

Защита на Информацията

- Сигурността в Интернет и сигурността и защитата на данните и програмите е проблем, за всеки който има някакво отношение към персоналните компютри, мрежите и информационните системи.
- Всяко действие, което възпрепятства системата Ви да работи по предназначение, трябва да бъде смятано за атака
- Атаките и неприятните намеси се възползват от следните слаби места:
 - Сигурност на мрежовите устройства – свободата на достъпа до мрежовите устройства, включително и приложения клиенти;
 - Пропуски на ниво чисто физическа защита на системата;
 - Дефекти в операционната система и приложенията;
 - Зле конфигурирана система;
 - Човешки грешки;
 - Дефекти на IP протоколния комплект.

Според целта атаката бива:

- Компрометиране – невъзможност за работа по предназначение – атаки от този тип са:
 - Отказ от услуга
 - Вируси
 - Непозволен достъп до информация:
 - Троянски коне
- Снифиране /наблюдения на трафика, заради типа информация, която може да достави: потребителски имена, пароли, e-mail адреси или пък да събира IP информация
- Открадване на сесия /трети участник – хакер е в състояние да се вмъкне между връзката на двама потребители в момента, в който те се свързват или пък при създадена вече връзка.
- Социално инженерство

Според начина на осъществяване атаката бива:

- Осъществяване на пряк физически достъп до компютър или мрежово устройство или влизане с права на легитимен потребител:
- Физически достъп до компютър, който авторизиран потребител е оставил незащитен
- Открадване на парола.
- Отдалечен достъп:
- Троянски коне
- Задни вратички
- Hijacking /открадване на сесия

Вирусите - главен проблем за потребителите

- Вирусът е програмен сегмент, който е прикрепен към легитимна програма, с цел да зарази други програми. Типичният вирус работи по следния начин:
 - Авторът на вируса разработва полезна нова програма, която съдържа скрит код на вируса.
 - Когато програмата се стартира, тя започва да преглежда двоичните файлове дали вече са зарезани. Здрава програма, тя се инфектира чрез добавяне на вирусния код накрая на файла, а в началото се записва преход към него. Когато вирусният код се изпълни, започва изпълнението на нормалната програма. По този начин,

при всяко изпълнение на заразената програма се инфектират нови програми.

- По-нататък всяка заражена програма сама става източник на зараза и чрез разпространяване на заразени файлове от компютър на компютър вирусът се разпространява, което го различава от Троянските коне например. Троянските коне са статични програми – не се разпространяват сами.
- *Важна черта от поведението на вируса е, че той не може да се разпространява без човешка намеса. На компютъра Ви може да има заразен файл, но той не може да заразява други файлове докато не бъде стартиран.*
- *Възможно е вирусът, освен заразяването на други програми, да причинява и щети, като изтриване, модифициране на файлове. Например вирус може да инфектира зареждащия сектор (boot) на твърдия диск, с което да направи невъзможно пускането на компютъра.*

Според поведението си вирусите биват:

- Паразитни – традиционните и най-разпространени вируси, които се прикрепят към изпълнимите файлове.
- Резидентни – разполагат се в основната памет като, част от резидентните системни програми, откъдето могат да инфектират всяка изпълнявана програма.
- boot секторни – инфектират главния зареждащ запис или други зареждащи записи, когато системата се зарежда от инфектиран диск.
- Невидими – stealth – форма на вирусите, които са разработени да се крият от антивирусните програми.;
- Полиморфни – мутират с всяка инфекция, правейки невъзможно разпознаването на сигнатурите им.
- Тунелиращи –, тунелирането се състои в опит вирусът да действа преди антивирусната програма, използвайки софтуеърни прекъсвания.
- Бързо действащи – когато са активни в паметта инфектират не само изпълняваните програми, но файлове, които са само отворени.
- Бавно действащи – Slow infectors – активни са в паметта, но инфектират само новите или модифицираните файлове.

Червеи

- Червеят е програма, която се самокопира и изпраща свои копия по мрежата от компютри. При пристигането си в някакъв възел, червеят може да се активира, за да се възпроизведе и разпространи отново. Освен това, червеят изпълнява някои нежелани функции – може да се държи като вирус, да вмъкне Троянски кон или да върши разрушителни действия.

Бактерии

Бактерията е програма, която се самокопира (обикновено се възпроизвежда експоненциално). Нейната задача е да консумира системните ресурси (процесор, памет, дисково пространско), лишавайки по този начин потребителят от достъп до тях.

