може да биде извршена на два начини, агресивно или нормално. И на двата начини мора да се изврши автентикација и да се постави иницијалната ISAKMP SA, но агресивниот начин користи двојно помалку пораки за да ја постигне целта.

Агресивниот начин на воспоставување ISAKMP SA, во случај на користење на предефинирани клучеви, е подложен на „човек во средина“ тип на напади, иако е ова единствениот начин на функционирање на агресивниот начин, бидејќи нормалниот начин не подржува користење на предефинирани клучеви со непознати соговорници. Агресивниот начин исто така не подржува заштита на идентитетот, и го транспортира идентитетот во чист текст. Агресивниот начин најчесто се користи со веќе познати соговорници со кои предефинираните клучеви не се проблем.

Во втората фаза, IKE протоколот е задолжен од иницијалната ISAKMP SA да воспостави вистински SA за секоја еднонасочна врска. Најчесто постои само еден ISAKMP SA кој се користи во фазата на иницијализација, кој подоцна ги воспоставува вистинските SA (најмалку два).

7.4 МЕНАЏМЕНТ СО КЛУЧЕВИТЕ

Менаџирањето на клучевите се однесува на процесот на работа со клучевите од моментот кога се креирани до моментот кога се повлечени или уништени. Менаџирањето на клучевите ги вклучува следниве активности:

- Централизирани vs. децентрализирани креирања на клучеви
- Чување и дистрибуција на клучеви
- Фонд на клучеви
- Истекување на клучевите
- Отповикување на клучевите
- Суспендирање на клучевите
- Поправка на клучеви и архивирање
- Обнова на клучеви
- Уништување на клучеви
- Користење на клучеви

Забелешка: Низ оваа секција, терминте сертификат и клуч ќе бидат користени со меѓусебна замена. Сертификатите содржат клучеви кои овозможуваат безбедност.

Терминот животен циклус на клучот ги опишува стадиумите кои клучот ги поминува во неговиот живот. Можете да го замислите тоа како ситуација - од раѓање до гроб. Со користење на овие релации во рамки на животен циклус, евалуацијата на секоја фаза на користењето на клучот - од креирањето до неговото уништување, станува полесна. Ако некој аспект од животот на клучот не се работи како што треба, целиот безбедносен систем може да стане нефункционален и компромитиран.

Менаџирањето на клучевите е еден од основните аспекти на ефективен криптографски систем. Клучевите, како што можеби се сеќавате, се единствени лозинки или кодови кои се користат за енкрипција или декрипција на порака. Можете да го сметате клучот како за една од примарните компоненти на сертификатот. Токму заради тоа, овие термини се користат заедно. Сертификатите се користат за транспорт на клучевите помеѓу системите. Следните секции ги опишуваат централизираните и децентрализираните генерирања на клучеви, како и чувањето и дистрибуцијата на клучевите. Други аспекти од менаџирањето на клучевите се исто така покриени.

7.4.1 Централизирано и децентрализирано генерирање на клучеви

Генерирањето на клучеви (креирањето на клучот) е прв важен чекор во процесот на работа со клучевите и сертификатите. Сертификатите се еден од примарните методи користени за испорачување на клучевите на крајните корисници. Должината на клучот и методата користена за креирање на клучот, исто така влијаат на безбедноста на системот кој се користи. Безбедноста на клучот се мери по тоа колку е тешко да се пробие клучот. Колку повеќе време е

потребно за пробивање на клучот, толку тој се смета за посигурен. Според RSA, потребни се 3 милиони години и буџет од 10 милиони долари за да се пробие клуч со должина од 1024 бита. Количеството време кое е потребно за пробивање на клуч од 2048 бита е непресметливо. Секако, овие бројки се базираат на претпоставката дека алгоритмот е сигурен и други методи на напад не би можеле да го пробијат алгоритмот или клучот.

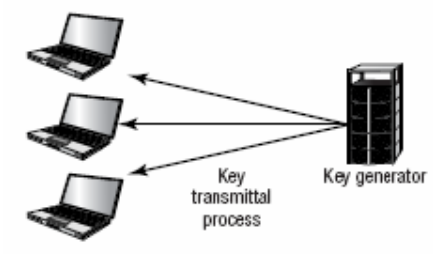
Забелешка: Познат метод кој се користи за генерирање на клучеви - креира многу големи прости броеви. Прости броеви се оние броеви кои се делат само со себе и со 1, како на пример 1, 2, 3, 7, 11, 13, 17. Пресметувањето на прости броеви бара работа. Повеќето системи користат софистицирани методи на апроксимација за да пресметаат прост број, наместо да го пресметуваат директно. Ако методата е погрешна, броевите можеби нема да бидат прости, па со тоа ќе биде полесно да се откријат.

Една битна работа е - каде да се креира клучот. Дали да се генерираат на централна машина или во децентрализирана околина? Третиот метод кој се користи за генерирање на клучеви се нарекува split generation system, кој е комбинација од централизиран и децентрализиран процес.

Централизирано генерирање на клучеви

Централизираното генерирање на клучеви си дозволува процесот да ги користи големите системи. Алгоритмите за генерирање на клучеви знаат да бидат екстремно напорни врз процесорите. Со користење на централизиран сервер, процесот може да се менаџира во еден голем систем. Сепак проблемите се појавуваат кога клучот се дистрибуира. Како може да се транспортира до крајните корисници без да се компромитира безбедноста?

Сликата 7.13 покажува процес на централно генерирање. Во овој пример сите физички ресурси се на една единствена локација, под централизирана контрола. Централизираното генерирање има предност што дозволува да додатните функции за менаџирање - да бидат централизирани. Главната негативност е тоа што процесот на архивирање и чување може да биде ранлив на напади против едната централна точка, наместо на цела мрежа. Сигурноста, безбедноста и архивирањето можат да се адресираат, ако системите се поставени како што треба со процедури и политики.

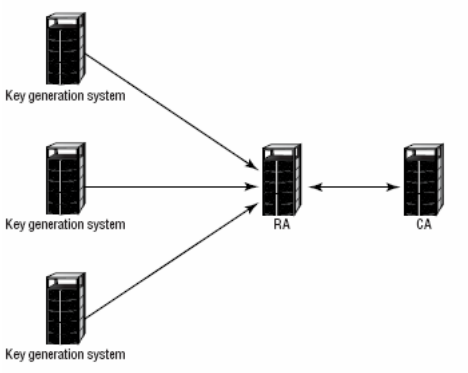


Сл. 7.13: Централизирано генерирање на клучеви

Децентрализирано генерирање на клучеви

Децентрализирано генерирање на клучеви му дозволува на процесот на генерирање на клучеви да се постави во рамки на организацијата. Предноста на овој метод е дека ви дозволува да работите децентализирано и ризикот е поделен. Овој систем не е ранлив на напади на една точка. Децентрализираното генерирање го решава проблемот со дистрибуирањето, но креира проблем за чување и менаџирање.

Сликата 7.14 го покажува децентрализираниот систем. Во оваа ситуација, загубата на еден генератор на клучеви не ја пореметува целата мрежа. RA на сликата се однесува на авторитетот за регистрација, а CA се однесува на авторитетот за сертификација.



Сл. 7.14: Децентрализирано генерирање на клучеви

Споредба со Split-System

Многу системи, вклучувајќи го и PKI системот, бараат користење на split системот. Во овој систем, централниот сервер ги креира клучевите за енкрипција. Дигиталните потписи и клучевите се креираат кај клиентот, или на смарт картичката.

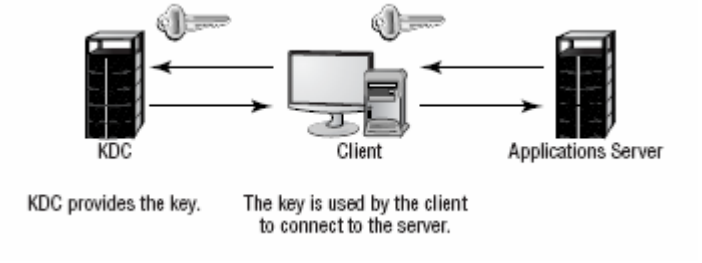
Чување и дистрибуција на клучеви

Според тоа каде и како клучевите се чуваат, се одредува начинот на дистрибуција. Типично тоа се врши со користење на Key Distribution Center (KDC), како што се прави во Kerberos, или со користење на Key Exchange Algorithm (KEA), како што се прави во PKI.

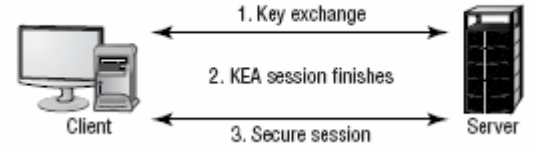
Забелешка: За да функционира правилно Kerberos, временската синхронизација мора да работи коректно. Ако часовниците не покажуваат точно време, проблеми ќе се појават при компарирање на временските печати и автентикацијата.

KDC е сервис или сервер кој ги чува, дистрибуира, и одржува клучевите на криптографските сесии. Кога системот сака да пристапи до некој сервис кој користи Kerberos, барањето се прави преку KDC. KDC генерира клуч на сесијата и го извршува процесот на конектирање на овие два системи. Предноста на овој процес е што кога еднаш ќе се имплементира, станува автоматски и не бара дополнителни интервенции. Главната негативност е тоа што KDC е една точка, ако е нападнат тогаш целиот систем може да се компромитира. Сликата 7.15 го покажува KDC како креира сесија помеѓу два системи.

KEA процесот работи малку поразлично од KDC. KEA преговара за таен клуч помеѓу двете страни, тој клуч е краткорочен и за една употреба. KEA процесот не треба да се користи за транспорт на јавни и приватни клучеви. Сликата 7.16 го илустрира KEA процесот. Процесот се прекинува штом клучот успешно ќе се префрли. Заштитата на клучевите од неавторизиран пристап, додека ги правите достапни за авторизиран персонал, е важна. Процесот може да користи мерки за физичка безбедност како заклучени плакари и сефови, а може и да инволвира софтвер како што е Kerberos и PKI.



Сл. 7.15: KDC процес во Kerberos околина



Сл. 7.16: KEA процес

Забелешка: Физичката заштита вклучува уреди кои се поставаат под клуч. Значи кабинети и сефови.

Клучевите можат да бидат хардверски или софтверски уреди. Како пример за хардверски уред може да се земе смарт картичката. Софтверските клучеви се генерираат од страна на CA-ориентираните системи како што е PKI. Без оглед дали се хардверски или софтверски - клучевите се есенцијални за безбедносните системи.

Заштитата на клучевите е тежок процес. Јавните клучеви не бараат заштита; тие само бараат заштита на интегритетот. Приватните клучеви бараат комплетна заштита. Откривањето на приватен клуч во симетричен или јавен/приватен клуч

систем потенцијално го компромитира системот. Ако го има приватниот клуч - напаѓачот може да ја чита комплетната комуникација. Следнава секција накратко го дискутира приватниот клуч и неговата заштита, како и заштитата на серверот, поради тоа што и двете работи се битни за безбеден систем.

Заштита на приватните клучеви

Физички приватните клучеви треба да се чуваат под блиска супервизија. Ако е возможно, различни клучеви треба да се користат за отворање на локацијата за чување, и два клуча никогаш не треба да се чуваат заедно. Ако двајца луѓе се одговорни за чување на клучевите - и двајцата треба да се присутни на отворањето на локацијата.

Серверите за клучеви исто така се место за безбедносни проблеми, и од страна на контрола на пристап, и од аспектот наречен физички пристап. Најголемите проблеми во овој тип на заштита се лоцираат во физичката безбедност, или се човечки грешки. Осигурете се дека клучевите се добро чувани.

Забелешка: Познато е дека во никакви услови не треба да се дава личниот клуч. Ако го дадете ја загрозувате вашата гаранција дека само вие сте одговорен за вашите податоци и нивната безбедност.

7.4.2 Користење на Фондовите за клучеви

Овој систем ги чува клучевите за потребите на законот. Ако постои криминална истрага, агентите со налог за претрес можат да пристапат и да бараат записи во рамките на налогот. Генерално, системот за архивирање ќе го овозможи потребниот пристап. Овој систем се води посебно токму поради неговата улога во полициските истраги.

Забелешка: Фондот за клучевите се однесува на систем или организација која ги чува клучевите за понатамошен пристап.

Еден од предложените методи за работа со key escrow, инволвира чување на информацијата за клучевите кај трета страна, која се нарекува фонд за клучеви. Оваа агенција ќе овозможи информација за клучевите само кога ќе добие наредба од судот. Генерално, фондот за клучеви се води од системот за архивирање на клучеви.

Забелешка: Во почетните енкрипциски системи понудени од страна на NSA за цивилна употреба, NSA работеше како key escrow агенција. Системот се викаше Clipper, и не беше широко прифатен од индустријата. Key escrow контраверзата е една од главните причини за нејзиниот слаб пристап.

Key escrow системите може да земат учество во процесот на поправка на клучевите. Неколку владини агенции сакаат да имплементираат правила за задолжителен key escrow. Задолжителниот key escrow ќе им дозволи на полициските агенции да истражуваат корисник на системот без тој да знае. Многу индивидуи и организации го гледаат ова како напад на приватноста, и тие се борат

против задолжителното постоење на овој систем поради тоа што ја нарушува личната слобода. Овој процес е покриен подетално во секцијата "Враќање и архивирање на клучевите" подолу во оваа глава.

7.4.3 Истекување на клучевите

Датумот на истекување на клучот кажува кога клучот не е повеќе валиден. Нормално, клучот е запечатен со датум: тоа значи дека по специфичниот датум - тој станува некорисен. Нов клуч или сертификат нормално се издава пред датумот на истекување. Клучевите со датуми на истекување работат слично како кредитни картички кои истекуваат. Обично издавачот на картичката испраќа нова на клиентот, пред да истече старата.

Повеќето апликации кои работат со клучеви и сертификати го проверуваат датумот на истекување и му јавуваат на корисникот дека клучот е истечен. PKI му дава на корисникот можност за прифаќање и користење на новиот клуч.

7.4.4 Отповикување на клучевите

Клучевите се отповикуваат кога тие се компромитирани, ако пропаднал автентикацискиот процес, кога луѓето се префрлаат, или ако се случи некој друг безбедносен ризик. Отповикувањето на клучот го чува клучот од погрешно користење. Отповикан клуч се претпоставува дека е расипан или можеби компромитиран.

Аналогијата со кредитните картички постои и тука. Замислете дека кредитната картичка е украдена од клиентот. Оваа картичка, за своите намери и цели, е сертификат. Продавачот може да ја искористи шансата и да ја прифати картичката, или може да верификува дека картичката е точна со проверување на картичката низ машинката за верификација за да се провери статусот. Ако картичката е пријавена како украдена, авторизацискиот процес ќе го одбие плаќањето.

Системите како PKI користат CRL за да направат проверки на статусот на отповиканите клучеви. Отповикувањата се перманентни. Штом сертификатот е отповикан, тој не може да биде повторно користен: мора да се генерира нов клуч и тој да се користи.

7.4.5 Суспендирање на клучевите

Суспендирање на клучевите е привремена ситуација. Ако вработениот земе отсуство, неговиот клуч може да се суспендира додека тој не се врати назад на работа. Оваа привремена суспензија ќе осигура дека клучот нема да биде употребуван за време на отсуството. Суспензија исто така може да се појави ако голем број на промашени автентикации или ненормални активности се случуваат. Привремената суспензија ќе им даде време на администраторите и менаџерите време да видат што се случува.

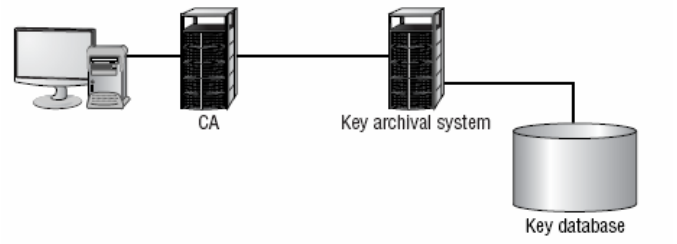
Проверувањето на статусот на суспендираните клучеви се постигнува со проверување во серверот за сертификација, или со користење на други механизми. Во PKI системот, CRL се проверува за да се одреди статусот на сертификатот. Овој процес може да се одвива автоматски или мануелно. Повеќето системи за менаџирање на клучеви или сертификати овозможуваат механизам за репортирање на статусот на клучот или сертификатот.

Забелешка: Системите за менаџирање на клучевите ги користат истите генерални процеси како кога се проверува статусот на клучевите. Треба да се прави разлика помеѓу проверката на статусот за суспензија и отповикувањето. Главната разлика е дека отповикан клуч не може да се употребува повторно, додека статусот на суспендиран клуч може да се менува за да дозволи повторна употреба на клучот. Штом клучот е отповикан - нов клуч се бара.

7.4.6 Враќање и архивирање на клучевите

Еден од проблемите со системите кои се базирани на клучеви е тоа што постарите информации, освен ако се процесираат со нов клуч, можат да станат непристапни. На пример, ако имате две години стар документ во вашиот систем и ако сеуште е енкриптиран, дали ќе се сетите кој клуч се користел за негова енкрипција пред две години? Ако сте како повеќето луѓе, нема да се сетите. Ако не можете да ги декриптирате податоците, документот е неупотреблив.

За да се справите со овој проблем, архивирањето на старите клучеви е есенцијално: Секогаш кога корисник или генератор на клучеви креира или издаде клуч, клучот мора да биде пратен во системот за архивирање на клучеви. Ова најлесно се прави на сервер кој нуди безбедно чување. Постарите клучеви можат да се чуваат и повлекуваат кога е потребно. Сликата 7.17 покажува која е релацијата со CA. Овој сервер бара силна физичка безбедност и исто таква сигурност кај системот за генерирање на клучеви.



Сл. 7.17: Систем за архивирање на клучеви

Враќањето на клучевите е битен дел на енкрипциискиот систем. Информацијата која се чува со користење на постари клучеви, ќе биде непристапна со користење на нов клуч. Враќањето на клучевите дозволува информацијата да биде пристапена иако е енкриптирана со постари клучеви. На пример, враќањето на клучевите може де се користи за враќање на информации од бивш работник. Три различни фактори мораат да се земат во предвид кога се имплементира систем за архивирање на клучеви:

Моментални клучеви - Моменталните клучеви се оние клучеви кои се користат во сегашно време. Тие не биле повлечени. Ако моментален клуч се изгуби, уништи или оштети, треба да се направи начин за враќање на клучот за да не се изгубат податоците. Смарт картичката исто така може да се оштети, и мора да се воспостави метод за да се врати каричката со информации за клучот. Ако моменталниот клуч не може да се врати, сите информации кои биле енкриптирани со тој клуч ќе бидат недостапни. Ова губење на податоци може да биде скапо. Некои понови системи дозволуваат креирање на виртуелни смарт картички кои можат да се користат привремено за да иницијализираат нова картичка. Оваа картичка ќе биде добра само за краток временски период, на пример до крајот на смената. Овој процес треба да биде релативно лесен за администраторите да го работат, поради тоа што луѓето понекогаш забораваат да ги носат своите идентификациски уреди на работа.

Минати клучеви - Минатите клучеви скоро истекле и не се веќе моментални. Вработен кој доаѓа на работа денеска можеби и не знае дека клучот истекол сè додека не проба да го отвори вчерашниот е-мејл. Во зависност од тоа што содржи вчерашниот е-мејл - тоа може да биде катастрофа. Многу нови системи чуваат копии од скоро истечени клучеви во своите системи: овој систем може да ги чува последните два или три клуча. Ако нема локален чувар, тогаш реставрација на клучот ќе се бара од системот за архивирање. Повторно, ова може да бара рачна интервенција од администраторот.

Архивирани клучеви - Архивираните клучеви беа дискутирани порано. Треба да очекувате дека од време на време постари пораки ќе бидат потребни. Ова е посебно случај кога има судски спор - за време на откривањето, сите записи, кореспонденција и меморандуми мора да се презентираат на адвокатите ако се побара. Ако не сте во можност да го сторите тоа, може да бидете казнети од судот. Замислете да треба да пристапите до сите пораки и податоци од одреден оддел за последните пет години. Ова може да отвори многу работа.

Многу системи за обнова и архива го користат системот M од N за пристап. Овој метод, едноставно вели дека за да се пристапи на серверот - ако N администратори имаат можност да го извршат процесот, M од тие администратори мораат да се автентицираат за пристапот да се дозволи. Ова може да бара од администраторот физички да биде присутен.

Забелешка: Не се чудете на m од n нотацијата. Двете букви се само пример за вистинските броеви кои се користат (3 од 6, 8 од 10 и така натаму).

Типична M од N контрола може да вели дека шест луѓе имаат пристап до серверот со архивите и дека минимум тројца мора да бидат присутни за да се постигне пристапот. Во оваа ситуација m = 3 и n = 6. Оваа ситуација обезбедува дека никој не може да го компромитира безбедносниот систем.

Важно е да се запамети дека системот за архивирање на клучеви ја содржи комплетната историја на сите клучеви кои се издадени од вашиот систем. Оваа информација исто така ги содржи и сегашните клучеви. Пристапот кон овој

сервер е еквивалентен на откривањето на Rosetta Stone на вашата организација. Напаѓач со оваа информација има комплетен и нерестриктивен пристап кон секоја информација на вашата мрежа.

7.4.7 Обновување на клучевите

Обновувањето на клучевите го дефинира процесот на употребување на клучот по неговата планирана дата за истекување. Клучот може да се реиздаде за одредено време во оваа ситуација. Овој процес се вика key rollover. Во повеќето случаи, процесот се прави за одреден временски период. Што би се случило ако организација се најде во ситуација каде roll over не смее да се случи. Многу системи овозможуваат начини за да се обноват постоечките клучеви, наместо да се прави rollover.

Генерално, обновувањето на клучевите е лоша пракса и не треба да се изведува освен во безизлезни ситуации. Што подолго се користи клучот, поголема шансата да се компромитира. Ако се случи земјотрес во вашата околина и вашата зграда е недостапна две недели, ќе сакате постоечките клучеви да се користат сè додека побитните работи не се решат.

7.4.8 Уништување на клучевите

Ова е процес на уништување на клучевите кои станале невалидни. На пример, електронскиот клуч може да се избрише од смарт картичка. Во постарите системи со механички клучеви, клучевите физички се уништувале се чекан. Многу симетрични енкрипциски системи користат дедицирани уреди за носење на клучевите за енкрипција. Овие клучеви физички се испорачуваат до локацијата која користи систем за енкрипција. Старите клучеви се земаат и се уништуваат.

Забелешка: Секогаш запаметете дека симетричната енкрипција користи ист клуч за енкрипција и декрипција на податоците (основна слабост на системот е делењето на клучот со други). Асиметричната енкрипција користи два клуча: еден за енкрипција и друг за декрипција на податоците.

Сценарио од вистинскиот живот - што да правиме со заборавените програмери?
Работите како мрежен администратор во компанија за развој на софтвер. Претседателот на компанијата читал весници, и се замислил за индустриската шпионажа. Сака да имплементира систем кој ќе бара користење на смарт картички за пристап и автентикација на сите вработени. Вашата компанија користи бецови за вработените веќе неколку години, и сега треба да имплементирате понова технологија. Сте забележале дека вашите развивачи на софтвер работат многу часови и понекогаш ги забораваат бецовите. Оваа не е голем проблем, поради тоа што вие можевте да издадете привремени бецови кога ви требаат. Како ќе се справите со вработен кој ќе ја заборави смарт картичката дома? Можете да имплементирате систем кој дозволува виртуелни смарт картички да се креираат за кратко време. Супервизорот може да авторизира издавање на виртуелни смарт картички. Вие треба да се грижите дека - само луѓе од доверба ќе можат да авторизираат издавање.

Без оглед дали користите физички клучеви или софтверски ориентирани системи, старите клучеви мора да се уништат на таков начин на кој ќе бидете сигурни дека нема да паднат во раце на неавторизиран персонал.

Сценарио од вистинскиот живот - продавање на старите компјутери на фирмата
Од вас е побарано да ги одредите компјутерите што вашата компанија треба да ги ликвидира и да утврдите дали се спремни да се продадат. Кои чекори треба да ги преземете за да се осигурете дека нема да се случи неавторизиран пристап кон информациите? Треба да сте загрижени за две теми во овој случај. Прво, треба да сте сигурни дека сите корпоративни записи, софтвер и други осетливи информации се избришани од системот. Второ, треба да бидете сигурни дека специјалните уреди за пристап и енкрипциските системи се исто така тргнати. Енкрипциските системи можеби ги чуваат клучевите во скриени делови на дисковите. Како главна пракса - дисковите треба да се форматираат, со тоа ги спречуваме осетливите информации да излезат надвор.

7.4.9 Резиме

Во оваа глава, научивте за стандардите, агенциите, и асоцијациите кои се вклучени во криптографија. Исто така научивте за стандардите поврзани со криптографските системи и менаџментот на клучевите и нивниот животен циклус. Неколку владини агенции се задолжени за преглед на безбедноста и енкрипцијата. NSA и NIST се двете засегнати со владините стандарди за енкрипција. NIST примарно се занимава со не воени стандарди; NSA/CSS се занимава со воени апликации.

IEFT, ISOC, ITU и IEEE се индустриски асоцијации кои се занимаваат со различни аспекти на безбедноста. Од нив не се бара да ги координираат нивните активности, но како генерално правило тие го прават тоа. IEEE публикува многу стандарди и упатства кои се прифатени од многу производители.

Серијата на состојби кои се појавуваат како процес на менаџирање на клуч или сертификат се вика животен циклус на клуч/сертификат. Животниот циклус ги потенцира сите големи аспекти на животот на еден клуч или сертификат од моментот кога е креиран до моментот кога е повлечен. 10 состојби постојат во еден животен циклус на клучот:

- Креирања на клучеви
- Чување и дистрибуција на клучеви
- Фонд на клучеви
- Истекување на клучевите
- Отповикување на клучевите
- Суспендирање на клучевите
- Поправка на клучеви и архивирање

- Обнова на клучеви
- Уништување на клучеви
- Користење на клучеви

Треба да ги земете во предвид сите состојби кога имплементирате клучеви или сертификати во вашата организација. Ако не успеете како што треба да ги поставите сите овие работи, можете да го компромитирате процесот или да си отворите повеќе работа. Ако не ги следите процесите, целиот систем може да биде ранлив. Треба да проценете дали ќе користите централизиран или децентрализиран систем за генерирање на клучеви. Централизираниот систем може да креира инка или една точка за пад на системот. Децентрализираното генерирање на клучеви може да креира администраторски и безбедносни проблеми. Повеќето модерни имплементации ги поддржуваат двата типа на генерирање на клучеви.

Квалитетното чување на клучевите е критично за одржување на безбедна околина. Клучевите треба да се чуваат во цврсти системи или под физички надзор. Можат да се чуваат во шкафови или на сервери. Проблемите со чувањето на клучевите се обично резултат на човечка грешка. Дистрибуцијата на клучевите и нивниот транспорт се безбедносни предизвици. Приватните клучеви никогаш не треба да се испраќаат преку комуникациска мрежа; out – of –band трансмисијата треба да се користи за нивна дистрибуција. Ако постоечкиот клуч е компромитиран, новиот клуч исто така ќе биде компромитиран. Јавните клучеви се наменети за циркулација, сепак нивниот интегритет мора да се чува.
Фондовите на клучевите претставуваат процес во кој клучевите им се достапни на органите на законот кога вршат истрага. Клучевите таму се чуваат и се даваат само на авторизирани лица. Клучот истекува кога ќе дојде до крајот на својот животен циклус. Типично тој момент е врзан со датум. Истечен клуч може да се ре-издаде со процес на роловер, но тоа се смета за лоша пракса. Колку повеќе се употребува еден клуч - толку е поверојатно да биде пробиен.

Кога клуч или сертификат се идентификува како корумпиран, компромитиран, или загубен, тој може да биде отповикан. CRL ги информира крајните корисници и CA дека сертификатот е отповикан. Штом е отповикан - сертификатот веќе не може да се користи. Клучевите се суспендираат за да се оневозможат за одредено време. Суспензијата може да се направи поради тоа што клиентот е болен или земал отсуство. Клучот може да се врати во нормала и да се користи повторно.

Враќањето на клучот е можност да се врати изгубен клуч или да се користи претходно активен клуч. Три типови на клучеви се разгледуваат во овој процес: моментални клучеви, поранешни клучеви и архивирани клучеви. Организацијата може да користи систем за архивирање за да врати информации кои биле енкриптирани со постари клучеви. Овие системи обично користат типови на контрола на пристап каков што е M од N пристапот, кој бара да дел од луѓето бидат присутни за да се пристапи до архивата на клучеви. Системот за архивирање обично работи заедно се системот за генерирање. Уништувањето на клучевите е процес на правење на клучевите неупотребливи. Физичките клучеви мора физички да се уништат. Софтверските клучеви и смарт картиците треба да се избришат.
□

8. БЕЗБЕДНОСТ НА БЕЗЖИЧНИ МРЕЖИ

Разгледувањето на сигурноста на безжичните комуникациски системи предизвикува дискусија за тоа кои сигурносни закани се однесуваат на безжичните системи. Применувањето на концепти за безжична сигурност кај мрежите и мрежната опрема е комплексен процес. Развиени се неколку различни таксономии за подобро да им се претстави на дизајнерите што сè треба да содржи во себе еден сигурносен систем кога станува збор за обезбедување сигурност за безжични мрежи, опрема и информациони операции. Од посебен интерес се моделот на Waltz наречен Information Warfare и придонесот на Shannon во теоријата на информации; заедно, даваат рамка за проценка на ефективноста на различно дизајнирани системи. Моделот Information Warfare помага во дефинирањето на релациите при разгледувањето на сигурноста на безжичен комуникациски систем. Сепак, неопходно е интегрирање на концептите со посебни мерки – криптографски, мерки против попречување на сигналот (anti-jamming, A/J), ниска веројатност за детекција (low probability of detection, LPD) и нивно применување во комерцијални или воени операции на начин кој ќе помогне во формирањето на финалниот дизајн. Понатаму, Шеноновите информациски концепти и релациите на ризик на Ryan се користат за да се дефинира контекстот на информациона сигурност и релативната вредност на евентуално нејзино компромитирање или загуба.

