INFOKOMMUNIKÁCIÓS SZOLGÁLTATÁSOK ÉS ALKALMAZÁSOK

Hálózatbiztonság, Tűzfalak

Szabó Sándor
Lendvai Károly
BME Híradástechnikai Tanszék
szabos@hit.bme.hu

2011. május 11.,
Budapest

Már i.e. megmondták…

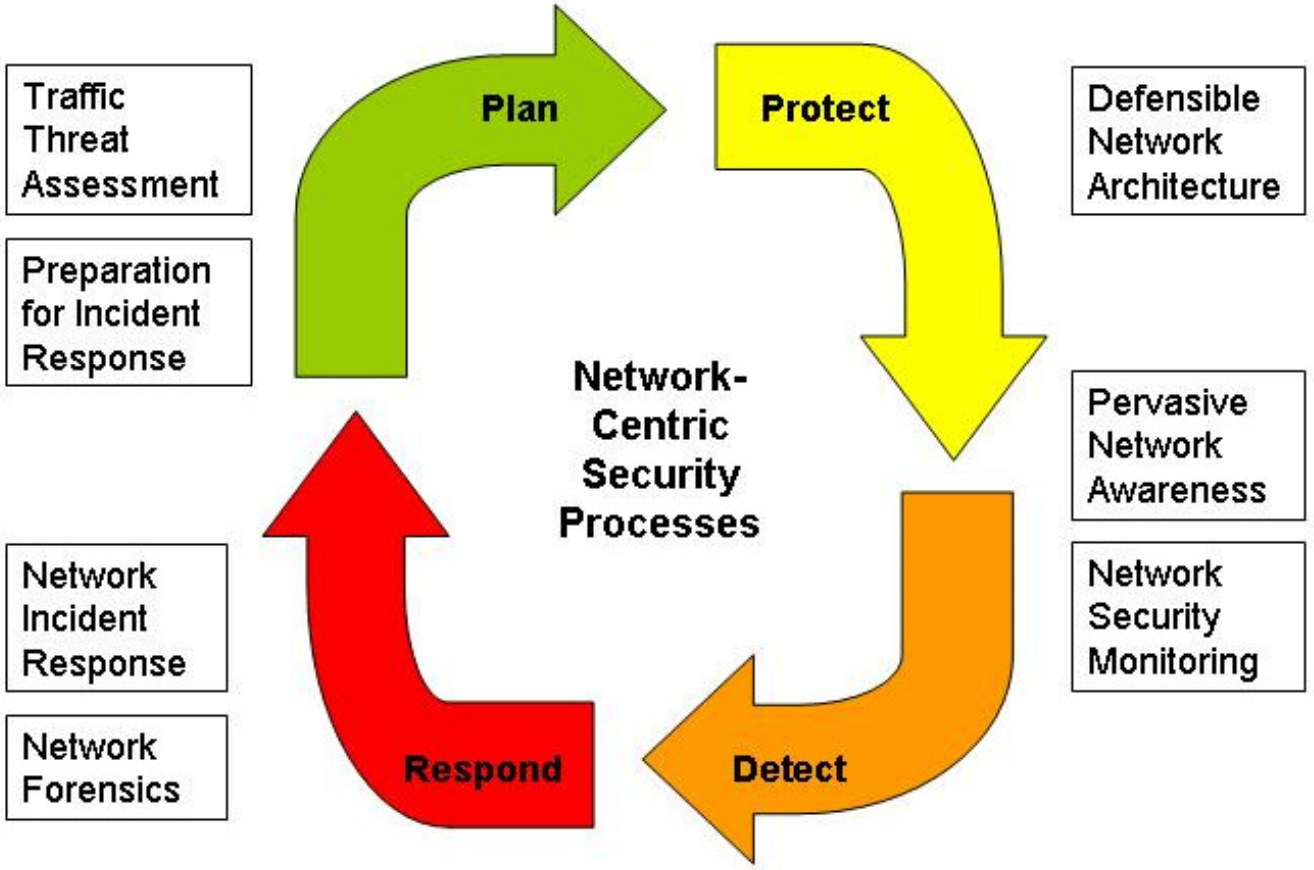
Szun-Ce, A hadviselés törvényei:

„…ha ismerjük az ellenséget és ismerjük magunkat is, akkor száz csatában sem jutunk veszedelembe; ha azonban nem ismerjük az ellenséget, csak magunkat ismerjük, akkor egyszer győzünk, másszor vereséget szenvedünk; és ha sem az ellenséget, sem magunkat nem ismerjük, akkor minden egyes csatában feltétlenül végveszély fenyeget bennünket…”

Bruce Schneier:

„A biztonság nem egy termék, hanem egy folyamat.”

A folyamat


Traffic Threat Assessment
Preparation for Incident Response
Plan
Protect
Defensible Network Architecture
Network-Centric Security Processes
Pervasive Network Awareness
Network Security Monitoring
Network Incident Response
Network Forensics
Respond
Detect

Biztonságos hálózat

Mi az a biztonság?

Nehéz definiálni, mivel mindenkinek mást jelent

Példák:

- Fontos adatállomány esetén illetéktelenek ne juthassanak hozzá az adatokhoz (jövő heti ZH feladatok)
- Illetéktelenek adott esetben bizonyos adatokat csak olvasni tudjanak, módosítani ne (kipublikáljuk a ZH eredményeket, ne lehessen átírni őket)
- Felhasználói jogosultságkezelés

Kockázat

Tökéletesen biztonságos rendszer nem létezik.

