Механика Транспорт Комуникации

Научно списание

ISSN 1312-3823

брой 3, 2008 г.

статия № 0312

http://www.mtc-aj.com

ПРОБЛЕМЪТ ЗА СИГУРНОСТТА И ЗАЩИТАТА НА ИНФОРМАЦИОННИТЕ СИСТЕМИ

Маргарита ПЕЛТЕКОВА

mpeltekova@hotmail.com

гл. ас. Маргарита Пелтекова, Висше Транспортно Училище "Тодор Каблешков", София,

БЪЛГАРИЯ

Резюме: *В доклада се разглеждат механизмите за защита на информацията в съвременните компютърни информационни системи. Направен е кратък обзор на механизмите за защита в кабелните и безжични компютърни информационни системи. Разгледана е компютърна информационна система с видеонаблюдение, реализирана в една от лабораториите на катедра СОТС на Висшето Транспортно Училище "Тодор Каблешков", София.*

Ключови думи: *информационни системи, защита на информацията сигурност на информацията, конфиденциалност, интегритет.*

ВЪВЕДЕНИЕ

Информационната сигурност и защитата на данни е едно от най важните изисквания към съвременните информационни системи. Защитата на информация и материални ценности е скъпа, но последствията и цената, която ще струва ако се пренебрегне са непредвидими.

Широкото използване на Интернет и характерните за процеса хакерство, вируси, спам на електронната поща, DoS атаки и т.н. заостриха вниманието към защитата на информационните системи и мрежи. На практика се изменя същността на атаките и риска от тях, в резултат на което възниква необходимостта от нови решения за сигурност и нови стандарти (и на базата на съществуващите). Изискванията към тях са за конфиденциалност, интегритет и наличност на данните, автентификация и non-repudation (не отричане).

Управлението на информационната сигурност се характеризира с три основни аспекта: конфиденциалност, интегритет и достъпност

Петте изисквания, на които трябва да отговарят системите за сигурност, заложени в Open Standard Interconnection (OSI) модела (ISO 7498-2), са:

1.Автентификация (Authentication) - предпазва системата от достъп на неоторизирани потребители - AAA, RADIUS, Digital Certificates, Xauth (Extended authentication), etc.

2.Контрол на достъпа (Availability) - осигурява достъп до информация на хора които имат право на достъп - IPsec, Remote Dual Tunnel.

3.Конфиденциалност на данните (Confidentiality) - достъп до информацията имат само оторизирани лица.

4.Интегритет на данните (Integrity) - критерии, който показва до каква степен информацията правилно се записва, съхранява, обработва и пренася. Интегритетът реализира защита от повреда или измама с данните.

5.Non-repudation - получателят и изпращачът не могат да се отрекат от данните.

Посочените изисквания се реализират чрез богато разнообразие от апаратни и софтуерни средства – между мрежови устройства (маршрутизатори), защитни стени, антивирусни програми и протоколи за защита

на данните функциониращи на различни нива на OSI (Open Systems Interconnection Basic Reference Model) стандарта (фиг. 1).

Application (PGP, HTTPs)
Transport (TLS, SSL)
Network (IPSec)
Data link (PPP, PPTP, L2TP)
Physical

фиг. 1. - Open Systems Interconnection Basic Reference Model (OSI)

2. ИЗГРАЖДАНЕ НА СИГУРНА ИНФОРМАЦИОННА СИСТЕМА

Създаване на отказоустойчиви информационни системи, изисква:

1. Защита на достъпа до данните и приложенията чрез различни технологии и механизми, както апаратни така и софтуерни, между които най-популярните са: firewall продукти, криптографски технологии, внедряване на решения за антивирусна защита и на средства за откриване и засичане на неоторизиран достъп.

2. Физически контрол на достъпа до информационните ресурси, който включва охрана, средства за идентификация, системи за видеоконтрол и наблюдение.

