IP biztonság – 1. rész

oktatási segédanyag az „IP alapú távközlés” c. tárgyhoz

Készült:

Lencse Gábor

Hálózatok biztonsága

című jegyzetének felhasználásával.

Szerkesztette: Lencse Gábor

Az anyag témaköre:

- Bevezetés a hálózati támadásokról
- Biztonsági megoldások a kommunikáció védelmére:
  - SSL/TLS infrastruktúra és alkalmazásai
  - VPN (értelmezése és IPsec)

Tartalomjegyzék

1. Bevezetés: hálózati támadások alapgondolatai

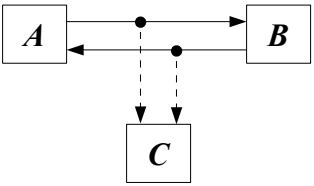
Az internet protokollkészlet kidolgozásakor ezeket a protokollokat jóhiszemű felhasználásra tervezték. Az volt a céljuk, hogy egyszerűen és hatékonyan oldják meg a kívánt feladatot. Hálózati alkalmazásaink nagyon jól működnek, amíg valaki nem kíván visszaélni velük (pl. ellopni másnak a jelszavát, kéretlen leveleket küldeni, megbénítani egy kiszolgálót, stb.)

Mi a hálózati támadásoknak a motivációja? Ez sokrétű lehet. A hálózaton keresztül érzékeny információ utazhat, pl. személyes, üzleti, katonai, stb. adatok, bármi, amit a tulajdonosa nem kíván nyilvánosságra hozni. Ennek megszerzése az illetéktelen számára hasznos lehet, vagy pusztán kárt, kellemetlenséget okozhat vele. A hálózaton keresztül elérhető szolgáltatásokhoz való illetéktelen hozzáférés (pl. nyomtatni, filmeket letölteni) is csábító lehetőség némelyek számára. Sőt, a cél lehet olyan károkozás is, mint szolgáltatások megbénítása. Hálózaton keresztül történő támadás irányulhat valamely rendszer feltörésére, rosszindulatú program(ok) bejuttatására is...

Ebben a fejezetben csak a hálózati kommunikációval kapcsolatos támadásokkal foglalkozunk.

1.1 Passzív támadás

Az érzékeny információ megszerzésére irányuló hálózati támadás a *lehallgatás* (evesdropping, wiretapping), amit passzív támadási formának nevezünk, mert végrehajtása során a támadó nem módosítja az átviteli csatorna tartalmát.



1. ábra: passzív támadás

A lehallgatás megvalósítására a gyakorlatban sokféle módszert használnak. Osztott közegen való kommunikáció esetén elegendő egy vevőt elhelyezni. Például Ethernet hálózatoknál 10Base2 és 10Base5 esetén mindig, valamint 10BaseT, 100BaseTX és 1000BaseT-nél hub alkalmazása esetén az adott szegmens hálózati kártyáinak mindegyikéhez eljut az információ, de azok normál működés során az üzenetszórás és többesküldés kivételével kizárólag azokat a kereteket veszik, amelynél a célcím megegyezik a kártya saját MAC címével. Ha a kártyát a támadó átkapcsolja olyan módba, hogy minden keretet levegyen, akkor máris rendelkezésére áll a kívánt információ. A támadás WLAN-ok esetén még veszélyesebb,

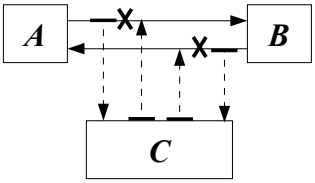
hiszen a támadónak nem is kell engedélyezett módon jelen lennie a hálózatban.

Bérelt vonal használata hamis biztonságérzetet nyújthat, ennek gyakorlati megvalósítása során a szolgáltatók gyakran egy közös IP gerinchálózatot használnak; megtörtént már olyan, hogy az útvonalválasztás hibája miatt az egyes előfizetőkhöz idegen IP datagramok kerültek.