8.1 ПРИВАТНОСТА КАЈ БЕЗЖИЧНИТЕ МРЕЖИ

Правилата можат да влезат во судир со приватноста исто како што можат да ја заштитат. Приватноста отсекогаш била грижа на модерното општество; неотуѓиво право е да се чува приватноста на поединецот во однос на други индивидуи или владини институции. Во последните години, чувствителноста во врска со приватноста расте и покрај широката употреба на технологија која е способна за прекршување на правилата за приватност на кои сме навикнале. Причините за спуштањето на нивото на толеранција можат да се бараат на повеќе места, од филмови во кои се демонстрира како некој го следи секој ваш чекор до владини програми за следење и пресретнување на e-mail и SMS пораки.

Сепак, барањата за заштита на приватноста не се без причина; во нашиот виртуелен свет имаме online банкарство, плаќаме сметки online, купуваме online но сите овие погодности имаат и своја цена: мораме да ги делиме своите витални информации со виртуелни личности. Број на кредитна картичка, датум на раѓање, матичен број се само неколку од податоците кои не може да се заклучат во фиока – тие се “отворени” тајни во виртуелниот свет. Проблемите на приватноста не се однесуваат само на безжичната технологија но фасцинира начинот на кој безжичното поврзување ги менува нашите погледи во однос на потребниот степен на приватност. За подобро чување на податоците “надвор” од канцеларијата, мора да се откажеме од некои поволности кои ги нуди безжичната конекција. Еве неколку конкретни решенија во таа насока:

- Ограничување на употребата на безжични уреди.

- Подобрување на сигурноста и приватноста со додатни мерки или преку формулација на посебни полиси и процедури.
- Продолжување на работа со безжични мрежи секогаш и секаде ризикувајќи пресретнување на податоците.

Постоечките закони не се ефективни во заштитата на приватните комуникации. Безжичните телефони можат да послужат за прислушување на туѓи разговори ако се постават на истиот канал. Но ако не може да се докаже дека прислушувањето било намерно, не можат да се преземат конкретни мерки. Потрошувачите го кажуваат бројот на кредитната картичка по мобилен телефон - без никаква гаранција дека нема да биде пресретнат и злоупотребен. За жал, не постои инстант решение на ваквите проблеми. За ублажување на ваквите опасности некои компании нудат scrambling услуги, но и таа бариера е неефективна против дигиталните експерти ако навистина сакаат да ги добијат податоците. Сепак, решението не е само во чекањето на технолошки подобрувања кои би ја подобриле состојбата. Илјадници мобилни телефони се продаваат секоја година за да му ја овозможат на општеството посакуваната удобност. Прашањето е дали корисниците, доколку би постоел метод на апсолутно осигурување на приватноста, би сакале да платат повеќе за сигурноста на телефоните. Постојат повеќе енкрипциски решенија (најчесто додатоци кои се приклучуваат на телефон или факс), но сеуште не се широко прифатени поради значителната цена и нискиот квалитет (QoS). Како и да е, енкрипцијата на безжични телефони било да ја нуди телефонската компанија или произведувачот е едно од решенијата кои можат да се покажат корисни.

8.1.1 Јавноста и приватноста

Употребата на безжични уреди води кон големи измени во тоа како и кога ќе се одвиваат работите и како телефонските компании ќе ги опслужуваат клиентите во иднина. Како што безжичната врска еволуира од секундарен начин на комуникација во примарен, исто така го менува и начинот на кој се изведуваат како личните така и деловните работи. Се намалува потребата од удвојување на опремата и системи на фиксни локации; всушност, безжичните мрежи и уреди ја намалуваат потребата од поставување на временски и просторни граници помеѓу личните и деловните активности. На пример, кога вработените ги напуштаат своите канцеларии немаат опција за константна врска со канцеларијата. Може да носат податоци во лаптоп или PDA но за пристап до деловните податоци мора да се приклучат на корпоративната мрежа. Во светот на безжичните мрежи, на вработените би им се овозможила вистинска мобилност.

Потребни се нови стратегии и бизнис модели за одржување на граница помеѓу жичени и безжични медиуми, како и за одделување на личното од професионалното. Безжичната врска овозможува праќање, примање и одговарање на деловни предлози на пат, во банка, во продавница, во парк, на велосипед, во брод итн. На крајот, безжичните мрежи би додале повеќе слободно време и со тоа би го подобриле квалитетот на живот обезбедувајќи навистина флексибилно работно време. Може да се интегрира приватниот живот со деловниот и да се намалат конфликтите меѓу нив. Безжичните мрежи навлегуваат во сите области: интересно е да се спомене дека болничката индустрија го прифати IEEE 802.11

стандардот побрзо отколку големите корпорации. Многу хотелски ланци овозможуваат безжичен пристап до локална мрежа со самото пријавување во нив. Аеродроми, ресторани па дури и кафетерии исто така обезбедуваат безжичен пристап до Интернет и LAN за потребите на нивните клиенти. Лошата страна на целиот овој пристап е дека тоа што порано било доверлива информација сега е достапно за јавноста.

8.1.2 Степени на сигурност

Пред воопшто да се одреди политиката на дејствување и enterprise решение, мора да се вкалкулираат сите ризици. Најчесто прашањето не е дали може туку дали треба да се имплементира. Нивото на ризик најпросто кажано би било еднакво на заканата помножена со ранливоста во однос на контра-мерките кои би можеле да се преземат. Констатацијата дека сигурноста на безжичниот систем или сигурноста на било кој информациски систем е доволна - би била наивна; сепак, може доста да се стори за намалување на безбедносните ризици до прифатливо ниво. Доколку се изработува комплетно безжично деловно решение, треба да се сторат напори во него да се вградат и безбедносни механизми.

Сигурносните стандарди ги обезбедуваат правилата и насоките на деловните процеси во согласност со развојот на самиот систем, управувањето со конфигурирањето, пристапот итн. Повеќе организации и владини агенции работат на формирањето на сигурносните стандарди за безжичните мрежи. Од една страна, продуктивноста е зголемена со неограниченият пристап до информациите без оглед на местоположбата на вработените, но сепак не сме сигурни како да ги споредуваме погодностите со ризиците. Појавувањето на Интернетот овозможи појавување на хакери, кракери, измамници и крадци, во најголем број случаи анонимни, кои ја загрозуваат сигурноста на поединци и компании. Интернетот служи како бојно поле, а нападите се вистински и доаѓаат во форма на малициозен код: вирус, црв, Тројански коњ. Веб страниците се често мета на луѓе кои бараат публицитет или дури одмазда и најчесто таквите обиди завршуваат со успех. Интернетот како ентитет е минимално регулиран па голем дел од критичната инфраструктура останува минимално заштитен. Интернетот и безжичните мрежи се толку тесно поврзани, - сè што се однесува на Интернетот на еден или друг начин се однесува и на безжичната околина. Кога Интернетот и безжичната околина ќе станат целосно интероперабилни, опасностите и ранливостите кои го афектираат Интернетот ќе се одразат и на безжичните мрежи во иста мера.

8.1.3 Сигурносни регулативи

Во текот на следните 20 години, развојот на безжичната индустрија ќе биде обликуван од безбедносните стандарди и правила. Некои од тие правила би вклучиле:

- Разлики помеѓу јавните и приватните мрежи,
- Разлики во регулативата за broadcast мрежи и Интернет,
- Разлики помеѓу националните и меѓународните правила за заштита на податоци,

- Степени на сигурност.

Прашањата на заштита на податоци, цената на спектрите и сигурноста се особено важни за континуираниот раст и развој на индустријата за безжични комуникации. Сигурноста може да стане најбитното од сите регулаторни прашања со кои се соочува безжичната индустрија. Довербата на потрошувачите во безжичните трансакции е условена од сигурноста на безжичниот медиум. Сигурноста вклучува не само заштита на податоците, туку и заштита од надгледување. Стравот од надгледување е потенцијална пречка во популаризацијата на употребата на безжични мрежи. Иако компаниите од безжичната индустрија се борат за предност на пазарот, постои извесна поделба на ресурси меѓу нив со цел намалување на производните трошоци. Иако намалувањето на трошоците е добро за работата, делењето на ресурси претставува проблем за организациите кои се занимаваат со правилата за сигурност и редунданција. Примарните фактори кои мора да бидат земени во предвид се следните:

- Безжичните комуникации, бидејќи не бараат физичка поврзаност имаат поголеми изгледи да преживеат различни природни непогоди: урагани, земјотреси, поплави, вулкански ерупции и слично.
- Безжичните трансмисии се полесни за пресретнување од трансмисиите кои се одвиваат преку некој вид на кабел. Иако пресретнувањето на трансмисиите низ жичена врска воопшто не е невозможно, во јавноста владее мислење дека жичените конекции сепак обезбедуваат значително ниво на сигурност. За подобрување на заштитата на безжичните трансмисии може да се користи и дигитална енкрипција.
- Употребата на оптички кабли и безжична технологија се најдобрите алтернативи за обезбедување на високо ниво на употребливост.

Доколку индустријата во целост го прифати моделот на делење на ресурси, можно е да се појават точки на прекин кај големите телекомуникациски инфраструктури. За ваквите случаи потребно е да се обезбеди адекватна редунданција.

Уште едно важно подрачје за иднината на безжичните комуникации е апликацискиот простор. Во моментов, безжичните апликации се концентрирани на мобилен Интернет, мобилна комерција, мобилна забава и мобилно лоцирање. Најкритичниот момент во развојот на безжичните локални мрежи (WLANs) е развивањето и имплементацијата на мерки за сигурност, доверливост, интегритет и достапност за корисничка комуникација. Во поглед на останатите фактори, иднината на безжичните мрежи е светла: важат за прикладна и често поевтина алтернатива на жичените локални мрежи (LANs). Индустриските подобрувања во поглед на цената, управувањето и брзината многу допринесоа во успехот на безжичните мрежи. Испитувањето спроведено од Wireless LAN Alliance (WLANA) покажува дека трошоците за инсталација најчесто се враќаат за 12 месеци, но сигурноста е сеуште проблематична. Како одговор на ова, производителите на безжична опрема заедно го креираат Wireless Equivalent Privacy (WEP) како енкрипциска шема за заштита на WLAN податочни трансфери. Оригинлно, WLANA предвидела десеткратно зголемување на бројот на WLAN корисници до 2003, и тоа од 2,3 на 23 милиони. Сепак, криптографската основа на WEP протоколот беше побиена во две одделни студии и тоа од Adi Shamir и Itsik Mantin

од Weitzmann Институтот во Израел и од AT&T Lab истражувачкиот тим на чело со Aviel Rubin што имаше далекусежен инхибиторен ефект на целата WLAN индустрија. Во 2000 година, Cellular Telecommunications & Internet Association (CTIA) заедно со Wireless Advertising Association даваат неколку предлози околу wireless privacy и spamming. Една од рамките е наречена locate, inform, save, alert (LISA). LISA веќе се употребува за следење на автомобили, камиони и стока во транзит; за сега не може да се каже до кој степен би било изводливо следење на луѓе на ваков начин.

8.2 ТАКСОНОМИЈА НА БЕЗЖИЧНИТЕ МРЕЖИ

8.2.1 Безжични мрежи

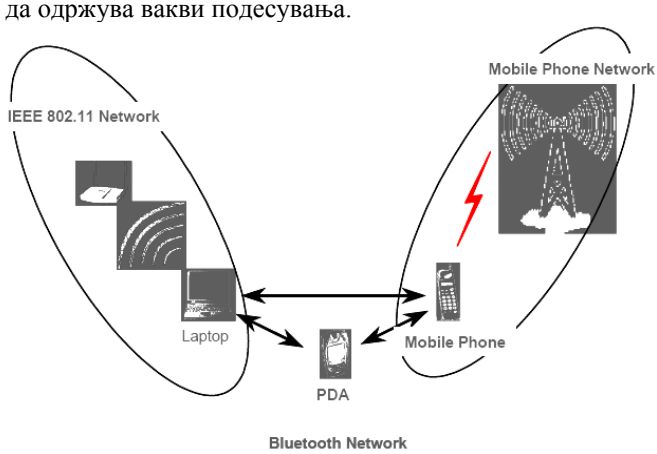
Безжичните мрежи служат како транспортен механизам помеѓу мобилните уреди (лаптоп, мобилен телефон, PDA) и традиционалните жичани мрежи (enterprise мрежите и Internet). Безжичните мрежи постојат во многу различни варијанти, но најчесто се категоризираат во три групи, врз база на зоната што ја покриваат: безжични широкопојасни - Wide Area Networks (WWAN), безжични локални - WLAN, и безжични персонални мрежи (WPAN). WWAN претставуваат технологии за покривање на широки подрачја и во нив спаѓаат: 2G cellular, Cellular Digital Packet Data (CDPD), глобален систем за мобилни комуникации (GSM), Wi-Max и Mobitex. WLAN, ги претставува безжичните локални мрежи, и вклучува 802.11, HiperLAN, и некои други. WPAN, т.е. безжичната персонална мрежа ги претставува Bluetooth и IR (инфрацрвен сигнал). Сите овие технологии се навистина "без жица" - тие примаат и испраќаат информации со помош на електромагнетни (EM) бранови. Безжичните технологии користат бранови должини од радио спектарот (RF), па сè до инфрацрвениот спектар IR. Фреквенциите од RF-спектарот покриваат значаен дел од EM-спектарот, почнувајќи од 9 kilohertz (kHz), најниската можна безжична фреквенција, па до илјадници gigahertz (GHz). Како расте фреквенцијата над RF-спектарот, EM енергијата се движи кон IR и видливиот спектар. Во продолжение ќе се фокусираме на WLAN и WPAN технологиите.

Безжични LAN

WLAN овозможува поголема флексибилност и портабилност во однос на традиционалните локални мрежи (LAN). За разлика од традиционалните LAN, кои бараат жичана конекција од корисничкиот компјутер до мрежата, WLAN ги поврзува компјутерите и другите компоненти во мрежата користејќи уред - access point. Access point-от комуницира со уредите преку безжични мрежни адаптери; тој се поврзува на жичаната Ethernet LAN преку RJ-45 port. Access point-те типично имаат покриеност околу 100 метри. Оваа зона на покриеност е наречена ќелија или ранг. Корисниците се движат слободно низ ќелијата со лаптопот или друг мрежен уред. Access point-те можат да се поврзат меѓусебно и да им овозможат на корисниците "roaming" низ цела зграда или низ околните згради.

Ad Hoc мрежи

Ad hoc мрежите, како Bluetooth, се мрежи за динамичко поврзување на оддалечени уреди на пр. мобилни телефони, лаптопи, и PDA. Овие мрежи се наречени "ad hoc", заради нивната променлива мрежна топологија. Додека WLAN користи фиксна мрежна инфраструктура, ad hoc мрежите одржуваат случајна мрежна конфигурација, и се базираат на master-slave систем, кој преку безжични врски им овозможува на уредите да комуницираат. Во Bluetooth мрежата, мастерот ја контролира промената на мрежната топологија. Тој исто така го контролира текот на податоци помеѓу уредите кои се способни да воспоставаат директни линкови помеѓу себе. Бидејќи уредите се движат во непредвидлива насока, овие мрежи мора да се ре-конфигурираат летечки за да овозможат динамичка топологија. Рутирачкиот протокол што го применува Bluetooth - му овозможува на мастерот да воспостави и да одржува вакви подесувања.



Сл. 8.1: Пример на Bluetooth-enabled мобилен телефон, кој се поврзува на мобилна мрежа, се синхронизира со PDA address book, и симнува e-mail од IEEE 802.11 WLAN.

8.2.2 Сигурност кај безжичните мрежи

Првата поента што се наметнува е дека сигурносните мерки за безжични мрежи припаѓаат во поширокаата категорија на Information Warfare. Безжичните комуникации, со нивната мобилна природа и конзервативна употреба на електромагнетниот спектар се подложни на потенцијално успешни Information Warfare напади и одбрани. Ова важи како за воени, така и за комерцијални или приватни цели. Таксономијата мора да се конструира врз база на INFOWAR (IW) објективите, функциите, контрамерките и ефектите на целната информациона инфраструктура. Барањата кои треба да се задоволат се доверливост, интегритет и достапност (confidentiality, integrity, availabibity, CIA).

- Достапноста на информациските сервиси (процеси) може да биде нападната за да се предизвика пад на системот, или denial of service напад.
- Интегритетот на информационите системи може да биде цел на напад кој би предизвикал измама, манипулација со податоци, селективно зголемување или дезинформација.

- Доверливоста или приватноста на сервисите или информациите се можни цели на напад со цел искористување на туѓи ресурси.

Било која IW операција (напад) врз безжична инфраструктура или возило може да биде еднократна, повеќекратна или комплексна комбинација од специфични тактички елементи за постигнување на основните цели: вметнување на податоци, загуба, дезинформација, попречување, детекција и разоткривање. Функционалните IW акции кои се применуваат за постигнување на целта се:

- Denial of Service (DoS), може да се постигне со предизвикување на загуба или привремен прекин на информационата содржина или сервисите. Попречување, преоптоварување, интерференција со електромагнетен пулс (EMP) или физичко уништување на безжичните линкови и процесори, се карактеристични примери при предизвикувањето на вакви проблеми.
- Корупција (Corruption), вклучува замена, вметнување или бришење на информации или сервиси со што би се постигнале многу неочекувани ефекти (измама, пад на системот). Пример – вируси со corruption engines, worm за бази на податоци, man-in-the-middle (MIM) напади врз криптографските протоколи и попречувачи на сензори.
- Експлоатација (Exploitation) – се изведува на надворешно ниво (пасивно набљудување) или на внатрешно ниво со цел добивање на информации кои биле класифицирани како доверливи.

Одговорот на сигурносниот систем на ваквите напади може да се следи преку следните три параметри: детекција, одговор и опоравување.

- Детекција – нападот не е детектиран од целта, детектиран при појавувањето или некое време откако се појавил.
- Одговор – стартување на испитувачки активности, мигрирање на понатамошната штета, стартување на заштитни акции.
- Опоравување - бекап и ре-групирање.

Од гледна точка на безжичен систем и инфраструктура, оваа таксономија ги вклучува само првите ефекти. Еден недетектиран напад може да има мали последици додека друг може да предизвика сериозни проблеми. За било кој план за напад или одбрана, IW таксономијата може да се користи за развивање и категоризација на контра-мерки кои може да се употребат. Нападите на безжичните системи имаат додатен ефект – деградација на перформансите. Блокирањето или попречувањето на безжичен систем ги деградира системските перформанси (техничка деградација или деструкција) и ефективноста на самиот систем. Едноставно преоптоварување може да предизвика колизии во системот за доставување на информации.

Ризикот е неизбежен во секој сегмент од животот. Бидејќи е антитеза на сигурноста, се стремиме да го елиминираме. Целосна елиминација на ризикот, како што ни покажува и искуството не е возможна. Вистинска опасност за луѓето, опремата, инвентарот и останато се природните непогоди па треба да се земат во предвид при проектирањето на поголеми системи. Во информациските системи

зборот закана се користи за опишување на поограничена компонента на ризик. Заканата за информациите или компјутерското процесирање и комуникациските системи може да е од надворешни лица кои бараат пристап до информации, но почесто заканата доаѓа од внатре, од личности кои од најразлични причини сакаат да навлезат во системот.

Менаџерите мора да ги земат во предвид последиците од можните напади; секој напад може да се однесува на некоја потенцијална ранливост. Не постои еднонасочна кореспонденција закана-ранливост, па не можеме да сметаме дека со елиминација на некоја ранливост ќе се заштитиме од сите закани. Било која закана која нема асоцирана ранливост или ранливост без закана воопшто не го зголемува ризикот, а ја поедноставува анализата.

Традиционално, заканите за безжичните комуникации доаѓале во три области:

- Пресретнување на радио-брановите
- Пристап до мобилните сервиси
- Интерференција во самите безжични мрежи

Нападите врз радио-брановите вклучуваат пресретнување на податоци “во воздух”, недоверливост на корисничките податоци, недоверливост на сигнализацијата и недоверливост во информациите за идентитетот на корисниците. Илегалниот пристап до мобилните сервиси генерално се врти околу некоја шема на претставување како претплатник на системот, додека се користи истиот. GSM моделот вклучува испитувачки уреди какви што се мобилните станици, SIM (Subscriber Identity Module) картици, регистар на посетители и центар за автентикација. Безжичните мрежи имаат ранливости насекаде вклучувајќи ги тука корисничката машина, серверот, рутер/гејтвеј, патеката на комуницирање и структурата на протоколот. Уште од 1940г. - стратегијата за заштита на безжичните мрежи вклучувала повеќе развиени техники за прикривање како што се spread-spectrum, direct sequence, frequency hopping и опции за повеќекратна енкрипција. Овие опции се применети на мноштво безжични податочни сервиси вклучувајќи банкарство, трансфери, детали за сметки, заеднички фондови, квоти како и e-commerce (Business-to-Business), лабораториски сервиси, GPS, вести, временска прогноза итн.

8.3 КАРАКТЕРИСТИКИ НА БЕЗЖИЧНАТА СИГУРНОСТ

Има четири фундаментални разлики помеѓу безжичните и жичените мрежи:

- Проток (Bandwidth)
- Поднесливи рати на грешка
- Доцнење и варијабилност
- Ограничувања наметнати од потрошувачката на енергија

Многу од овие разлики може да се согледаат на мрежните нивоа. Безжичните мрежи генерално се базираат на мобилни уреди кои комуницираат преку некаква електромагнетна трансмисија и соодветни приемни методи како на пример:

- Радио-фреквентни (RF) мрежи HF, VHF, UHF (3 MHz до 3 GHz)
- Сателитски комуникации (SAT) SHF, EHF (3 GHz до 300 GHz)
- Инфрацрвени бранови (IR)- IrDA

Безжичните мрежи се карактеризираат со генерално слаб квалитет на услуга (QoS). Многупати се употребуваат уреди со мали димензии со слаба моќност и мала пропусна моќ. Безжичните мрежи споредени со жичените се релативно недоверливи, бидејќи загубата на пакети се случува почесто отколку кај жичените мрежи. Имаат поголемо доцнење и варијабилност поради ретрансмисиите. Ограничувањата на мрежата бараат ефикасно комуницирање и сигурносни протоколи. Дизајнерите имаат повеќе променливи во дизајнот на безжичните мрежи: очекувања на корисници, рати на грешка, проток, overhead на протоколот, компресија, доцнење, траење на батеријата и протоколи за заштеда на енергија, конективност на мрежата, покривање со сигнал и слично. Интернетот го прави проблемот уште покомплексен – жичените Интернет протоколите (IPSec, SSL, SSH) воопшто не се оптимални за безжични мрежи. Од друга страна, сигурните мобилни уреди имаат:

- Релативно мала пресметувачка моќ (споредено со десктоп PC),
- Ограничување во криптографските алгоритми кои може да се употребат,
- Ограничен капацитет за чување на податоци,
- Заштеда на моќност наметната од ограничувањата во функционалноста,
- Фундаментални рестрикции на пропусна моќ, рата на грешка, доцнење и варијабилност,
- Мала големина и компактен I/O,
- Ограничени графички можности, GUI станува покомплициран со различни form фактори,
- Чуствителност на протокот на компресија и overhead на протоколот.

Повеќето од постоечките сигурносни технологии, протоколи и стандарди се дизајнирани за жичената high bandwidth околина. Во многу случаи не се добро прилагодени за безжичната мобилна околина, бидејќи имаат премногу overhead и прикажуваат мали timeout интервали. Затоа, ја редефинираме безжичната сигурност за да значи:

- Адаптација и интеграција на постоечките решенија и инфраструктура.
- Промоција на постојаност и интероперабилност помеѓу различниот спектар на мобилни и безжични уреди.
- Обезбедување на високо ниво на сигурност без непријатни искуства за корисникот.

Во безжичната мрежа, сигурносните опции се разликуваат значително кај различни протоколи, и имплементацијата на сигурносните полиси е зависна од

носачот. На пример, наведени се некои од репрезентативните разлики во одредени слоеви од OSI моделот.

8.3.1 Сигурност на физичко ниво

- Обезбедува scrambling на сигналот за заштита од воздушни (over-the-air, OTA) прислушувања.
- Технологија базирана на цепкање на бит-стримот на мали фрагменти наречени радио рамки врз кои потоа се применува некеква фреквентна scrambling техника.
- Радио рамките патуваат на spread spectrum фреквенции, при што секој фрагмент е идентификуван со дигитален код познат само на уредот и базната станица.
- Ниеден друг уред не може да ја прими трансмисијата.
- За секоја конекција има милиони кодни комбинации на располагање.
- Пример: CDMA.

8.3.2 Сигурност на data link и мрежно ниво

- Некои протоколи како CDPD и GSM обезбедуваат доверливост на податоците на овие нивоа.
- CDPD применува енкрипција на секој сегментиран дијаграм пред трансмисијата.
- GSM користи subscriber identity module (SIM) картичка за запишување на асиметричен клуч познат само на мобилниот телефон и автентикацискиот центар.

8.3.3 Сигурност на транспортно ниво

- Secure Socket Layer (SSL) се користи екстензивно во Web апликации за осигурување на TCP/IP конекции.
- Јавни клучеви (RSA) за размена на сесиски клуч (RC4 и други алгоритми) за масовна енкрипција.
- Протокол за управување на сесија/конекција за воспоставување на сесија, продолжување и терминирање.
- Дизајниран за конекции со голема пропусна моќ. Не е оптимизиран за мрежи со високо доцнење.
- Автентикација на клиенти и сервери преку X.509 сертификати.
- X.509 сертификатите имаат голем footprint и бараат голема пресметковна моќ за процесирање.
- SSL не е добро прилагоден за безжични апликации.

8.3.4 Сигурност на апликациско ниво

- Специфична автентикација на корисници за секоја апликација,
- Кориснички ID и лозинка,
- Биометрика,
- Интегритет на пораки,

- Енкрипција на апликациско ниво: RC5, Троен DES, Rijndael и слично,
- Дигитални потписи на автентикација на апликациско ниво: PKI, RSA, ESCDSA, ECC.

Носечките слоеви се употребуваат за да се осигури OTA линкот и да се спречи евентуалното прислушување. Транспортното ниво ја вклучува сигурноста со цел подобрување на доверливоста. Но имплементацијата е испрекината поради бројните точки на премин помеѓу безжичните и жичените протоколи. Сигурноста на апликациско ниво обезбедува контрола на пристап, автентикација и доверливост.

8.3.5 Таксономија на можни напади

Можеме да разгледаме два различни приоди кои му се на располагање на напаѓачот:

- Директен (внатрешен) упад: напаѓачот навлегува во комуникациски линк, компјутер или база на податоци, со цел добивање или користење на внатрешни информации, модификација на информации (додавање, вметнување, бришење) или инсталација на малициозен процес.
- Индиректен (надворешен) упад: напаѓачот не може да биде детектиран од сензорите. Ги напаѓа сензорите со вметнување информации во нив или го набљудува нивното однесување.

Целта на нападот дефинира две категории на напади кои ги оштетуваат информациите:

- Напади врз содржината: содржината на информациите во системот може да биде нападната со цел да се измами корисникот. Нападите врз содржината се фокусирани на real-time податоци и информации кои произлегуваат од нив.
- Темпорални напади: информацискиот процес може да биде нападнат на таков начин што се влијае на навременоста на пренесената информација. Се внесува каснење при приемот на податоците или се праќаат погрешни податоци маскирани како легитимни.

8.4 СИГУРНОСНИ МЕРКИ КАЈ БЕЗЖИЧНИТЕ МРЕЖИ

Самата природа на безжичните комуникации ја прави сигурноста значаен фактор на кој мора да му се посвети внимание за да можат безжичните комуникации да го постигнат својот несомнено голем потенцијал. Денес мнозинството на безжични уреди го користат спектарот на радио-бранови. Бидејќи истите се зрачат насекаде, секој кој се наоѓа во близина и поседува приемник поставен на погодна фреквенција може да ја следи трансмисијата.

Сигурноста е комбинација на процеси, процедури и системи кои се користат за да се обезбеди доверливост, интегритет и достапност на информациите. Доверливоста значи заштита на информацијата од неовластени личности,

интегритетот ги заштитува податоците од неовластена модификација, а достапноста овозможува пристап до системот односно до податоците во секое време. Некои од постојните предизвици за сигурноста би биле проблеми како: изгубени или украдени уреди, внатрешни напади, клонирање на уреди итн. Додатни сигурносни проблеми би биле: вируси, denial of service напади, напредни уреди за радио-пресретнување и заштита на безжични LAN. Општо, сигурно мобилно решение е она кое ги содржи следниве функционалности:

- **Автентикација:** Проверка на идентитетот на корисникот
- **Енкрипција:** Оневозможување на прислушувањето
- **Контрола на пристап:** Корисниците да имаат пристап само до оние информации за кои имаат дозвола да ги видат
- **Кражба:** Централно исклучување на уредите во случај тие да паднат во раце на неавторизиран корисник

Клиентите на мобилната трговија мора да имаат комплетна доверба дека нивните податоци и комуникации ќе бидат адекватно заштитени пред да ја прифатат новата технологија во целост. На пример, многу луѓе го користат Интернетот за пребарување на информации за различни продукти, но немаат доволно доверба во Интернетот за да ги пратат своите податоци за плаќање, иако повеќето компании кои работат со кредитни картички ја гарантираат сигурноста на информациите. Секако, еден од главните проблеми со Интернетот е автентикацијата; имено, корисниците сакаат да знаат дека сигурно се поврзани со оној со којшто мислат дека се поврзани.

Ќе ги разгледаме главните сигурносни иницијативи кои се одвиваат кај безжичните мрежи Wired Equivalent Privacy (WEP), WPA и Bluetooth. Целта на WEP моделот е да се спречи прислушување и навторизирано модифицирање на податоци. WEP користи RC4 40-битен stream cipher алгоритам за енкрипција на 32 бита CRC. Според студијата објавена од Internet Security Applications Authentication and Cryptography (ISAAC), WEP има погрешен алгоритам и забележани се неколку специфични напади кои можат да се применат против него. Проблемот со алгоритмот е што RC4 е подложен на честа употреба на одреден след на цифри (keystream reuse) што се коси со сите стандарди за енкрипциски шеми. Опишаните напади на WEP вклучуваат собирање на рамки за статистичка анализа, употреба на SPAM за декриптирање на рамки, bit flipping за модификација на пораки и слично. Се прават големи напори за подобрување на ефикасноста на WEP; модификациите вклучуваат транспарентна надградба на 128 бита и многу посигурен upgrade режим на работа базиран на Advanced Encription Standard (AES). Поновите верзии ќе имаат и подобрени автентикациски и авторизациски својства.

