Тема 7

Мрежова сигурност

Увод

- Организациите разчитат на силата на Интернет не само за продажби на стоки и реклама, но и за комуникация, например с клиенти, партньорски организации или доставчици.
- Този достъп цели лесно разпространение на информация за провеждане на различни бизнес функции, както и да осигури отдалечен достъп до уеб услуги, информационни системи и масиви от данни.
- Независимо дали са малки или големи организациите използват предимствата на свързване на своите информационни системи или в локални мрежи или през Интернет.
- Стимулирана от напредъка в социалните мрежи и мобилните устройства, тази тенденция ще продължи да се засилва и в обозримо бъдеще.

Компютърни мрежи (КМ)

- Колкото и да са мощни съвременните компютри, с каквито и периферни устройства да разполагат, в наши дни все по-често се налага да се ползват огромни обеми данни за обработка или съхранение или нуждата от достъп до устройства, които физически не са непосредствено до КС.
- От друга страна нуждата от обработка на данни със специфичен софтуерен продукт налага тази обработка да става на отдалечена КС.
- Използването на хардуер или софтуер отдалечено дава много предимства като: съкращава разходите - купува се: един лиценз за софтуер, един сървър и множество работни станции със скромни характеристики, един мрежови принтер и др.
- Примерите за употреба са много - централизирани БД, принт сървъри, сториджс, интранет ИС, видео обработка, компилиране, съхранение на документи и мн. др.
- За да се постигне това е необходима специална инфраструктура наречена КМ или просто мрежа.

• • •

- КМ представлява множество от свързани елементи/устройства.
- Всеки елемент на мрежата изпълнява различни функции и съдържа данни или предоставя информационни услуги отговарящи на различните изисквания за сигурност.
- Някои устройства в мрежата съдържат силно чувствителна информация, която може да навреди на една организация, ако се разпространява от неоторизирани лица, например размери на заплати, вътрешни меморандуми, документи за ценова политика, бъдещи бизнес намерения, списъци с клиенти или вътрешни документи за приходи и разходи.
- Други устройства имат по-голяма уязвимост, която се дължи на местоположението им в мрежата. Например, вътрешни файлови сървъри ще бъдат защитени по различен начин от публично достъпните уеб сървъри.
- На други може да се съхраняват резервни копия на данни, ключове за криптиране, софтуер за управление на самата мрежа или администрация на системи и БД.

Какво е мрежова сигурност?

- Защита на мрежовата инфраструктура на една организация от неоторизиран достъп, злоупотреба или друго нежелано действие.
- Изразява се в създаване на сигурна инфраструктура за работа на различни устройства, приложения и потребители.
- Инфраструктурата е съобразена с модела на слоеве за защита на различни нива. На всяко ниво могат да се използват различни технологии, политики и контроли за сигурност, като контрол на достъпа, имейл сигурност, Data loss prevention (DLP), антивирусни приложения, защитни стени, уеб сигурност, сегментиране и др.
- Един от най-важните и полезни контроли е анализ/мониторинг на мрежата за нетипично поведение.
- Отличителна характеристика е автоматизацията.

Типове мрежи

- **Локална мрежа** е вид малка компютърна мрежа, обслужваща група компютри. Представлява група компютри, свързани един с друг с цел споделяне на ресурси, вкл. информация. Свързването може да стане посредством няколко различни конфигурации на топологично и йерархично структуриране. Днес почти всяка организация има собствена локална мрежа.
- **Глобална мрежа** е комуникационна или инфраструктурна мрежа, чиито комуникационни връзки покриват пространство от порядъка на стотици километри. Географски погледнато глобалната мрежа е най-голямата от регионалната, районната, локалната, и персоналната комуникационни мрежи. Най-голямата, а и най-известната за сега глобална мрежа е Интернет.

Типове мрежи

- **Интранет** се нарича вътрешната частна мрежа на една организация (фирма, болница, държавно учреждение, университет и т.н.), защитена от достъп от външни за организацията лица или информационни системи.
- Интранет мрежите се използват за съхранението, категоризирането и приоритизацията на информацията на тази организация, като например политики, правила и процедури, на дейностите във фирмата, вътрешна поща, както и информация за наличности, финанси, продукти и др.
- Тенденция при изграждането на интранет мрежите е използването на доказано функциониращи в Интернет среда протоколи (TCP/IP), софтуер и мрежово-архитектурни решения.

