FRI-216-2-NMTS(S)-03

NETWORK SECURITY PROTOCOLS

Viktorija Rashkova
Principal Assist. Prof. PhD
Department Computer science
University of Ruse "Angel Kanchev", phone: 082-888 412
e-mail: vkr@ami.uni-ruse.bg

Abstract: With the development of information technology the need for network security increases. Network security must be planned before the network construction. The choice of security tools depends on the field of business activity; by its size; the risk of an attacks; invested funds and etc. This paper presents the basic network security protocols.

Key words: network security, security protocol, authentication, data integrity, access control.

ПРОТОКОЛИ ЗА МРЕЖОВА ЗАЩИТА

Резюме: С развитието на информационните технологии нараства необходимостта от увеличаване сигурността на мрежата. Мрежовата сигурност трябва да бъде планирана преди самото изграждане на мрежата.

Ключови думи: мрежова защита, протоколи за мрежова защита, контрол на достъп

ВЪВЕДЕНИЕ

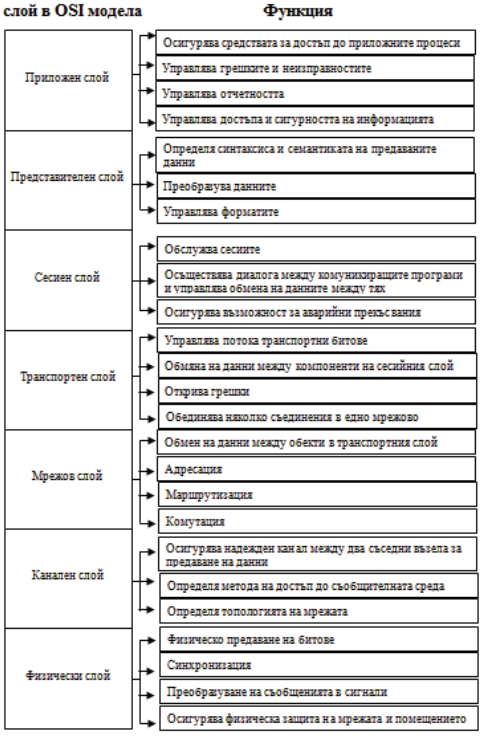
Мрежовата сигурност е сериозен проблем в света на информационните технологии [3]. Този проблем се засилва още повече от факта, че днес почти всеки потребител използва услугите на Интернет. Достъпът до Интернет прави всяка LAN и WAN мрежа още по-уязвима от редица мрежови атаки от страна на злонамерени потребители. Сигурността в мрежата трябва да включва защита както на физическата мрежа, като например средства за физическо ограничаване на достъпа до помещението (сградата), така и средства за защита на локалния достъп до компютрите в мрежата; защита от използването на различни подслушващи устройства на канала за достъп; защита от неоторизиран достъп чрез атакуване на различни слабости от използваните мрежови протоколи на различните слоеве от използвания стандартизиран модел; защита от вируси и др. [6]. Средствата за мрежова защита е необходимо да бъдат планирани още преди физическото изграждане на самата мрежа [13]. Важно е да се дефинира желаната сигурност, отговаряйки си на въпроси, като: за каква дейност ще се използва мрежата; какъв ще бъде типът на данните, които ще съхраняваме в мрежата; как ще организираме управлението на мрежата; какво бъдещо развитие на мрежата се планира, за да се определи и правилната мрежова топология; какви реални заплахи от несанкциониран достъп съществуват; каква политика на мрежова сигурност ще бъде използвана и др.

Защитата се приема за достатъчно сигурна, ако за нейното преодоляване са необходими по-големи разходи, отколкото би била очакваната изгода от несанкционирания достъп.

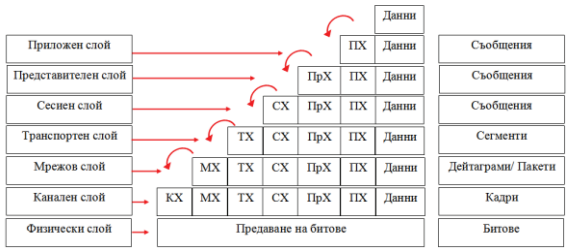
ПРЕНОС НА ДАННИТЕ ПО МРЕЖАТА И УСЛУГИ ЗА СИГУРНОСТ

В периода 1977-1984г. международната организация по стандарта ***ISO (International Standards Organization)*** създава мрежовия модел ***OSI (Open System Interconnection)***. Целта на този модел е унифициране на правилата за комуникация в мрежата. Моделът дефинира мрежова рамка за изпълнение на протоколи в седем слоя (нива). Слоевете, започвайки от долу нагоре са: физически, канален, мрежов, транспортен, сесиен, представителен и приложен слоеве. Всеки слой изпълнява определени функции, представени на Фиг.1.