Bizonyos esetekben a lehallgatás végrehajtása előtt a támadók aktív módszereket is használnak, például egy Ethernet switch-et nagy mennyiségű (hamis) MAC címmel elárasztva elérik, hogy az ne legyen képes a címeket tárolni, ezért hub-ként működve minden keretet minden portjára továbbítson. Egy számítógépet be lehet csapni egy routing redirect ICMP üzenettel illetve egy RIP-es routert egy hamis távolságvektorral... stb.

1.2 Aktív támadások

A passzív támadásokkal szemben az aktív támadás jellemzője, hogy a támadó maga is forgalmaz csatornán.



2. ábra: aktív támadás

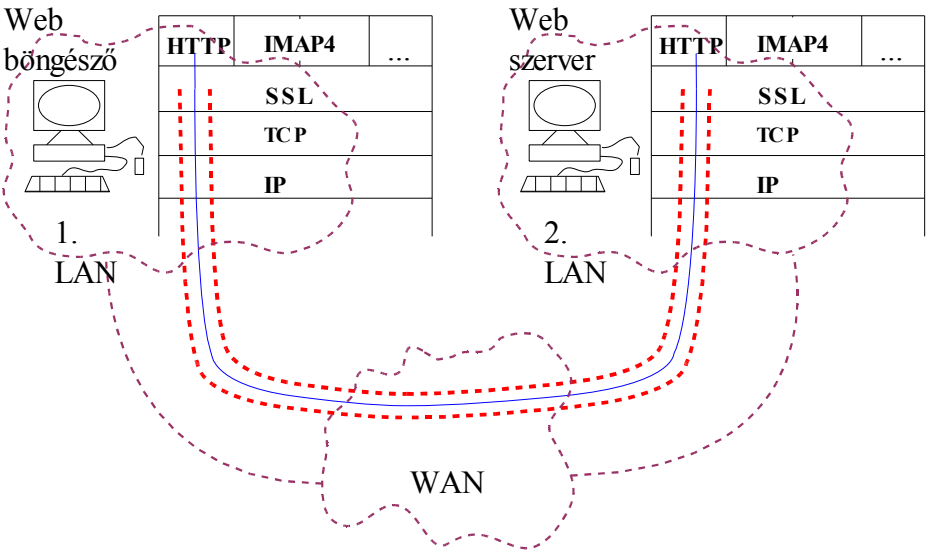
Ennek több módja lehet: az *üzenetmódosítás* azt jelenti, hogy a kommunikációban részt vevő felek közé beékelődve elfogja az adó üzeneteit és a vevőnek mást tartalmú üzenetet küld. Egy másik forma a *megszemélyesítés*, amikor a támadó más nevében küld (vagy fogad) üzenetet. Ilyen támadás például, ha rlogin-nal való belépés érdekében valaki a saját gépének IP címét átállítja olyan címre, ahonnan a megtámadott gép jelszó nélkül beenged. *Visszajátszás*nak nevezzük, ha a támadó a kommunikációban részt vevő egyik fél lehallgatott üzenetét módosítás nélkül újra elküldi a másik félnek. Képzeljük el, hogy a támadó a bankjegykiadó automata forgalmát lehallgatva újra elküldi a bankkártya számát, a PIN kódot és a kért összeget a bank felé, majd felveszi a pénzt. (Természetesen a gyakorlatban alkalmazott protokollok tartalmaznak visszajátszás elleni védelmet.)

A *szolgáltatás megtagadás* (DoS – denial of service) típusú támadások közös jellemzője, hogy a megtámadott kiszolgálót hamis kérésekkel árasztják el, ezzel kimerítik az erőforrásait, és így a valódi kérésekre nem tud válaszolni.