Интранет

- Интранет не трябва да се разглежда, задължително като локална мрежа.
- Интранет може да бъде множество от частни мрежи, които физически се намират понякога на големи разстояния.
- Интранет използва стандартни мрежови хардуерни и софтуерни технологии, като Ethernet, Wi-Fi, TCP / IP, уеб браузъри и уеб сървъри. Интранет на дадена организация обикновено включва достъп до интернет, но е зад защитна стена или прокси сървър, така че компютрите не могат да бъдат достъпвани директно отвън.
- Предимствата са изразяват във високо ниво на защита на информацията и бързината на пренос на данните.

Екстранет

- **Екстранет** е контролирана частна мрежа, която използва Интернет технологиите. Използва обществената телекомуникационна система за безопасно споделяне на част от информацията на организацията.
- Екстранет може да се разглежда като част от Интранета на конкретната компания, но насочен и към потребители извън компанията. Информацията в мрежата може да се управлява и от администраторите и на външните /партньори потребители, но без да се дава достъп до цялата корпоративна мрежа.
- Основните преимущества са, че Екстранет осигурява ниво на сигурност като при Интранет мрежа, но предоставя достъп и на външни за организацията потребители. Информацията в Екстранет може да бъде обновявана, променяна или изтривана много бързо.

Екстранет (прод.)

Фирмите могат да използват екстранет например за:

- Размяна на големи масиви от данни.
- Споделяне на продуктови каталози изключително с търговците на едро.
- Съвместно да разработят и използват програми за обучение с други фирми.
- Осигуряване достъп до услугите, предоставяни от едно дружество на група от други компании, като например онлайн банкиране.
- Споделяне на новини от общ интерес единствено с партньорски фирми.

DMZ (demilitarized zone)

- Понякога се нарича периметър-мрежа и е физическа или логическа подмрежа, която съдържа и предлага за външен достъп услугите на дадена организация към по-голяма и ненадеждна мрежа, обикновено Интернет.
- Целта на DMZ е да се добави допълнителен слой на сигурност на локалната мрежа на дадена организация; външен нападател има директен достъп само до софтуер и хардуер в демилитаризираната зона, и забрана за достъп във всяка друга част на мрежата.
- Името произлиза от термина "демилитаризирана зона", това е площ между две държави, в която не се разрешава военна операция.

Видове заплахи за КМ

- **Man in the Middle Attack (MIM)** Атака се изразява в поставяне в КМ на хакера между клиентска програма и сървър. В тази ситуация(място) той може да прихване комуникацията между клиента и сървъра и да разбере пароли, номера на карти и всякаква информация за клиентски акаунт/профил.

- Обикновено се осъществява като хакера изгражда WiFi hotspots с публичен достъп. Така всеки използващ хотспота и не използващ криптирани връзки/приложения може да бъде прихванат и предаваната информация да бъде прочетена. Ако връзката е криптирана хакера също може да декриптира информацията, чрез един вид от следните атаки: **HTTPS spoofing**, **SSL BEAST**(само за TLS 1.0), **SSL hijacking (SSL stripping)**

- Или хакера да създаде имитиращ сайт например на банкова институция и потребителя реално да достъпва него. Този вид атака е известен като **DNS Poisoning.** Хакера получава достъп до DNS server и така пренасочва трафика.

- **Защита –** основен метод: избягване на използването на отворени публични мрежи

Видове заплахи за КМ (прод.)

- **Denial-of-Service/DDoS (Distributed Denial of Service)**. Атака за отказ на услуга, съкратено DoS attack — DoS атака) е опит даден ресурс, предоставян от компютър (наричан жертва), да бъде направен недостъпен за целевите му потребители. Обикновено жертви на такива атаки стават популярни уеб сървъри, мейл услуги и др., като целта е те да станат недостъпни от Интернет.
- DoS/DDoS атаките биват два основни вида:

➢ Принуждаване на жертвата(чрез твърде много заявки/трафик) да се рестартира или спре, така че вече да не може да предоставя исканата услуга - Buffer overflow attack;

➢ Възпрепятстване на комуникацията между жертвата и потребителите на услугата, така че те вече да не могат да я достъпват адекватно, например чрез прекалено много ICMP Ping заявки вътре в мрежата на жертвата. Тук основната цел е самата мрежа.