Всеки слой от OSI модела комуникира със своите съседни слоеве, т.е. със слоя който е над и под него. Предаването на данните се извършва в посока от горе надолу (от приложния към физическия слой), като данните от по-горен слой се записват в хедъра на протоколите от по-долен слой [5]. Този процес е показан на Фиг. 2.



Фиг. 1. Функции на седемте слоя от OSI модела



Фиг. 2. Протоколни единици за данни

Означенията ПХ, ПрХ, СХ, ТХ, МХ и КХ са съответно за хедърите на приложно, представително, сесийно, транспортно, мрежово и канално ниво. Когато данните достигнат следващата работна станция в мрежата и започне получаване на данните, започва обхождане в обратен ред [6], [9].

Стандартът ISO определя пет базови услуги за сигурност, които са: автентификация; управление на достъпа; конфиденциалност на данните; цялостност на данните и съпричастност. В Таблица 1 са показани поддържаните услуги за сигурност на отделните слоеве в OSI модела, като при поддържането на дадена услуга тя се означава със символа „+", а при отсъствието с „-".

Таблица 1. Поддържани услуги на сигурност на различните слоеве в OSI модела

Услуги на сигурност	Слой от OSI модела						
	Физически слой	Канален слой	Мрежов слой	Транспортен слой	Сесиен слой	Представителен слой	Приложен слой
Автентификация	-	-	+	+	-	-	+
Управление на достъпа	-	-	+	+	-	-	+
Конфиденциалност на съединение	+	+	+	+	-	+	+
Конфиденциалност извън съединение	-	+	+	+	-	+	+
Избирателна конфиденциалност	-	-	-	-	-	+	+
Конфиденциалност на трафика	+	-	+	-	-	-	+
Цялостност с възстановяване	-	-	-	+	-	-	+
Цялостност без възстановяване	-	-	+	+	-	-	+
Избирателна цялостност	-	-	-	-	-	-	+
Цялостност извън съединението	-	-	+	+	-	-	+
Съпричастност	-	-	-	-	-	-	+

След създаването на Arpanet през 1974 г. се налага замяната на OSI модела с четирислойния TCP/ IP мрежови модел. TCP/IP моделът обхваща всички 7 слоя от OSI модела, но обединява някои от тях. Структурата на TCP/IP модела е показана на Фиг. 3.

ОСНОВНИ ПРОТОКОЛИ ЗА МРЕЖОВА ЗАЩИТА

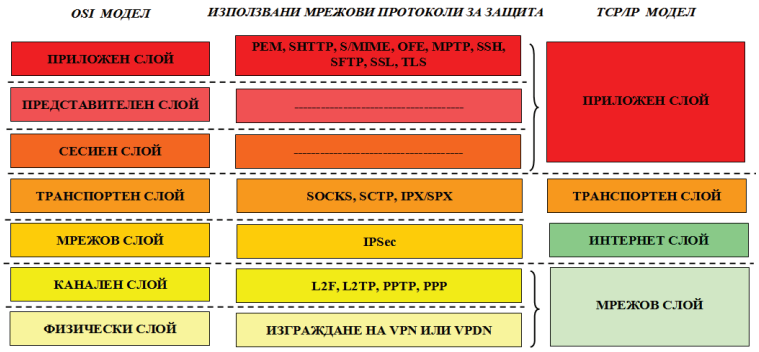
Както вече споменахме TCP/IP моделът съдържа 4 слоя, които обхващат всички 7 слоя от OSI модела. За реализирането на определените функции се използват редица протоколи, като по-долу са посочени основните протоколи за мрежова защита. Те са:

PEM (Privacy Enhanced Mail) е протокол за сигурност, разработен от IETF (Internet Таск Force Engineering). Той осигурява конфиденциалност на електронните съобщения в Интернет [1]. Целта му е да създаде стандарт, който може да се реализира на всеки хост и да бъде съвместим със съществуващите е-майл доставчици. Протоколът изплозва DES и RSA криптографски алгоритми за криптиране на данните, управление на ключове и цифрови подписи.