Развојот на WPA сигурносни продукти е условен од популаризација и бројот на WPA уреди кои се користат низ светот – околу 25 милиони. WPA сигурносниот модел има четири компоненти:

- Wireless Transport Layer Security Protocol (WTLSP) – обезбедува доверливост, интегритет и автентикација.

- WPA Identity Module (WIM) – обезбедува преносливост на препораките (credential portability) и автентикација на клиентите.
- WPA Public Key Infrastructure (WPKI) – безжична интерпретација на PKI (Public Key Infrastructure) техниката.

Идејата за персонален комуникатор кој може да служи како телефон, да пресметува, да води календар на состаноци и да забавува во исто време е повеќе од атрактивна. Но колкумина би употребиле таков уред ако секој може да добие, менува, да додава податоци или да ги брише од меморијата на уредот без знаење на неговиот сопственик? Ова прашање особено добива на важност сега кога има голема експанзија на Bluetooth уреди и апликации. Сега, уредот може да послужи и за лоцирање на неговиот сопственик; ова својство може да е добредојдено кога се работи за итни повици и повици за помош, може да значи и дека некој друг од било кои побуди може да го следи вашето движење.

8.4.1 Обезбедување WLAN сигурност

Бежичните локални мрежи (WLAN) се флексибилен податочен комуникациски систем имплементиран како екстензија или алтернатива на "жичаните" локални мрежи. Овие мрежи праќаат и примаат податоци со помош на радио бранови минимизирајќи ја со тоа потребата од жичани конекции и комбинирајќи ја конективноста на податоците со мобилноста на корисниците. WLAN конфигурациите се движат од едноставни peer-to-peer топологии до комплексни мрежи кои нудат дистрибуирано податочно поврзување и roaming. Освен можноста за дистрибуирано податочно поврзување во мрежна околина, безжичните мрежи обезбедуваат физичка портабилност на мрежата, овозможувајќи и на мрежата да се движи заедно со корисниците. Цената што мора да се плати за флексибилноста и мобилноста на овие мрежи е опасноста од неовластени упади.

Безжичните мрежи се многу по-изложени на напад; може да се изврши упад во мрежата од автомобил паркиран во близина. IEEE 802.11 стандардот обезбедува доверлив трансфер на податоци, но е ранлив на прислушување. WLAN ја елиминира физичката врска во мрежата, овозможувајќи им на корисниците да се конектираат директно во даден дистрибуиран систем без интер-конекциски врски и кабли. Мрежниот backbone не е повеќе скриен зад повеќе sидови и врати, ниту пак мора да се наоѓа на конкретна локација. Со самото инсталирање на WLAN, мрежата добива послободна инфраструктура, слободна е да расте и да се движи во зависност од потребите на организацијата.

Безжичните мрежи оперираат на сличен начин како и жичените со таа разлика што податоците се пренесуваат преку безжичен медиум, најчесто радио-бранови, наместо преку кабли. Секако, и безжичните мрежи имаат слични слабости како и жичените, но и некои дополнителни. Овде се дискутираат вообичаените закани со кои се соочува секоја безжична мрежа и некои од контра-мерките кои се дизајнирани за справување со тие закани како и јачината и ограничувањата на тие контра-мерки.

Можни напади кои би се јавиле кај безжична мрежа се следните:

- Уфрлање на неавторизиран access points, ad-hoc мрежа или клиент.
- Скенирање на порта (SNMP агенти или непознати web/ telnet интерфејси).
- Прислушување однадвор:
    - прислушување на 802.11 пакети,
    - идентификација на IP адреси,
    - детекција на внатрешниот сигнал.

8.4.2 Прислушување

Првенствената закана е можноста за неавторизирано прислушување на радио-сигналите испратени помеѓу безжичната станица и пристапната точка (access point, AP), со што се компромитира сигурноста на чувствителните информации. Прислушувањето е пасивен напад; кога радио оператор праќа порака во етерот, сите корисници опремени со соодветна опрема може да ја примат. Понатаму, прислушувачот може да ја слуша пораката без да ја измени, па неговото присуство лесно може да остане незабележано. Жичените мрежи се исто така осетливи на прислушување, но не до тој степен како безжичните. Жичената мрежа може да емитува електромагнетно зрачење околу каблите, но прислушувачот треба да е многу блиску до нив за да може било што да стори. За разлика од тоа, ако некој сака да прислушува безжична мрежа доволно е да се позиционира на одредено растојание од мрежата, а понекогаш и надвор од физичкиот простор каде мрежата е сместена. Ова доаѓа оттаму што радио-сигналите емитувани од WLAN лесно пробиваат надвор од оригиналната област на дејствување, можат да пробиваат низ ѕидови и други физички пречки, зависно од технологијата на пренос и јачината на сигналот. Опрема за пресретнување на "безжичен" сообраќај е достапна на пазарот во форма на wireless адаптери и други 802.11 - компатибилни продукти. Тешкотијата е да се декодира 2.4 GHz дигитален сигнал, бидејќи повеќето WLAN системи користат Spread-Spectrum технологија која е донекаде отпорна на прислушување. Се користи и додатна енкрипција, но и покрај сите мерки, прислушувањето претставува сериозен проблем во WLAN комуникацијата.

8.4.3 Недозволен пристап

Втора закана за WLAN сигурноста е можноста натрапникот да влезе во мрежата маскиран како авторизиран корисник. Откако ќе влезе во мрежата, натрапникот може да влијае на мрежниот сообраќај со праќање, примање, модифицирање или фалсификување на пораки, загрозувајќи го интегритетот на мрежата. Ова е активен напад и може да се изврши со помош на wireless адаптер кој е компатибилен со целната мрежа или со употреба на компромитиран (на пример, украден) уред кој е поврзан на мрежата. Најдобрата заштита од недозволен пристап е развој на автентикациски механизми кои ќе овозможат влез во мрежата исклучиво за автентикувани корисници. Ваквите механизми се редовна практика кај жичените мрежи, не само да спречат недозволено влегување во мрежата, туку и да ги детектираат евентуалните упади. Откривањето на натрапниците кои се обидуваат да влезат во WLAN не е едноставно. Ова е затоа што неуспешните напади можат да бидат погрешно интерпретирани како неуспешни logon обиди предизвикани од високата рата на грешка (bit error rate,

BER) на радио трансмисиите или од станици кои припаѓаат на друга безжична мрежа. Една варијанта на неавторизиран пристап е сетирање на фалсификувана пристапна точка (AP). Кога безжична станица се вклучува за прв пат, или кога влегува во нова микро-ќелија, одбира AP на кој ќе се поврзе врз база на јачината на сигналот и ратите на грешка на пакети. Ако е примена од AP, мрежната станица се поставува на радио каналот кој го користи AP. На ваков начин, со поставување на лажна пристапна точка со доволно силен сигнал, напаѓачот може да ја намами станицата на својата мрежа со цел да ги добие logon лозинките. Исто така, напаѓачот може да не успее со logon обидите, но да ги зачува пораките пренесувани за време на самиот logon процес со истата цел. Првиот тип на напад е многу тежок за изведување, бидејќи напаѓачот треба да има детални информации за да може да ја измами станицата да поверува дека пристапила во своја мрежа. Во спротивно, нападот многу лесно се открива. Вториот тип на напад полесно се изведува, бидејќи на напаѓачот му требаат само приемник и антена компатибилни со целните станици. Овој вид на напад е потежок за детекција, бидејќи неуспешните logon обиди се релативно чести во WLAN комуникациите. Најдобрата заштита во двата случаи е употреба на ефикасен автентикациски механизам кој им овозможува на безжичните станици да се автентицираат на пристапните точки без откривање на тајните клучеви или лозинки.

8.4.4 Интерференција и попречување

Трета закана за WLAN сигурноста е радио интерференцијата која може сериозно да го деградира протокот. Во многу случаи интерференцијата е случајна; бидејќи безжичните мрежи користат нелиценцирани радио-бранови, други електромагнетни уреди кои работат во инфрацрвено подрачје или 2.4 GHz радио фреквенција можат да предизвикаат препокривање со WLAN сообраќајот. Потенцијални извори на интерференција се аматерски, воени, индустриски или комерцијални предаватели со голема моќност. Друг извор на проблеми е и оперирањето на две безжични мрежи близу една до друга. Секако, интерференцијата може да е и намерна: ако напаѓачот има доволно силен трансмитер, може да генерира сигнал способен да ги препокрие послабите сигнали со што би ја прекинал комуникацијата. Оваа состојба е позната како попречување (jamming) и е напад од тип denial of service. Двата типа попречувачи кои може да се користат за jamming на работата на мрежите се пулсирачки full-band попречувачи со висока моќност кои ја прекриваат целата фреквенција на која се наоѓа целниот сигнал, и парцијални band попречувачи со помала моќност кои го покриваат само оној дел од фреквенцијата на кој се наоѓа сигналот. Опремата за попречување е комерцијално достапна, а може и лесно да се изработи. Понатаму, вакви напади може да се изведат од оддалечена локација. Опремата за откривање може да детектира извор на попречувачки сигнали, но не секогаш на време за да го спречи попречувањето.

8.4.5 Физички закани

Безжичните мрежи можат да се оштетат и со уништување самата мрежна инфраструктура. Како и жичените мрежи, и безжичните мрежи зависат од мноштво физички компоненти, пристапни точки, кабли, антени, wireless адаптери

и софтвер. Оштетувањето на било која од овие компоненти може да доведе до ослабување на сигналот, ограничување на областа на покривање, редукција на протокот и воопшто достапноста на информациите кои постојат на мрежата. Во краен случај, компромитирањето на физичката инфраструктура може да доведе и до паѓање на целата мрежа. Инфраструктурните компоненти се чувствителни на околината во која работат; AP може да биде попречуван од снег, мраз и изобличени радио сигнали. Антените се истотака проблематични; можат да се изместат или да го сменат аголот што посебно се одразува на антените со мала широчина на beam, на пример параболичните beam антени. На крајот, несреќа или непрописно ракување може да ги оштети безжичните адаптери и станици. Физичките компоненти се исто така подложни на напад. Генерално, безжичните мрежи се помалку зависни од физичките компоненти отколку обичните жичени мрежи, но и тие не се сосема сигурни. На пример, напаѓачот може да ја прекине врската од AP до жичената мрежа, со што би изолирал одредени микро-ќелии и би го прекинал напојувањето на приемникот. Исто така, можен е напад или дури и уништување на AP или антена поврзана на него. Исто така, можен е напад или кражба на безжичната станица или адаптер и нивна употреба за пресретнување на WLAN сообраќај или добивање на неовластен пристап во мрежата. На крајот, напаѓачот може да ја избегне безжичната мрежа и да ја онеспособи жичената, - оневозможувајќи го притоа и оперирањето на сите WLAN поврзани на неа.

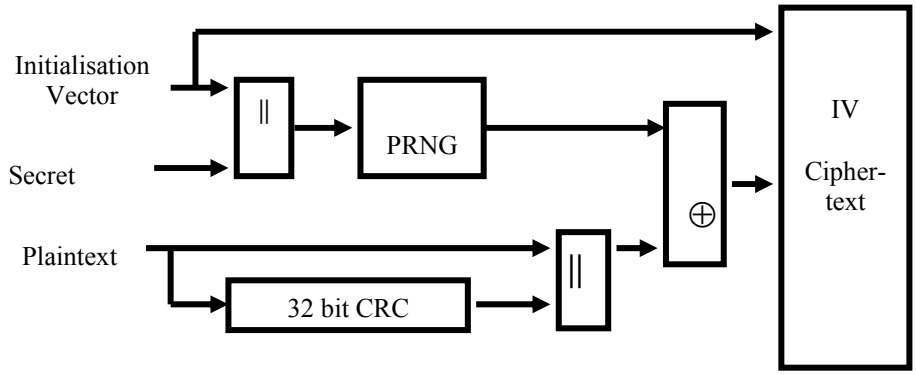
8.5 WEP – WIRELESS EQUIVALENT PRIVACY

Иако WLAN системите можат да се одбранат од пасивно прислушување, единствен начин да се спречи компромитирање на пренесените податоци е употреба на енкрипција. Целта на WEP е да се осигура дека безжичните системи ќе го имаат она ниво на приватност кое го имаат и жичените мрежи. Секундарна цел на WEP алгоритмот е спречување на неовластен влез во мрежата, т.е. обезбедување на автентикација. WEP е критичен елемент во осигурувањето на доверливоста и интегритетот на податоците на безжичните системи базирани на 802.11, како и обезбедувањето на контрола на пристап преку автентикација. Како резултат на сето ова, повеќето од 802.11 продукти го поддржуваат WEP како стандард или барем како опција.

8.5.1 Енкрипција

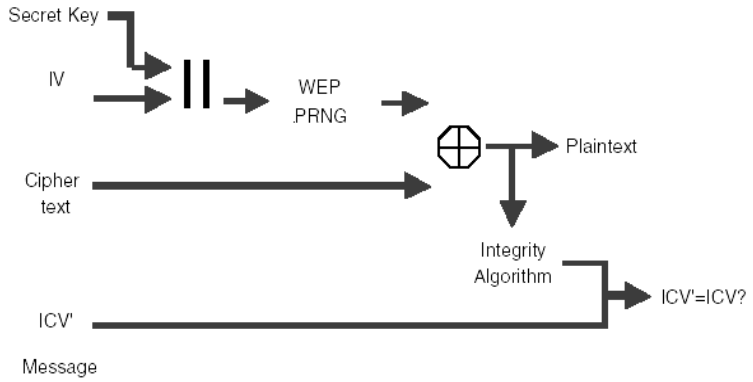
WEP користи заеднички таен клуч кој е познат само на безжичната станица и AP. Сите податоци кои се пратени и примени помеѓу овие два уреди можат да се енкриптираат со помош на тој клуч. 802.11 стандардот не специфицира како се воспоставува клуч, но во пракса, еден клуч е заеднички за сите станици и пристапни точки во еден систем. WEP овозможува податочна енкрипција со користење на таен клуч со должина од 40 бита (слаб) или 128 бита (јак) и RC4 генератор на псевдо-случајни броеви (PRNG). Над обичниот текст се извршуваат два процеси: едниот го енкриптира, а другиот ја заштитува енкриптираната содржина од недозволен пристап и модифицирање при транзит. Тајниот клуч се конкатенира со случаен иницијализациски вектор (IV) кој додава уште 24 бита. Овој клуч потоа се вметнува во PRNG кој генерира долга псевдо-случајна низа на клучеви. Испраќачот врши логичка XOR операција на низата од

клучеви со текстот, за да генерира енкриптиран текст (ciphertext) и го емитува кон приемникот заедно со IV.



Сл. 8.2: WEP енкрипција

По примањето на шифрираниот текст, приемникот го употребува IV и својата копија од тајниот клуч за да продуцира своја низа од клучеви, која е идентична на низата генерирана од предавателот. Приемникот потоа прави XOR на низата од клучеви со шифрираниот текст за да го добие оригиналниот текст. За заштита на шифрираниот текст од модификација додека е во транзит, WEP му додава на текстот и алгоритам за проверка на интегритет (CRC-32) што пак продуцира ICV (Integrity Check Value). ICV се закачува на шифрираниот текст и се праќа кон приемникот заедно со IV. Приемникот го комбинира шифрираниот текст со низата од клучеви за да го открие оригиналниот текст. Примената на алгоритмот за интегритет кај обичниот текст, и споредувањето на добиениот ICV со оној кој е добиен од предавателот, додатно ја верифицира декрипцијата. Ако двата ICV се идентични, пораката е автентична.



Сл. 8.3: WEP декрипција

И покрај потенцијалната сила на WEP во заштитата на доверливоста и интегритетот на податоците, има ограничувања кои можат донекаде да се

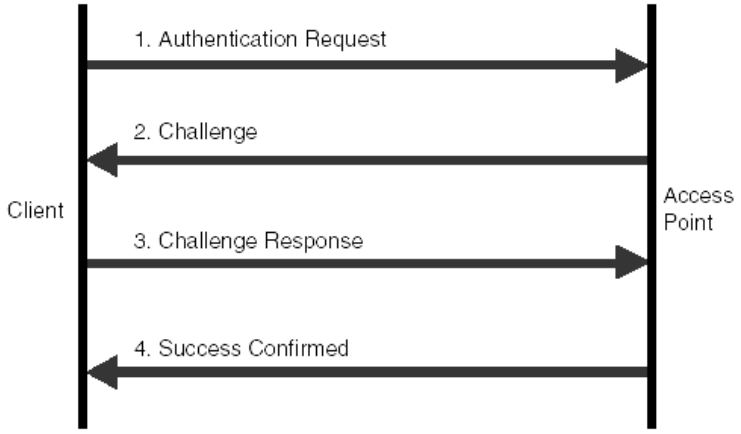
надминат само со соодветно управување. Првиот проблем произлегува од употребата на IV. IV се содржи во неенкриптираниот дел од пораката, па приемникот знае кој IV да го користи кога ја генерира низата од клучеви за декрипција. 802.11 стандардот препорачува, но не обврзува, IV да се менува после секоја трансмисија. Ако IV не се менува постојано, туку се искористува повторно за последователни пораки, прислушувачот може да ја анализира низата од битови генерирани од IV и тајниот клуч, па така да ги декриптира пораките. Проблемот на ре-употреба на IV потенцијално води кон друг проблем. Имено, кога напаѓачот ќе ја дознае низата од клучеви за некоја енкриптирана порака базирана на повторно употребен IV - може да ја искористи таа информација за да креира енкриптиран сигнал и да го вметне во мрежата. Процесот вклучува креирање нова порака, калкулирање на CRC-32 и модификација на оригиналната енкриптирана порака. Напаѓачот потоа може да ја испрати пораката до AP или безжична станица која пак ќе ја прифати како валидна порака. Промената на IV после секоја порака е едноставен начин за спречување на ваквите проблеми.

Друг проблем е дистрибуцијата на клучеви. Најголем дел од безжичните мрежи делат еден клуч за сите станици и пристапни точки во мрежата. Не е многу веројатно дека клуч користен од толку многу корисници ќе остане таен засекогаш. Некои мрежни администратори го решаваат овој проблем така што сами ги конфигурираат тајните клучеви кај безжичните станици, наместо тоа да им го препуштат на крајните корисници. Решението не е идеално: тајниот клуч сепак е зачуван на корисничките компјутери каде што е небезбеден. Понатаму, ако се компромитира клуч од само една станица, сите станици во системот мора да се реконфигурираат со нов клуч. Подобро решение е да се додели уникатен клуч на секоја станица и да се менуваат клучевите почесто.

Иако WEP енкрипцијата е дизајнирана да биде ефикасна, може да го редуцира протокот. Според истражувањата, 40-битната енкрипција го намалува протокот за 1 Mbps, а 128-битната за 1 до 2 Mbps. Ова намалување е релативно мало, но некои корисници може да го почувствуваат особено ако сигналот се пренесува со FHSS кој има рата на пренос од само 3 Mbps. Во многу случаи, точното влијание ќе зависи од уредот кој се употребува и од бројот на корисници во системот.

8.5.2 Автентикација

WEP обезбедува два типа на автентикација: Open System (default), каде што сите корисници имаат пристап во мрежата, и автентикација со заеднички клуч, која го контролира пристапот до мрежата и спречува недозволен влез. Секако, вториот начин е посигурен. Користи таен клуч кој е заеднички за сите мрежни станици и пристапни точки во безжичниот систем. Кога некоја станица ќе проба да се поврзи со пристапна точка, пристапната точка одговара со случаен текст. Станицата мора да ја употреби својата копија од тајниот клуч за да го енкриптира текстот и да го врати назад кон пристапната точка со цел да се автентицира. Пристапната точка го декриптира одговорот со помош на истиот таен клуч и го споредува со текстот кој претходно го испратила. Ако текстот е идентичен, пристапната точка праќа потврда кон станицата и ја прифаќа во мрежата. Ако станицата нема клуч или прати погрешна порака, пристапната точка ја одбива и го спречува нејзиниот влез во мрежата.



Сл. 8.4: Автентикација со заеднички клуч

Овој начин на автентикација работи само ако се користи WEP енкрипција. Ако не се користи WEP, системот по default оди во Open System режим на работа дозволувајќи скоро на секоја мрежна станица во дометот да пристапи до мрежата. Ова креира можности за неовластен влез во системот, па може да се примаат, праќаат, менуваат и фалсификуваат пораки. Значи, секогаш кога има потреба од автентикација, WEP треба да е вклучен. Дури и кога автентикацијата со заеднички таен клуч е вклучена, може сите безжични станици во мрежата да го немаат истиот клуч поради различната инсталација на системот. За вакви системи, индивидуалната автентикација не е возможна – сите корисници, дури и неавторизираните, можат да пристапат на мрежата со помош на заедничкиот клуч. Ваквите слабости резултираат со недозволен пристап посебно ако системот има многу корисници. На крајот, во многу WLAN системи, клучот кој се користи за автентикација е истиот клуч кој се користи и за енкрипција. Понатаму, напаѓачот може не само да влезе во мрежата туку и да ги декриптира пораките. Решението е во дистрибуцијата на различни клучеви низ системот – еден за автентикација и еден за енкрипција. Сепак, покрај заштитата што ја нуди, WEP има додатна ранливост во поглед на игнорирањето на неавторизиран сообраќај или декрипција, вметнати од напаѓач кој ја изиграл пристапната точка. Токму поради овие причини, веројатно е дека WEP во иднина ќе се користи само во конјункција со VPN (virtual private network).

8.5.3 Други автентикациски техники

Освен автентикацијата со заеднички клуч може да се користат и други техники. Една од почесто користените техники е Extended Service Set Identification (ESSID). ESSID е број програмиран во секоја пристапна точка кој дефинира во која подмрежа се наоѓа пристапната точка. Оваа вредност може да се користи за автентикација на безжичните станици кои сакаат да се приклучат во мрежата. Ако станицата не го знае ESSID нема да може да се приклучи на мрежата. Исто така,

некои производители обезбедуваат MAC (Media Access Control) табели во т.н. листа на контрола на пристап (access control list, ACL) која пак е вклучена во пристапната точка. Кога некоја станица ќе проба да се приклучи кон мрежата, рутерот во пристапната точка ја чита единствената MAC адреса од wireless адаптерот на безжичната станица и одредува дали ја има во својата листа за контрола. Пристапот кон мрежата е овозможен за оние станици кои се на листата, а останатите се одбиваат. Ова им овозможува на мрежните администратори да вклучуваат и исклучуваат мрежни станици од мрежата. Оваа можност обезбедува дополнителен степен на заштита, не само за исклучување на надворешни станици, туку и на оние станици кои припаѓале на мрежата, но биле компромитирани, на пример – украден компјутер.

8.5.4 WPA (Wi-Fi Protected Access)

WPA претставува напреден енкрипциски стандард за безжични мрежи, чиј главни карактеристики се следните:

- Работи со 802.11b, a и g - мрежи,
- "Ги поправа" проблемите на WEP,
- Може да го користи постоечкиот хардвер.

WPA користи автентикација на корисничко ниво 802.1x TKIP, чиј главни особини се:

- RC4 сесиски-базирани, динамички енкриптирани клучеви,
- Промена на клучот за секој пакет,
- Unicast и broadcast менаџмент со клучот,
- Нов 48-битен IV со нов секвентен метод,
- Michael 8-бајтен код за интегритет на пораките (MIC),
- Опциона AES поддршка за замена на RC4.

802.1x претставува општо-наменски мрежен механизам, а WPA има 2 режими на работа:

- Pre-shared режим, кој користи pre-shared клучеви,
- Enterprise режим, што користи extensible автентикациски протокол (EAP), со RADIUS сервер за автентикациски одлуки.

EAP го претставува транспортот на автентикацијата, а не самата автентикација; EAP овозможува случајни методи за автентикација. На пример, Windows поддржува EAP-TLS за кој се потребни клиентски и серверски сертификати, и PEAP-MS-CHAPv2.

Секако дека постојат и нападите на WPA:

- Напад на речникот кај pre-shared key режимот (CoWPAtty, Joshua Wright),
- Denial of service attack (ако WPA опремата види два пакети со погрешен MIC во 1 секунда - сите клиенти ќе се дисконектираат, сите активности ќе запрат за

1-2 минути, па два погрешни пакети во минута ќе ја сопрат целата безжична мрежа).

Најнова верзија е WPA2 (802.11i), која:

- Претставува робусна мрежна заштита, како проширување на WPA,
- Користи контра-мерки со Cipher Block Chaining Message автентикациски - код протокол (CCMP),
- Се базира на AES, со 128-битни клучеви и 48-битен IV,
- Користи динамичко договарање за алгоритмите на енкрипција и автентикација,
- Флексибилна е за натамошни усовршувања,
- Не побарува нов хардвер.

□

9. БЕЗБЕДНОСТ НА E-MAIL

Во март 2006, бројот на корисници на Internet во светот достигна една милијарда. Најголем дел од корисниците имаат email account-и (електронска пошта) на еден или повеќе email системи, што е голем скок во однос на 1971, кога Ray Tomlinson, истражувач од Министерството за одбрана на САД, го испратил првиот email до самиот себе. ARPANET, претходникот на Internet, бил проект на Агенцијата ARPA за развој на комуникациски протоколи кои поврзувале компјутери на различни географски локации. Електронската пошта била достапна на компјутерите од ARPANET; сепак, корисниците можеле да испраќаат пораки само локално во една мрежа. Tomlinson го модифицирал тогашниот систем на пораки така што корисниците можеле да испраќаат пораки и на оддалечени ARPANET системи. Откако модификацијата на Tomlinson станала достапна за другите истражувачи, email-от набрзо станал најкористена апликација на ARPANET.

И кога ARPANET прераснал во Internet, email-от останал најкористена апликација за персонални и бизнис потреби. Бидејќи ARPANET на почеток била мала и доверлива заедница, немало потреба за безбедност. Како што растел Internet - се зголемила и потребата за безбедност. За жал, безбедноста недостигала, бидејќи првите email стандарди не ја имплементирале воопшто. Одржувањето на компатибилност со тие почетни стандарди и денес ја усложнува безбедноста на електронската пошта.

9.1 ОСНОВНИ ПОИМИ ЗА ЕЛЕКТРОНСКА ПОШТА

За да се разбере email безбедноста - потребно е разбирање за тоа како email пораките се составуваат, пренесуваат, и чуваат. За повеќето корисници на email, откако пораката ќе се напише и испрати, таа го напушта нивниот компјутер и магично се појавува во поштенското сандаче кај примачот. Ова можеби изгледа едноставно, но доставувањето на email пораките е сложено како и обичната пошта, со процесирање, сортирање и меѓу-локации, пред да пристигне на саканата дестинација.

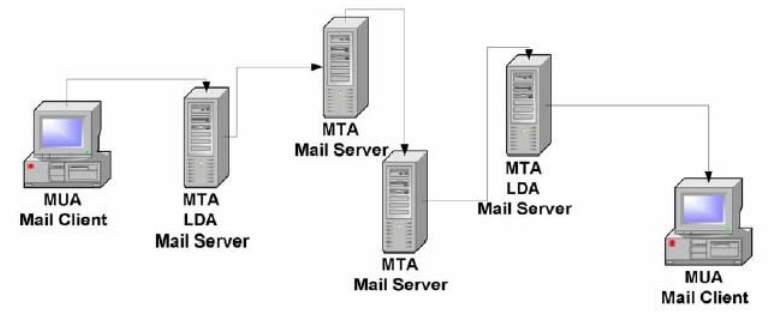
Процесот почнува со составување на пораката. Повеќето email клиенти - обично бараат од корисникот да внесе: subject (предмет), тело на пораката, и адреса на примачот. Кога ќе се пополнат тие полиња и корисникот ја испрати пораката, таа се трансформира во специфичен стандарден формат (Интернет формат за пораки) - т.н. Request for Comments (RFC) 2822. На најбазично ниво, двата главни делови на пораката се заглавје и тело. Заглавјето ги содржи виталните информации за пораката - датум на испраќање, испраќач, примач(и), патека за достава, субјект, и информација за форматот. Телото на пораката ја содржи самата содржина.

Откако пораката се преведе во RFC 2822 формат, таа се пренесува. Со користење на мрежната конекција, клиентот - т.е. неговиот mail user agent (MUA), се поврзува со mail transfer agent (MTA) кој е обезбеден од mail серверот. По иницијалната комуникација, клиентот му го кажува на серверот идентитетот на испраќачот. Потоа, користејќи серверски команди, клиентот му кажува на серверот кои се

примачите. Иако пораката содржи листа на примачи, mail серверот не ја зема сам таа информација, туку ја чека од клиентот. После тоа, доставата на пораката е под контрола на серверот.

Откако mail серверот ќе ја процесира пораката, се активираат неколку настани: идентификација на серверот на примачот, воспоставување на конекција, и пренос на пораката. Со примена на Domain Name System (DNS), испраќачкиот mail сервер го пронаоѓа mail серверот на примачот. Потоа, серверот отвора конекција до mail серверот на примачот и ја испраќа пораката со процес сличен како оној на оригиналниот клиент. Во тој момент, може да се случи еден од следните настани. Ако сандачињата на праќачот и примачот се лоцирани на ист mail сервер, пораката ќе се достави со локален агент за достава (LDA). Ако сандачињата се лоцирани на различни mail сервери, испраќањето се одвива преку MTA сè додека пораката не стигне кај примачот.

Кога LDA ја контролира пораката, можат да случат повеќе настани. Зависно од конфигурацијата, LDA може да ја достави пораката претходно филтрирајќи ја (филтрирањето се прави врз база на некои особини на пораката). Откако пораката е доставена, таа се сместува во сандачето на примачот каде се чува сè додека примачот не направи некоја акција (пр., ја чита, ја бриши) со помош на MUA. Сл. 9.1 го илустрира текот на пораката низ различните компоненти што ги објаснивме. Тоа е општиот процес за испраќање на email.