2. Biztonságos kommunikáció

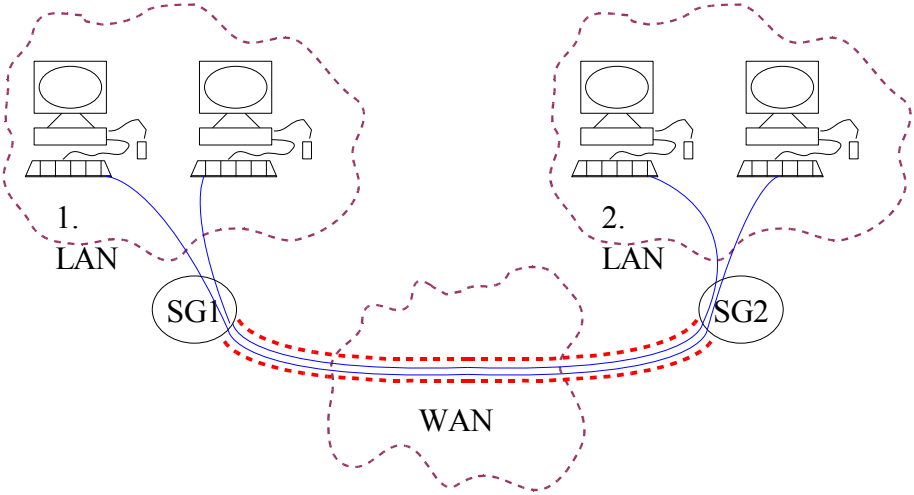
Ebben a fejezetben az IPv4 alapú nyilvános hálózatokon történő kommunikációval foglalkozunk. A biztonságos átvitel megvalósítására többféle modellt használhatunk. Most abból a szempontból vizsgáljuk meg ezeket, hogy a biztonság eléréséhez mit nyújt a hálózat és mit az alkalmazások.

Amennyiben a hálózat nem nyújt támogatást, akkor az alkalmazások a felelősek a biztonságért: a kommunikáció 2 végpontja (socketek) között az alkalmazások építenek ki egy biztonságos csatornát, ezt valósítja meg az SSL (Secure Socket Layer), illetve az azt felváltó TLS (Transport Layer Security). Ezt mutatja be a 3. ábra.



3. ábra: SSL kapcsolat

A másik megközelítés szerint a hálózat nyújtja a biztonságot. Ennek például akkor van jelentősége, ha egy szervezetnek több telephelye van, amelyeket nyilvános hálózaton keresztül kapcsolnak össze. Az egyes helyi hálózatoknak a nyilvános hálózat felé való kijáratai (security gateway) egymás között a nyilvános hálózatra építve értéknövelt szolgáltatással oldják meg a telephelyek között az információ biztonságos átvitelét: VPN (Virtual Private Network), ezt mutatja be a 4. ábra.



4. ábra: VPN kialakítása

Ebben a fejezetben a továbbiakban először az SSL/TLS megoldással, majd pedig a VPN-nel foglalkozunk.

2.1 SSL/TLS infrastruktúra és alkalmazásai

2.1.1 SSL/TLS, OpenSSL

Az SSL a Netscape fejlesztése, 3.0-s verziójának specifikációját 1996-ban Internet Draft-ként tették közzé, lehetővé téve ezzel, hogy a protokollt bárki implementálhassa. Ez képezte az alapját az 1999-ben közzétett TLS 1.0 protokollnak (RFC 2246). (Jegyezzük meg, hogy az SSL 2-es verziója biztonsági rést tartalmaz, nem szabad használni! Régi böngészőkben még választható ez a protokoll…)
Az SSL/TLS tulajdonképpen egy új, biztonsági réteget definiál a TCP/IP fölött és az alkalmazások (pl. HTTP) alatt.
Az SSL/TLS protokoll nyílt forrású implementációja az „Open SSL Project" keretében készült, gyakorlatilag felhasználható nyílt forrású és kereskedelmi szoftverek fejlesztésére is. A projektről bővebben olvashatunk a http://www.openssl.org/ webhelyen. Az OpenSSL programkönyvtár (library) egy olyan funkciókészletet (API – Application Programming Interface) nyújt, amelyet felhasználva biztonságos kommunikációt folytató programok írhatók. Rendelkezik parancssoros interfésszel is, így a felhasználók közvetlenül is elérhetik a szolgáltatásait. (Például kriptográfiai függvények elérése a parancsértelmezőből.)