- **S-HTTP (Secure Hyper Text Transfer Protocol)** е протокол за сигурност, предназначен да осигури поверителност от край до край, както и цялостност и автентичност за HTTP клиенти и сървъри. Той първоначално е бил разработен от Enterprise Integration Technologies (сега VeriFone, Inc.) през 1995 г. [1]. Протоколът се основава на протокола HTTP, но включва възможност за: поддръжка на MOSS и CMS; синтактична съвместимост; рекурсивна защита и независими алгоритми.
- **SET (Secure Electronic Transaction)** е протокол за сигурност, разработен съвместно от Visa и MasterCard. Той е създаден, за да осигури сигурно плащане на транзакции с кредитни карти над отворени мрежи. SET е електронен еквивалент на транзакция с кредитна карта [1]. SET изисква две двойки асиметрични криптиращи ключове и два цифрови сертификата - един за обмен на информация и друг за цифрови подписи.
- **S/MIME (Secure/Multipurpose Internet Mail Extensions)** първоначално е проектиран от RSA Data Security, S/MIME спецификацията и понастоящем се управлява от IETF S/MIME Working Group [1]. Използва се за надеждно изпращане на електронни съобщения.
- **TLS (Transport Layer Security) /SSL (Secure Socket Layer)-** Протоколът SSL е предшественик на протокола TLS. И двата протокола са криптографски и са проектирани да осигуряват сигурност на комуникациите през компютърна мрежа [1], [2]. За повече от 10 години протоколът SSL се наложи, като може би най-широко използвания протокол, за осъществяване на криптирана връзка между клиент и уеб сървър в Интернет [4]. SSL може да бъде имплементиран в почти всяка операционна система, която поддържа TCP/IP протокол, без да е необходима специална конфигурация на ядрото на системата или TCP/IP стека. Това обстоятелство дава на SSL голямо предимство пред други протоколи като IPSec (IP Security Protocol) например. Протоколът SSL използва публичен ключ за криптиране с X.509 сертификат и симетрични алгоритми за криптиране. Текущата версия на протокола поддържа криптографски алгоритми като: DES, RC2, RC4, IDEA, RSA, SHA, MD5 и др.
- **OFE (Open Financial Exchange)** е създаден от CheckFree, Intuit и Microsoft в подкрепа на широк кръг от потребители за банкиране в малкия бизнес по Интернет [1]. Протоколът е отворена спецификация, достъпна за всяка финансова институция или продавач. Той използва SSL сертификат.
- **MPTP (Micro Payment Transfer Protocol)** е част от World Wide Web Consortium (W3C) [1]. В момента, MPTP е W3C работен проект. Спецификацията се основава на вариации на Rivest и Shamir Pay-Word, Digital's Millicent, and Bellare's iKP. MPTP е много гъвкав протокол, който може да надгражда HTTP или MIME за предоставяне по-широк обхват на операциите. Той е високоустойчив на закъснения в предаването, което позволява голяма част от обработката на сделката да се осъществи онлайн.
- **IPSec (IP Security)** е протокол за IP сигурност и представлява фамилия от отворени стандарти, които гарантират сигурни частни комуникации през Интернет [7]. IPSec осигурява конфиденциалност, цялостност и достоверност на данните при преминаването им

през обществените мрежи. IPSec осигурява криптиране и автентикация на мрежово ниво. IPSec добавя допълнителни услуги, липсващи в IP, като например: криптиране на трафика; цялост на данните и удостоверяване между участващите страни. Тези услуги се осъществяват чрез следните протоколи, от които се състои IPSec: AH (Authentication Header); ESP (Encapsulating Security Payload); IKE (Internet Key Exchange); PKI (Public Key Infrastructure).

- **PPP (Point to point)** е протокол, който се използва за изпращане на дейтаграми през серийна връзка. Освен това, той е създаден за преодоляване на някои от недостатъците на протокола SLIP [14]. Протоколът PPP притежава множество възможности, като за всяка от тях има отделен протокол [10], като например: PPP PAP (Password Authentication Protocol); PPP CHAP (Challenge Handshake Authentication Protocol); PPP EAP (Extensible Authentication Protocol) (канално ниво); PPPoE (Point to Point protocol Over Ethernet).
- **PPTP (Point to Point Tunneling Protocol)** се използва за изграждане на WANs. Протоколът е изграден на основата на протокола PPP и осигурява капсулирането и маршрутизацията на мрежовия трафик през несигурна обществена мрежа, каквато е Интернет [4].
- **L2F (Layer 2 Forwarding)** е технология, която е разработена през 1996 от Cisco Systems и включва техния софтуер IOS. Като алтернатива на PPTP, L2F има възможност да използва ATM и Frame Relay протоколи за тунелиране. За разлика от PPTP, който изисква IP, за да работи L2F не изисква. L2F осигурява автентикация на крайните точки на тунела.
- **L2TP (Layer 2 Tunneling Protocol)** е резултат от сътрудничеството на Microsoft и Cisco. Той е комбинация от възможностите на PPTP и L2F.
- **SSH (Secure Shell)** е протокол за криптирано предаване на данни и се използва най-често за достъп и изпълнение на команди на отдалечена машина като предоставя високо ниво на сигурност по време на комуникация между машините [4]. Протоколът се използва и за предпазване от редица атаки като: DNS spoofing, Троянски кон, Man in the middle attack и др. [11].
- **SFTP (SSH File Transfer Protocol)** се използва за трансфер на файлове чрез SSH протокола [11]. Този протокол е бинарен, т.е. всички команди и заявки се пакетират в бинарни съобщения, които се изпращат към сървъра. Отговорите от сървъра се предават отново на пакети в бинарен вид [4].
- **SOCKS (Socket Security)** е VPN протокол [4]. Той позволява на мрежовите администратори да ограничават VPN трафика на определени програми. Протоколът е подходящ за използване от Unix/Linux ОС, но не е известен сред по-популярните настолни системи.
- **IPX/SPX (Internetwork Packet eXchange/Sequenced Packet eXchange) –** протоколът IPX работи заедно със SPX, за да осигури маршрутизируеми мрежови комуникации. IPX/SPX е разработен от Novell за техните NetWare сървъри и клиенти, но тези протоколи могат да се използват и с друг операционни системи (като Microsoft Windows). При IPX/SPX конфигурирането е по-лесно и производителността е по-висока в сравнение с TCP/IP. IPX/SPX понякога се използва за вътрешни LAN комуникации като част от план за сигурност [12].
- **SCTP (Stream Control Transmission Protocol)** е стандартизиран надежден транспортен протокол, предоставящ многопотоково предаване на данни [8]. В рамките на една SCTP сесия могат да се предават независими HTTP отговори [2].