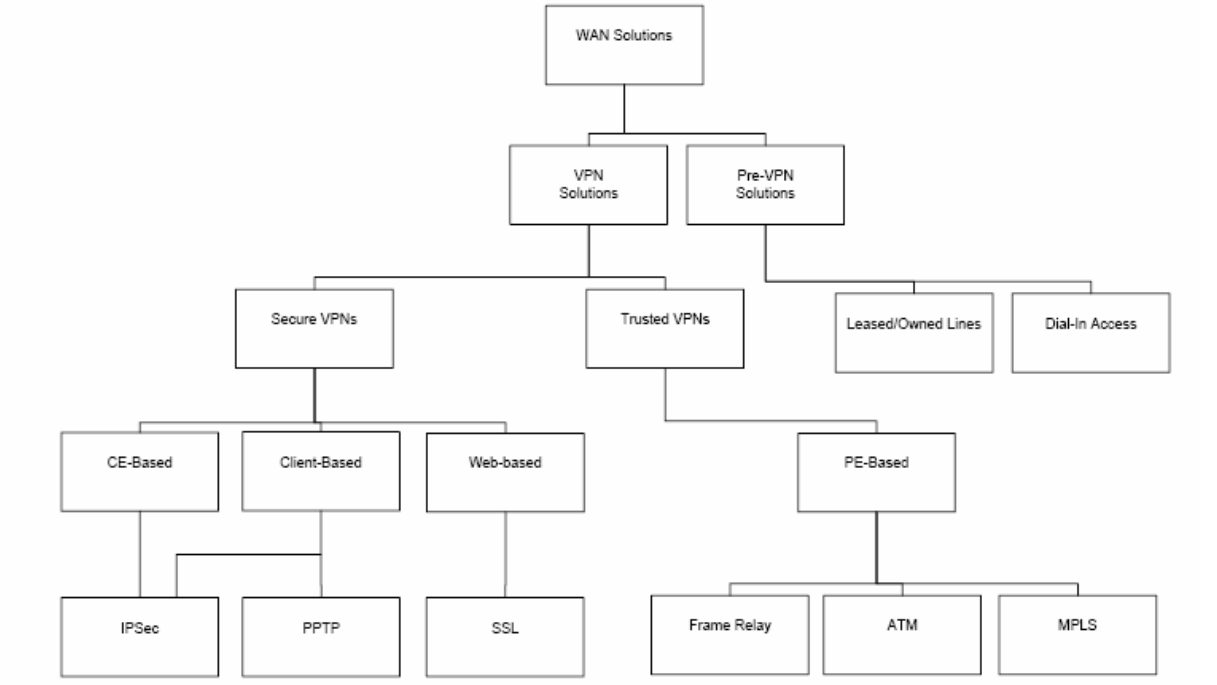
Най често използваните механизми за защита са: Firewall, Network Address Translation (NAT, Stateful Packet Inspection (SPI) Firewall, Virtual LAN и Virtual Private Network (VPN).

Network Address Translation (NAT) технологията скрива адресите на устройствата, зад маршрутизатор.

Stateful Packet Inspection (SPI) Firewall – инспектира пакетите от данни влизащи в мрежата, за да провери техният произход. Тази функция се изпълнява от SPI маршрутизатор, който отхвърля пакетите с непознат произход.

Virtual LAN технологията разделя локалната мрежа на няколко отделни логически подмрежи, всяка от които имат различни мрежови адреси. Устройствата ат едиа и съща логическа подмрежа могат да комуникират директно, докато устройствата от различни подмрежи комуникират през устройство от 3-ти слой на Open Standard Interconnection (OSI) стандарта.

Фиг. 2 Видове Виртуални частни мрежи



Virtual Private Network (VPN) технологията (фиг. 2), позволява комуникация през Internet чрез защитена, криптирана връзка. Тази технология се използва за изграждане на отдалечена защитена връзка (тунел) между частна мрежа и компютър/мрежа, разположени на разстояние и ползващи взаимно ресурсите си (фиг. 3).

Виртуалните частни мрежи (VPN) изграждат т.н. тунел между източника и получателя на информацията - логическа връзка от типа точка-точка, реализираща автентикация и криптиране на данните при предаването им от едното крайно устройство на тунела до другото. Виртуалните частни мрежи използват протоколите IPSec (Internet Protocol Security) и SSL (Secure sockets layer)/ TLS (Transport Layer Security).

IPSec - протокол за сигурност на мрежовия слой, чиято цел е осигуряване на криптографски услуги за сигурност. Той дефинира рамката от спецификации, чието ядро се базира на Authentication Header (AH), IP Encapsulating Security Payload (ESP), Internet Key Exchange (IKE).

AH верифицира идентичността на изпращача на пакета и автентичността на съдържанието на пакета.

ESP криптира пакета преди да го изпрати.