Троянските коне са едни от най-коварните средства за атака

- Характерно за троянските коне е, че те включват в себе си неавторизиран код, който изпълнява неизвестна и най-вероятно нежелана от потребителя функция. Тези нежелани функции могат понякога да бъдат такива като на вирус и тогава изпълняващата ги програма може да бъде квалифицирана и като вирус и като троянски кон. Това което отличава троянския кон от вируса е начинът му на разпространяване – за разлика от вирусите троянските коне не инфектират други

файлове, но щетите, които те могат да нанесат на сигурността на системата, могат понякога да бъдат много по-големи от тези, нанесани от вирусите. Известни са дори случаи на вмъкване на троянски коне от разработчиците на ОС. В последния случай те не създават щети, а са насочени към събиране на информация.

Средства за разпространение използвани от вирусите и червеите и др.

- Интернет
- Електронна поща – 80 % от различните видове заплахи за сигурността се използват този начин, защото той предлага бързо разпространение – едно заразено съобщение може за няколко минути да зарази хиляди компютри;
- Разглеждане на Web – някои Web страници използват Java аплети, ActiveX контроли и скриптове, които могат да заразят компютъра или да го пренасочат към заразени сайтове;
- FTP – FTP сайтовете могат да съдържат заразени файлове, освен това всяко “сваляне” на файл от други сайтове се извършва по FTP ;
- Новинарските групи и Чатовете;
- Мрежите
- Споделени дискове;
- Работни станции;
- Сървери, включително прокси сървери и стени.
- Устройства за съхраняване на информация – твърди дискове, CD и DVD, сменяеми дискове, споделени мрежови дискове, флопи дискове

Възможни атаки

сканиране на мрежата с цел установяване на услугите които даден хост изпълнява

отказ от услуга

наблюдения на трафика, заради информация от типа: потребителски имена, пароли, e - mail адреси

разбиване на пароли

социално инженерство

програми показващи реклами

спам

FTP атаки

DNS атаки

DoS (отказ от услуги)

• DoS атаките могат да бъдат извършени по няколко начина. Тези типове атаки понякога се наричат също *нюк (nuke) атаки*

• DoS атаките не предизвикват срив на компютъра, а прекъсват или попречват на установяване на връзка към мрежата. Те работят, като наводняват мрежата с непотребни пакети, или като емулират мрежов проблем, който кара компютъра да прекрати установената връзка.

Сигурност на съобщенията по електронната поща

• Електронната поща прилича на открита пощенска картичка, която може да бъде прочетена от всеки, който я пренася по време на нейното пътуване от подателя до получателя

•Съобщенията от електронната поща са много лесни за прихващане Ако не е криптирано или подписано с цифров подпис,съобщението може лесно да бъде прочетено, копирано или променено във всяка една точка по неговия път.

Информационната защита цели:

- конфиденциалност – не се допуска неауторизиран достъп до текста на съобщението
- цялостност на данните – не се допуска промяна на съобщението /фалшификация/
- идентификация на изпращача – не се допуска изпращане на съобщение от името на друго лице
- доказване на авторството – подателя не може да отрича, че е изпратил съобщението

При предаване през публични мрежи защитата на информацията се гарантира с използване на криптографски методи – публичен ключ; секретен ключ и цифров подпис

Криптиране

•*Криптирането* включва конвертиране на данните във форма, която не може лесно да бъде разбрана от другите. •Когато документите са криптирани на диска, може да ги разглежда само потребител, който има правилен ключ. Ако други опитат да осъществят достъп, тогава или файлът няма да се отвори изобщо, или ще се появи като объркани безсмислени знакове. Конфиденциалните данни трябва да бъдат защитени както с позволения за достъп, така и с криптиране.

- Криптографските системи работят по следния начин – Данните, които иска да изпрати подателят, се кодират от тяхната първоначална текстова форма (чист, прост текст) в зашифрован текст (криптограма). Криптограмата, въпреки че е четлива, не дава никакъв смисъл. Зашифрваният текст може да се записва във файлове или да се изпраща по незащитени линии. За да стане разбираем шифрваният текст, той трябва да се разшифрова обратно в чист текст. Тази схема предполага алгоритми за шифроване и разшифроване (някои, от които могат да бъдат реализирани и апаратно) и ключ за всяко приложение, чието предаване трябва да става по особено секретни канали.

Безопасността на системата се базира на секретността на ключа, а не на секретността на алгоритмите. Криптоанализ (анализ на шифъра) се състои във възстановяване на открития текст, без да се познава ключа за разшифроване. Ако криптоанализът не може да възстанови текста, криптографската схема се смята за безопасна.