➢ **Distributed Denial of Service** се осъществява с помощта на ботнет (мрежа от заразени устройства синхронизирано), докато **Denial-of-Service** от едно устройство.

Denial-of-Service -DDoS (Distributed Denial of Service)

- Щетите от такива атаки, могат да бъдат - от забавяне на достъпа на WEB сайтове, напълно неработещи програми разчитащи на комуникация с други компютри в мрежата до незаконни действия, които остават прикрити и др.
- При този вид атаки не изтриват, променят или крадат файлове от системата, нито се придобива достъп до нея, но въпреки това те могат да са причина за съществени финансови загуби за компании зависещи в голяма степен от присъствието си в Интернет или от наличието на информация в реално време.
- Обикновено са кратки за час или малко повече.

Техники за защита

- Като стандартно решение може да се посочи осигуряването на няколко пъти **повече ресурси**, отколкото са нужни за нормалното функциониране на системата, които ще осигурят работоспособността й дори при атака.
- Защитата на дадена услуга или сървър се състои от три компонента.

1. Първият компонент включва подобряване на общата сигурност, надеждност и производителност на машината. Това е превантивна мярка намаляваща вероятността за успешна атака и евентуалните щети.
2. Вторият компонент включва блокирането(напр. с firewall) на фалшивия трафик първо на входа на мрежата, за да се възстанови нормалната й работа и да не се затрудняват следващите действия. След това фалшивият трафик трябва да се блокира, колкото се може по-далеч от периметъра, за да се изчистят и комуникационните канали и да се възстанови нормалния достъп на потребителите до услугите. Може да се използват и специализирани устройства като **SmartWall®** или уеб услуги като **Nexusguard**
3. Третият компонент е провеждането на задълбочен анализ върху регистрирания фалшив трафик, за да се разбере къде е бил проблемът и да се отстранят причините за успешната атака.

Неоторизиран достъп

- В тази категория мрежови заплахи могат да се обединят заплахи като: изпълнение на команди (вкл. скриптове), преконфигуриране на системите, фалшифициране или изтриване на данни.
- Целта на тези атаки е да се осигури достъп до някои ресурси, които не следва да се предоставят на нападателя.
- Например, достъпа до уеб сървър или защитени секции на него - т.нар. администраторски, от потребител, което прави такова искане за достъп, но не е администратор.

Неоторизирано изпълнение на команди

- Очевидно е нежелателно за неизвестен и ненадежден човек да бъде в състояние да изпълнява команди на сървър.
- Има две основни категории потребители с достъп до сървърите: нормален потребител и администратор.
- Един нормален потребител може да направи няколко неща на система (като четене на файлове, да ги изпрати на други хора и т.н.), докато нападателят не трябва да бъде в състояние да го направи.
- От друга страна обаче, един хакер може да иска да направи промени в конфигурацията на сървъра(може да променя неговия IP адрес, изпълни скрипт при стартиране, за да накара машината да се изключва всеки път, когато е стартирана или нещо подобно). В този случай, нападателят ще трябва да получи администраторски права върху сървъра.

Фалшификация, изтриване на информация

- Друга категория заплахи са свързани с информацията, която се съхранява на системите в една мрежа.
- Целта на нападателя може да бъде фалшификация на някаква информация, например промяна на сума по депозит, резултат от изпит или друго.
- Друга опасност е достъп до класифицирана и лична информация.
- Или заплаха от изтриване на цялата или част от информацията (БД) на даден сървър.

Други атаки

- **IP Spoofing.** IP спуфинг е метод за маскиране на едно устройство като друго. Реализира се, чрез промяна в TCP хедъра на пакетите на изпращащия компютър. IP адресът на изпращащия компютър се подменя с друг IP адрес. По този начин съобщенията от гледна точка на компютъра получател изглеждат така, сякаш са изпратени от компютър с друг IP адрес. IP спуфингът може да бъде използван за **неотозизиран достъп, за кражба на данни и др.**

- **ARP Positioning**. Атаката променя маршрута на мрежовия трафик, така че той да преминава през атакуващата машина. Атакуващата машина изпраща фалшиви (spoofed) ARP (Address Resolution Protocol) пакети към машината жертва и към нейния gateway. Принуждава целия интернет трафик на жертвата да преминава през атакуващия компютър, като **така извлича цялата информация предназначена за жертвата**.