IKE управлява трансфера на ключове между изпращача и получателя. Намира приложение при виртуалните частни мрежи;

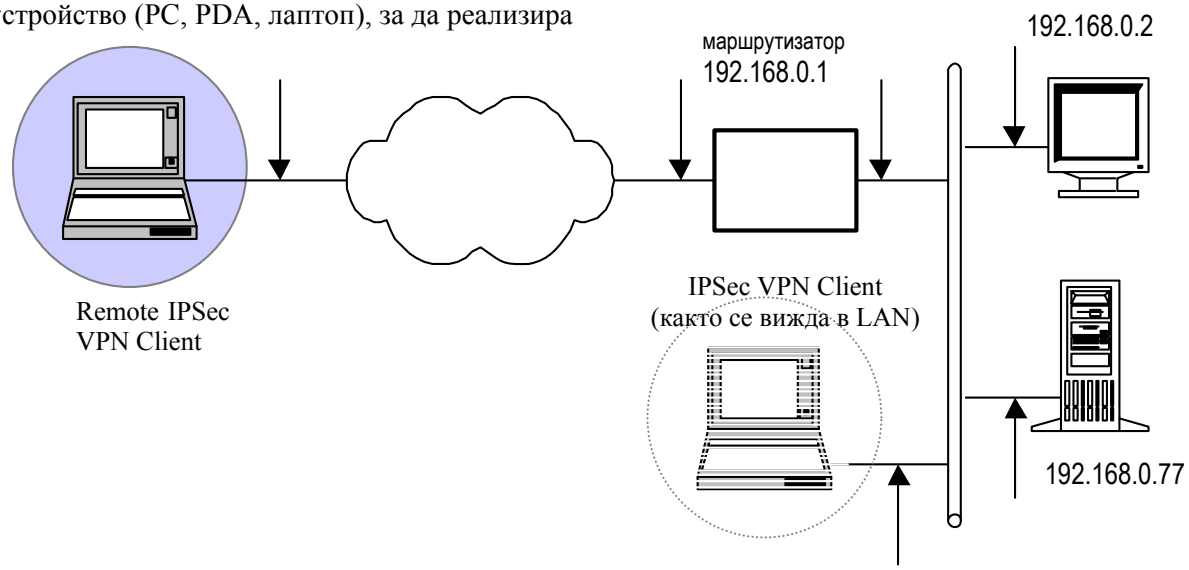
Протоколът IPsec изисква инсталиране на "IPsec client" софтуер на всяко отдалечено устройство (PC, PDA, лаптоп), за да реализира криптиране на данните по тунела.

SSL – протокол за сигурност на сесийния слой, предоставящ множество криптографски алгоритми за защина на данните. По подразбиране HTTP използва Transmission Control Protocol (TCP) port 80, докато SSL (HTTPS) използва TCP port 443.

TLS (Transport Layer Security) протоколът е дефиниран в RFC 2246. Позволява на клиент/сървър приложенията да комуникират по сигурен и защитен начин. Състои се от два слоя - TLS Record Protocol и TLS Handshake Protocol. Първият взема съобщенията, които трябва да се изпратят, фрагментира данните в управляеми блокове, компресира данните, прилага Hashed message Authentication, криптира и изпраща резултата. Получените данни се декриптират, верифицират, декомпресират, реасемблират и доставят на клиентите от по-високия слой. Вторият се състои от набор от три подпротокола, проектирани да позволят на страните да се споразумеят за параметрите на сигурността на съответния слой.

TLS ще замести използваният в повечето браузъри SSL.

Когато се осигурява защита на данни предавани по безжична връзка, се прилагат различни схеми на криптиране на данните, които зависят от безжичните междумрежови устройства, които се използват. Wired Equivalent Privacy или Wireless Encryption Protocol (WEP) протокола за безжична връзка, реализира криптиране на данните на физическия и канален слой на OSI модела.



Фиг. 3. Виртуална частна връзка

Стандарта WEP е част от стандарта IEEE 802.11x, който предоставя спецификации за безжични локални мрежи (WLAN). Протоколът не предлага пълна защита на връзката. Основната слабост на WEP е, че този протокол използва статични криптиращи алгоритми (ключове).

Тази слабост на WEP протокола се преодолява в подобрената версия на

протокола за безжична връзка - Wi-Fi Protected Access (WPA).

За да използват възможностите на WPA, всички устройства в мрежата, трябва да се конфигурират за WPA криптиране. Стандартът WPA има две подобрения спрямо WEP:

- Използва динамични криптиращи ключове реализирани чрез TKIP (Temporal Key Integrity Protocol) протокола. Протоколът TKIP променя динамично криптиращите ключове чрез т.н. "hashing" алгоритъм, като добавя проверка на цялостта (integrity-check), за да предотврати нежелана промяна на криптиращия ключ. Друга реализация на WPA ползвува Extensible Authentication Protocol (EAP). Този протокол се използва при създаване на защитена корпоративна връзка и изисква RADIUS (Remote Authentication Dial-In User Service) сървър.
- Реализира автентификация на потребителите (User authentication), която липсва при WEP стандарта, чрез протокола EAP (extensible authentication protocol). WEP регулира достъпа до безжичната мрежа в зависимост от MAC адресите, които лесно могат да бъдат променени, докато EAP е изграден на базата на по-защитена PKE (public-key encryption system) и осигурява достъпа до мрежата само на ауторизирани потребители на мрежата.