Има два главни вида криптиране според типа ключ – секретен и публичен

- **Секретен ключ** – симетрична криптография – използва се един и същ ключ за криптиране и декриптиране. Симетричното криптиране може да криптира текста на блокове или на потоци (по един байт). Първият тип се използва за криптиране на данни с предварително известна дължина, а вторият за неизвестни големини като мрежов поток между рутери. Предимства на симетричното криптиране са простота на употребата, а недостатъците се отнасят до дистрибуцията и съхраняването на ключа. Алгоритми от този тип са:
 - DES – Data Encryption Standard
 - IDEA – International Data Encryption Algorithm
 - CAST – наречен на инициалите на създателите си – Carlisle , Adams , Stafford и Tavares
 - Blowfish
 - Ron's

– SEAL – Software Oriented Encryption Algorithm

Хеширане

- При хеширането множество от стойности **K** (ключове) се преобразува в друго множество **A** (например адреси или индекси на масив) с помощта на функция **h**, която се нарича хеш-функция. Или ако **K** е множеството на ключовете, **A** – друго множество, например адреси, то се търси изображението **H**, което изобразява множеството **K** в множеството **A**. Или $H: K \rightarrow A$. Изискванията към хеш функциите са да се разполагат разпръснато, да създават възможно най-малко колизии (един и същ елемент от множеството **A** да е образ на повече от един елемент от множеството **K**) и др. Хеширането се използва за най-разнообразни случаи например за решаване на проблема време-памет, но в случая на сигурността се използват криптографски силни хеширащи алгоритми, които не създават колизии и служат да се уверим, че данните не са променяни по някакъв начин, при пароли и др. Примери за криптографски силни алгоритми са: SHA – Secure Hash Algorithm, MD 2, MD 4, MD 5 (MD – Message Digest).

Кодиране със симетричен ключ

- кодирането и декодирането се извършва с един и същ секретен ключ
 - конфиденциалност на данните – да
 - цялостност на данните – да
 - идентификация на изпращача – да (ако един ключ се използва само от двама кореспонденти)
 - доказване на авторство – **не**
- Проблем на тази схема е разпространението на ключовете. Необходим е сигурен начин за доставяне на секретния ключ до кореспондентите

Кодиране с публичен ключ

- Публичният ключ е общодостъпен, а секретният е известен само на собственика му.
- Публичният и секретният ключ са математически свързани
 - кодирането със секретния ключ се декодира само с публичния
 - кодирането с публичния ключ се декодира само със секретния

Цифрови подписи

- Цифровите подписи се използват, за да се удостовери самоличността на подписалия съобщението и, че документът не е подправен (променян, добавян). Цифровите подписи са трудни за подправяне, в идеалния случай цифровият подпис гарантира, че съобщението принадлежи на подписалия го. При цифровите подписи се използват две криптографски техники: криптиране и хеширане. Оригиналото съобщение се криптира със секретния ключ на изпращачия, след това се хешира. Всеки, който има публичния ключ на изпращачия може да се увери, че хеш стойността е на оригиналното съобщение. Последното се отнася за операционни системи, в които са включени като команди на операционната система някои криптографски алгоритми.
 - конфиденциалност – **не**
 - цялостност на данните – да
 - идентификация на изпращача – да
 - доказване на авторство – да

Кодиране с публичен ключ + цифров подпис

- конфиденциалност – да
- цялостност на данните – да
- идентификация на изпращача – да
- доказване на авторство - да

Проблем – гарантиране автентичността на публичния ключ

Комбинацията на цифров подпис и публичен ключ се нарича **сертификат**

- Сертификатът е потвърждение на идентичност дадена от оторизиран сертифицикатор. При искане на цифров идентификатор се проверява самоличността на заявителя.
- Има различни класове идентификатори с различни нива на сигурност.
- В Outlook Express може да се провери дали е валиден сертификатът на подателя.
- Outlook Express поддържа за Европа шифроващите алгоритми: RC2 (40-bit) и DES (56-bit). Може да дешифрира писмо шифрирано с RC2 (64-bit). Като разбъркваш алгоритъм при изпращане на писма ползува SHA-1. Дължината на битовете на секретния ключ е различна, в зависимост от нивото на получения сертификата и методът използван за генериране на ключа.
- Секретните ключове инсталирани с използване на системата от криптографски компоненти на Microsoft не се предават на издаващите сертификата органи и не се съхраняват в държавни агенции. Те са запомнени в съответния компютър и сигурността им се определя от неговата сигурност.