- **TCP kill.** Атаката използва механизма за изграждане на TCP сесии. В резултат от IP спуфинг атака, атакуващият знае TCP sequence номерата (поредните номера на сегментите) на отворена сесия на компютъра-жертва. Той генерира RST (reset) сегмент, с подменен IP адрес и правилен TCP sequence номер, в резултат на което прекратява връзката. Атаката прекратява съществуващите TCP сесии и не позволява отварянето на нови – **прекратява интернет достъпа до машината-жертва**.

Защита от мрежови атаки

- От самото начало трябва да е ясно, че използването само на технологии само по себе си не може да направи една КМ сигурна. Причината е, че в основата на всички технологии за сигурност лежи човешкият фактор.
- Защитата следва да бъде комплексна, като се започне от организационните политики за сигурност, премине се през правила и инструкции и се стигне до специфични мрежови решения.
- За защита на мрежови информационни ресурси се прилагат и специфични методи, като **сегментиране на мрежата, филтриране и блокиране на файлове, URL филтриране и филтриране на съдържание**.
- Други мерки за защита са обучение на потребителите, автентикация и оторизация, криптиране, антивирусна защита и контрол на достъпа.

. . .

- Мрежовата сигурност (МС) задължително трябва да се разглежда и като интегрирана част от цялостната система за сигурност.
- Съсредоточаването само върху МС може да доведе до неглижиране на другите аспекти, които са не по-малко важни. Например много потребители смятат, че инсталирането на една защитна стена и антивирусна програма решава всичките им проблеми, като в същото време си позволяват инсталиране на хакнат софтуер.
- Ако за обикновения потребител в домашни условия това е валидно, то за бизнеса не е.
- Например, ако тази защитна стена е конфигурирана неправилно, тя може да затрудни/да забави работата на системата.
- Друг пример е тукашната (ФМИ) организация на компютърните зали, където не е необходимо да се инсталира антивирусна програма на всяка КС.

Сегментиране на мрежата

- Сегментирането представлява разделяне на мрежата на малки части с цел по-добро представяне и защита.
- Осигурява управление на трафика в различните части. Така в една част може да се спре или ограничи(по някакви критерии) при необходимост, докато в друга работата да продължи.
- Използва се вътрешни защитни стени, Access Control List (ACL) или Virtual Local Area Network (VLAN).
- Предимствата са множество - от подобряване на защитата от хакерски атаки, през по-бърза и надеждна работа на мрежата като цяло до по-голяма удовлетвореност на потребителите на мрежови ресурси.

Филтриране на файлове

- Един доста често използван метод е филтрирането на файлове. По зададени критерии, като име, тип или големина на файла се извършва „пресяване“ на трафика в мрежата.
- Тъй като е известно какви типове файлове са атакувани (изпълними, файлове документи и т.н.) най-често, то този метод е много ефективен.
- Типичен пример е сървърът за електронна поща. Той комуникира с външната среда и е податлив на атаки. Често се получават файлове, които се иска да се стартират, което е сериозен риск. Затова имейл сървърите имат вградени средства за филтриране.
- Разбира се и този подход има някои недостатъци, например, ако потребителите в работата си се налага да си изпращат определени типове файлове, то те не бива да се филтрират. Примери са архивите rar и zip, особено криптираните, с които има затруднения при изпращане по е-поща.

URL филтриране

- URL филтър се използва, за да категоризира сайтове в интернет и да позволява или блокира достъпа до тях на уеб потребителите на организацията.
- Филтрирането се извършва на базата на вече категоризирани адреси в централна база данни, или чрез класифициране на интернет страниците в реално време.
- URL филтриране може да се прилага само през определени периоди от един ден или дни на седмица, ако е необходимо. Например в почивките определени сайтове да са достъпни или пък други само в работно време или др. в зависимост от политиките за сигурност на организацията.
- Пример за такъв инструмент е **WebTitan**

Предимства и недостатъци на URL филтрирането

- Както бе споменато по-рано, URL филтрирането помага на организациите да подобрят производителността, като се уверят, че времето на служителите не се изразходва в ненужни дейности в работно време.
- URL филтрирането също така може да помогне за предотвратяване на разпространяването на злонамерен код / шпионски софтуер, фишинг и други, които могат да бъдат потенциално опасни за организацията. Също помага за блокиране на Peer-to-Peer софтуер и съобщения, които използват повече мрежови ресурси, време и са заплаха за сигурността.
- Недостатъците на метода са главно в нуждата от непрекъсната актуализация на т.нар. черни и бели списъци и увеличаване на натовареността на отдела по IT поддръжка.