Сл. 9.1: Тек на пораката

9.2 ПОВЕЌЕНАМЕНСКИ INTERNET MAIL ЕКСТЕНЗИИ (MIME)

RFC 2822 обезбедува стандард за пренос на пораки со текстуална содржина; сепак, не опфаќа пораки што содржат attachment, како на пр. word document или слика. Додавањето на заглавја на RFC 2822 пораката, т.е. Multipurpose (повеќенаменски) Internet Mail екстензии (MIME) обезбедува безброј можности за структурата на пораките. MIME користи конвенција за типот на содржини кои ќе бидат пренесувани. Некои типови на содржини се следниве:

- Audio – за пренос на звук (или глас).
- Application – за пренос на апликации и бинарни податоци.
- Image – за пренос на слики.
- Message – за вметнување на порака во порака.

- Multipart – за комбинирање на неколку различни пораки.
- Text – за пренос на текст со јазична поддршка.
- Video – за пренос на видео.

Тековните MIME стандарди имаат 5 делови: RFC 2045, 2046, 2047, 4289 (кој го заменил 2048), и 2049. Тие го дефинираат телото на пораката, типот на медиум, не-ASCII екстензии во заглавјето, регистрациони процедури, и критериуми за потврда. Со оваа додатна функционалност, email-от овозможува attachment-и, а исто така и HTML. Иако MIME екстензиите овозможуваат бинарна содржина, таквата содржина се сместува во RFC 2822 со примена на Base64 кодирање, т.е. текстуален приказ на бинарни податоци.

9.3 СТАНДАРДИ ЗА ПРЕНОС НА ПОРАКИТЕ

За да се обезбеди компатибилност помеѓу различните email апликации, воспоставени се стандарди за пренос на mail. Во најпростото сценарио, електронската порака се испраќа од еден на друг локален корисник. Во овој случај, LDA ја сместува пораката во соодветното сандаче. Кога пораката се праќа на не-локален примач, MTA ја испраќа пораката од локалниот mail сервер на далечниот mail сервер. Во зависност од типот на системите, можни се различни MTA, кои имплементираат различни протоколи за пренос на пораките.

Најопшт MTA протокол за пренос е Simple Mail Transfer Protocol (SMTP). SMTP е de-facto Internet стандард за испраќање електронска пошта. Секој Internet-базиран систем за пораки мора да поддржува SMTP со цел да обезбеди поврзување со други email апликации. Секако - постојат и други MTA протоколи за пренос на пораки, но во најголемиот број случаи, таквите MTA се индивидуални и работат само на некои системи.

9.3.1 Едноставен протокол за пренос на пошта (SMTP)

Jon Postel од Универзитетот на Јужна Калифорнија го развил SMTP во август 1982. Како RFC 821, "SMTP бил развиен да обезбеди доверлив и ефикасен начин за пренос на пораки". На најбазично ниво, SMTP е минимален јазик што дефинира комуникациски правила за пренос на пораки. Сл. 9.2 ги дава SMTP командите и синтаксата дефинирана со RFC 2821, нов Simple Mail Transfer Protocol, кој го заменил RFC 821.

HELO <domain>	(Hello) Се конектира на сервер специфицирано со <domain>
MAIL FROM:<reverse-path>	Му го кажува на серверот идентитетот на праќачот даден со <reverse-path>
[Mail-parameters]	
RCPT TO:<forward-path>	(Recipient) Му го кажува на серверот идентитетот на примачот
[Rcpt-parameters]	<forward-path>
DATA	Го пренесува телото на пораката на сервер
RSET	(Reset) Ја ресетира серверската конекција
VRFY <string>	(Verify) Го прашува примачот дали го препознал корисникот

EXPN <string>	(Expand) Го прашува примачот дали ја препознал адресата
HELP [<string>]	Добива помошни информации
NOOP [<string>]	(No operation) Нема операција, но испраќачот е уште конектиран (“жив”)
QUIT	Ја затвора серверската конекција

Сл. 9.2: SMTP команди

Кога корисникот испраќа порака, клиентот го контактира својот SMTP сервер и прави “конверзација” со примена на SMTP јазик. MUA типично е дел од клиентската апликација (пр., Outlook, Eudora). Ако MUA е недостапен, пораките можат да се испратат преку telnet client конектиран на SMTP сервис. Сл. 9.3 прикажува едноставна SMTP конверзација преку telnet. Командите telnet и SMTP внесени од корисникот се дадени во bold. За време на една SMTP telnet сесија, може да се користи команда HELP за да се види кои SMTP команди се овозможени на серверот.

telnet mail.nowhere.com 25
Connected to mail.nowhere.com.
Escape character is '^]'.
220 test.mail.com SMTP Service (Sample Mail Сервер String)
HELO test.mail.com
250 test.mail.com
MAIL FROM: jdoe@nowhere.com
250 Sender <jdoe@nowhere.com> Ok
RCPT TO: jsmith@somewhere.com
250 Recipient <jsmith@somwhere.com> Ok
DATA
354 Ok Send data ending with <CRLF>.<CRLF>
Hello World!
.
250 Message received: GM1BAR00.F4M
QUIT
221 mail.nowhere.com SMTP сервер closing connection.
Connection closed by foreign host.

Сл. 9.3: Едноставна SMTP конверзација

Многу апликации (пр., email, Web, File Transfer Protocol) што работат серверски - му одговараат на клиентот користејќи banner. Banner е текстуална порака што содржи информации за серверот - на пр. кој оперативен систем го има, верзија исл. Овие информации може да бидат корисни за напаѓачите и треба да се сменат како што ќе кажеме подолу. Повеќето mail клиенти не прикажуваат никаков banner.

9.3.2 Екстензии на Simple Mail Transfer Protocol

Како што растел бројот на email корисници, се јавила потреба за дополнителни сервиси на клиентите и SMTP серверите. За да SMTP серверите ги поддржат додатните услуги, направени се екстензии на SMTP. Во 1993, RFC 1425 го воведува концептот на SMTP екстензија. Потоа, RFC 1425 бил наследен од RFC 1651 во 1994, RFC 1869 во 1995, и RFC 2821 во 2001. Овие RFC додаваат 3 делови во SMTP рамката:

- Нови SMTP команди (RFC 1425)
- Регистрација на SMTP сервисните екстензии (RFC 1651)
- Дополнителни параметри на SMTP MAIL FROM и RCPT TO командите (RFC 1869).

Заради компатибилност со старите SMTP сервери, се јавило потреба да клиентот може да одреди дали серверот поддржува екстензии. Ова се овозможило преку "enhanced hello" (EHLO) командата. Кога се конектира на сервер, mail клиентот може да активира команда EHLO. Ако серверот поддржува SMTP екстензии, тој успешно ќе одговори и ќе даде листа на екстензии што ги поддржува. Ако серверот не поддржува SMTP екстензии, тој ќе јави грешка и ќе му каже на MUA да комуницира со стандардната HELO команда. Серверите што поддржуваат SMTP екстензии, познати како Extended SMTP (ESMTP), обично одговараат со ESMTP во нивниот банер.

9.3.3 Сопствени Mail транспорти

Како што спомнавме, некои системи на MTA пораки не поддржуваат SMTP или ESMTP. Ваквите MTA се дизајнирани да работат во изолирана средина. Големите владини, академски, и приватни организации имаат свои MTA системи за пораки. Сепак, и овие организации користат SMTP или ESMTP-MTA за комуникација со надворешниот свет. Некои системи за пораки креирале сопствен MTA за Lotus Notes и Microsoft Exchange. Дискусијата за предностите и недостатоците на користењето на сопствен MTA протокол за пренос на пораки не спаѓа во доменот на оваа книга.

9.4 СТАНДАРДИ ЗА КЛИЕНТСКИ ПРИСТАП

Откако пораката е доставена од LDA, корисникот треба да пристапи на mail серверот за да ја побара пораката. Mail клиентите (MUA) се користат за пристап до mail серверот и за пребарување на пораките. Постојат неколку методи за клиентски пристап до поштенското сандаче, а наједноставен е - директниот пристап.

Наједноставно сценарио е кога сите корисници имаат директен пристап до своето сандаче (се среќава кај оперативниот систем Unix). За секој корисник на системот, постои сопствено сандаче во home директориумот на корисникот. Кога пораката ќе пристигне, корисникот може да стартува mail програма од командна линија, на пр. mail или pine, и директно да пристапи до своето сандаче. Иако овој метод е

едноставен, тој бара сите корисници што пристапуваат до mail серверот (за да преземат пораки), да имаат свој кориснички налог и пристап до командната линија на хостирачкиот оперативен систем.

Да им се дозволи на корисниците, (а посебно на надворешни корисници), да имаат пристап до командната линија - претставува значителен безбедносен ризик. За да се избегне овој ризик, развиени се протоколи за пристап до сандачето. Два најшироко распространети протоколи за пристап до сандаче се Post Office Protocol (POP) и Internet Message Access Protocol (IMAP). Тие се опишани во продолжение. Како и кај MTA протоколите за пренос на пораки, и тука постојат сопствени протоколи за пристап до сандаче кои се користат од некои големи корпорации. Важно е да се напомене дека POP, IMAP и повеќето приватни протоколи во својата default конфигурација користат текстуални password-и за автентикација, и како такви можат да бидат пресретнати од било кој хост приклучен во мрежата. Поглавјето 9.4.4 се осврнува на протоколите што ги користат Web-базираните mail клиенти.

9.4.1 Post Office Protocol

POP бил развиен во 1984. Суштината на POP е само да ги копира пораките од сандачето на mail серверот кај mail клиентот. Значи работи слично како обичните пошти. Mail клиентот отвора конекција до mail серверот, ги симнува сите пораки, и ја затвора конекцијата. Како што е опишано во RFC 918, кај POP биле можни само девет команди (делот “Basic Commands” на Сл. 9.5).

Basic Commands from RFC 918

USER <name>	Поставува username
PASS <password>	Поставува password
STAT	Го проверува статусот на mailbox, обично го дава бројот на пораки
LIST [msg]	Ги листа пораките од mailbox; опционен аргумент е [msg]
RETR <msg>	Ја пребарува пораката <msg>
DELE <msg>	Ја брише пораката <msg>
QUIT	Излегува
NOOP	No operation
RSET	Reset

Optional Commands from RFC 1939:

TOP <msg> <n>	Ги пребарува првите <n> линии од пораката <msg>
UIDL [msg]	Го бара единствениот id на [msg]
APOP <name> <digest>	Поробусен метод за автентикација во однос на USER/PASS

Extension Command from RFC 2449

CAPA	Побарува листа на опции поддржани од POP3 серверот

Сл. 9.4: POP 3 команди

По 1984, POP има неколку промени и неговата трета верзија се дефинира како RFC 1939. Основните команди се слични како оние од 1984; сепак, POP 3 нуди некои додатни команди, дадени на Сл 9.4. Од безбедносно гледиште, додавањето на

APOP е значајно, бидејќи е избегнат преносот на password. Наместо тоа, се користи механизам challenge/response, со кој клиентот одговара со криптографски hash на поставеното прашање од серверот (и со својот password), по што POP mail серверот го верифицира корисникот.

RFC 2449, POP3 екстензијата, им овозможува на клиентите да откријат додатни информации за POP3 серверите, како што се дополнителните команди што ги поддржуваат. POP сандачето има одредени ограничувања. Типично, кога корисникот ја бара својата порака, ја презема кај себе, и таа се брише од серверот. Ова значи дека само корисникот е одговорен за одржување на својата архива на пораки.

9.4.2 Internet протокол за пристап до пораки (IMAP)

За да се разрешат спомнатите проблеми на POP, во 1988 бил развиен IMAP. Протоколот IMAP е развиен како функционално над-множество на POP 2 протоколот. На најбазично ниво, IMAP бил дизајниран да користи сандачиња што се централно лоцирани и до кои се пристапува од повеќе email клиенти или MUA.

Иницијално, IMAP нудел многу малку функции што ги немал POP, но по 1988, тој прераснал во робусен протокол за пристап до сандачето. Тековната верзија на IMAP стандардот е RFC 3501: Internet Message Access Protocol – верзија 4, ревизија 1 (4rev1). Бидејќи IMAP 4rev1 поддржува многу особини, тој содржи многу повеќе команди во однос на POP. Табела 9.2 ги дава соодветните RFC на постоечките IMAP екстензии. IMAP е проширен со challenge/response механизам, слично како APOP, кој е наречен Challenge-Response Authentication механизам (CRAM). CRAM бара од клиентот да даде забелешка на прашањето поставено од серверот и да одговори со стринг кој се состои од името на корисникот, бланко, потпис кој се добива преку hash алгоритам врз временската марка на поставеното прашање од серверот, и користење на заедничка тајна - клучот.

Табела 9.2: RFC документи за IMAP екстензиите

IMAP Екстензија	**Соодветен RFC**
IMAP URL шема	2192
IMAP/POP AUTHorize екстензија за обичен Challenge/Response	2195
IMAP4 ID екстензија	2971
IMAP4 IDLE команда	2177
IMAP4 Login реферали	2221
IMAP4 Mailbox реферали	2193
IMAP4 Multi-Accessed сандаче	2180
IMAP4 именски простор	2342
IMAP4 не-синхронизирачки литерали	2088
IMAP4 QUOTA екстензија	2087
IMAP4 UIDPLUS екстензија	4315

9.4.3 Сопствени механизми за пристап до пошта

Сопствените протоколи за пристап до сандаче се дизајнирани да работат во затворени околини. Microsoft Exchange и Lotus Notes се примери на системи за пораки кои користат сопствени протоколи за пристап до сандаче. Овие сопствени протоколи имаат додатни функции кога се користат кај клиентите. Скоро сите сопствени механизми за пристап ги поддржуваат и стандардните протоколи, вклучително SMTP, POP, и IMAP, со цел да бидат компатибилни со другите MTA и MUA. Организациите мора да решат дали ќе поддржат сопствени протоколи во нивните email клиенти и сервери. Како што спомнавме погоре, без оглед дали стандардите се сопствени, повеќето протоколи се со слаби автентикациски механизми (користат некриптирани информации). Затоа, организациите треба да ги конфигурираат протоколите за да обезбедат појака форма на автентикација.

9.4.4 Web-базирани клиенти

Web-базираните mail клиенти сè повеќе се користат како средство за достава на пошта, бидејќи Web пребарувачите што овозможуваат пристап до клиентите се достапни на скоро секој Internet-уред. Корисникот може да стартува Web прелистувач и да се конектира на Web сајт што хостира Web-базиран клиент. Конекцијата се прави преку Hypertext Transfer Protocol (HTTP) или HTTP со безбедност на транспортно ниво (TLS), позната и како HTTPS. HTTPS ја криптира комуникацијата, што ја заштитува и автентикацискатa информација и содржината на пораката. Самиот HTTP не нуди никаква заштита, па организациите треба да користат HTTPS за Web-базираните mail клиенти.

Web-базираните mail клиенти комуницираат со нивните mail сервери со примена на протоколот за пристап до сандаче како и обичните mail клиенти - SMTP, POP, и IMAP, но и преку сопствени протоколи. Протоколите за пристап до сандаче се користат само помеѓу Web серверите и mail серверите; овие протоколи не служат за комуникација помеѓу Web серверите и Web прелистувачите.

9.5 ЕНКРИПЦИСКИ СТАНДАРДИ ЗА E-MAIL

Два главни механизми за заштита на содржината на email пораките се: Open Pretty Good Privacy (OpenPGP) и Secure/Multipurpose Internet Mail Extensions (S/MIME). И двата се базираат на криптографија со јавен клуч, пришто корисникот мора да има пар од клучеви: јавен клуч што може да го знае секој, и приватен клуч што го знае само сопственикот. Јавниот клуч на примачот се користи за испраќање на криптираните информации што можат да се декриптираат само со приватниот клуч. Приватниот клуч на испраќачот се користи за испраќање на дигитално потпишани информации, чија автентичност може да биде верификувана од секој што го има јавниот клуч. Дигиталните потписи се креираат врз база на т.н. заверка на информацијата (т.е., пораката е испратена) со помош на криптографски hash, која може да биде потпишана поефикасно отколку целата порака.

Продуктите базирани на OpenPGP и S/MIME се способни за енкрипција на пораките за да ја заштитат нивната содржина, и за потпишување на пораките - за

да се гарантира нивниот интегритет и да се потврди идентитетот на испраќачот. Во многу случаи, пораките се потпишуваат, но не се криптираат, бидејќи доверливоста на пораката не мора да се заштитува. Ако пораката треба да се криптира, таа скоро секогаш е потпишана за да примачот биде сигурен дека пораката е легитимна.

Заради пресметковната комплексност на криптографијата со јавен клуч, поефикасната криптографија со симетричен клуч исто така се користи за заштита на email. Криптографијата со симетричен клуч бара еден заеднички клуч помеѓу комуникациските страни, испраќачот и примачот на пораките. Процесот обично бара да испраќачот генерира случаен клуч и да ја криптира пораката со алгоритам за симетричен клуч. Потоа испраќачот го криптира клучот со јавниот клуч на примачот со алгоритам за јавен клуч, и ги праќа и криптираната порака и криптираниот симетричен клуч на примачот. Овој процес е хибриден и користи јавен клуч само за енкрипција на симетричниот клуч. Бидејќи само примачот го има приватниот клуч што е потребен за откривање на симетричниот клуч, никој друг нема да може да ја декриптира пораката.

Иако денес S/MIME и OpenPGP се два најважни стандарди за енкрипција на email, многу други механизми се предложени во меѓувреме. Еден од тие механизми е Privacy Enhanced Mail (PEM), развиен во 1987, и MIME објектно-безбедносни сервиси (MOSS). Бидејќи тие не се широко прифатени, нема да ги објаснуваме во детали.

Иако енкрипцијата на email-от обезбедува голема безбедност, таа има одредена цена, па организацијата треба да реши дали ќе го криптира својот email:

- Скенирањето за вируси и други штетни компоненти кај firewall-от и mail серверот е многу посложено ако користите енкрипција. Ако firewall-от или mail серверот нема метод за декрипција, нема да може да ги чита пораките за во нив да открие вирус.

- Енкрипцијата и декрипцијата бараат процесорско време. Организациите можеби ќе треба да купат нова - побрза опрема за оваа намена.

- Организациите што користат енкрипција можеби ќе треба да вработат додатен персонал. Тој ќе се грижи за генерирање и распределба на клучевите, исл.

9.5.1 OpenPGP

OpenPGP претставува протокол за криптирање пораки и креирање сертификати со помош на криптографија со јавен клуч. Тој е базиран на претходно развиениот PGP, креиран од Phil Zimmerman и имплементиран како продукт во јуни 1991. Иницијалниот PGP бил приватна сопственост и користел енкрипциски алгоритми кои исто така биле интелектуална сопственост. Во 1996, дефинирана е верзија 5.x на PGP од IETF RFC 1991, т.н. PGP формат за рамена на пораки. Следствено, OpenPGP е развиен како нов стандард базиран на PGP верзија 5.x.

OpenPGP се дефинира со RFC 2440, OpenPGP формат на пораки, и RFC 3156, MIME безбедност со OpenPGP.

Многу бесплатни и комерцијални продукти што го користат OpenPGP стандардот се достапни на пазарот. Софтверот може да се симне или купи од Web сајтови, од кои некои се дадени во Табела 9.3.

Табела 9.3: OpenPGP софтвери

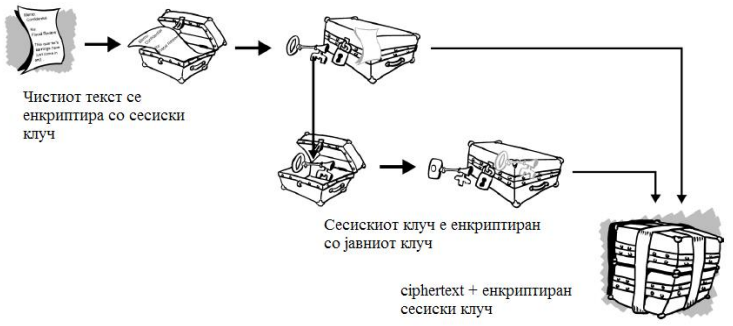
Организација	**URL**
Free Software фондација	http://www.gnupg.org/
Hushmail	http://www.hushmail.com/
International PGP site	http://www.pgpi.org/
OpenPGP site	http://www.openpgp.org/
PGP Site (комерцијална верзија)	http://www.pgp.com/

Некои OpenPGP-базирани продукти целосно поддржуваат криптографски алгоритми препорачани од Федералната влада на САД со NIST стандард- FIPS PUB 140-2 и други публикации, кои ги вклучуваат следните алгоритми:

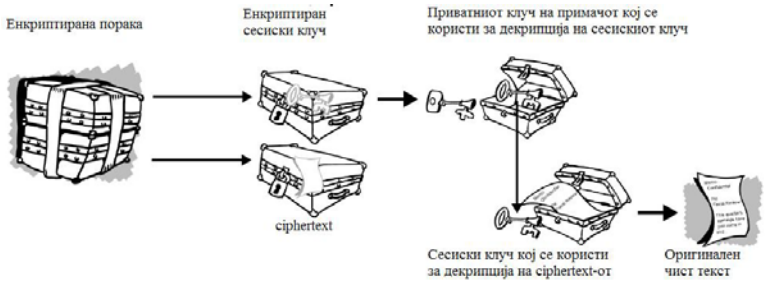
- Троен Data Encryption Standard (3DES) за податочна енкрипција,
- Напреден (Advanced) Encryption Standard (AES) за податочна енкрипција.

Државните агенции во САД мора да користат FIPS- (Федерални информатичко-процесирачки стандарди) -одобрени криптографски алгоритми. CMVP Web сајтот е лоциран на http://csrc.nist.gov/cryptval/; тој содржи целосна листа на FIPS-одобрени алгоритми.

- Digital Signature Algorithm (DSA) - алгоритам за дигитален потпис,
- RSA алгоритам за дигитален потпис,
- Secure Hash Algorithm (SHA-1, SHA-256) - алгоритам за хеширање.



Сл. 9.5: PGP системот за енкрипција.



Сл. 9.6: PGP системот за декрипција.

Некои имплементации на OpenPGP поддржуваат други енкрипциски шеми кои не ги спомнавме. Државните институции треба да користат алгоритми што се одобрени од Владата. И други организации може да изберат енкрипциски алгоритми одобрени од Владата, бидејќи се добро тестирани и многу сигурни. Многу не-одобрени алгоритми биле пробиени. Затоа, не-одобрените алгоритми (пробиени или не) може да внесат ранливост за организацијата ако ги користи. Ако институцијата избере OpenPGP-базирани продукти, таа треба да го следи упатството од Табела 9.4:

Табела 9.4: Препорачани OpenPGP шифрирања

Се препорачува за:	**Шифрирање**
Највисока безбедност:	Енкрипција: Advanced Encryption Standard (AES) 128, 192, или 256-битна енкрипција Автентикација и заверка: дигитален потпис (DSS) или RSA со големина на клуч 2048 бита или поголема, и SHA со големина 256 бита (SHA-256)
Безбедност и перформанси:	Енкрипција: AES 128-битна енкрипција Автентикација и заверка: DSS со големина на клуч 1024 бита или повеќе и SHA-1
Безбедност и компатибилност:	Енкрипција: троен Data Encryption Standard (3DES) 168/112-битна енкрипција (забелешка: 3DES е значително побавен од AES) Автентикација и заверка: DSS со големина на клуч 1024 бита или повеќе и SHA-1
Автентикација и детекција на напад:	Автентикација и заверка: DSS со големина на клуч 1024 бита или повеќе и SHA-1 / SHA-256

Иако некои опции на OpenPGP не користат криптографија со јавен клуч, како на пр. дигиталното потпишување на пораките, самата енкрипција на пораката се прави со алгоритам со симетричен клуч, како што кажавме погоре. Во продолжение даваме опис на потпишувањето и енкрипцијата на порака со OpenPGP (некои чекори се можни и во друг редослед):

- OpenPGP го компресира текстот, со што се редуцира времето на пренос, се зајакнува криптографската безбедност и се оневозможуваат напаѓачите да пребаруваат по клучен збор.
- OpenPGP креира случајна сесија за клуч (во некои имплементации на OpenPGP, корисниците треба да го движат глушецот случајно по екранот за да се генерира клуч).
- Дигиталниот потпис се генерира од пораката со користење на приватниот клуч на испраќачот, кој се додава кон пораката.
- Пораката и потписот се енкриптираат со сесискиот клуч и симетричен алгоритам (пр., 3DES, AES).
- Сесискиот клуч се енкриптира со јавниот клуч на примачот и се додава на почеток од криптираната порака.
- Криптираната порака се испраќа кон примачот.

Примачот ги прави обратните чекори за да го добие сесискиот клуч, да ја декриптира пораката, и да го верифицира потписот. Популарните email клиенти како Mozilla Thunderbird, Apple Mail, Eudora, и Microsoft Outlook бараат инсталирање на plug-in за да му овозможат на корисникот да праќа и прима OpenPGP-криптирани пораки. OpenPGP дистрибутерите нудат инструкции како се користи OpenPGP преку различни клиентски апликации. Тие претставуваат и безбедносни gateway сервери што можат да користат OpenPGP за енкрипција, декрипција, и потпишување на пораките во име на корисниците.

9.5.2 S/MIME

S/MIME, кој оригинално бил предложен во 1995 од RSA Data Security, Inc., се базира на нивниот сопствен (и широко поддржан) стандард за енкрипција со јавен клуч (PKCS) #7 за податочен формат на криптирани пораки, и X.509 верзија 3 - стандардот за дигитални потписи. S/MIME верзија 2 добил широка прифатеност кај Internet mail индустријата. Иако не е признат како IETF стандард, тој е специфициран со следните меѓународни RFC:

- S/MIME верзија 2 - спецификација за пораките (RFC 2311)
- S/MIME верзија 2 - ракување со сертификати (RFC 2312)
- PKCS #1: RSA енкрипција, верзија 1.5 (RFC 2313)
- PKCS #10: Барање за сертификати, верзија 1.5 (RFC 2314)
- PKCS #7: Синтакса за криптографски пораки, верзија 1.5 (RFC 2315)
- Опис на RC2 енкрипциискиот алгоритам (RFC 2268).

S/MIME верија 3 бил развиен од IETF S/MIME работната група и е прилагоден на IETF стандардот во јули 1999. S/MIME верзија 3 е специфициран со следните RFC:

- Криптографска синтакса на пораките (RFC 3852)
- S/MIME верзија 3 спецификација за пораки (RFC 3851)
- S/MIME верзија 3 ракување со сертификати (RFC 3850)
- Diffie-Hellman метод за договор за клучот (RFC 2631)
- Проширени сервиси за безбедност на S/MIME (RFC 2634).

IETF S/MIME работната група денес го координира целокупниот развој на S/MIME стандардот. Бидејќи бил развиен во 1995, стандардот S/MIME требало да ги помине сите американски закони за извозна контрола на криптографски код. Тоа значело дека S/MIME имплементацијата била принудена да поддржува несигурен 40-битен RC2 алгоритам. Овие контроли денес се послаби. Сепак, заради барањата да се поддржи 40-битен RC2, S/MIME е критикуван како "криптографски слаб." Ова е точно само кога ќе се применува слаб алгоритам. До денес – јавно не се евидентирани слабости на протоколот S/MIME. Сепак, S/MIME клиентите што користат енкрипција со 40-bit RC2 можат да бидат кракирани со методот brute force преку Windows. S/MIME е компатибилен со голем број енкрипциски алгоритми што му овозможуваат да биде целосно сигурен. Процесот со кој S/MIME- mail клиентите ги испраќаат пораките е сличен со оној на OpenPGP.

Најзначајна особина на S/MIME е неговата внатрешна "автоматска" природа. Заради вмешаноста на многу производители, S/MIME функционално постои како инсталација на повеќе email клиенти, како што се Mozilla и Outlook Express. Исто како и OpenPGP, постојат безбедносни gateway сервери што го користат S/MIME за енкрипција, декрипција, потпишување и верификување на email пораките во име на корисниците. S/MIME верзија 3.1 поддржува два енкрипциски алгоритми поддржани со FIPS PUB 140-2: AES, кој е препорачан, но опционален за имплементација, и 3DES, кој е обврзан за сите имплементации. За да се задржи и компатибилност со претходните верзии, S/MIME исто така поддржува и RC2 64-битен и DES.

9.5.3 Избор на алгоритам за енкрипција

Изборот на соодветен алгоритам за енкрипција зависи од неколку фактори кои се различни за секоја организација. Иако можеби изгледа дека треба да се користи најјаката енкрипција што е достапна, тоа не секогаш е точно. Ако е повисоко нивото на енкрипција, поголемо е нејзиното влијание врз перформансите на mail клиентот и врз брзината на комуникацијата, бидејќи енкрипцијата значително ја зголемува големината на email пораките. Исто така, некои земји сеуште имаат рестрикции за увоз, извоз и користење на криптографија. Патентите и лиценците исто така влијаат врз енкрипциските шеми кои се користат во различни земји. Конечно, изборот на email енкрипцискиот стандард (OpenPGP, S/MIME, исл.) може да го лимитира изборот на енкрипциски алгоритам. За среќа, владините институции користата едноставен и моќен стандард - 3DES или AES.

Фактори кои влијаат врз изборот на енкрипциски алгоритам се следните:

- Заштита.
- Вредност на податоците за организацијата и нејзините ентитети. Колку се повредни податоците, толку треба да биде појака енкрипцијата.
- Временско значење на податоците. Ако податоците се скапи само во краток временски период (пр., денови, а не години), може да се примени и послаб метод за енкрипција. Таков пример се password-те што се менуваат на дневна база, па

применетата енкрипција ќе го заштитува password-от само 24 часа.
- Закани за податоците. Ако нивото на закана е високо, појака треба да биде енкрипцијата.
- Други заштитни мерки што ја редуцираат потребата за јака енкрипција. Пример се заштитените комуникациски мрежи (посебни затворени кругови) наместо јавен Internet.
- Перформанси. Барањата за високи перформанси сугерираат примена на слаба енкрипција, но ова не би требало да важи за email-от.
- Системски ресурси. Послабите ресурси, како на пр. процесорска брзина или помала меморија (пр. кај рачните компјутери) може да бара послаба енкрипција, но ова не важи за email клиентите.
- Законски рестрикции. Рестрикциите за увоз, извоз и користење на криптографија во некои земји се пример за ограниченоста на изборот.
- Енкрипциски шеми. Криптографските апликации што се поддржани од mail клиентот и оперативниот систем можат да влијаат врз изборот на алгоритам.