Правилно конфигуриран, WPA предлага несравнимо по-добра защита от WEP, но все пак не може да се твърди, че защитата на WPA е "желязна", тъй като нека се запитаме, каква форма на защита реализира протокола?

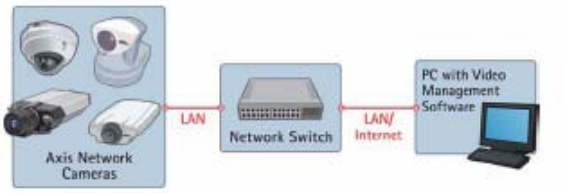
Дори да отменим SSID, да филтрираме MAC адресите и да въведем WPA пасфраза (passphrase) толкова дълга колкото е възможно, остава проблем, свързан с физическата защита на устройствата свързани в информационната мрежа, който трябва да бъде решен по друг начин.

Стандартът WPA2 е втора генерация (подобрена версия) на WPA, напълно съвместим с него. Основната разлика между WPA и WPA2, е че WPA2 изисква Advanced Encryption Standard (AES) стандарта, за да криптира данните, докато WPA използва TKIP. Стандартът AES предоставя достатъчна защита, за да покрие високите изисквания на всяка правителствена или частна организация. Канто оригиналният WPA, така и WPA2 поддържат както частна и корпоративна версия. Стандартът WPA2 е строго препоръчителен, ако и маршрутизатора и лаптопа/PC, свързан към него, поддържат този мощен механизъм за защита.

2. СИГУРНОСТ НА ИНФОРМАЦИОННА СИСТЕМА ЗА КОНТРОЛ НА ДОСТЪПА

Физическият контрол на достъпа до информационните ресурси се реализира чрез: охрана, видеоконтрол, средства за идентификация на входа на сградата, в която е разположена информационната система, в компютърната зала и/или при самите устройства, изграждащи информационната система.

Преди да се пристъпи към избор на решения за сигурност обаче задължително трябва да се разработи политиката за сигурност. Това е документ, който дефинира как една организация планира своята физическа и логическа сигурност, по-точно как планира да защити своите информационни системи и мрежи.



Фиг. 4. Информационна система с видеонаблюдение

Една от най-скъпите мерки е възстановяване на инфраструктурата след аварии. Ключово значение в случая има оценката на риска и изборът на подходяща схема за резервиране на основните модули.

На фиг. 4 е дадена схемата на информационна система с видеонаблюдение, проектирана за една от лабораториите на катедра СОТС. Системата е реализирана с AXIS мрежови ведеокамери. Връзката към междумрежовото устройство се реализира чрез стандарта RJ45. Камерите автоматично определят скоростта на локалната мрежа (10BaseT/100BaseTX Ethernet). За да се предотврати нежелан достъп до камерите се

въвеждат пароли за достъп за оторизирани потребители, а за останалите присъствието на камерите в мрежата би могло да е невидимо.

3. ЗАКЛЮЧЕНИЕ.

За да се гарантира защита на данните в съвременните информационни системи е необходимо да се използват динамични криптиращи алгоритми, които реализират изискванията за интегритет и конфиденцалност на информацията. За достигане на по-висока степен на защита на информацията е необходимо комбинирането на симетрични и асиметрични криптомеханизми, съчетани със система за видеоконтрол на устройтвата и помещенията, където е разположена информационната система.

ЛИТЕРАТУРА:

[1] сп. Информационна сигурност
[2] www.cisco.com
[3] www.linksys.com
[4] www.axis.com

.

SAFETY AND SECURITY AS AN ISSUE IN INFORMATION SYSTEMS

Margarita PELTEKOVA

"Todor Kableshkov" Higher School of Transport, Sofia, str. Geo Milev. 158,
BULGARIA

***Abstract**: Computer networks are utilized for sharing services and resources. Information travelling across a shared IP-based network, such as the Internet, could be exposed to many devious acts such as eavesdropping, forgery and manipulation. Fortunately, there are several mechanisms that can protect any information that needs to be sent over a network. This paper introduces security threats to today's IP-based networks and explains available security mechanisms to effectively prevent such threats from happening.*

***Key words**: Computer networks, security mechanisms, confidentiality, integrity.*