Филтриране на съдържание

- При компютърните мрежи, филтриране на съдържанието, е използването на програма за скрининг и отказ от достъп до уеб страници или електронна поща, които се считат за нежелателни.
- Филтриране на съдържанието се използва от корпорации като част от защитната стена.
- Филтриране на съдържанието обикновено работи, чрез определяне на списък от забранителни символни низове, и ако съдържанието на даден сайт съвпада с някой низ от списъка не се показва или се извежда предупредително съобщение.
- Типичен пример е филтриране на порнографско съдържание, на насилие или омраза.
- Инструменти – ContentProtect, Umbrella Everywhere, Secure Web Gateway, Websense Web Filter, SentryPC

Intrusion - проникване

- Intrusion - неоторизирано влизане в съоръжение или система.
- Всяко проникване в система следва да се разглежда като инцидент със сигурността независимо дали има нанесена щета.
- То е показател, че има пропуски.
- Тези пропуски могат да бъдат в различни посоки, от некомпетентен персонал до уязвимост на софтуерен продукт.
- Докато уязвимост на софтуерен продукт може лесно да се отстрани или не допуска с навременно инсталиране на т.нар. патчове, то други пропуски може да са трудни за отстраняване.
- Например погрешно проектирана и разработена информационна система, използване на остарели технологии, доказано несигурни и др. (пример – ученикът от Пловдив проникнал в инф. система на МОН, същият обвинен за проникване на сървър на НАП от 2019 г.)

Intrusion Prevention System (IPS)

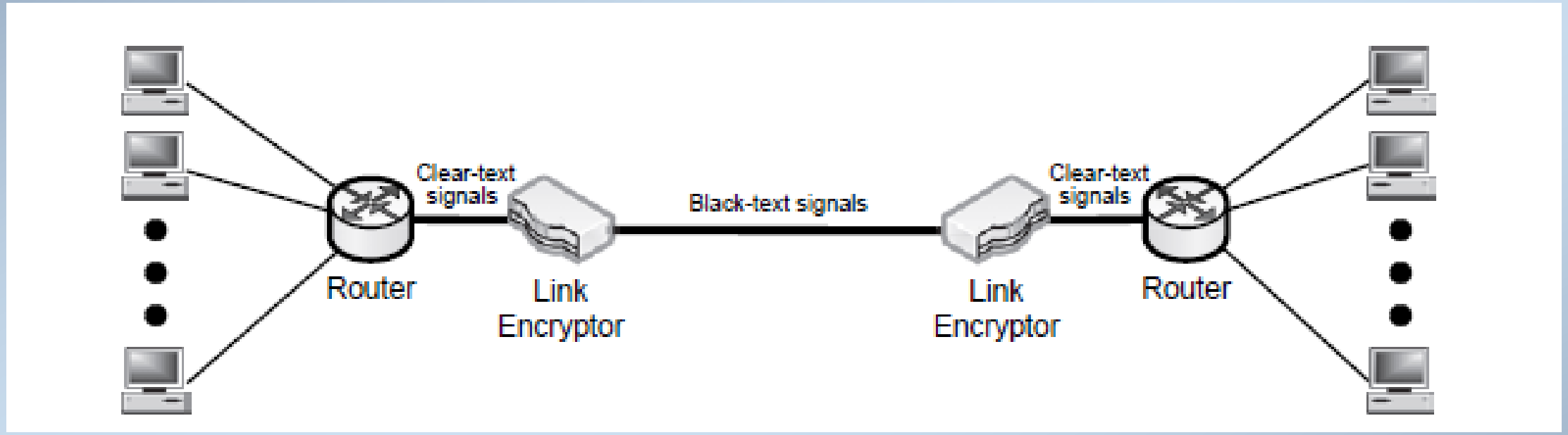
- Система за предотвратяване на проникване (IPS) е технология за превенция и мрежова сигурност, която проучва мрежовия трафик за откриване и предотвратяване на уязвимости в системите в цялата мрежа. Може да бъде реализирана като устройство или софтуер.
- Заплахите обикновено идват под формата на зловреден ресурс за целево приложение или услуга, която нападателите използват, за да се прекъсне и да поеме контрола над машината.
- След успешното атакуване, нападателят може да забрани стартиране на услугата/приложението цел (резултатът е състояние на отказ от услуга), или може потенциално да получи достъп до всички системи в мрежата с всички права и разрешения.
- Системата следи за подозрителна активност, регистрира я, прави опит да блокира тази активност и изпраща предупреждение до администратора.
- Примери: McAfee NSP, Trend Micro TippingPoint, Hillstone NIPS, Huawei NIP, Cisco Firepower NGIPS и др.