9.5.4 Менаџмент со клучевите

Најголема разлика помеѓу OpenPGP и S/MIME е во менаџментот на клучевите. Традиционалниот модел што го користи OpenPGP за менаџмент со клучевите се вика "web на доверба", и нема централен клуч или одговорен авторитет. Web-от на доверба се базира на корисничкиот менаџмент и контрола. Ова е погодно за индивидуални корисници и мали организации, но е неприменливо за средни и големи организации. Затоа, S/MIME работи со класичен, хиерархиски дизајн. Типично, постои главна регистрација т.е. авторитет што одобрува, наречен Certificate Authority (CA), со подредени локални авторитети за регистрација. Табела 9.5 прикажува некои од независните S/MIME CA.

Табела 9.5: S/MIME CA

Име на CA	**URL**
Entrust	http://www.entrust.com/
Thawte	http://www.thawte.com/
Verisign	http://www.verisign.com/

По default, S/MIME-овозможените mail клиенти зависат во довербата од нивните надредени CA кога обработуваат S/MIME трансакции. Овој авторитет е или независен (third-party) CA, како во Табела 9.5, или CA што е контролиран од организација што издава сертификати.

Размената помеѓу OpenPGP и S/MIME-заштитените email-и помеѓу различни организации обично е многу сложено, и нетранспарентно за корисниците. Најголем предизвик претставува размената на клучеви и воспоставувањето на

врска на доверба помеѓу организациите. Организациите можат да ги користат сопствените PKI, или да користат заеднички независен PKI, но во секој случај има технички и законски проблеми. Исто така, поддршката за OpenPGP и S/MIME се разликува во зависност од тоа кој email клиент се користи. Постојат и независни сервиси што им овозможуваат на организациите да разменуваат криптиран email без да воспостават врска на доверба и без да се грижат за компатибилноста на mail апликациите, но таквите сервиси бараат сместување на доверливите пораки на тие third-party (независни) сервери, што може да претставува безбедносна закана.

Почнати се одредени обиди за олеснување на менаџментот со клучеви. Енкрипцијата базирана на идентитет (IBE) е еден вид енкрипција со јавен клуч што дозволува било кој стринг да се користи како јавен клуч. Со примена на email адресите како јавни клучеви, IBE може да го упрости менаџментот со клучеви, со што ќе им го олесни на испраќачите праќањето на email пораките. OpenPGP и S/MIME стандардите не поддржуваат IBE, но почнати се Internet-дебати за тоа како IBE треба да се вметне во S/MIME.

9.5.5 OpenPGP versus S/MIME

Изборот помеѓу OpenPGP и S/MIME зависи од многу фактори. Многу email продукти се способни да ги поддржат и двата протоколи. Разликите во самите протоколи, а не во нивните софтверски имплементации, се примарен фактор за избор на едниот или другиот. Предности на OpenPGP се следните:

- Погоден за мали групи и поединци,
- Не бара, но поддржува, надворешна инфраструктура со јавен клуч (PKI) ако е потребно (S/MIME бара организацијата да купи сертификати или да постави свој сертификатен авторитет),
- Може да се користи со било кој mail клиент, иако со повеќе чекори.

Предности на S/MIME се:

- Погоден е за големи групи и организации,
- Покомпатибилен е со енкрипциските стандарди,
- Поддржува вградени email клиентски апликации,
- По-транспарентен е за крајниот корисник.

9.6 КОРИСТЕЊЕ НА MAIL СЕРВЕР

По осигурувањето дека оперативниот систем на mail серверот е целосно безбеден, следниот чекор е да се инсталира mail серверска апликација и да се заштити од можните закани. Во продолжение ќе ги изложиме овие две акции.

Во многу случаи, безбедната инсталација и конфигурација на mail серверската апликација е слично со инсталирањето на оперативен систем. Битен принцип е да се инсталираат само сервисите потребни за mail серверот и да се елиминираат ранливостите преку соодветни закрпи. Сите непотребни апликации и сервиси што

се инсталирани – треба да се избришат откако е инсталиран mail серверот. За време на инсталацијата на mail сервер, треба да се направат следните чекори:

- Инсталирајте го mail серверскиот софтвер на посебен хост,
- Применете ги сите закрпи за веќе познатите ранливости,
- Креирајте посебен физички диск или логичка партиција (посебно од оперативниот систем и mail серверската апликација) за поштенските сандачиња, или чувајте ги сандачињата на посебен сервер,
- Избришете ги или оневозможете ги сите сервиси што се инсталирани на mail серверот, а што не се потребни (пр., Web-базиран mail, FTP, далечинска администрација),
- Од серверот избришете ја целата документација за производителот,
- Избришете ги сите тест-фајлови од серверот,
- Применете соодветен безбедносен template за серверот,
- Реконфигурирајте ги SMTP, POP, и IMAP сервисните банери за да не ги јавуваат типот и верзијата на mail серверот и оперативниот систем (ова можеби нема да биде можно за некои mail сервери),
- Оневозможете ги опасните и непотребни mail команди (пр., VRFY и EXPN).

9.6.1 Конфигурирање на оперативниот систем и mail сервер-от

Повеќето оперативни ситеми на mail серверите овозможуваат да се специфицираат привилегиите за пристап индивидуално за фајловите, уредите, и другите ресурси што се наоѓаат на хостот. Секоја информација дека mail серверот има пристап до одредени контроли - може потенцијално да биде дистрибуирана до сите корисници што пристапуваат на mail серверот. Софтверот на mail серверот најчесто вклучува механизми за обезбедување дополнителни контроли за пристап до фајловите, уредите и ресурсите - специфични за нивната употреба. Важно е да се постават идентични дозволи за оперативниот систем и за mail серверската апликација; во спротивно, може да се појави преголем или премал пристап за некои корисници. Mail серверските администратори треба да проучат како најдобро се конфигурираат контролите за пристап за да ги заштитат информациите што се наоѓаат на јавниот mail сервер од две перспективи:

- Го ограничува пристапот на mail серверската апликација до множеството на системски ресурси,

- Го ограничува пристапот на корисниците преку додатни контроли на пристап дефинирани од mail серверот, опишани со подетални нивоа на пристап.

Соодветните поставки на контролата на пристап можат да го спречат ширењето на рестриктивните информации кон јавноста за која не се наменети. Исто така, контролата на пристап може да го ограничи користењето на ресурсите при појава на DoS напад врз mail серверот.

Типични фајлови до кои треба да се контролира пристапот се следниве:

- Апликативниот софтвер и конфигурациските фајлови,
- Фајлови кои се поврзани со безбедносните механизми,
- Password hash фајлови и други фајлови за автентикација,
- Фајлови што содржат авторизациска информација што се користи за контрола на пристап,
- Криптографски клучеви што се користат за доверливост, интегритет, и други заштитни сервиси,
- Серверскиот log и системските audit фајлови,
- Системскиот софтвер и конфигурациските фајлови.

Треба да се обезбеди да mail серверската апликација се извршува уникатно за индивидуалните корисници и групи - со многу рестриктивна контрола на пристап. Така, треба да се дефинираат посебни идентитети за новите корисници и групи, кои ќе се користат во mail серверскиот софтвер. Новиот корисник и новата група треба да се независни и единствени во однос на другите корисници и групи. Ова е потребно во имплементацијата на контролата на пристап што е опишана подолу. Иако серверот може да биде стартуван преку root (Unix) или преку администраторски (Windows 2000/2003) привилегии кои се доделуваат на соодветните TCP порти, на серверот не му се дозволува да продолжи да работи на тоа ниво на пристап.

Исто така, mail серверскиот оперативен систем се применува за да го ограничи пристапот до фајловите од mail серверските процеси. Овие процеси треба да имаат read-only пристап до фајловите што се потребни за извршување на сервисот и не треба да имаат пристап до други фајлови, како на пр. серверските log фајлови. Контролата на пристап на оперативниот систем на mail серверот се користи за следното:

- Привремените фајлови креирани на mail серверот се сместуваат само во точно одреден под-директориум (ако е можно).

- Пристапот до привремените фајлови креирани од mail серверот е лимитирано само на процесите од mail сервер-от што ги креирале тие фајлови (ако е можно).

Потребно е да се обезбеди да mail серверот не може да снима фајлови надвор од специфицираната фајл структура доделена на mail серверот. Ова може да биде конфигурирано во серверскиот софтвер, или да биде опција во оперативниот систем со која се контролира серверскиот процес. Осигурете се дека до таквите

директориуми и фајлови (надвор од специфицираното директориумско стебло) не може да се пристапи, дури и кога корисниците ги знаат локациите на тие фајлови.

Да ја разгледаме командата “chroot jail” од Linux и Unix хостовите, која се применува на mail серверите. Примената на chroot го менува погледот на mail серверскиот фајл систем, така што root-директориумот не е вистинскиот root directory, туку еден од неговите под-фолдери. Така, ако mail серверот биде нападнат, напаѓачот ќе има пристап само до одреден дел од фајл системот, кој е достапен со chroot. Ова е многу моќна безбедносна мерка.

За да ги избегнеме ефектите на одредени DoS напади, го конфигурираме mail серверот така што да ги ограничи ресурсите на оперативниот систем што може да ги конзумира. Такви примери се следниве:

- Инсталација на корисничките сандачиња, по можност, на различни серверски дискови, или логички партиции, а не онаму каде што е оперативниот систем и mail серверската апликација,
- Конфигурирање на mail серверската апликација така што да не може да го потроши целиот простор на хард дискот или на партицијата,
- Лимитирање на големината на attachment-и што се дозволени,
- Обезбедување log фајловите да се чуваат на локација која има соодветна големина.

9.6.2 Заштита на Email од malware (штетни компоненти)

Email-от интензивно се користел како средство за испраќање на бинарни фајлови во форма на attachment. Иницијално, ова не претставувало безбедносен ризик, бидејќи attachment-те биле мали word документи или слики. Откако организациите почнале да го користат email-от за секојдневна соработка, величината и типот на email attachment-те пораснале. Денес, многу email пораки се испраќаат со attachment-и кои се егзекутивни програми, слики, и музика. Многу форми на malware, вклучително вируси, црви, тројански коњи, и spyware сакаат да ја нарушат приватноста на корисникот и се пренесуваат преку attachment. Вообичаено, напаѓачите користат email при напад на одредени организации пред да се открие типот на ранливост. Цел на овие напади најчесто е софтверот, т.е. му даваат контрола на напаѓачот над корисничките работни станици. Оваа контрола значи доделување привилегии, пристап до доверливи информации, мониторинг на корисничките акции (пр., тастери), и одредени штетни акции.

Ако се смета дека email attachment-те се битни, администраторот на mail серверот треба да одлучи кои типови на attachment-и ќе ги дозволи. Наједноставен пристап е да се дозволат сите типови attachment-и. Ако тоа е случај, тогаш треба да се инсталира некаков malware скенер (пр., anti-virus, anti-spyware) на патеката на пораките, а пожелно е и кај клиентот, за да ги спречи штетните егзекутивни attachment-и да се стартуваат. Подобар пристап е да се забранат опасните attachment-и (пр., .vbs, .ws, .wsc file екстензии) кај mail серверот / mail gateway-от, а

останатите пораки пак да се скенираат. Иако филтрирањето на некои екстензии е добар чекор, неговата ефикасност е лимитирана, бидејќи напаѓачите ги менуваат екстензиите. Наместо проста проверка на екстензијата, филтерот треба да ги провери header-от, footer-от, и други аспекти на фајлот со цел да го идентификува attachment-от.

Филтрирањето на attachment-и е неефикасно ако се забранат сите attachment-и. Некои од најупотребуваните attachment-и, како оние од office пакетите, исто така имаат одреден ризик. Софистицираните напаѓачи можат да го вметнат штетниот код на различен начин. На пример, напаѓачот може да прати по email - hyperlink до некој штетен Web site; ако корисникот кликне на линкот и користи HTTPS наместо HTTP, штетниот фајл ќе се симне маскиран од HTTPS, со што ќе ги заобиколи мрежните безбедносни контроли. Организациите треба да ги филтрираат активните hyperlink-ови од email пораките за да го спречат ова, но ова ќе ја намали употребливоста на email пораките кај корисниците.

Email енкрипцијата го прави филтрирањето посложено и неефикасно. Откако пораката е криптирана, филтрирањето на mail сервер-от и периметарските уреди е неефикасно, бидејќи треба да се декриптира пораката, да се скенира, и да се рекриптира. Ова е проблем, бидејќи бара големи перформанси. Постојат и проблеми со приватноста ако се примени овој тип на решение. Општо кажано, ако се користи енкрипција, филтрирањето треба да се прави кај клиентот (на работна станица).

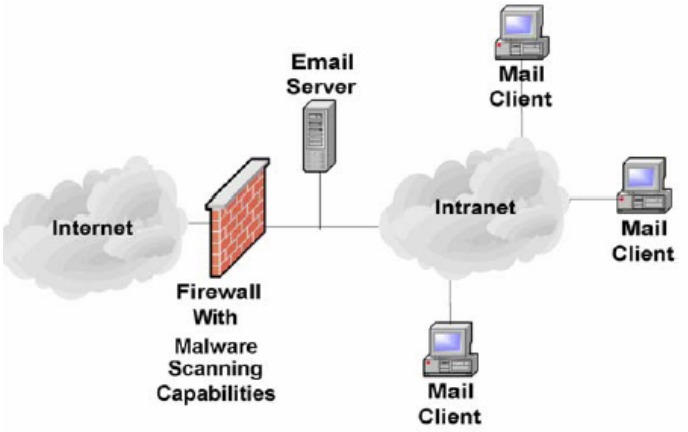
Покрај со email attachment-те, malware може да се пренесува преку email и со други средства. На пример, многу email клиенти поддржуваат HTML-базирани пораки. Овие пораки често имаат активна содржина во форма на клиентски скриптен јазик што може да го зарази клиентот. Најпопуларни типови на активна содржина се ActiveX, Java, JavaScript, и Visual Basic Script (VBScript). Организациите треба да одлучат дали ќе ги блокираат или не активните содржини од mail пораките. HTML-базираните пораки исто така може да содржат несакани компоненти, како spam и phishing. Phishing се однесува на користење на email-от за залажување на поединци да издадат доверливи лични информации. На пример, напаѓачот може да испрати email пораки што изгледаат како да се пратени од добро-позната организација, како на пр. некоја финансиска институција (банка). Email-от е наменет да ги предизвика корисниците да одговорат на него и да ги пратат своите лични податоци. Ако mail серверот нема софтвер за скенирање malware (пр., anti-virus софтвер, anti-spyware), или софтверот е неефикасен, ќе постои потенцијална безбедносна закана за крајните корисници.

9.6.3 Скенирање на malware

За да се заштитиме од вируси, црви, и други типови на malware, потребно е скенирање во една или повеќе точки од процесот на доставување email. Malware скенирањето може да се имплементира на firewall, mail relay, или mail gateway т.е. на местото каде што поштата влегува во организациската мрежа, или на самиот mail сервер, но и на клиентските компјутери. Секоја опција има свои јаки и слаби страни, како што ќе видиме подолу. Општо земено, организацијата треба да имплементира најмалку две нивоа на of malware скенирање - едно на клиентско

ниво и едно на mail сервер или firewall/mail relay/mail gateway ниво, а пожелно е да имплементира и скенирање на сите три нивои.

Првата операција е скенирање на malware кај firewall-от (апликациски proxy), mail relay (Сл. 9.7), или mail gateway, кој ги пресретнува пораките пред тие да стигнат во mail серверот. Уредот слуша на порта TCP 25 за SMTP конекции, ги скенира сите пораки, и ги проследува пораките што не содржат malware кон mail серверот, кој се конфигурира да слуша на слободна порта, а не вообичаената порта 25. Слабост на овој пристап е што постојаното скенирање на SMTP-текот ги редуцира перформансите на firewall/ mail relay/ mail gateway-от. Дали падот на перформансите ќе биде голем ќе зависи од оптоварувањето со пораки, т.е. од бројот на email-ви дневно и од нивната величина. Еден метод за подобрување на перформансите е да се прави malware скенирањето на посветен сервер.



Сл. 9.7: Скенирање за malware имплементирано со firewall

Предностите на скенирањето пошта со помош на firewall, mail relay, или mail gateway се следниве:

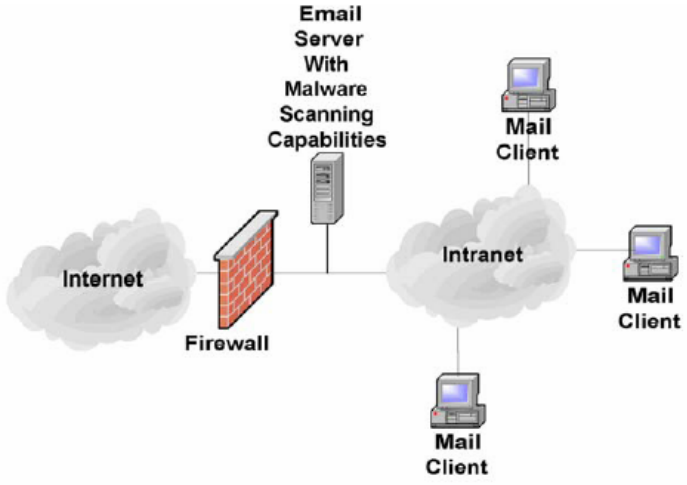
- Поштата може да се скенира и во двете насоки (кога влегува и кога излегува од организацискатa мрежа),
- Може да ги стопира поголемиот број пораки што содржат malware во периметарот - пред да влезат во мрежата и да стигнат до mail серверот,
- Можат да имплементираат скенирање на поштата што доаѓа со мали промени во конфигурацијата на mail серверот,
- Може да се редуцира бројот на пораки што стигнуваат во mail серверот, овозможувајќи му да работи поефикасно - т.е. со помала оперативна цена,
- Може централно да се управува со скенирањето за да се обезбеди компатибилност со организацискатa безбедносна политика и регуларна примена на ажурирана листа на штетни кодови (вируси исл.),

- Некои mail firewall уреди, можат да обезбедат сигурносна автентикација за пристап до Web-базирани mail апликации.

Скенирањето на malware со помош на firewall, mail relay, или mail gateway има и одредени слабости:

- Може да бара модификација на конфигурацијата на mail серверот кога ја скенира излезната пошта,
- Не може да скенира криптирани пораки,
- Не нуди заштита на внатрешните корисници откако штетната компонента ќе влезе во мрежата, освен ако мрежата не користи посебен скенер за SMTP сообраќајот, пред тој да дојде до mail серверот,
- Бара појаки (поскапи) сервери и уреди - потребни за големите организации.
- Може да детектира само закани што се идентификувани; нуди слаба заштита за новите ранливости.

Втора опција за сместување на malware - скенерот е самиот mail сервер (Сл. 9.8). Достапни се многу независни апликации за скенирање на содржината на пораките кај популарните mail сервери. Овие апликации го проверуваат email-от што се испраќа локално помеѓу внатрешните корисници, и кој не поминува низ организацискиот firewall/ mail relay/ mail gateway. Скенирањето кај mail серверот обезбедува и дополнително ниво на заштита од malware, и оневозможува внатрешно ширење на malware-от. Некои mail сервери нудат програмски интерфејси (API) што поддржуваат интеграција на malware скенирање, филтрирање на содржини, блокирање на attachment-и, и други безбедносни сервиси внатре во MTA.



Сл. 9.8: Скенирање за malware имплементирано кај mail сервер-от

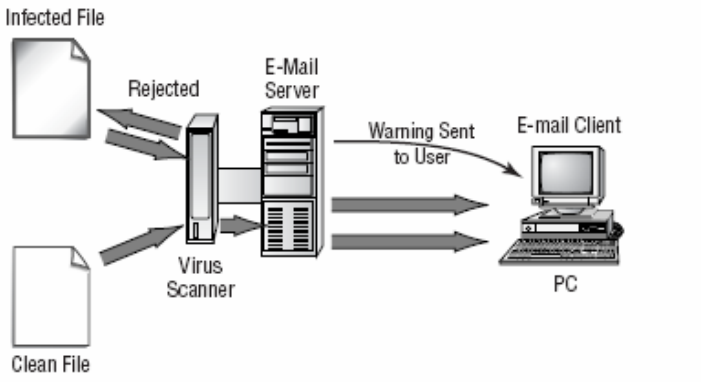
Главна слабост на malware скенирањето кај mail серверот е негативниот ефект врз перформансите на mail серверот, предизвикан од потребата да се скенираат сите

пораки. Друга слабост е што malware скенирањето кај mail серверот бара значајни модификации на постоечката конфигурација на mail сервер-от. Сепак, оваа опција обезбедува и некои предности:

- Може да скенира во две насоки (влезна и излезна),
- Може да се менаџира централно за да се обезбеди компатибилност со безбедносната политика на фирмата и да се ажурира постојано,
- Нуди заштита на внатрешните корисници во случај да штетната компонента влегла во внатрешната мрежа.

Скенирањето на malware кај mail серверот има и одредени слабости:

- Бара значајни промени на конфигурацијата на mail серверот (не мора да бара само кај новите mail сервери),
- Не може да скенира криптирани пораки,
- Бара помоќни (поскапи) сервери - потребни за големите организации.
- Може да детектира само закани што се идентификувани; нуди слаба заштита за новите ранливости.



Сл. 9.9: Скенирање за вируси имплементирано кај mail сервер-от

Кога се применува malware скенирање кај mail сервер-от, треба да се знае дека тоа:

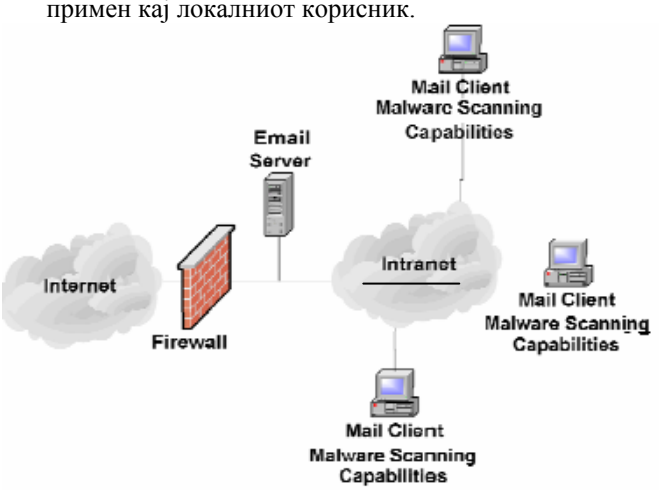
- Детектира и чисти разни типови на malware типични за email (пр., вируси, црви, тројански коњи, spyware),
- Овозможува евристичко скенирање (заштита од нови и непознати типови malware),
- Овозможува филтрирање на содржина,
- Има механизми за заштита од внатрешни пораки,
- Овозможува лесен менаџмент,
- Овозможува автоматско симнување и инсталирање на update-ти,
- Овозможува често ажурирање (многу битно),
- Може да идентификува различен тип на содржини,
- Овозможува робусен механизам за тревожење,

- Овозможува детална евиденција.

Malware скенерите исто така може да се наоѓаат и кај клиентот (Сл. 9.10). Овој тип на malware скенер се инсталира на работните станици и мобилните уреди (PDA). Влезните пораки се скенираат кога ќе се отворат од корисникот, а излезните пораки се скенираат кога ќе бидат испратени. Најважна предност на оваа конфигурација е што скенирањето е дистрибуирано низ многу хостови и затоа товарот има минимален ефект врз секој индивидуален систем. Исто така, ако клиентската машина се зарази со malware, ова ниво на заштита може да го стопира malware-от од ширење кон mail серверот и другите mail клиенти.

Предности на клиентското скенирање на malware се следните:

- Не бара модификација на mail серверот,
- Може да скенира криптирани пораки, кога се декриптираат кај корисникот,
- Го дистрибуира malware скенирањето и со тоа го намалува оптоварувањето на серверот,
- Нуди заштита на внатрешните корисници, дури и кога malware-от е примен кај локалниот корисник.



Сл. 9.10: Скенирање за malware имплементирано на Workstation

Недостатоци на клиентското скенирање на malware се следните:

- Тешко е за централизирана контрола, посебно за мобилните клиенти (пр., laptop-и),
- Потребно е време да се ажурираат сите клиенти, што внесува можност за одредени ранливости,
- Може несакајќи да биде стопирано од одредени корисници.
- Може да детектира само закани што се идентификувани; нуди слаба заштита за новите ранливости.

За да се обезбедат повеќе нивоа на заштита од malware, организациите треба да применуваат продукти од различни производители. Бидејќи секој производител користи различни методи за детекција, различни продукти се подобри за различни типови на закани. Како додаток на anti-virus софтверот и другите скенери на malware, организациите треба да ги едуцираат корисниците за опасностите од email- malware-от и за начините за избегнување на закани, како на пример следново:

- Никогаш не отворајте attachment-и од непознат испраќач.
- Не отворајте attachment-и со сомнителни имиња или екстензии (пр., attachment.txt.vbs, attachment.exe) дури и од познати праќачи.
- Бидете сомничави кон email-те од познати испраќачи во кои subject-от или содржината се несоодветни (пр., порака со subject "I love you" од некој колега) или со општ subject (пр., "Look at this, it's interesting").
- Скенирајте ги сите attachment-и пред отварањето, со malware скенирачки софтвер, со конфигурирање на софтверот - да го прави ова автоматски.
- Ажурирајте ја базата на malware скенирачкиот софтвер на дневна база или кога ќе има нова верзија на malware.
- Предупредете ги корисниците за malware и како да идентификуваат пораки што содржат malware.

Друга работа што треба да се спомене за attachment-от е неговата величина. Заради различните потреби за чување и процесирање на големите пораки, mail сервер-те треба да ја ограничат максималната прифатлива величина на пораката. За бинарен фајл, на пр. слика прикачена кон пораката, таа не се испраќа во нејзиниот оригинален формат, туку е кодирана. Како што кажавме погоре, бинарните attachment-и кои се претставени со блокови од Base64-кодиран текст. Овој тип на кодирање внесува 33% зголемување на пораката. На пример, пораката која има 1MB- attachment станува порака со величина 1.33 MB.

9.6.4 Филтрирање на содржина

Филтрирањето на содржина работи на сличен начин како скенирањето на malware кај firewall-от или mail серверот, освен што бара пораки што содржат несакана содржина (а не malware), како spam или недолична содржина. Кога имплементираме рестрикции на одредени типови фајлови и malware скенирање, се обезбедува само одредено ниво на безбедност. Содржината на пораките и нивните attachment-и може да направи поголема штета дури и од вирус. Во овој случај, треба да се примени некаков облик на филтрирање на содржина. За максимална ефикасност, треба да се направи филтрирање на содржина за сите влезни и излезни пораки на истото место каде што се прави скенирање на malware - кај firewall-от/mail relay/mail gateway-от, mail серверот, и клиентската работна станица. Всушност, многу продукти се достапни за популарните mail системи, што вклучуваат филтрирање на содржина, malware скенирање, и рестрикција на file-типови. Вклучувањето на овие особини во продуктот може да ја редуцира администрацијата на безбедносните контроли.

Во општ случај, се дефинираат правила за проследување, карантин, чистење, или бришење на податоците што минуваат низ серверот во зависност од резултатите на скенирањето. Типични компоненти што треба да се филтрираат и врз кои треба да се преземе акција се следните:

- Email-от што содржи активна содржина (пр., ActiveX, JavaScript) се чисти од активниот код и се проследува кон примачот.
- Spam пораките и phishing обидите треба да се бришат редовно.
- Extra-големите фајлови треба да се испраќаат надвор од шпицот.

Друга важна особина на филтрирањето на содржини е скенирањето на излезните податоци. Може да се направи лексичка анализа што ги скенира пораките за зборови и фрази кои се несоодветни за користење во службениот email. Лексичката анализа исто така може да послужи за детекција на внатрешна штетна содржина, како на пр. spam, кој е креиран внатре во организацијата. Исто така, лексичката анализа која пребарува зборови и фрази, може да индицира дека доверливи податоци излегуваат од компанијата.

Пред да се имплементира филтрирање, треба да се определи како работат мрежата и апликациите. Ова значи примена на мрежни анализатори (sniffers); анализирачки рутер, firewall, и серверски log фајлови; и соодветна обука на мрежните администратори. Друг ефикасен начин за намалување на бројот на несакани пораки кои стигнуваат во mail серверот е примената на лесниот протокол за пристап до директориум (LDAP), кој се користи кај mail gateway-от или firewall-от како филтерски механизам. LDAP lookup им овозможува на gateway-от и firewall-от да го пребаруваат корисничкиот директориум директно за корисничките информации. Кога пораката пристигнува во gateway-от или firewall-от, таа го контактира корисничкиот директориум за да види дали пораката е адресирана до корисник што навистина постои. Ако корисникот не е во директориумот, пораката се враќа и не доаѓа до mail серверот. Голем дел од spam-от се праќа кон множество на примачи, со примена на база на податоци од вообичаени имиња. Повеќето од овие адреси не постојат за одреден домен, но е лесен метод за spammer-ите да ги испратат пораките до многу корисници на брз начин. Примената на LDAP lookup ги заштитува пораките од забавување на mail серверот.

Многу Internet service провајдери (ISP) и независни компании нудат скенери на malware и филтери на содржини, вклучително и spam филтрирање. Овие сервиси можат да им користат на организациите кои сакаат екстра ниво на заштита, но не сакаат самите да го одржуваат тоа ниво на заштита. Овие сервиси ги бришат пораките пред да стигнат кај mail серверот, со што се зголемува ефикасноста. Бидејќи овие сервиси можат да надгледуваат email на повеќе организации, тие ги идентификуваат несаканите пораки многу брзо. Недостатоци на овој сервис се следните:

- Приватност. Целокупниот влезен email патува низ серверите на провајдерот и се скенира кај нив.
- Лажни предности. Решението за филтрирање на сервис провајдерот може автоматски да ги брише пораките што се означени како spam, без

да им дозволи на администраторите да ги проверат ознаките на пораките.
- Достапност. Ако сервисот стане недостапен, организацијата треба да ја смени патеката на mail-от и треба да го спречи доцнењето на поштата.