2.1.2 OpenSSH

Az OpenSSL-re épül az OpenBSD projekt részeként kifejlesztett OpenSSH szoftvercsomag. Ez a biztonságos távoli bejelentkezésen (Secure Shell) kívül biztonságos fájl átvitelre (scp, sftp), X11 átvitelre, port-továbbításra is használható. A csomag nyílt forrású és bárki bármilyen célra felhasználhatja. Ezt úgy érték el, hogy a szabadalommal védett részeket eltávolították a kódból (pl. az IDEA titkosítást teljesen kihagyták) és amire szükség volt, azt külső könyvtárakkal oldották meg (pl. OpenSSL).
A projektnek még magyar nyelvű weblapja is van: http://www.openssh.com/hu/

2.1.3 Az s végű protokollok

Ha megnézzük az IANA jól ismert port számainak (well known port numbers) listáját, akkor láthatjuk, hogy jó néhány protokoll (pl. **`http`**, **`telnet`**, **`pop3`**, **`imap4`**, **`ftp`**, stb.) biztonságos megfelelője számára lefoglalták a port számokat. Ez azt jelenti, hogy ehhez a porthoz kapcsolódva az adott protokoll egy SSL/TLS réteg fölött érthető el. Így például a **`https`** protokoll portszáma: 443, a **`pop3s`** portszáma: 995, az **`imap4s`** portszáma 993, stb.
http://www.iana.org/assignments/port-numbers

2.2 VPN

2.2.1 A VPN értelmezése

Mielőtt a Internet használata általánossá vált, a cégek az egymástól távol elhelyezkedő telephelyeiken levő hálózataik összekapcsolására valamely távközlési szolgáltatótól vonalat béreltek. A bérelt vonal kezdetben a vonal (pl. réz érpár) kizárólagos használatát jelentette, a bérlő az általa megválasztott modulációval a (fizikai lehetőség határain belül) tetszőleges adatsebességgel forgalmazhatott. Később a szolgáltatók kötött sebességű (pl. n*64kbit/s), de garantált minőségű adatátviteli szolgáltatást nyújtottak bérelt vonal néven. A kapacitást az adott előfizető kizárólagosan használta, és amennyiben nem használta ki, akkor sem használhatta más.

A csomagkapcsolt technológia előretörésével elterjedt az a megoldás, hogy a szolgáltatók a kapacitások jobb kihasználása érdekében az egyes előfizetők forgalmát statisztikai multiplexelés segítségével ugyanazon csomagkapcsolt hálózaton viszik át. A felhasználóknak azonban gyakran igénye van arra, hogy a szolgáltató a bérelt vonalakéhoz hasonló minőségi paramétereket garantáljon (pl. garantált sávszélesség, késleltetés, késleltetésingadozás). Azt is elvárhatják, hogy a forgalmuk ne juthasson illetéktelenek kezébe, hanem a bérelt vonalakéhoz hasonló védettséget élvezzen. Ezen

elvárásokat kielégítő megoldás a ***trusted VPN***. Ebben az esetben a szolgáltató természetesen képes lenne a hálózatán áthaladó forgalom lehallgatására, sőt módosítására, de élvezi az előfizető bizalmát, hogy ilyent nem tesz, sőt a legjobb gyakorlat szerint mindent megtesz ennek az elkerülésére.

Egészen más megközelítés a ***secure VPN***, ami egy nyilvános adathálózaton áthaladó forgalom biztonságát garantálja. Ebben az esetben a nyilvános hálózatba való belépéskor a forgalmat megfelelő módon titkosítják, majd a kilépéskor dekódolják. A titkosítás jelenti a garanciát, hogy az esetleges támadó ne jusson hozzá az előfizető által birtokolt információhoz, illetve aktív támadás esetén sem jusson el az előfizetőhöz a módosított adatfolyam. A secure VPN-t megvalósíthatja a szolgáltató is, de igen gyakran az előfizető teszi meg.