Intrusion Detection System (IDS)

- Ако IPS системата е инструмент за контрол, то системата за откриване на проникване (IDS) е инструмент за наблюдение/видимост.
- Може да бъде реализирана като устройство или софтуер.
- IDS се използва само за следене на трафика, тази система не предприема активни действия само се известява администратора.
- Това е инструмент, който се ползва от мрежовия администратор с цел да има възможност за задълбочен преглед на мрежата и да види какво се случва в нея, понякога с много големи детайли. IDS е „анализатор“ за инженера/администратора по сигурността.
- Чрез системата за откриване на проникване (IDS) се следи дълбоко навътре в мрежата и се вижда какво се случва там от гледна точка на сигурността.
- Примери: SolarWinds Security Event Manager , Snort на Cisco Systems, OSSEC и др.

Защита на физическо ниво

- За някои организации заплахите по отношение на информационните ресурси могат да бъдат фатални. Такива са правителствените и военните.
- В такава ситуация се прилага метода на криптиране на информацията по самия канал за връзка (оптични или метални връзки) със специално устройства (link encryptors).
- Тези криптиращи устройства напълно криптират всички цифрови сигнали, сигналите са модулирани по трасето и криптираните сигнали пътуват между две мрежови устройства.
- Примери: Datacryptor (Thales e-Security), Fibre Channel encryptors(SafeNet) и Centauris (ID Quantique)


Clear-text signals
Black-text signals
Clear-text signals
Router
Link Encryptor
Link Encryptor
Router

IP Security (транспортно ниво)

- IPsec (Internet Protocol Security) е пакет от протоколи за осигуряване на защитена Интернет протокол (IP) комуникация, чрез установяване автентичността и криптиране на всеки IP пакет на една комуникационна сесия. Може да се прилага за отделно приложение и за няколко мрежи едновременно.
- IPsec използва криптографски услуги за защита на комуникации през компютърни мрежи. IPsec поддържа: партньорска идентификация на мрежово ниво, удостоверяване произхода на данните, целостта на данните и поверителност на данните (криптиране).
- IPsec използва следните протоколи: Authentication Headers (AH), Encapsulating Security Payloads (ESP) и Security Associations (SA) чрез Internet Security Association and Key Management Protocol (ISAKMP)
- Реализира се като услуга в операционните системи или мрежови устройства.
- IPsec се използва за изграждане на VPN.

Заключение

- Мрежовата сигурност в наши дни вероятно е най-важният аспект от множеството засягащи информационната сигурност.
- Използването на множество свързани устройства и мрежови услуги, вкл. Интернет предполага и повишен интерес от страна на хакерите.
- Ограничаването или прекъсването на определени услуги може да бъде и критично - припомнете си сривът за около 14 дни в Търговския регистър през 2018, когато съмненията стигнаха и до проблеми в мрежата, а не само в дисковете.

Практически упражнения

- В рамките на един учебен час потърсете в Интернет пространството информация за разглежданите в темата понятия, дефиниции и аспекти. Търсенето може да направите и на чужди езици, които владеете.
- Анализирайте намерената информация и я сравнете с поднесената тук.
- Проучете домашната си мрежа – рутер и устройства за правилни настройки за сигурност.