9.6.5 Блокирање на Spam-сервери

Без оглед на комуникацискиот медиум, секогаш постојат ентитети што сакаат да ги искористат средствата за комуникација за да ги шират нивните идеи и продукти. Email-от не е исклучок. Општ назив за овие пораки е непожелен комерцијален email (UCE), исто така познат и како spam. Повеќето email корисници добиваат spam секојдневно. Бидејќи email-от во глобала е нерегулиран, систем администраторите треба да применат одредени механизми со цел - серверите да го редуцираат бројот на spam пораки што пристигаат кај корисниците. Друга предност на имплементацијата на сервер-базирана spam контрола е што ја редуцира величината на поштенското сандаче, т.е. го редуцира потребниот простор за складирање кај серверот.

За контрола на spam пораките, администраторите мора да ги спроведат следните мерки: (1) да се осигураат дека spam не може да се испрати од mail серверите што тие ги контролираат; (2) да имплементираат spam филтер за влезните пораки; и (3) да ги блокираат пораките од познати spam-испраќачки сервери, што ќе го објасниме подолу. Бидејќи Internet нема централизиран авторитет, не-профитните организации и комерцијалните компании креирале листа на mail сервери што се идентификуваат како испраќачи на unsolicited email пораки. Овие листи често се нарекуваат отворени црни листи (ORB) или DNS црни листи (DNSBL). Повеќето популарни mail сервери можат да се конфигурираат да пребаруваат повеќе ORB и да ги одбиваат пораките од тие mail сервери. Овие листи се ажурираат на дневна база; затоа, нивната примена може да го редуцира spam-от. Дополнително, повеќето mail сервери може да се конфигурираат да враќаат пораки од точно дефинирани домени. ORB spam контролата не е потврдлива. Црните листи се менуваат постојано. Администраторите на mail серверот кои сакаат да пријават одреден сервер да биде на црна листа - може да испратат поплаки од UCE до Web страниците кои се наведени во Spam Resources.

9.6.6 Автентикација

Како што спомнавме погоре, конфигурирањето на автентикацијата ги намалува шансите дека некој ќе го користи вашиот mail сервер за да испраќа spam. Друга предност на автентикацијата претставува поголемата безбедност и употребливост. Достапни се два метода за контрола на mail relay. Првиот е да се контролира множеството домени од каде се испраќаат пораките. Овој метод е ефикасен ако периметарот на целиот mail систем спаѓа во познат адресен опсег. Сепак, ако оддалечените корисници имаат системи со различни адресни опсези, овој метод е неприменлив. За да се прифатат оддалечени корисници, потребна е поробусна конфигурација.

Вториот метод бара корисниците да се автентицираат пред испраќање на било која порака. Ова е познато како автентикациски relay, или SMTP AUTH, што претставува SMTP екстензија за поддршка на автентикацијата. За жал, default конфигурацијата на повеќето mail сервери не имплементира автентикациски relay; затоа, администраторите на mail серверот мора да го конфигурираат серверот соодветно. Автентикационият relay претставува едноставна, но многу моќна безбедносна особина на mail серверите. (Побарајте документација од производителот за конфигурирање на SMTP AUTH).

Администраторите на mail серверот мора да имплементираат автентикациски relay. Несоодветно конфигурираниот mail сервер може да се искористи за праќање на spam. Ако mail серверот претставува open relay (отворен круг), тој може да се најде на црна листа (како што кажавме погоре). Организациите што ги применуваат овие црни листи - не можат да примаат пораки од сервер кој е на црната листа, без оглед дали пораките се spam или валидна пошта.

Ако администраторите на mail серверот дознаат дека нивниот mail сервер е на црна листа, треба да го поправат проблемот со отворен круг и да извршат тестирање дека серверот не е повеќе "круг". Потоа администраторот треба да утврди на која (кои) црна листа е серверот и да контактира со администраторот на црната листа за да добие инструкции како да се избрише серверот од листата. Додека серверот не се избрише од сите црни листи и ажурираните црни листи не се достават до претплатниците, излезната пошта од организацијата нема да стигнува до сите примачи.

9.6.7 Сигурен пристап

Погоре беа дискутирани различни протоколи за транспорт и пристап до поштата. Како и Internet протоколите, повеќето од нив иницијално не вклучуваат енкрипција ниту автентикација. Ова носи три проблеми за корисниците на mail. Прво, за оние што испраќаат пораки, содржината може да се пресретне, прочита и модифицира во секој хост на патеката помеѓу испраќачот и примачот. Пораката во тој случај е како разгледница. Секој што ќе ја дофати разгледницата - може да прочита што пишува на неа отпозади. Второ, примачот не може да верификува дека пораката потекнува директно од испраќачот или била модифицирана при транзитот. Овие проблеми беа спомнати погоре, кога дискутиравме за заштита на пораките. Трето, наместо да ги заштити автентикациските информации, корисникот испраќа незаштитен password низ мрежата, кој може да биде пресретнат и ре-употребен од напаѓач. За жал, во default конфигурациите, mail клиентите го испраќаат незаштитен password-от, дозволувајќи да биде пресретнат од други компјутери во мрежата, низ кои тој се проследува до mail серверот.

Овој проблем може да се реши со примена на методот што се користи за безбедност на World Wide Web (WWW) сообраќајот – протокол за безбедност на транспортно ниво (TLS). TLS е сличен со Secure Sockets Layer (SSL) протоколот, врз кого се базира, и може да се користи во комбинација со POP, IMAP, и SMTP за криптирана комуникација помеѓу mail клиентите и серверите. RFC 2595 дефинира како се користи TLS во борба против штетните компоненти, како се имплементира

заштитен пристап до сандаче, и за натамошно зајакнување на SMTP MTA со користење на SMTP AUTH.

9.7 СИГУРНОСТ НА КЛИЕНТОТ

Илјадници mail клиенти пристапуваат до активниот mail сервер. Без оглед дали безбедноста е сместена на mail серверот, важно е да се заштити и клиентската страна. Во многу случаи, клиентската страна претставува поголем безбедносен ризик отколку mail серверот. Треба да се преземат повеќе мерки за да се обезбеди соодветно ниво на безбедност на email клиентите. Во продолжение даваме општи препораки што важат за сите email клиенти. Не се наведени специфичните препораки за поедините mail апликации.

9.7.1 Ажурирање на mail-клиентите

Најважен чекор за обезбедување безбедност на клиентот е да се обезбеди да корисниците да користат најнова и најсигурна верзија на mail клиент со сите потребни закрпи. Најголемиот број клиенти имаат многу ранливости. За да се идентификуваат сите ранливости на mail клиентите, треба да се провери NIST - национална база на ранливости (NVD). Најдобар извор за закрпи се Web страниците на производителите. Треба често да се посетуваат тие Web страни. Ажурирањето на некои mail клиенти се прави релативно сложено, бидејќи тие работат во спој со Web пребарувач. На пример, тесната врска помеѓу Microsoft Outlook, mail клиент, и Internet Explorer - Web пребарувач, овозможуваат - конфигурациските поставки и ранливости да се префрлаат од едниот на другиот. Во таква ситуација, треба да се ажурираат и mail клиентот и Web пребарувачот со најновите закрпи. Ако не се користи сигурна верзија на mail клиент - се намалува ефикасноста од користењето на безбедносните мерки кои се опишани подолу.

9.7.2 Конфигурирање на безбедноста на клиентот

Mail клиентите може да не бидат конфигурирани безбедно во нивната default конфигурација. Mail клиентите треба да се конфигурираат за да:

- Оневозможат автоматски преглед на пораката.
- Оневозможат автоматско отворање на пораките.
- Оневозможат автоматско вчитување на сликите во пораката.
- Оневозможат симнување на активни содржини. Такви примери се ActiveX контроли, Java аплети, и JavaScript. Ова може да предизвика проблем кај email апликациите кои се поврзани со Web пребарувач, бидејќи исклучувањето на овие функции може да влијае врз функционалноста на Web пребарувачот. Во тој случај, треба да се направи внимателно о(не)возможување на активните содржини. Во случај на Microsoft Outlook и Internet Explorer, треба да се дефинираат посебни безбедносни зони за секој од нив, со што ќе се овозможи Internet Explorer да има послаби безбедносни поставки во однос на Outlook.

- Овозможат anti-spam и anti-phishing опции. Овие опции обично се ставени по default, но од безбедносна перспектива - најдобро е да се постават на највисоко ниво. Исто така, корисниците треба да се едуцираат да ги филтрираат пораките. Некои mail клиенти им овозможуваат на корисниците да филтрираат - т.е. да креираат листа на безбедни испраќачи и испраќачи што треба да се блокираат.

Постојат дополнителни мерки за мобилните email клиенти, како што се мобилните телефони и PDA. Користењето на мобилни email клиенти е во пораст изминативе години. Корисниците треба да водат сметка за информациите што ги чуваат во уредите, и треба да преземат мерки во случај уредот да биде изгубен или украден. Покрај неопходната физичка безбедност, корисниците треба да ги ре-конфигурираат уредите, кои типично се конфигурираат по default. Безбедносни акции што треба да се преземат се следниве:

- Добивање на password или PIN за пристап до уредот.
- Енкрипција на локалните податоци, вклучително на пораките и на симнатите attachment-и.
- Енкрипција и потпишување на пораките, со поддршка на S/MIME или OpenPGP и управување со дигитални сертификати.
- Енкрипција на комуникацијата помеѓу email клиентот и mail серверот, со примена на SSL-енкрипција за заштита на POP, IMAP, и SMTP комуникацијата.
- Далечински мониторинг на уредот и бришење на неговите информации ако е нападнат.
- Тестирање за постоење на Bluetooth-уред со цел да се спречи неавторизираниот пристап.

9.7.3 Конфигурирање на автентикацијата

Почетните mail клиентски апликации не барале автентикација на корисникот, бидејќи поштенското сандаче било ограничено на локалниот file-систем и припаѓало само на неговиот сопственик. Како што еволуирал MUA - обезбедил функции за далечински пристап до сандачето - преку POP и IMAP (види погоре), па автентикацијата станала неопходна. Типично, ова се прави такашто корисниците внесуваат username и password кога пристапуваат до сандачето. За да бидат “user-friendly”, mail клиентите имаат конфигурациски фајлови кои содржат (т.е., “памтат”) username и password за пристап до mail серверот. Иако ова внесува леснотија во користењето, тоа внесува безбедносна слабост, бидејќи одреден напаѓач кој има физички пристап до mail клиентот - ќе може да пристапи до автентикациските информации, а потоа и до содржината на сандачето. Исто така, ако се овозможи автоматско комплетирање на корисничкиот внес, - локален напаѓач ќе може да ги разоткрива password-ите постојано. Оневозможувањето на password recall функцијата претставува ефикасен начин за зголемување на mail-клиентската безбедност. Ако не може да се исклучи, тогаш многу е битно сигурното чување на овие конфигурациски фајлови. Повеќето оперативни системи содржат механизми за контрола на пристап, кои нудат одреден степен на заштита. Кај системите кои овозможуваат вакви контроли, обезбедете да конфигурациските фајлови на mail клиентот бидат достапни само на сопственикот. Дополнително,

обезбедете да фајлот биде сместен во директориумот што се контролира од сопственикот. Во случаи кога контролите за пристап се недостапни, најдобро решение е да се избрише корисничкиот password од конфигурациските фајлови.

Друг проблем што треба да се реши е комуникацијата помеѓу mail клиентот и mail серверот. Како што спомнавме погоре, целата мрежна комуникација со default конфигурација на SMTP, POP, и IMAP е некриптирана. Ова ги прави корисничките имиња, password-и, и содржината на пораките подложни на напади. За да се зголеми client-to-сервер безбедноста, комуникацијата треба да се криптира со користење на SSL/TLS. Повеќето mail клиенти поддржуваат SSL/TLS; треба да се користат ако се достапни. TLS верзија 1 се препорачува за примена; минимум, треба да се користи SSL верзија 3. Изборот на email адреси и кориснички имиња исто влијае врз автентикацијата. Користењето на account името како email адреса треба да се избегнува, за да не може напаѓачот да го открие account-от од личната email адреса. Примери за вакви конвенции се - ime.prezime.countrycode @domain.gov за странска адреса, и ime.prezime.ctr@domain.gov за адреса на соработник.

9.7.4 Безбедност на клиентскиот оперативен систем

Повеќето оперативни системи обезбедуваат голем број конфигурациски поставки и други мерки за зголемена безбедност на клиентот - директно или индиректно. Хост оперативниот систем е клучна компонента за целокупната безбедност на клиентскиот хост. За да го заштитите оперативниот систем - треба да го направите следново:

- Ажурирајте го со најновите закрпи.
- Конфигурирајте го да овозможува - само соодветните корисници да пристапуваат до локалните пораки и конфигурирачки фајлови.
- Конфигурирајте го (само на Windows хостовите) - Windows Script Host (WSH),
- Избришете го WSH или дозволете пристап само на администраторот до него,
- Сменете ја default акцијата за следните file екстензии - од егзекутивна во едитирачка:
    - JS (JavaScript)
    - JSE (JavaScript Encoded фајл)
    - VBE (VBScript Encoded фајл)
    - VBS (Visual Basic Script)
    - WS (Windows Script фајл)
    - WSC (Windows Script компонента)
    - WSF (Windows Script фајл)
    - WSH (Windows Script Host Settings фајл)
- Кај Windows хостовите, конфигурирајте ги да ги прикажуваат сите file екстензии (ова ќе обезбеди да email attachment-от iloveyou.txt.vbs - биде прикажан точно, а не како iloveyou.txt).

- Инсталирајте anti-virus и конфигурирајте го автоматски да ги скенира сите влезни пораки и attachment-и што ги содржат. Исто така, инсталирајте anti-spyware апликација ако anti-virus софтверот не содржи anti-spyware опции.
- Инсталирајте личен firewall за заштита на компјутерските комуникации, освен ако веќе има постоечки уреди за мрежна безбедност (пр., мрежен firewall).
- Обезбедете да оперативниот систем користи најслаби привилегии, бидејќи штетниот код се стартува во безбедносен контекст во кој е креиран (т.е., на корисничко ниво). На пример, корисниците треба да читаат и составуваат email користејќи налози што немаат администраторски привилегии.
- Обезбедете да критичните компоненти на оперативниот систем бидат заштитени од штетен код.
- Користете енкрипција за заштита на пораките кои се чуваат локално на корисничкиот хард диск (ова е посебно важно за laptop-те и другите мобилни уреди, кои можат да бидат и украдени).

9.7.5 Безбедно пишување пораки

За да се заштитат email пораките што содржат доверливи информации, треба да се користи енкрипција. Два најважни методи за енкрипција на пораките се S/MIME и OpenPGP, што беа дискутирани погоре. И двата нудат слично ниво на заштита, иако нивните архитектури се различни. Многу mail клиенти имаат вградено S/MIME, додека OpenPGP обично доаѓа во форма на plug-in. Вообичаено, изборот на решение зависи од потребите на организацијата. Како општо правило, сметајте дека некриптираната порака треба да се третира како разгледница – секој може да ја прочита и модифицира.

Заштитата на пораките со S/MIME или OpenPGP бара дигитални сертификати и за примачот и за испраќачот. Дигиталниот сертификат има неколку компоненти, вклучително име и email адреса на лицето на кое се издава сертификатот, јавниот клуч и неговиот датум на траење, информација за CA што го издава сертификатот (вклучително и дигиталниот потпис), и серискиот број на сертификатот. Кога испраќачот ги има дигиталните сертификати на испраќачот и примачот, тој може дигитално да ги потпише и криптира email пораките кон примачот. Дигиталното потпишување на пораката е битно, заради следново:

- Автентикацијата му овозможува на примачот да биде сигурен дека пораката доаѓа од испраќачот.
- Не-одбивањето обезбедува да испраќачот не смее да одбие да креира порака.
- Интегритетот обезбедува да пораката не биде променета случајно или намерно за време на преносот од праќачот кон примачот.

Дигиталните сертификати се добиваат или од внатрешен авторитет за сертификати (CA) или од јавен, независен CA. За mail клиентот што е конфигуриран да праќа и прима криптирани пораки, сите примени пораки треба да се чуваат во криптирана форма. Mail клиентот може да биде конфигуриран да испраќа и прима некриптирани, но автентицирани пораки, чиј интегритет е од примарно значење.

Зависно од важноста на пораката, mail клиентот треба да бара password секогаш кога пораката се отвора за читање.

9.7.6 Закрпи (plug-ins)

Многу различни закрпи се достапни за mail клиентите. Овие закрпи нудат дополнителни функции надвор од основната конфигурација на mail клиентот. Mail енкрипцијата, anti-virus, pop-up blocker, и заштита од malware се мало множество на достапните закрпи. Некои обезбедуваат напредни опции за филтрирање, а други - звучно известување дека стигнала нова порака. Без оглед на типот на plug-in, треба да се обрне внимание за нивна инсталација. Општо земено, треба да се инсталираат закрпи само од доверливи производители. Имајте предвид дека некои закрпи не се дистрибуираат од производителите во дигитално-потпишан облик. Некои закрпи може да содржат spyware што ги меморира Web страните што ги посетува корисникот, или adware што испраќа комерцијални огласи. Тие доаѓаат во форма на toolbar што автоматски се инсталира во вашиот Internet пребарувач. Користењето само на оригинални закрпи- ја намалува шансата за инсталирање на штетен plug-in.

9.7.7 Web-базиран пристап до Email сервери

Од корисничка гледна точка, пристапот до mail сервер преку Web прелистувач е корисно и ефикасно. За жал, многу безбедносни аспекти треба да се разгледаат пред да се имплементира Web-базиран пристап до mail серверот. Многу од работите се исти како и стандардните mail клиенти. На пример, default конфигурацијата на Web-базиран пристап вообичаено ги испраќа password-от и податоците заедно, како кај POP и IMAP. За поголема безбедност, организациите треба да го конфигурираат својот mail сервер да прифаќа Web конекции само преку 128-битни SSL/TLS конекции. Оваа поставка прави да и корисничката автентикација и содржината на пораката се енкриптираат за време на преносот од корисничкиот Web пребарувач кон Web серверот. Сепак, ова не ја заштитува содржината додека се пренесува од mail серверот кон примачите; некои облици на енкрипција, како S/MIME или OpenPGP, би требало да се користат ако се бара доверливост на пораката. За жал, повеќето Web-базирани email системи не ги поддржуваат нив. Едно решение е да се криптираат податоците пред да се внесат во пребарувачот (ова лесно се прави со OpenPGP). Овозможувањето на Web-пристап ја намалува целата безбедност на mail серверот. Организациите мора да се свесни за ризиците кога ќе имплементираат Web-пристап до нивниот mail сервер.

Сериозен ризик со Web-базираните email системи е пристапот од јавни компјутери (пр., библиотеки, Internet café-а). Во овие случаи, пребарувачот може да се конфигурира да ги памти username и password-от автоматски. Ако е конфигуриран на тој начин, неавторизирано лице (што ќе седне на компјутерот после вас) може да добие пристап до вашиот mail сервер. Друга опасност е што компјутерот може да има снимач на тастери, што ги меморира сите тастери притиснати од корисникот, вклучително username и password. Потоа тие податоци можат да се искористат за пристап до вашиот mail сервер. Web пребарувачите привремено ги кешираат податоците за корисникот - одреден период после логирањето. Ако

корисникот не го испразни кешот откако ќе го затвори пребарувачот, можно е некое неавторизирано лице да го искористи кешот за да ја добие вашата лозина за пристап до mail серверот. Примената на SSL/TLS во општ случај не дава заштита за ваквите напади.

□

10. ХАКЕРСКИ НАПАДИ - ДЕТЕКЦИЈА И ПРЕВЕНЦИЈА

10.1 ХАКЕРИ И КРЕКЕРИ

Со појавувањето на првите компјутери во светот се појавуваат и првите лица и институции кои се трудат на секој начин да упаднат во туѓиот систем, со цел да ги откријат податоците што ги содржи, да ги контролираат, да ги променат или пак да ги оштетат или уништат истите. Со појавата на Интернет - овие напади се интензивираа. Во исто време, почнуваат да се развиваат и разни видови на системи и програми за откривање на нападите на системот и негова заштита од истите. Иако е тешко да се споредуваат мрежите од касните 70-ти и 80-ти со мрежата позната како Интернет денес, сигурно е дека трендовите на нападите не се опаднати, туку напротив зголемени. Постојат сигурни докази дека нападите базирани на Интернет можат да се користат во политички цели, шпионажа и друго. Денес сигурносните технологии се многу сложени, но Интернетот и понатаму лесно се "крекува". Иако многу луѓе го користат терминот *хакирање* кога зборуваат за илегални напади, терминот *крекирање* би можел да биде покоректен. Крекирањето се однесува на недозволени напади кои ги трпи жртвата додека е на мрежа. Постојат различни степени на напади, на пример:

- Напаѓачот добива пристап до системот и ништо повеќе (пристапот се дефинира како недозволен влез во мрежата која бара пријава и лозинка).
- Напаѓачот добива пристап, ги уништува, корумпира или на поинаков начин ги менува податоците.
- Напаѓачот добива пристап и воспоставува контрола врз дел од системот или пак врз целиот систем, може да забранува пристап и на привелигирани корисници.
- Напаѓачот добива пристап, и при тоа тој фалсификува пораки во вашиот систем.
- Напаѓачот не добива пристап, но наместо тоа тој имплементира злобни процедури кои доведуваат до проблеми, рестартирање и други манифестации на неоперативност која е трајна или привремена.

Современите техники за сигурност можат да го направат крекирањето потешко. Меѓутоа разликата помеѓу зборот тешко и невозможно е сеуште голема. Денес крекерите имаат пристап до големо богатство на безбедносни информации, а многу од нив се бесплатни и на Интернет. Рамнотежата на знаењето помеѓу крекерите и добрите специјалисти за сигурност не е несразмерна. Во стварност, неспорно е дека секоја страна поседува компоненти што и недостасуваат на другата страна, што ја прави рамнотежата поинтересна. Секој веб сајт може да биде крекиран, вклучувајќи ги и следните типови:

- Банки
- Воени сервери
- Универзитети
- Интернет сервис провајдери (ISP)

Не очекувајте дека ќе се смени оваа клима. Се појавуваат нови и поефикасни методи на крекирање, а на чекор се од тоа да станат и побрзи. Новите алати за крекирање и вирусите се произведуваат секојдневно, а тие алати, кои се играчки за хакерите и крекерите, денес стануваат моќно оружје. Овие методи се достапни на сите непријателски страни кои целат да ја уништат националната информациона инфраструктура на земјата, но и на децата кои сакаат да нападнат некој популарен веб сајт. За информационото водење на војна, постојат неколку клучни методи, но овие четири се исклучиво истакнати:

- Спречување на функционирањето на целниот компјутерски сервис
- Уништување на целниот компјутерски систем
- Крадење на податоци
- Модифицирање на податоци (за остварување на лична корист)

Денешните напади со denial-of-service и вирусите - формираат основа за утрешниот арсенал на информационото водење на војна. Сметајќи дека без разлика кој, без разлика каде - може да ги добие тие алати, да ги компајлира и да ги развие за минута, блиската иднина изгледа прилично страшна. За да ја разберете методологијата на хакерите и крекерите, морате да разберете прво што е хакер, а што е крекер. Интернет ентузијастите ја докажуваат разликата помеѓу хакерите и крекерите. Прифатливата дефиниција за хакерите и крекерите би можела да изгледа вака:

- *Хакер* е личност која е интензивно заинтересирана за таинствените и нејасни работи на некој компјутерски оперативен систем. Хакерите се често програмери. Како такви, хакерите имаат напредно познавање за оперативните системи и програмскиот јазик. Можат да откријат дупки внатре во системот и причините за таквите дупки. Хакерите константно бараат поголемо знаење, го нудат бесплатно тоа што го откриле и никогаш намерно не ги уништуваат податоците.
- *Крекер* е оној што влегува, или на друг начин ги повредува Интернет системите на оддалечените машини и е со злобна намера. Имајќи недозволен пристап, крекерите ги уништуваат виталните податоци, им го забрануваат сервисот на легитимните корисници, и своите мети ги доведуваат до проблеми. Крекерите можат лесно да се идентификуваат, затоа што нивните акции се злобни.

Додатно, треба да се напомене дека постојат два главни типа на крекери. Првата група е за среќа мала и тоа се крекери - експерти кои откриваат нови сигурносни дупки и често пишуваат програми кои ги користат. Другиот тип, корисниците на скрипти (script kiddie), знаат само како да дојдат до овие програми и како да ги покренат. Корисниците на скрипти се побројни, но е лесно да се откријат и да се спречат.

10.2 ОТКРИВАЊЕ НА УПАДИ (INTRUSION DETECTION – ID)

Откривањето на упади (ID) и реагирањето, е задача на мониторинг системите за откривање на упади или за несоодветна употреба. Тоа подразбира известување на засегнатите страни да преземат дејства за да се утврди сериозноста на инцидентот и за да се отстранат последиците од инцидентот. Intrusion detection не претставува превентивна функција, бидејќи се активира по самиот упад и опфаќа следење на два главни концепти:

- создавање и одржување на системи и процеси за откривање на упади преку:
  - мониторинг на хостот или на мрежата;
  - нотификација на настан;
- создавање на тим за реакција на компјутерски инцидент (Computer Incident Response Team - CIRT) преку:
  - анализа на нотификацијата за настан;
  - реакција на инцидент доколку анализата тоа го бара;
  - процедури за патека на ескалација;
  - разрешување, следење на состојбите по инцидентот и доставување извештај до засегнатите страни.

10.2.1 ID системи

Многу снабдувачи нудат разни видови системи за откривање на упади. Секој систем администратор треба да ги запомни двата фундаментални начини на кои тие уреди функционираат: а) системи базирани на мрежа, наспроти системи базирани на хост, и б) системи базирани на знаење, наспроти системи базирани на однесување. Даден е и краток опис на разликите, заедно со некои ставови за и против за секој од нив.

ID системи базирани на мрежа, наспроти ID системи базирани на хост

Двете највообичаени имплементации на откривањето на упади се базирани на мрежа и базирани на хост. Нивните разлики се како што следува:

- ID системите базирани на мрежа:
  - обично се наоѓаат во дискретен сегмент на мрежата и го следат сообраќајот на тој сегмент на мрежата;
  - обично се состојат од мрежен уред со мрежна интерфејс картичка (МИК) (Network Interface Card (NIC)) која што работи во недискриминирачки мод и ги пресретнува и анализира мрежните пакети во реално време.
- ID системите базирани на хост:
  - користат мали програми (разузнавачи) кои се наоѓаат во компјутерот-хост и постојано го следат оперативниот систем;
  - внесуваат записи во фајловите за логирање и активираат аларми;

- откриваат несоодветна активност само на компјутерот-хост – не го следат целиот мрежен сегмент.

ID системи базирани на знаење, наспроти ID системи базирани на однесување

Двата концептуални приоди кон методологијата за откривање на упади се: ID системи базирани на знаење и ID системи базирани на однесување, кои понекогаш се нарекуваат ID системи - базирани на потпис и ID системи - базирани на статистички аномалии.

ID системи базирани на знаење. Овие системи користат база на податоци од претходните напади и познатите слабости на системот, за да откријат обиди за искористување на нивните слабости, и активираат аларм ако откријат таков обид. Овие системи се позастапени од ID системите базирани на однесување.
Предностите на еден ID систем базиран на знаење се:

- Овој систем се карактеризира со ниски стапки на лажно алармирање (или позитиви).
- Нивните аларми се стандардизирани и безбедносниот персонал може лесно да ги разбере.

Недостатоци на еден ID систем базиран на знаење се:

- Овој систем бара многу ресурси – базата на податоци треба постојано да се одржува и ажурира.
- Новите, уникатните или оригиналните напади често остануваат незабележани.

ID системи базирани на однесување. Овие системи динамично откриваат отстапувања од научените шеми на корисничко однесување и активираат аларм кога ќе се појави активност која се смета за натрапничка (надвор од нормалната системска употреба). ID системите базирани на однесување се помалку застапени од ID системите базирани на знаење.
Предностите на ID системот базиран на однесување се:

- Системот може динамично да се прилагоди на нови, уникатни или оригинални слабости.
- ID системот базиран на однесување не е толку зависен од конкретни оперативни системи, како што е ID системот базиран на знаење.

Недостатоците на ID системот базиран на однесување се:

- Овој систем се карактеризира со високи стапки на лажно алармирање. Високите позитиви се највообичаеното откажување на овие ID системи и тие може да донесат бучава од податоци, што го прави системот неупотреблив.
- Активноста и однесувањето на корисниците (додека се поврзани во мрежа) може да не се доволно статични, за да може ефикасно да се имплементира ID системот базиран на однесување.

Запомнете: Откривањето на упади е повеќе откривање, отколку превенција.

10.2.2 Тим за реакција на компјутерски инцидент

Како дел од структурираната програма за откривањето на упади и реакција - обично се создава тим за реакција на компјутерски итни случаи

(Computer Emergency Response Team (CERT)), или тим за реакција на компјутерски инцидент (CIRT). Бидејќи терминот „CERT“ е заштитен со авторско право, почесто се користи терминот „CIRT“. Примарната директива на секој CIRT е управувањето со реакцијата по инцидентот, т.е. реакцијата на компанијата - на настани што претставуваат ризик за нивната мрежна околина.

Управувањето често се состои од следново:

- координирање на известувањата и дистрибуција на информациите поврзани со инцидентот до засегнатите страни (оние кои треба да знаат за тоа), преку претходно утврдена патека на ескалација;
- ублажување на ризиците за претпријатието со минимизирање на нарушувањата за нормалните бизнис - активности и на трошоците поврзани со отстранувањето на инцидентот (вклучувајќи ги и јавните односи);
- составување тимови од технички персонал, за истражување на потенцијалните слабости и разрешување на конкретни упади.