IPSec протокол

- Криптирането на файловете защитава данните, съхранявани на диска, но то не предлага сигурност за данните по време на тяхното пътуване по мрежата.
- IPSec реализира сигурност на данните на нивото на отделния пакет. Тъй като работи в мрежовия слой на референтния OSI модел, приложенията не го забелязват.
- Cisco Systems включва поддръжка на IPSec в своите маршрутизатори, а Windows 2000 включва IPSec в своя TCP/IP стек.

IPSec използва два протокола:

- **Authentication Header (AH)** -Позволява проверка на самоличността на изпращачия IPSec
 - **Encapsulating Security payload (ESP)** – гарантира конфиденциалността на самите данни•Тези два протокола могат да бъдат използвани поотделно или заедно. IPSec може да работи в два режима: транспортен и тунелен. Транспортният режим осигурява *сигурност от край до край*; т.е. криптирането се извършва от компютъра източник до този на местоназначението. Тунелният режим защитава данните от изходната точка на една мрежа до входната точка на друга..

Защитни стени и проксита

- Засилените мерки за сигурност на периметъра е друго важно съображение при създаване на политики на сигурност. *Защитните стени (firewalls)* и *прокситата* могат да бъдат използвани за създаване на бариера между локалната вътрешна мрежа и връзката към външния свят. Тази област може да бъде инсталирана в нейна собствена подмрежа и понякога бива означавана като *демилитаризирана зона (DMZ)* или *прикрита подмрежа (screened subnet)*
- Защитната стена е хардуеър – устройство на защитната стена – например маршрутизатор (router) плюс съответния софтуеър за настройването му – определяне правилата на защитната стена.

Защитните стени изследват определени характеристики на мрежовия трафик и въз основа на определените чрез софтуеъра им правила пропускат или отказват този трафик.

- Защитната стена обикновено се намира на *шлюза {gateway}* на мрежата, който е точката, в която мрежата се свързва към друга мрежа.
- Защитните стени извършват три базови типа филтриране на:
 - пакети
 - вериги
 - приложения
- При *филтрирането на пакети* пакетите от данни се филтрират на базата на информацията в IP, TCP/UDP и ICMP хедърите. При филтрирането на пакети може да разрешите или блокирате конкретни IP адреси или номера на портове.
- *Филтрирането на вериги* е базирано на текущата връзка. Ако даден пакет не е част от установена връзка, той няма да бъде пропуснат през защитната стена.
- *Филтрирането на приложения* филтрира в зависимост от протоколите, използвани за конкретни IP приложения. Например могат да бъдат блокирани само Java аплети или скриптове на Visual Basic

Защитните стени имат способността да изследват следните пакетни характеристики:

- Тип на IP протокол (TCP, UDP, ICMP и т. н.);
- IP адрес и/или порт на източника;
- IP адрес и/или порт на получателя;
- TCP флагове
- Мрежов интерфейс, на който се предават пакетите

Защитните стени могат да бъдат със и без състояния. Защитна стена без състояния анализира всеки пакет поотделно без връзката му с други, пристигнали вече пакети. Когато защитната стена е със състояния тя анализира пакетите в контекста на сесията, част от която са те - т.е. следи за очаквания номер на пакет.

Връзки

Ако постъпи заявка от вътрешен хост за услуга предлагана от външен сървър, стената проверява достъпността на услугата и само, ако сървърът е достъпен създава връзката между вътрешния хост и сървъра.

Приложения

- Защитните стени както и рутерите могат да защитават и на ниво приложение чрез разрешаване или забраняване на порта, на който се изпълнява дадено приложение.

Прокси сървери

- Прокси сървърите работят като „посредници“ в мрежата, като изпълняват функции, подобни на защитни стени. Компютрите във вътрешната мрежа комуникират с проксита, което след това комуникира „от тяхно име“ с компютрите от външната мрежа.
- осигуряват също услуги, като *реверсно прокси* и *реверсно хостване*. Реверсното прокси позволява даден прокси сървър да пренасочва външни HTTP заявки само към една специално предназначена за целта машина. Това осигурява сигурност на достъпа до вътрешен Web сървър, без излагане на сървъра пред външната мрежа. Реверсното хостване позволява на прокси сървъра да пренасочва HTTP заявки към повече от един Web сървър, като асоциира няколко сървъра към един логически адрес. Прокситата осигуряват също кеширане на Web страници за подобряване на производителността в Web.