Фиг. 3. Често използвани протоколи за защита на мрежата

Други средства за мрежова защита са: изграждане на VPN или VPDN; контрол на достъпа; използване на програми за защита на електронната поща; използване на защитни стени и проксита и др. [7].

ЗАКЛЮЧЕНИЕ

Все пак е важно да се знае, че няма напълно защитена мрежа. Винаги съществува опасност от пробив в сигурността. Въпреки това всеки мрежови администратор се стреми да осигури максимална вътрешна и външна защита на мрежата, тъй като рисковете от мрежови атаки са големи. Необходимо е да се използват средства за IT сигурност, които помагат да се намали уязвимостта на мрежата [6]. Добра практика е мрежите да бъдат сегментирани, за да осигурят разпределение на отговорността.

ЛИТЕРАТУРА

[1] Bill Stackpole, Data security management. Application layer security protocols for networks, 1999.

[2] Holly Lynne McKinley, SANS Institute InfoSec reading room, SSL and TLS: A beginner's guide, http://www.sans.org/reading-room/whitepapers/protocols/ssl-tls-beginners-guide-1029.

[3] Александър Милев, Борислав Найденов, Администриране на мрежи, 2010.

[4] Атанас Василев, Атанас Ладжов, Росен Русев, Сигурен отдалечен достъп, СУ „Св. Климент Охридски" http://www.iseca.org/downloads/2004_2005-1/papers/43599_43695_43697_RAS.pdf.

[5] Генчо Стоицов, Компютърни мрежи и комуникации, Пловдивски университет „Паисий Хилендарски", 2013.

[6] Ирена Иванова Николова, Стефан Димитров, Методи и средства за защита при мрежови комуникации, Софийски университет „Св. Климент Охридски", 2007, https://research.uni-sofia.bg/bitstream/10506/199/1/diplomna_rabota_Irena_Nikolova_fnM21870.pdf.

[7] Румен Дончев, Политика за мрежова сигурност, Списание Professional, брой 7, http://profisec.bg/bg/490/politika-za-mrezhova-sigurnost-4/.

[8] Христо Вълчанов, Иван Русев, TCP/SCTP web прокси сървър, Научни трудове на Русенски университет, Том 52, 2013, http://conf.uni-ruse.bg/bg/docs/cp13/3.2/3.2-1.pdf.

[9] Христо Тужаров, Архитектура на сигурността. Услуги за информационна сигурност и моделът OSI, 2010, http://tuj.asenevtsi.com/Asec10/AIS04.htm.

[10] Канално ниво. Кадри, предаване, грешки, номерация, прозорци, elearn.uni-sofia.bg/mod/resource/view.php?id=11544&redirect=1.

[11] Какво е SSH, SFTP и FTPES?, 2013, http://my.icnhelpdesk.net/knowledgebase/article/View/36/28/kkvo-e-ssh-sftp-i-ftpes.

[12] Компютърни мрежи. Раздел 4. Обзор на мрежови протоколи и услуги, http://193.192.57.240/po/courses/problemni/mrezi/HTML/section4_theme1.html#_IPXSPX.

[13] Планиране на политиката за мрежова сигурност, http://193.192.57.240/po/courses/problemni/komputarni%20mrezi/pdf/20.pdf.

[14] Протоколът PPP, http://www.kumanov.com/software/Linuxnag/html/Ch08.htm.

За контакти:

Гл. ас. д-р Виктория Рашкова, Катедра "Информатика и информационни технологии", Русенски университет "Ангел Кънчев", тел.: 082-888 412, e-mail: vkr@ami.uni-ruse.bg