Дополнителни примери на активности на CIRT се:

- управување со мрежните логирања, вклучувајќи го и собирањето, задржувањето, разгледувањето и анализирањето на податоци;
- управување со разрешувањето на инцидент, управување со отстранувањето на слабостите и доставување извештаи за настанот - до засегнатите страни.

10.3 ОПШТИ КЛАСИ НА ЗЛОУПОТРЕБА НА МРЕЖИ

Сега ќе објасниме неколку класи на напади на мрежи што еден инженер за заштита треба да ги знае. Овие класи се групирани многу општо, и не треба да се сметаат за комплетен список на напади или злоупотреби на мрежата.

Класа А: неовластен пристап до ограничени мрежни услуги со измама на контролите за безбедносен пристап

Овој вид на напад се вика злоупотреба на логирање. Се однесува на легитимните корисници кои имаат пристап до услугите достапни во мрежата, што вообичаено се ограничени на нив. За разлика од мрежните упади, овој вид на злоупотреба главно се фокусира на оние корисници кои можат да бидат интерни за мрежата, на легитимните корисници од друг систем, или на корисници кои имаат пониска безбедносна класификација. Терминот што се употребува кога еден корисник се преправа дека е друг корисник е „преправање“. Пример за овој вид на преправање би бил напаѓач кој манипулира со лозинки што ги добива од ISP (Internet Service Provider – доставувач на Интернет-услуги).

Класа Б: неовластена употреба на мрежа за цели што не се поврзани со работата

Овој начин на злоупотреба на мрежа се однесува на употреба на мрежата што не е поврзана со работата, или - употреба на мрежата за лични цели од страна на

овластени корисници, како што е Интернет сурфање на страници со несоодветна содржина (туризам, порнографија, спорт итн.). Според $(ISC)^2$ препораките на Етичкиот код на однесување (Code of Ethics) и Советодавниот одбор за Интернет (Internet Advisory Board - IAB), употребата на услугите поврзани во мрежа за цели што не се поврзани со работата, може да се смета за злоупотреба на системот. Додека повеќето работодавачи не спроведуваат екстремно строги правила за сурфање на Интернет, има повремени судски спорови за вознемирување од тоа што вработените влегуваат на порнографски Интернет страници и од тоа што вработените водат приватни Интернет бизниси, користејќи ја инфраструктурата на компанијата, можат да претставуваат неовластена употреба.

Класа В: прислушкување

Овој вид на напад на мрежа се состои од неовластено пресретнување на мрежниот сообраќај. До напади со прислушкување се доаѓа преку пресретнување на мрежниот сообраќај. Одредени методи на мрежен пренос, како што се пренос преку сателит, безжичен телефон, мобилен телефон, PDA, итн., се подложни на напади со прислушкување. Прислушкувањето се однесува на физичкото пресретнување на медиумот за пренос (како на пример - поставување кабелски продолжетоци или создавање на индукциска јамка, за да се примаат електромагнетски еманации од бакарот).

Пасивно прислушкување. Прикриено следење или слушање на преносот, што не е овластено ниту од испраќачот ниту од примачот.
Активно прислушкување. Штелување на преносот за да се создаде прикриен канал за сигнализирање, или активно тестирање на мрежата, за добивање инфраструктурни информации.

Една активна варијација на прислушкувањето се нарекува прислушкување преку „прикриен канал (Covert Channel)“, кое се состои од користење на скриена неовластена мрежна конекција за размена на неовластени информации. Каналот за прикриено складирање (Covert Storage Channel) функционира така што ги впишува информациите во складиштето со еден процес, а потоа ги чита користејќи друг процес од друго ниво на безбедност. Прикриениот темпиран канал (Covert Timing Channel) ги пренесува информациите до друг процес, така што ја намалува сопствената употреба на ресурси - за да има време за одговор на друг процес. Прислушкувањето и тестирањето се честопати прелиминарни чекори кон грабнувањето на сесии и други мрежни упади.

Класа Г: одбивање на услуга и други нарушувања на функционирањето

Овие видови на напад создаваат прекин на работата, што се должи на презаситеност на ресурсите поврзани во мрежа. Оваа презаситеност може да биде насочена кон мрежните уреди, серверите или кон инфраструктурната ширина на опсег – која било мрежна област што може да биде деградирана од голем волумен на сообраќај. На пример, нападот „дистрибуирано одбивање на услуга (Distributed Denial of Service - DDoS)“ што се случи во февруари 2000 година, не се смета за конкретно хакирање, бидејќи основната цел на нападот не беше да се приберат информации (доверливоста или интегритетот не се намерно компромитирани),

туку да ја запрат работата така што ќе го преоптоварат системот. Овој напад, меѓутоа, може да се употреби како диверзија за да се овозможи - со намерното хакирање - да се приберат информации од различен дел на системот, додека ресурсите на информатичката технологија (IT) на компанијата се пренасочени на друго место. Детални примери за DoS напади се дадени подолу во текстот.

Класа Д: упади во мрежата

Овој вид на напад се однесува на употребата на неовластен пристап за да се провали во една мрежа, главно од надворешен извор. За разлика од нападот со злоупотреба на логирање, се смета дека натрапниците не и се познати на компанијата. Највообичаената концепција за хакирање се наоѓа во оваа категорија. Познат и како пенетрирачки напад, тој ги искористува познатите безбедносни слабости во безбедносниот периметар.

Spoofing. Ова се однесува на напаѓач кој намерно наведува еден корисник (субјект), или уред (објект) да преземе погрешно дејство - давајќи му неточни информации.
Поддржување (Piggy–backing). Ова се однесува на напаѓач кој се здобива со неовластен пристап до еден систем, користејќи конекција на легитимен корисник. Еден корисник остава отворена сесија или неправилно се одјавува, овозможувајќи му на напаѓачот да ја продолжи сесијата.
Напади од задна врата (Back–door attacks). Обично се однесува на упади преку надворешни мрежни конекции со телефонско или асинхроно бирање.

Класа Ѓ: Тестирање (Probing)

Тестирањето е активна варијација на прислушкувањето. Обично се користи за да му даде на напаѓачот мапа на мрежата, додека се подготвува за упад или за напад со DoS. Тоа може да му даде на прислушкувачот список на достапни услуги. Анализа на сообраќајот преку употребата на „душкало“ (Sniffer) е еден вид тестирање на прислушкување, каде што се употребени скенирања на различните хостови за документирање на тоа - кои системи се активни во една мрежа и кои порти се отворени. Тестирањето може да се направи мануелно или автоматски. Мануелните проверки на слабостите се вршат со користење на алатки како што е Телнет (Telnet) - конектирање на далечинска услуга за да се види што се слуша. Автоматските скенери на слабости се софтверски програми кои автоматски ги извршуваат сите чекори на тестирање и скенирање и доставуваат до корисникот извештаи за тоа што го откриле. Бидејќи скенерите се достапни бесплатно на Интернет, бројот на овој вид автоматски тестирања од неодамна многу порасна.

10.3.1 Вообичаени напади со престанок на работа (DoS)

DoS нападот може да користи некои од следниве техники за да ги преоптовари ресурсите на целта на нападот:

- пополнување на просторот за складирање на хард дрејвот на жртвата - користејќи огромни атачменти на електронска пошта или трансфери на фајлови;

- праќање порака, која ја ресетира подмрежната маска на целниот хост, предизвикувајќи нарушување на подмрежното рутирање кај жртвата на нападот;
- искористување на сите ресурси на жртвата за прифаќање на мрежни конекции, што резултира во тоа што се одбиваат дополнителни мрежни конекции.

Следниот список се дополнителни специфични типови на DoS напади:

Напад со преоптоварување на баферот. До основен напад со *преоптоварување на баферот* доаѓа кога процесот прима многу повеќе податоци отколку што очекува. Ако процесот нема програмирана рутина за справување со вакво преголемо количество податоци, тој се однесува на непредвидлив начин - кој што натрапникот може да го искористи. Постојат неколку видови на напади со преоптоварување на баферот, а највообичаениот е „*Звукот на смртта" (Ping of Death)* (праќање на голем пакет), или користењето на кориснички имиња, или имиња на фајлови во електронска пошта составени од преку 256 карактери. Нападот со ping во голем пакет вклучува употреба на Интернет протокол за контрола на пораки (Internet Control Message Protocol - ICMP), и пакетен Интернет гропер (Packet Internet Groper (PING)). Натрапникот испраќа „ping" што се состои од нелегално модифициран и многу голем IP датаграм, и на тој начин ги преоптоварува системските бафери и предизвикува системот да се рестартира или да падне.

SYN напад. До *SYN напад* доаѓа кога напаѓачот го користи просторот на баферот за време на сесијата за иницијализација (поздравување) на контролниот протокол за пренос (TCP). Напаѓачот ја преплавува малата (in–process) редица на системот кај жртвата со барања за конекции, но не одговара кога системот на жртвата ќе одговори на тие барања. Ова предизвикува системот на жртвата да „паузира" (time out) додека чека на соодветен одговор, што прави системот да падне или да стане неупотреблив.

Teardrop напад (Teardrop Attack). *Teardrop нападот* се состои од модифицирање на должината и фрагментацијата на офсет полињата кај секвенцијалните пакети на Интернет протоколот (Internet Protocol - IP). Системот на жртвата тогаш станува збунет и паѓа откако ќе прими контрадикторни инструкции за тоа како фрагментите се офсетираат кај тие пакети.

Smurf. *Smurf нападот* користи комбинација на IP spoofing и ICMP за да ја презасити мрежата на жртвата со сообраќај, со што лансира напад со престанок на работа. Тој се состои од три елементи – изворен сајт, отскочен сајт и целен сајт. Напаѓачот (изворниот сајт) испраќа spoofed PING пакет на емитуваната адреса на голема мрежа (отскочниот сајт). Овој модифициран пакет ја содржи адресата на целниот сајт. Тоа предизвикува отскочниот сајт да ја емитира дезинформацијата до сите уреди на својата локална мрежа. Сите овие уреди сега одговараат со одговор до целниот систем, кој со тоа се презаситува од тие одговори.

10.3.2 Вообичаени напади со грабнување сесии

IP Spoofing напади. За разлика од Smurf нападот каде што spoofing се користи да се создаде DoS напад, IP spoofing се користи да се убеди системот дека комуницира со познат ентитет кој што на натрапникот му дава пристап. IP spoofing вклучува промена на пакетот на ниво на TCP, и се користи за напад на системите конектирани на Интернет, а кои даваат разни TCP/IP услуги. Напаѓачот испраќа пакет со изворна IP адреса на познат, доверлив хост. Хостот-цел на нападот може да го прифати пакетот и да дејствува на него.

Напади на TCP со секвенцијални броеви. Нападите на TCP со секвенцијални броеви ја искористуваат комуникациската сесија, која што е воспоставена помеѓу целта на нападот и доверливиот хост што ја започнал сесијата. Натрапникот ја измамува целта на нападот да верува дека е конектирана со доверлив хост и потоа ја грабнува сесијата така што го дознава почетниот TCP секвенцијален број на жртвата. Оваа сесија потоа често се користи за да се лансираат разни напади на други хостови.

10.3.3 Други напади со фрагментација

Нападите на IP со фрагментација користат разни IP датаграм - фрагментации за да ги маскираат своите TCP пакети пред уредите за филтрирање на IP кај целта на нападот. Примери на овие видови напади се следниве:

- До *напад на мал фрагмент (tiny fragment)* доаѓа кога натрапникот испраќа многу мал фрагмент што ќе замени некои од TCP полињата со заглавје во втор фрагмент. Ако уредот за филтрирање на целта на нападот не наложува минимална големина на фрагментите, овој нелегален пакет може потоа да се пропушти низ мрежата на жртвата.
- *Напад со преклопување на фрагмент (overlapping fragment)* е друга модификација со нулти офсет на еден датаграм (како teardrop напад). Последователните пакети ја преснимуваат информацијата за адресата - одредиште на првичниот пакет и потоа уредот за филтрирање на жртвата го пропушта вториот пакет. Ова може да се случи ако уредот за филтрирање на нападнатиот компјутер не наложува минимален офсет на фрагменти, за офсети што не се нула.

10.3.4 Интерпретација од доверлива мрежа

Еден од најважните документи на приближно дваесетина книги од серијата „Виножито“ (Rainbow) е интерпретацијата на доверлива мрежа (TNI), која што меѓу другото се нарекува и „Црвената книга“ (Red Book). Овие книги и произлезените стандарди се развиени од страна на Националниот институт за стандарди и технологија (National Institute of Standards and Technology - NIST).

„Црвената книга“ ги толкува критериумите опишани со Критериуми за евалуација на безбедноста на доверлив компјутер (Trusted Computer Security Evaluation Criteria - TCSEC, наречени „Портокалова книга“ (Orange Book)) за мрежи и мрежни компоненти, па оттука може да се опфати и во ова поглавје. Читателот

треба да забележи дека времето и технолошките промени ја намалуваат релевантноста на TNI во современото мрежно работење.

За да се справи со прашањата од техничка природа што се надвор од доменот на Портокаловата книга, Црвената книга ги разгледува толкувањата на Портокаловата книга во делот што се однесува на мрежите, и разгледува други безбедносни услуги што не се содржат во Портокаловата книга. TNI дава толкувања на Портокаловата книга за доверливи компјутерски и комуникациски мрежни системи и за барањата за безбедност. Прави процена на структурите за безбедност и дефинира дополнителни безбедносни услуги за мрежите - во областа на интегритетот на комуникациите, DoS и безбедноста на преносот. Исто така претпоставува дека веќе постојат физичките, административните и процедуралните заштитни мерки. Примарната цел на овие толкувања е да обезбедат стандарди за производителите кои инкорпорираат безбедносни механизми што функционираат на пре-дефинирани нивоа на безбедност, т.е. овозможуваат степен на доверба кој може да се измери.

10.4 СКЕНЕРИ НА РАНЛИВОСТ

Постојат две основни класификации на ранливост на оперативниот систем: прва, според која постојат локални изложени точки (ниво на хост) и втора, според која постојат оддалечени изложени точки (оддалечено ниво). Кај оддалечените изложени точки (Remote Exposure Points), постојат бројни методи што некој може да ги користи за да ја автоматизира проверката на ранливост. На пример, еден приод може да опфати користење алати за проверка на порти како што е Nmap, идентификација на оперативниот систем, а потоа пријавување на сите порти кои се прислушуваат. Потоа на корисникот ќе му биде дадена листа на порти (21, 25, 53, 80 итн.) и типот на оперативен систем (Linux, Kernel 2.2). Овој приод има неколку проблеми, бидејќи корисникот ги губи податоците (информациите за портите) и нема детали за тоа кои сервиси се навистина ранливи. Едноставно на корисникот му се дава шематски план на системот. Идентификацијата кои сервиси се преслушуваат и одредувањето дали се ранливи, се препуштени на корисникот. На пример, ако збирот на податоци кажува дека машината X која е подигната под Linux 2.2 Kernel има сервис кој се прислушкува на портата 21, сеуште не кажува за тоа дали има напад од некои wu-ftpd грешки на пречекорување на баферот. Дури и кога ќе се фатат поединчните порти, сеуште е потребно:

A. Да се идентификува кој ја прислушкува таа порта,
B. Да се идентификува која е верзијата на тој сервис,
C. Да се истражи дали постојат некој познати ранливости кои се однесуваат на тој сервис и бројот на верзијата.

Иако овој пристап можеби е изводлив за 10 машини, очигледно е дека нема да работи за средните и големите организации каде се наоѓаат 1000 машини. Задачата која ја имаме - од тешка станува невозможна. Попрактичен пристап би бил да изградиме првичен модел на скенирање на порти и идентификација на оперативен систем, а потоа да додадеме некој механизам за идинтификација на типот и верзијата на сервисот кој се преслушкува. Да се вратиме на wu-ftpd примерот на

пречекорување на баферот, со идентификување на верзијата на сервисот; сега би дознале:

A. Дека серверот е Linux kernel 2.2,
B. Дека се преслушкува портата 21
C. Кој е типот и верзијата на сервисот.

Последната компонента на овој процес е истражувањето (препознавањето) - кои сервиси се ранливи. Во многу случаи ова се поврзува со тоа што го прават напаѓачите: проверка, прашање, истрага и експлоатација. Во овој случај излегува дека wu-ftpd v2.4.2 е всушност познат тип на напад. Иако имплементацијата на деталите е променлива, со гледање на овие примери може да се заклучи дека постојат бројни заеднички компоненти на методите за проверка:

- Податок за ранливост - скенерите за проценка на ранливост имаат внатрешни бази на податоци за информацијата за ранливост, која им помага точно да ги идентификуваат оддалечените изложени точки на системот.
- Механизам за проверка - суштината на техниките на скенерот лежи во неговата способност сигурно да ги идентификува сервисите, потсистемите и ранливоста. Во зависност од тоа како е напишан скенерот, можеби не е ефикасно да се скенираат големи машини.
- Механизам на соопштување - пронаоѓање на проблемот е една работа, адекватно соопштување на тоа, е сосема нешто друго. Некои производи се појаки од другите во однос на тоа што откриваат.

Како и кај било која друга одлука за купување на производ, пред да одговорите на прашањето кој производ е добар, прво треба да се решите кои се вашите специфични барања. На пример, нешто што сакате да го автоматизирате е забрзувањето на процесот на пронаоѓање на ранливоста, потоа можноста производот да се пријави и да се изврши поголема проверка. Ако поседувате многу големо NetWare опкружување, можеби сакате да се уверите дека скенерот поседува посебни проверки за NetWare. Ако треба да проверите 50-100 хостови, ефикасноста можеби не е проблем. Меѓутоа, ако треба да проверите илјада, проблемите се специфични во однос на тоа што ќе направи вашиот скенер. Исто така, постојат некои заеднички точки кои се однесуваат на сите производи. Неколку проблеми на кои ќе наидете при изборот на скенерот на ранливости го вклучуваат следното:

- Потполност на проверка на ранливост – не треба да паднете во стапица со многуте комбинации кога бирате скенер. Меѓутоа, бројот на ранливости што ги препознава скенерот е важен. Како краен минимум, скенерите треба да бараат познати критични ранливости кои дозволуваат компромитирање на ниво на коренот/ администраторот.
- Точност на проверката на ранливост – важно е скенерите да имаат голем број на препознатливи ранливости. Меѓутоа, можноста скенерите точно да ја идентификуваат ранливоста е исто така важна. Испуштањето на дупките е непожелно како и соопштението за иденитфикација на стотина

непостоечки ранливости. Слично со системите за откривање на напади, некои производи за скенирање сеуште имаат проблеми со малата точност.

- Поле на проверка на ранливоста – треба да се напомене дека многу скенери на ранливост се дизајнирани да откријат оддалечена ранливост, а не локални (на ниво на хост) ранливости. Неколку производи како што се ISS и Webtrends имаат агенти на ниво на систем, кои исто така бараат локална ранливост - ранливост која не би била откриена со оддалечени проверки. Иако тие агенти често се однесуваат на големите степени на ранливост, тие исто така бараат инсталирање, што претставува ноќна мора на големите опкружувања.
- Временско ажурирање – иако скенерите секогаш ќе бидат еден чекор зад реализирањето на ранливоста, треба да се ажурираат во прилично истовремен интервал (еднаш месечно или почесто). Треба да барате скенер кој има значаен R&D тим зад себе, што доследно го ажурира производот.
- Можност за соопштување – пронаоѓањето на ранливоста е важно, но потребно е и опишување на проблемите и нивните следни поправки - како и точното рангирање на ранливоста. Ова посебно е важно за големите организации затоа што тие обично се потпираат на администраторите на системите - да ги поправат откриените проблеми. Некои скенери сега нудат можност за автоматско превземање и инсталирање на потребните решенија во апликациите. PatchLink е еден од најнапредните во оваа област.
- Лиценцирање и одредување на цена – некои од овие производи се лиценцирани по јазел, други по проверка на скенери, а некои како бесплатни. Некои од нив имаат лесен систем на лиценцирање (како што е NAI), други (како што е ISS) бараат конволуционен систем на отсекување на клучот. Треба да се напомене дека проблемот со лиценцата треба отворено да се испита, пред одлуката за купување. Кога се сомневате, секогаш е тука Nessus, кој е бесплатен.

Не постои скенер што ги има сите овие добри карактеристики, но Nessus и Internet security Scanner се прилично блиску.

Во идеален свет, решението за купување на технологија би било поддржано со посебни прибирања на понуди, посебни тестирања и реално буџетирање. Меѓутоа, луѓето ретко имаат луксуз да ги прават работите на тој начин. Поради тоа, ги избрав оние продукти кои ги сметам за најдобри скенери на ранливост достапни денес (ги набројувам подолу). Ова не значи дека другите производи нема да ја вршат работата- ова е само мој личен избор од моето искуство и тестирања.

Retina - eEye's Retina е релативно нова на полето на скенерите на ранливост, меѓутоа, брзо се движи кон врвот на ранг листата заради својот едноставен интерфејс, брзината на проверка и дневното ажурирање. Можете да видите дека апликацијата ги проверува и презема најновите дефиниции на ранливост од eEye's веб сајтот при своето подигнување. Retina не донесува претпоставки за протоколите на сервисот кои се подигнуваат на стандардни порти, туку го анализира сообраќајот за да одреди кои сервиси се подигнати. Исто така нуди функции за скенирање кои се подигнуваат во одредени интервали. Бидејќи е

минимално наметлива на системите кои се скенираат, може да се користи во вашите организации за да се автоматизираат проверките. eEye има јако R&D одделение кое нуди почетни извештаи за некои нови ранливости. Плус, додава особина наречена CHAM (Common Hacker Attack Methods), која се обидува да ги пронајде непознатите ранливости преку AI евристика.
Продавач: eEye Digital Security
Платформа: Windows, URL: http://www.eeye.com

NetRecon - NetRecon ги дополнува постоечките продукти за firewall и откривање на напади на Symantec. Предностите на NetRecon се интефејсот, можностите за соопштување, умереното зголемување на базата на податоци за ранливост и способност да се преземе она што се однесува на друга експлоатација – (користење на познати ранливости од еден сервер за проценка на друг сервер). NetRecon по традиција не е темелен како Nessus, Cybercop Scanner или ISS, туку е само просечен алат за проценка кој може да биде сосема доволен. Исто така може да се појави во Enterprise Security Manager (ESM), кој може да се користи за поопшти обиди за проценки на ризикот.
Продавач: Symantec (претходно Axent)
Платформа: Windows, URL: http://enterprisesecurity.symantec.com/

ISS Internet Scanner - ISS иницијално ја изградил својата компанија Internet Scanner, и историски се смета за стандард во индустријата за проверка на ранливост. Internet Scanner има строго известување и просечни можности на проверка на ранливост. ISS очигледно потрошил доста време на дотерување на производот за долгорочна проверка. На пример, скенерот снима значајна количина на податоци во позадина при секоја проверка на ранливост. Internet Scanner користи Microsoft ODBC за складирање на проверените податоци, кои можат подоцна да се користат за правење на долготраен циклус. Како и интеграцијата на Netrecon со ESM, Internet Scanner се интегрира со ISS Decisions. Заради чувањето на податоците во скенерот, ISS Decisions можат да се користат во комбинација со други производи за сигурност (firewalls, системи за откривање на напади итн.) и да ја насликаат глобалната слика на ранливост и точките на закана. Иако Internet Scanner традиционално немал многу проблеми со неточни детекции, сепак е послаб во однос на другите производи. Друга негативна особина, која е вредна да се спомене, е дека Internet Scanner станал помалку стабилен во 6.x серијата на реализација. Треба да се спомене дека ISS прави и други два производи за проверка, Internet Scanner и Database Scanner; иако и двата се базирани на агент – тие се неспособни за проверка на оддалечени системи.
Продавач: Internet Security Systems, Inc.
Платформа: Windows XP, URL: http://www.iss.net

Cybercop Scanner - Корените на Cybercop Scanner доаѓаат од NAI (Network Associates, Inc.), одделение на SNI (Secure Networks, Inc.) и нивниот Ballista производ. Иако Cybercop Scanner има импресивен број на проверки на ранливост и умерена способност за соопштување, исто така доаѓа со бројни изненадувачки корисни алатки. Две алатки кои се од посебно значење се CASL и SMB. CASL овозможува GUI кој се базира на конструкцијата на IP пакетот, а SMB е сличен со алатката за крекирање на лозинки - LophtCrack. Основната слабост на Cybercop е

неговата маана за некои фундаментално важни проверки на ранливост и неговата бизарна шема на лиценцирање. NAI обично се обидува да го продава Cybercop на основа на јазел, а не со бројот на проверени сервери. Така може да се креираат грозни шеми на плаќање, во зависност од регулирањето на јазлите и планот за продажба.
Продавач: Network Associates, Inc.
Платформа: Windows XP и Unix, URL: http://www.nai.com

Open Source Nessus Project - Nessus го напишал Renaud Deraison, автор на отворениот код кој живее во Париз, Франција. Renaud го открил Linux на 16 години и постојано го хакирал. До 1996 година, Renaud креирал 2600 напади и после тоа развил сигурност. Ова развило партнерски однос помеѓу Renaud и двајца други програмери, и заедно го напишале својот прв алат за проценка во 1997 год. По завршетокот на тој проект, Renaud го смислил Nessus (во почетокот на 1998 година). Nessus брзо станал софтвер за проверка на ранливост под Linux. Како член на движењето на слободен софтвер, за Nessus не се зборувало неколку години, но сега има свое место и понекогаш ги надминува своите комерцијални дупликати. Nessus користи додатен модул кој овозможува додавање на дополнителна сигурност на модулите за проверка. Ова му дава на Nessus развоен облик, затоа што било која проверка што ја нема - некој може да ја креира за одредено време (ако има способност за кодирање). Nessus користи модел на конзола, а конзолата може да се наоѓа на истиот компјутер на кој е и машината за проверка. Оваа дистрибуирана архитектура овозможува некои интересни флексибилности, затоа што не ви треба да бидете блиску до машината за проверка - за да вршите контрола. Во моментов, Nessus има повеќе од 500 проверки на ранливост, и некои од нив не се достапни во комерцијалните алати за скенирање. Во зависност од тоа како напредува развојот, во блиска иднина Nessus може да ги надмине комерцијалните скенери.
Платформа: Unix (можна Windows контрола), URL: http://www.nessus.org

Whisker - Whisker го напишал хакер со име Rain forest puppy (rfp), кој откривал ранливости на кои се базира Web-от. Whisker не одговара на генералната дефиниција за скенер на ранливост, затоа што посебно се фокусира на скенирање на познати CGI скрипти. Всушност, единствена работа што ја испитува, е ранливоста од CGI скрипти. Меѓутоа, неговата листа на CGI проверки е покомплетна од сите комбинирани листи на комерцијалните скенери. Заради ова, топло ви препорачувам да користите Whisker и како главен скенер.
Продавач: бесплатно – лабораторијата на rtf
Платформа: Windows и Unix, URL: http://www.wiretrip.net/rtf/

10.5 СРЕДСТВА ЗА ИДЕНТИФИКАЦИЈА НА НАПАД

Кога бирате систем за откривање на напад, потребно е да одберете две работи: Производ и Партнер (продавач) кој би го ажурирал тој производ. Бидејќи IDS се временски осетливи и зависат од ажурноста на производот, добриот систем ќе стане помалку корисен, ако за него не се грижиме редовно и умешно. Постојат неколку особини што го карактеризираат IDS уредот. Следи листата на компоненти што треба да ги процените кога донесувате одлука за избор на IDS:

- Поголема покриеност – една од важните компоненти на системот за откривање на напади е неговата можност да се открива многу напади. Иако добриот софтвер се одликува со голем број на опции, и привидно убав интерфејс, ако производот не е во можност да открие повеќе напади, ќе работи лошо. Уверете се дека NIDS решението кое го купувате може да открива различни типови на напади. Уверете се дека производот работи повеќе од проверка на неколку фајлови и дека ги подржува сите платформи кои треба да ги надгледувате.
- Точност на извештаите – ова е сложен фактор за одредување без темелно тестирање, но треба да се спомне дека не се сите извештаи еднакво креирани. Лажната сигурност е голем проблем кај повеќето NIDS решенија, а во големите опкружувања, погрешните извештаи можат да ја загрозат целата ефикасност за откривање на нападот.
- Робусна архитектура – постојат повеќе компоненти за откривање на нападот, а важно е - и машините и IDS рамките да бидат дизајнирани како силни. На страната машина/агент, производите треба да можат да издржат и напади и основни техники на избегнување. Иако избегнувањето по традиција е проблем кој се врзува за NIDS уредите (и највероајтно ќе ги мачи уште некое време), големите продавачи настојуваат да го решат тој проблем.
- Скалабилност – повеќе-слојноста на компонентите влијае на IDS "скалирањето", но два најголеми слоја се: широко-појасно надгледување и управувањето со податоци. Ширината на опсегот е еден од битните фактори кај NIDS уредите (во многу производи има проблеми на надгледување на широкиот мрежен опсег). На пример, ако развиете неколку десетина сензори на густ сообраќај, тие ќе испумпаат доста податоци назад во централизираната база на податоци. Некои back-end системи ќе се распаднат под таквиот наплив на податоци, или уште полошо, количината на податоци ќе го направи неверојатно тежок процесот на сортирање на предупредувањата.
- Управување со рамката – способноста за откривање на нападот е круцијална за IDS, но подеднакво е важна и способноста јасно и ефикасно да се претстави податокот кој се однесува на тие напади. Ако инженерите за сигурност не можат лесно да пристапат до податоците за нападот, глобалната употребливост на IDS е ограничена. Кога ги оценувате системите за откривање на напад, уверете се дека имате комфорност со управувањето на рамката на системот, и уверете се дека ви дозволува лесно да пристапите до информациите кои ги сакате.
- Временско ажурирање – слично како проценатa на ранливост и антивирусните производи, штом се појават нови напади, потребата за временско ажурирање на IDS производот станува критична. Работата со застарени IDS е аналогна со работата на аеродром без радар.
- Прифатливост за крајните корисници – некои производи за откривање на напади дозволуваат различно ниво на прифаќање, додека други се прилично статични и нефлексибилни. Во некои организации, прифаќањето на карактеристиките нема да биде голем

проблем, но кога бирате IDS продукт - треба да ги процените своите моментални потреби, како и идните потреби.