A két fajta VPN tehát mást nyújt. Biztonsági szempontból számunkra a második az érdekes, de a mai best effort jellegű IPv4 alapú hálózataink világában igen nagy értéket képviselnek a garantált minőségi paraméterek, ezért van értelme a kettő együttes alkalmazásának: ***hybrid VPN***. Ebben az esetben a minőségi paramétereket garantáló trusted VPN egésze vagy egy része fölött secure VPN-t is alkalmazunk. Természetesen csak a secure VPN-en belüli rész lesz biztonságos.

A továbbiakban VPN alatt a secure VPN-t értjük, eltérő esetben

külön jelezzük.

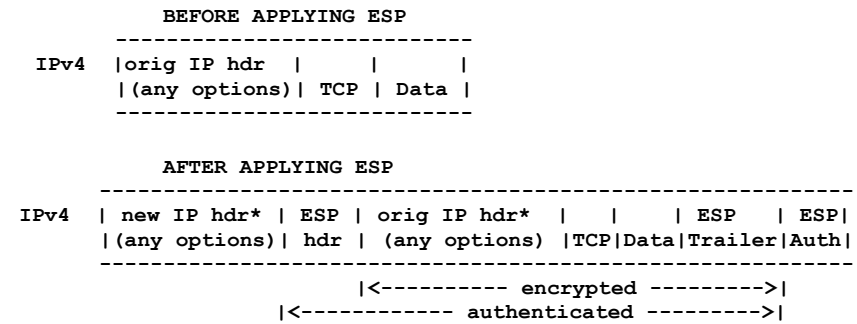
A témáról a Virtual Private Network Consortium (VPNC) honlapján többet is olvashatunk: http://www.vpnc.org/

2.2.2 Az IPsec protokollcsalád

Az IPsec protokollcsalád a VPN megvalósításának kiváló eszköze. Az IPsec egy rugalmas keretrendszer, amiben az egyes algoritmusok a felhasználás céljának megfelelően választhatók meg. Az IETF-en belül egy munkacsoport több évi munkájaként igen jelentős mennyiségű dokumentum (Internet Draft, RFC) jött létre a témában. Mivel számunkra a VPN megvalósítása szempontjából érdekes, ezért csak az ESP protokollal (Encapsulating Security Payload, RFC 2406), annak is csak a tunnel módjával foglalkozunk. Az érdeklődőknek megemlítjük, hogy az AH (Autentication Header, RFC 2402) az üzenetek integritásának ellenőrzését szolgálja, de nem nyújt titkosságot.

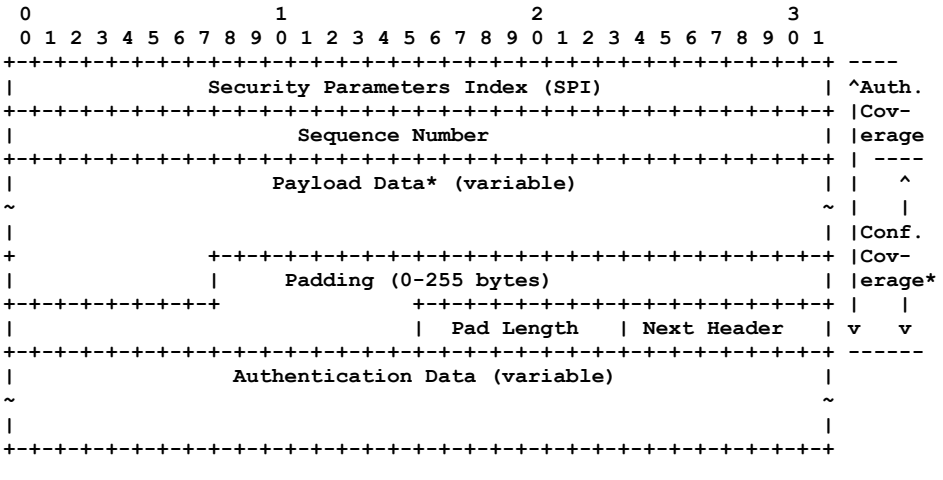
Ha az ESP-t alagút módban használjuk, akkor nem csupán az átvitt információt védi meg az illetéktelenektől, hanem a forgalom analízisének lehetőségeit is erősen rontja. Ezt úgy éri el, hogy az eredeti datagramot becsomagolva új fejrészt hoz létre, amiben a cél és a forrás IP cím mezők nem a üzenet címzettjének és feladójának IP címét hordozzák, hanem a VPN-t megvalósító két biztonsági átjáró (Security Gateway) IP címét. A datagram becsomagolása a

következőképpen történik:



Tehát az eredeti datagram elé kerül az ESP fejrész, az elé egy új IP fejrész és a datagram mögé is kerülnek mezők a becsomagolás során. Bár arra is lehetőség van, hogy a becsomagolt datagramot ne titkosítsuk (null encryption választásával), esetünkben nem így járunk el, hanem valamelyik ismert blokk titkosító algoritmust használjuk (pl. DES, 3DES, AES, RC5, IDEA, CAST, Blowfish).

Nézzük meg egy kicsit alaposabban az ESP csomag formátumát (most már az elé helyezett új IP fejrész nélkül):



Láthatjuk, hogy a beágyazott eredeti datagram egészét védi a titkosítás, illetve a titkosító blokkméretének többszörösére ki kell egészíteni a titkosítandó részt, aminek az utolsó oktetje az azt követő autentikációs rész hosszát, az előtte levő oktet pedig a helykitöltő hosszát adja meg. A sorszám a visszajátszás ellen véd, az SPI pedig annak az SA (Security Association) kapcsolatnak az azonosítója, amelyhez a csomag tartozik. Láthatjuk, hogy erre a kettőre is vonatkozik az autentikáció (ne lehessen útközben észrevétlenül megváltoztatni), de a titkosítás nem, hiszen pl. az SPI nyílt ismerete nélkül a címzett biztonsági átjáró nem tudna mit kezdeni a csomaggal!

Most már lássuk, hogy mi történik, amikor egy állomás VPN-en keresztül egy másik állomással szeretne kommunikálni! Fontos megjegyezni, hogy nem feltétlenül TCP kapcsolat kiépítéséről van szó, lehet UDP, ICMP üzenet is! Bár ezek kapcsolatmentes protokollok, és TCP esetén is maga az IP kapcsolatmentes, mégis szükség van egy kapcsolatra a két biztonsági átjáró között. Ennek a kapcsolatnak létre kell jönnie, mielőtt a VPN-en keresztül forgalmazni lehetne. A részletek ismertetése nélkül röviden annyit, hogy a biztonsági átjárók rendelkezhetnek előre manuálisan beállított közös kulccsal (pre-shared key), illetve valamely nyilvános kulcsú titkosításon alapuló módszerrel (pl. tanúsítványok használatával) is megállapodhatnak a blokktitkosításhoz szükséges kulcsban. Az

érdeklődők bővebben a 2409-es RFC-ben olvashatnak az IKE-ről (Internet Key Exchange). A biztonsági átjárók tehát a belső hálózatból származó forgalmat kifele becsomagolva továbbítják, míg a kívülről érkező forgalmat kicsomagolják és ellenőrzik, ha minden rendben van, akkor továbbítják a belső hálózatban található címzett felé. Mivel a nyilvános hálózaton mintegy „alagútban” a védendő információ becsomagolva utazik, így a VPN által összekapcsolt belső hálózatok szomszédosként látják egymást. (Ez kiderül pl. az IPv4 datagram TTL vagy az IPv6 datagram hop limit mezőjéből.) Ez arra is lehetőséget nyújt, hogy a két belső hálózat nem publikus IP címeket használjon, amelyekkel az Interneten egyébként nem tudnának egymás között kommunikálni!

2.2.3 FreeS/WAN és Openswan

A FreeS/WAN projekt keretében létrejött az IPsec egy nyílt forrású implementációja. http://www.freeswan.org/ A projekt ugyan befejeződött, de a fejlesztők egy csoportja és önkéntesek új céget alapítottak és folytatják a munkát. http://www.openswan.org/
A Linux 2.6 kernel pedig már natív IPsec implementációt tartalmaz.