- Вештина на одржување – уредите за откривање на напад треба да се третираат како било која друга компонента на IT, па така, додатна работа која е присутна за администраторите - се проблемите на одржување на IDS.

10.5.1 Листа на производи за откривање на напади

Cisco secure IDS - Cisco е многу активен на пазарот на IDS, тој има хост базиран производ, како и NIDS производи што ги развива во текот на повеќе години. Неговиот NIDS производ се подига на Solaris, Windows NT и Windows 2000. Cisco го продава својот NIDS како уред - идејата е да купите потполна кутија и да ја вметнете во својата мрежа со минимум инсталација.
Продавач: Cisco systems, Платформа: Solaris, Windows
Производ: Cisco IDS, URL: http://www.cisco.com

Computer Associates eTrust Intrusion Detection - Computer Associates го купила eTrust Intrusion Detection system, како и целата компанија, од Платина. Тој има неколку интересни карактеристики како што е URL блокирање (ги спречува вашите вработени да прегледуваат веб страни кои не смеат да ги прегледуваат).
Продавач: Computer Associates, Платформа: Windows
Производ: eTrust Intrusion Detection, URL: http://www.ca.com

Enterasys Dragon IDS - Enterasys го стекнал Dragon IDS со купувањето на Network Security Wizard во 2000 година. Dragon е систем што се базира на Unuxu, кој е изграден за лесно надгледување на широкопојасните околини. Dragon традиционално бил помоќен од многу други IDS продукти. Организациите што користат Unix утврдиле дека тој бара многу моќно NIDS решение, што веројатно ќе биде во голем дел како Dragon. Тие што користат помалку-барачки, или воглавно операции базирани на Windows - можеби би биле комфорни со други понуди. Enterasys исто така нуди HIDS агент кој се врзува со рамката на Dragon.
Продавач: Enterasys Networks, Inc., Платформа: Appliance и Unix
Производ: Dragon, URL: http://www.enterasys.com

Intrusion SecureNet NID/ SecureHost HID - Intrusion има интересна историја. Оригинално е познат како ODS и обезбедувал мрежен хардвер. На крајот на 1998 година станал и IDS. Во 2000 година го променил своето име во Intrusion.com, а потоа, откако пропаднал dotcom-от во 2001 година, станал само Intrusion. Неговата линија на производи се уредите SecureNet NIDS и secureHost HIDS за Windows.
Продавач: Intrusion, Inc., Платформа: Appliance и Windows,
Производ: SecureNet и SecureHost, URL: http://www.intrusion.com/default.asp

IntruVert IntruShield - IntruVert е релативно нов играч во IDS областа, на компанија која е основана во октомври 2000 година. IntruVert се фокусира на high end пазарот со производи кои може да управуваат со широка палета на мрежни операции. Тоа е комбинација на NIDS и систем базиран на аномалии.
Продавач: IntruVert, Платформа: Appliance,
Производ: IntruShield, URL: http://www.intruvert.com

NFR Network Intrusion Detection System - NFR е долго признат како еден од првите производи што поседуваат карактеристики на NIDS. NFR Network Intrusion Detection System е производ кој се базира на NIDS и кој дозволува висок степен на прилагодување преку употреба на ncode; развиен е и NFR скриптен јазик. NFR производот по традиција бил инспириран од искуството на хакерите. Иако производот имал можност за управување на различни типови на напади кои уништувале пакети, тежнеел да ги решава ситуациите со широк опсег. NFR го додал NFS Host Intrusion detection System кон својата производна линија.
Продавач: NFR Security, Inc., Платформа: Appliance
Производ: NFR IDS, URL: http://www.nfr.com

Symantec NetProwler и Intruder Alert - Компанијата Symantec IDS го интегрирала својот систем базиран на хост (Intruder Alert) со системот базиран на мрежа (NetProwler). Иако тие можат да се поврзат заедно со користење на заеднички управувачки платформи, нивните сличности тука завршуваат. NetProwler по традиција поседува некои интересни карактеристики кои не се наоѓаат во други IDS, но недостаток му е поддршка со управувањето на многу техники на NIDS. NetProwler се подига само на Windows NT, со исклучок на Console која се поддига на 2000/ XP, а нова верзија не е исфрлена веќе две години. Спротивно, HIDS Intruder Alert има една од пошироките поддршки на пазарот, во поглед на оперативните системи.
Продавач: Axent/Symantec, Платформа: Windows, различни верзии на Unix
Производ: NetProwler, Intruder Alert, URL: http://enterprisessecurity.symantec.com/

10.6 ПОВТОРУВАЊЕ ЗА FIREWALL

FireWall е било кој уред што се користи како механизам на мрежното ниво за контролата на пристап до одредена мрежа или збир на мрежи. Во многу случаи, firewall-от се користи да се заштити внатрешната мрежа од пристапот однадвор. Меѓутоа, тој може да се користи и за да се креираат посигурни пакети во внатрешноста на LAN за многу осетливи функции како што се процесот на исплата и R&D системите. FireWall-те се обично приватни хардверски уреди, често стартувани на приватни оперативни системи. Cisco PIX серијата е добар пример за firewall уред. FireWall-те се дизајнирани да служат како контролни точки кон и од вашата мрежа. Тие извршуваат конекциски барања како што ги примаат. Проверуваат дали треба или не да се дозволи мрежен сообраќај, што се базира на предефиниран збир на правила или начела. Се процесираат само барањата за конекција од авторизирани хостови кон авторизирани одредишта. Останатите конекциски барања се одбиваат.
Некои од карактеристиките на firewall-от вклучуваат:

- Филтрирање на содржината – Некои организации сакаат да ги спречат своите корисници да не пребаруваат одредени веб сајтови: веб сајтови кои се базирани на електронска пошта, "подземни" сајтови, дневен пристап до продавници, порнографски сајтови и др. Карактеристиките на филтрирање на содржината и сервисите можат да помогнат во блокирањето на овие сајтови, како и да спречат некои типови на ActiveX

и Java базирани кодови. Конечно, филтрирањето на содржината може да прави и некои видови на антивирусни проверки, иако е добра идеја да се поседуваат посебни антивирусни производи на компјутерот и серверите на електронска пошта.

- Виртуелно приватно вмрежување (Virtual Private Networking-VPN) – VPN се користи за да се проследи сигурно сообраќајот од точката А до точката Б, обично преку хостот на мрежата (како што е Интернет). Иако постои широка опфатеност на посветените VPN уреди во продажба, продавачите како што се Checkpoint и Cisco ги исфрлиле VPN сервисите од своите понуди на firewall. Многу производи на firewall сега нудат и клиент–кон-фирма VPN функционалност, и LAN-кон–LAN функционалност.
- Преведување на мрежни адреси (Network Address Translation-NAT) – Преведувањето на мрежните адреси често се користи за мапирање на илегални или резервирани блокови на адреси. Иако NAT не е неопходна особина на сигурност, првите NAT уреди кои се појавиле во корпоративните кругови се обично производи на firewall.
- Балансирање на вчитувањето – Повеќе од генерички термин отколку било што друго, балансирањето на вчитување е вештина на сегментирање на сообраќајот при неговото дистрибуирање. Иако балансирањето на вчитувањето е само опција, некои производи на firewall поддржуваат карактеристики кои ќе ви помогнат да го насочите веб и FTP сообраќајот при неговата дистрибуција.
- Толеранција на недостатоци – Некои од современите firewall како што е Cisco PIX и Nokia/Checkpoint поддржуваат некои прилично комплицирани карактеристики. Често се нарекуваат high-availability (HA) функционалности, т.е. напредни карактеристики на толеранција на недостатоците. Често им дозволуваат на firewall-ите да се покренат во пар, со еден уред кој функционира во резерва, ако другиот откаже.
- Откривање на влез – Терминот "откривање на влез" може да означува повеќе работи, но во овој случај, некои продавачи интегрираат сосема различен тип на опции (за детекција на упад) во својата понуда на firewall. Иако ова не значи креирање на проблем само по себе, луѓето треба да се претпазливи со опциите кои се инсталирани во нивниот firewall. Значи, firewall-от тешко може да замени систем за intrusion detection.

Firewall-те отсекогаш играле главна улога во моделите на организациска сигурност. Терминот KISS (Keep it simple stupid), е принцип кој е драг во светот на мрежната администрација, но може да се каже дека овој принцип не важи секогаш кај производите за мрежна сигурност. Не смееме да шпекулираме со безбедноста - постојат ранливости и на firewall-те, кои ја намалуваат нашата сигурност.

10.6.1 Firewall-от не е непробивен

Иако продавачите сакаат да мислат дека нивните firewall-и се имуни на проблемите што ги унесреќуваат оние кои ги одржуваат оперативниот систем и

апликациите, факт е дека и тие се исто така ранливи. Ќе разгледаме неколку примери што кружат за производите на firewall:

- Јули 2000: Во текот на брифингот на црните шешири, двајца добро познати истражувачи на сигурност, John McDonald и Thomas Lopatic, ги соопштиле поголемиот број на ранливости што ги пронашле во Checkpoint Firewall-1 производот. Ова е важно, затоа што производот Checkpoint е еден од најраспространетите firewall-и во светот.
- Јуни 2001: Cisco IOS пронашол дека има дупка во сигурноста со чија помош крекерот може да изврши привелигирани команди преку вграден HTTP сервер.
- Јули 2001: Checkpoint Firewall-1 и VPN-1 имале ранливост низ која крекерите го пропуштале својот сообраќај во и од мрежата, (а не би требале тоа да го можат).
- Октомври 2001: Cisco морал да замени многу PIX firewall-а на потрошувачките сајтови, затоа што известувале или се затворале заради хардверски грешки.
- Август 2002: Symantec Raptor firewall имал проблем со тоа што крекерот одземал сесии пратени низ firewall-от.

Оваа листа не е конечна, ова е само претстава на некои од проблемите кои се откриени во денешните firewall производи. Исто така, земете во предвид дека некои од слабостите се директно поврзани со функциите надвор од вообичаените firewall-опции, а кои се додадени од производителите: филтрирање на содржината и енкапсулација (за VPN употреба).

10.6.2 Типови на firewall

Во општа смисла, firewall-от се состои од софтвер и хардвер. Софтверот може да биде комерцијален, shareware или бесплатен. Хардверот може да биде било кој уред што подржува софтвер. Технологијата на firewall може генерално да се класифицира во една од трите категории:

- Филтер базиран на пакети (обично рутери, Cisco IOS);
- Филтер кој е базиран на состојбена инспекција (Checkpoint FW-1, PIX);
- Филтер кој е базиран на прокси.

Firewall базиран на филтер на пакети

Firewall филтрирањето на пакети типично се базира на рутирање. Со користење на основниот рутер за филтрирање на пакети, може да се дозволи или забрани пристап на вашата мрежа, врз база на неколку променливи, вклучувајќи:

- Адреса на изворот
- Адреса на одредиштето
- Протокол
- Број на порти.

Firewall-те кои се базирани на рутер се популарни затоа што лесно се имплементираат (едноставно го вградувате, дефинирате листа на пристапи и сте завршиле). Ако вашата мрежа постојно се конектира на Интернет, ќе ви биде потребен рутер. Па зошто да не убиеме две муви со еден потег? Од друга страна firewall-те кои се базирани на рутер имаат неколку маани. Прво, обично не се подготвени за управување со моментални типови на напад, на пр. denial-of-service. Многу од тактиките на denial-of-service на Интернет се базираат на уништување на пакетите, SYN претркување или појавување на други аномалии на TCP/IP. Основните рутери не се дизајнирани за справување со такви типови на напади. Второ, некои рутери од пониско ниво не може да го сочуваат flag-от на сесијата на податоци. Администраторите тогаш се присилени да ги задржат сите порти над 1024 отворени - да управуваат со TCP сесиите. Генерално, не е добра пракса да се оставаат некористените порти отворени кон надворешноста. Конечно, користењето на ACL (access control list) кај рутерите од повисоко ниво кои поддржуваат многу брзи мрежи - може да придонесе за деградација на перформансите и поголема работа на CPU-то. Меѓутоа, за побавни конекции (како што се T1), нормалното филтрирање на пакетите нема да го оптовари рутерот за некој значаен степен, дури и за пониско ниво на рутери (како што е Cisco 2500 серија на рутери).

Личен firewall

Друг тип на пакетен филтер кој стана популарен последните неколку години е личниот firewall. Тој одговара на домашните потреби, или дури на корпоративните здруженија, каде на одредени машини треба да им се додаде сигурност. Личните firewall-и се инсталираат на било кој компјутер кој се штити, а потоа софтверот на личниот firewall ќе ги надгледува сите доаѓачки конекции. Ќе прифати, одбие или ќе го праша корисникот да одлучи што да направи.

Firewall базиран на состојбена инспекција

Филтрирањето со состојбена инспекција се базира на концептот за филтрирање на пакети и има неколку чекори. Firewall-те се изградени по модел кој води евиденција за сесиите и конекциите во внатрешни табели на состојба и според тоа може да реагира. Овие firewall-и можат да откријат аномални ситуации кои го нарушуваат стандардниот протокол кој не може да го открие обичниот филтер на пакети. Ова му дозволува на состојбениот firewall да ги блокира нападите кои може да ги пропушти филтерот на пакетите. Поради ова, производите кои се базирани на состојбено филтрирање се пофлексибилни, отколку соодветните филтрирачи на пакети. Освен тоа, производите базирани на состојбена филтрација на пакети, се дизајнирани да заштитат од одредени типови на DoS напади, да ја зголемат заштитата на поштата која е базирана на SMTP, а имаат и други додатни методи за сигурност. Checkpoint развила т.н. “состојбена инспекција” (stateful inspection SI), која се заснова на состојбено филтрирање на пакетот. SI овозможува тестирање на корисните податоци, а не на адресите и портите.

Firewall базиран на прокси

Друг тип на firewall е базиран на прокси (понекогаш се однесува на пристапна апликација или апликациски-прокси). Кога оддалечениот корисник ја контактира мрежата со покревање на firewall кој е базиран на прокси, firewall-от остварува конекција. Со помош на овие две техники, IP пакетите се враќаат директно во внатрешноста на мрежата. Место тоа, firewall-от работи како цевовод и интерпретатор. Firewall-те кои се базирани на прокси отсекогаш биле побавни отколку оние кои се базирани на состојбено филтрирање на пакетите. Концептот протокол-протокол е посигурен отколку генеричкото филтрирање на пакетите, затоа што firewall-от разбира апликациски протоколи (HTTP, FTP, SMTP, POP). Firewall-от ќе отфрли сè што не е одредено со спецификациите на протоколот. Потешко е за напаѓачите да украдат нешто што е содржински надгледувано, отколку портите и IP адресите. Сега, за големината на мрежата (10 Mbps или побавно), оваа разлика е спорна. Меѓутоа, за мрежите со големи брзини (T3 на 45 Mbps, T3 на 100 Mbps итн.), ова станува клучна тема. Бидејќи технологијата напредува, разликата е помала, но за сега употребата на чиста технологија која е базирана на прокси е сеуште интерес на повеќето мрежи.

10.6.3 Програмери кои го заобиколуваат firewall-от

Многу компании имаат потреба да разменуваат податоци со партнерите и потрошувачите. Пред многу време (пред настанокот на рутерите), постоеле само програми базирани на сокет - со кој се остварувала директната конекција. Со firewall-от ова не може да се прави. Заради тоа, хакерите ги проучуваат начините да го заобиколат firewall-от со користење на HTTP како свој нов транспортен протокол. Можеби мислите дека HTTP не е опасен, зашто служи само за рамена на документи? Погрешно – протоколот каков што е SOAP (Simple Object Access Protocol) овозможува оддалечен пристап, т.е. повик на функции преку HTTP. Firewall сигурноста која работи со SOAP е од понов датум. Едно такво решение е Quadrasis SOAP Content Inspector.

Една стапица во светот за firewall е таа дека сигурноста може да биде конфигурирана многу строго, и со тоа да го намали процесот на вмрежување. На пример, проучувањата укажуваат дека употребата на firewall-от не е практична во мрежи во кои корисниците зависат од дистрибуција на апликации. Понекогаш, firewall-те може да имплементираат строги начела на сигурност, така што мрежните опкружувања застанат. Она што се добива во сигурност, се губи во функционалност. За некои, ова може да се смета едноставно како незгода, но проблемот може да има долготрајни ефекти кои доведуваат до поголеми штети. На пример, повеќето администратори се сретнале со случај кога на корисникот X му треба сервис Y и проблеми на сигурност кои го спречуваат барањето. Ако, на пример, администраторот го блокира сервисот Y, се јавува ризик дека корисникот е претседател на Управниот одбор (па ќе мора да го дозволи несаканиот сервис). Ова може да води кон тоа, одредени личности да ја рушат безбедноста на мрежата, па пред или подоцна - firewall-от ќе пропушти нешто што не треба. Сепак, паметните организации знаат да ги испитаат овие ситуации и да работат подеднакво за сите. За жал, не работиме сите во “паметни” организации...

Firewall-те можат да помогнат во креирање на различни потсистеми. На пример, ако некој имплементира систем на плаќање преку Интернет, се разгледуваат начините за контролирање на логирањето. Поделете ги системите на плаќање на одвоени подмрежи, имплементирајте јаки системи за проверка на пријавите, работете на остварување на IDS (Intrusion detection system), кој се имплементира во проблематичните сегменти. Друга сериозна тема е лажното чувство за сигурност. Администраторите кои имаат став дека нивниот firewall ќе ги заштити од сите опасности - ги чека непријатно изненадување. Дел од предизвикот во користењето на firewall е да се изгради чувство на сигурност без претерување. Причината зошто оваа рамнотежа е важна е што - без други нивоа на одбрана, не би можеле да опстанете. Ако вашиот firewall е пробиен, вашата внатрешна мрежа може лесно да биде уништена. Firewall-те се дел од сигурносните системи, тие не треба да се самостојни, затоа што имаат повеќе недостатоци.

10.6.4 Проценка и избор на firewall

Врз база на вашата мрежна околина, треба да процените и одлучите кој firewall производ ќе го купите. Пред да го купите, треба да направите истражување, т.е. да генерирате листа за тоа што ви треба. Следниот чекор е да се направат неколку тестирања на firewall во лабораторија. Меѓутоа, секој нема лабораторија за тестирање и неколку додатни недели да си игра со производите за сигурност. Следната добра работа е да се добие демо производ, (посетете некој кој има лабораторија, или прашајте го продавачот за совет) за тоа како можете да го видите производот во секојдневна работа. Ако вашиот продавач е љубезен, тогаш ќе ви помогне. Општи критериуми на многу луѓе при одлуката кој firewall ќе го купат, се:

- Можности – Може ли firewall-от да го поддржи преносот што го проценувате? Дали постои место за мерење? Типично, ако зборувате за брзина од T3 (45 Mbps) или побавна, скоро секој firewall ќе работи.
- Карактеристики – Потребно е firewall-от да поседува повеќе карактеристики. Уверете се дека вашиот firewall може да го работи она што ви е потребно. Меѓутоа, бидете реални со тоа - за што го користите. Исто така пријавувањето на проблеми е важен детаљ. Ако ви дава многу малку или погрешни информации, вие имате проблем.
- Кориснички интерфејс – Ако немате комфорен интерфејс, или ако не го разбирате интерфејсот, ќе ви биде отежнато користењето на firewall-от.
- Цена – Ова е секогаш фактор. Иако многу луѓе по традиција бираат Checkpoint FW-1, често пати дури и обичниот FW-1 е доволно силен, чинејќи пет до десет пати повеќе од другите производи. Разгледајте ги сите опции, понекогаш втората е најдобра и ќе ве штити за помала цена.

- Репутација – Дали продавачот одговара за ранливоста на производот? Што е со историјата на записи на производот? Дали има развиена корисничка база или е нова верзија на пазарот?

Исто така, земете ги во предвид наодите на независни тестирања во лабораториите и други технички списанија кои се занимаат со заштита.

10.6.5 Развој и тестирање на вашиот firewall

Конечно, откако сте го купиле вашиот firewall, ќе преминете кон инсталирање на firewall-от и неговите поддржани збирови на правила. Прво, уверете се дека firewall-от е сигурен. Ако уредот одговара, мали се шансите дека постојат надворешни промени (на пр. лозинки кои треба да ги ставите за да ја подобрите работата). Меѓутоа, ако е тоа firewall кој е базиран на NT или Unix, уверете се дека оперативниот систем на кој што е базиран firewall софтверот - е доволно јак. Следниот чекор е да го поставите вашиот firewall во вашата мрежна околина и да ги дефинирате правилата за филтрирање на сообраќај. Ако е ова планирано правилно, ќе можете да го пренесете firewall-от во мрежното опкружувањето со исклучување на еден сервер за момент. Меѓутоа, честопати не е толку лесно. Се очекуваат барем неколку проблеми, и понекогаш треба да совладате неколку прилично лути корисници. Тешко е веројатно дека ќе го направите правилно од прва, освен ако вашето мрежно опкружување е едноставно, или сте волшебник. Ако направите како што треба првиот пат, ви честитаме – Вие сте еден од ретките! Инаку, спаѓате во групата на останати и немој да бидете лути на себе. Конечно, треба да го тестирате вашиот збир на правила. Поради ова, ви препорачувам внимателно тестирање. Постојат две посебни фази:

1. Тестирање на збирот на правила од надвор,
2. Тестирање на збирот на правила од внатре.

Пред сè, потсетите се на DEFAULT DENY, т.е. она што не е потребно – забранете го. Ако не знаете што е содржината, не дозволувајте таа да помине низ вашиот firewall. Подобро да се бавите со учење на протоколот и апликациите, отколку да не ги познавате отворените дупки во вашето опкружување.

10.6.6 Комерцијални firewall-и

Ќе издвоиме неколку видови на firewall кои се користат во секојдневието:

BlackICE - Тип на Firewall: пакетен филтер (личен firewall)
Производител: ISS; Поддржана платформа: Windows 98 и подобри.

BorderManager - BorderManager е првиот firewall за Novell опкружување, но исто така ги заштитува системите кои се базирани на Unix и NT. Производот нуди централизирано управување, јако филтрирање и поголема брзина, го анализира мрежниот сообраќај во реално време. Исто така, BorderManager нуди можност за креирање на "мини firewall" внатре во вашата организација, за да се спречат внатрешни напади од страна на поединци или локални мрежи.

Тип на firewall: базиран на состојбена инспекција.
Производител: Novell Inc.; Поддржана платформа: Novell NetWare.

FireBOX - Тип на firewall: базиран на состојбена инспекција.
Производител: Observer; Поддржана платформа: Unix.

Firewall-1 - Checkpoint Firewall-1 е еден од најчесто користените firewall-и во индустријата денес. Особините на производот се: филтрирање на пакети, строго проценување на содржината, интегрирање на заштитата против spoofing, VPN опции, скенирање на вирусите во реално време и други карактеристики. Тој е еден од најкарактеристичните видови на firewall, но тој исто така е и најскап.
Тип на firewall: базиран на состојбена инспекција.
Производител: Checkpoint software technologies Ltd.;
Поддржани платформи: Windows XP и Unix.

Firewall server- Тип на firewall: базиран на прокси.
Производител: BorderWare.
Поддржана платформа: PC (оперативен систем подигнат на Интелов хардвер).

GNAT Box Firewall - GNAT е хардверски firewall уред. Можете да управувате со GNAT уредот - од командна линија или преку веб-базиран интерфејс. GNAT филтрирањето на доаѓачкиот сообраќај се базира на IP адресата на изворот, адресата на одредиштето, портата, мрежниот интерфејс и протоколот.
Тип на firewall: Базиран на состојбена инспекција
Производител: Global Technology Associates
Поддржана платформа: N/A (уред)

Guardian - Gurdian е firewall кој е базиран на XP.
Тип на firewall: базиран на состојбена инспекција.
Производител: netGuard Inc.
Поддржана платформа: Windows XP.

NetScreen- NetScreen е уред на firewall кој подржува IPsec, DES и Triple DES енкрипција.
Тип на firewall: базиран на состојбена инспекција.
Производител: NetScreen Technologies Inc.
Поддржана платформа: N/A (уред)

PIX Firewall - PIX и Firewall-1 се два најшироко користени производи на firewall денес. PIX е firewall уред кој не се базира на апликациски прокси, туку на сигурен оперативен систем внатре во самиот уред. Тој подржува IPsec, и може да се администрира преку Telnet или SSH сесија, или преку Cisco Security Policy manager (CSPM).
Тип на firewall: базиран на состојбена инспекција.
Производител: Cisco systems Inc.
Поддржана платформа: N/A (уред)

ZoneAlarm Pro- Тип на firewall: базиран на филтрирање на пакети (личен firewall).
Производител: Zone Labs.

Поддржана платформа: Windows 98 и понови верзии.

10.7 НЕКОЛКУ КОРИСНИ СОВЕТИ

Ќе понудам неколку упатства кои можат да ви овозможат посигурен компјутерски живот:

- Проверете ги сите предупредувања на вашето IT одделение. Без разлика дали сте раководител или администратор, уверете се дека постои познато начело по кое само еден систем инженер е задолжен за безбедноста. Ова ја намалува паниката, овозможува помала загуба на информации, и го смалува ризикот од несоодветни акции, кои би можеле да бидат полоши отколку неактивноста.
- Не им верувајте на додатоците (attachments), дури и од луѓе кои ги познавате и кои се достојни за доверба. Праќачот можеби нема злобна намера, но можеби нема современ анти-вирусен софтвер. Со тоа, вирусите на електронската пошта и црвите вообичаено се праќаат без знаење на личноста на чиј налог се примаат. Дури и легитимно, очекуваниот додаток може да биде инфициран со вирус. Во било што од следните случаи треба да се сомневате:
    - Од некој што не го познавате, кој нема легитимна причина да ви испраќа порака.
    - Ако добиете празна порака со attachment.
    - Текстот на пораката нема врска со attachment-от.
    - Текстот на пораката не изгледа дека има смисла.
    - Пораката не го карактеризира праќачот.
    - Пораката е насочена кон порнографски сајтови, еротски слики или други несакани содржини.
    - Пораката вклучува референци кои не се во потполност лични.
    - Attachment-и со имињата на фајловите кои се обидуваат да скријат дека фајлот е извршен, т.е. вирус. Следи листата на екстензии за имиња на фајлови кои укажуваат на извршен програм, или фајлови кои можат да содржат извршни програми во облик на макро.

BAT	.CHIM	.CMD	.COM	.DLL	.DOC	.DOT
EXE	.FON	.HTA	.JS	.OVL	.PIF	.SCR
SHB	.SHS	.VBS	.VBA	.WIZ	.XLA	.XLS

Оваа листа не вклучува сè. Постојат имиња на фајлови како што е .RTF кои не треба да вклучуваат во себе програми, но под некои околности можат (кога содржат вграден фајл, на пример). Имајте на ум дека Word документите (на пример) во принцип може да имаат и екстензија од друг вид на фајл. Исто така, зипуваните (компресирани) фајлови со екстензија .ZIP може во себе да содржат еден или повеќе различни видови на фајлови.

- Потсетете се дека жртвите на црвите обично не знаат дека им е пратен инфициран додаток (attachment). Не постои начин – attachment-те да се проверуваат со налог. Ако некој ви прати attachment, без некоја посебна причина, или ако се појави некој од претходните случаи, се потврдува дека тоа е направено намерно.
- Користете антивирусен софтвер и ажурирајте го. Меѓутоа, не претпоставувајте дека користењето на најновото ажурирање може да ве направи неранлив. Антивирусниот софтвер не може да го фати и дезинфицира секој тип на закана, посебно новите malware и дупликатите, и не може да ги одбие во целост нивните болни ефекти. Користете скенирање вклучено во позадина и само-ажурирање на вирусните дефиниции каде што е можно.
- Ако ви дозволува вашето опкружување, оневозможете го Windows Scripting Host.
- Не инсталирајте (и не дозволувајте на други да ви инсталираат) неавторизиран софтвер. Програмите како што се игрите, програмите за шега, заштита на екраните и неавторизираните помошни програми можат да доведат до потешкотии, дури и ако не се злобни по својата намера. Бидете внимателни со програмите кои ги наоѓате во несигурни опкружувања, како што се Интернет собите за разговор, дискусионите групи, spam - електронската пошта итн.
- Ако користите макро вирусни апликации како што е Word, уверете се дека макроата не се овозможени по default. Новите верзии на Office овозможуваат макроата да се оневозможат како подразбирачка опција. Ако примате документ со макро од извор на кој му верувате, прашајте за потврда. Но не и верувајте на оваа опција апсолутно. Ако е можно да работете со макро формати како што се .RTF (Rich Text Format), работете така.
- Оневозможете подразбирачко стартување (подигање) од дискета - во CMOS. Ова ја блокира инфекцијата со вирус на boot секторот.
- Понекогаш по пошта се праќаат енкриптирани документи со цел да бидат нечитливи за напаѓачите. Меѓутоа, ако се јави инфицирање со вирус, енкрипцијата ќе ја спречи анти-вирусната заштита. Енкриптираните додатоци не можат обично да се скенираат за вируси во транзит.
- Ако користите апликации и програми со познати ранливости, како што се IIS, Internet Explorer, Outlook и Outlook Express, уверете дека постојат најнови закрпи за нив.
- Бекап, бекап, бекап. И тестирајте ги вашите бекапи!

□

КОРИСТЕНА ЛИТЕРАТУРА

[1] John E. Canavan: Fundamentals of Network Security, © 2001 Artech House, Inc.

[2] Matthew Strebe: Network Security JumpStart, © 2002 SYBEX Inc.

[3] Simson Garfinkel, Alan Schwartz, Gene Spafford: Practical Unix & Internet Security, 3rd Edition, © 2003 O'Reilly & Associates.

[4] Иван Краљевски, Зоран Гацовски: Вовед во компјутерски мрежи, © 2006 Европски Универзитет, Скопје.

[5] http://csrc.nist.gov/ - Computer Security Division of National Institute of Standards and Technology.

[6] http://en.wikipedia.org/wiki/Computer_security – Wikipedia, the Free Encyclopedia.

[7] http://www.cert.org/homeusers/HomeComputerSecurity/ - CERT Computer Security.