A dolgokat a másik oldalról közelítsük meg.

Kockázat

- Egy adott rendszert fenyegető veszélyeket veszi számba, az általuk okozott károkat próbálja megbecsülni, összegezni
- Gyakorlatban: Kockázatelemzés, Kockázatcsökkentés
- Leggyengébb láncszem felderítése

Alapfogalmak

- Sértetlenség
  - Az elküldött üzenet változtatás nélkül ér célba
  - Esetleges módosítás detektálható
- Hitelesség
  - Az üzenetet valóban az küldte, akit feltételezünk és a hálózati továbbítás során nem módosult
- Letagadhatatlanság
  - Nemcsak a vevő, hanem tetszőleges harmadik fél felé is igazolható, hogy egy adott üzenetet tényleg a valódi küldő küldött, letagadni azt nem tudja

Alapfogalmak

- Bizalmasság
  - Az üzenetet egy támadó hiába hallgatja le, azt nem tudja értelmezni a titkos kulcs nélkül, mivel kriptográfiai módszerekkel titkosítva van.
  - Az emberek többnyire ezt értik biztonságos kommunikáción
- Távoli azonosítás
  - Akkor, ha két fél még nem ismeri egymást, és közöttük nincs egy biztonságos csatorna, akkor egyéb módszerek segítségével rendszerint harmadik fél bevonásával mutatkozhatnak be egymásnak biztonságosan. Rendszerint ezt a PKI infrastruktúra segítségével oldják meg.

Támadás

Mit értünk támadáson?

Adott egy illetéktelen személy (támadó), aki a **kommunikációnk során keletkező üzenetek** biztonságát különböző támadások során veszélyezteti.

(Itt most nem foglalkozunk például azzal, hogy a támadó ellophatja a számítógépünket, és lemásolhatja arról az adatokat, holott az is egy lehetséges támadás)

Miért?

Miért támadnak?

- A támadó haszonszerzésre törekszik
- A támadó a szolgáltató hírnevét próbája gyengíteni
- Jó szándékú támadó, csak a rendszer hibáira szeretné felhívni a figyelmet
- Erőfitogtatás, szórakozás
- **Ugródeszka más gépek feltöréséhez**

A támadásokat két nagy csoportba osztjuk:

- Passzív támadások
- Aktív támadások

Passzív támadások

A támadó csak **megfigyelést végez**, vagy **információt gyűjt** az információ tartalmának és továbbítási módjának **megváltoztatása nélkül**.

Két fő típus:

- Üzenet tartalmának felfedése
  - Üzenetek lehallgatása, küldött adatállományok tartalmának megfigyelése
  - Védekezés: titkosítással és/vagy a kommunikáló felek azonosításával

Passzív támadások

- Forgalomanalízis
  - A kommunikáló felek helyét, a kommunikáció gyakoriságát, idejét, időtartamát határozza meg
  - Ezen támadások ellen nem segít a titkosítás, azonosítás

Általánosságban elmondható, hogy a passzív támadások ellen védekezni nagyon nehéz, a megelőzés a legjobb mód.

A támadó személyének, helyének felderítése nagyon nehéz, mivel a támadás nem hagy nyomot az üzenetekben.

Aktív támadások

Aktív támadás esetén, a támadó valamilyen módon **megváltoztatja** az üzeneteket, vagy **hamis üzeneteket generál**.

Az aktív támadásoknak négy fő típusa létezik:

- Álcázás (masquerade), megszemélyesítés (impersonation), hamisítás (spoofing)
  - A támadó egy legális partnernek adja ki magát
  - Példa 1: FTP felhasználónév és jelszó lehallgatása, majd később ezen adatok felhasználása kapcsolat kiépítésére
  - Példa 2: Csomagban forrás IP cím cseréje

Aktív támadások

- Visszajátszás (replay)
  - Korában megszerzett üzenet / üzenetváltás későbbi időpontban történő újraküldése
- Módosítás (modification)
  - Egy szabályos üzenet bizonyos részeit a támadó módosítja, kitörli, vagy új részeket illeszt bele
  - Nem szükséges hozzá a teljes üzenet ismerete
  - Real time alkalmazása Man-In-The-Middle támadással lehetséges

Aktív támadások

- Szolgáltatásmegtagadás (Denial of Service – DoS)
  - A kommunikációs infrastruktúra normális működését zavarják meg, rontják el
  - Célja lehet egy adott számítógép, vagy adott program megbénítása, de adott esetben egy egész hálózat működésképtelenné tétele is
  - Például egy számítógép elárasztása hamis kérésekkel, így a valós kérdésekre nem tud válaszolni
  - Amikor a támadás egyszerre több gépről érkezik DDoS – Distributed Denial of Service támadásról beszélünk

Aktív támadásokat nehéz megelőzni, fő cél a detektálás és a normál működés leghamarabb történő visszaállítása, támadó helyének, személyének felderítése.

Social Engineering

Az ISO/OSI modellben a leggyengébb réteg a 8. réteg…

.. A felhasználó…

A social engineering az emberek bizalomra való hajlamát használja ki, nem a hardver, szoftver, vagy a hálózat hibáit. Napjainkban nagyon népszerű.

Például: Phishing

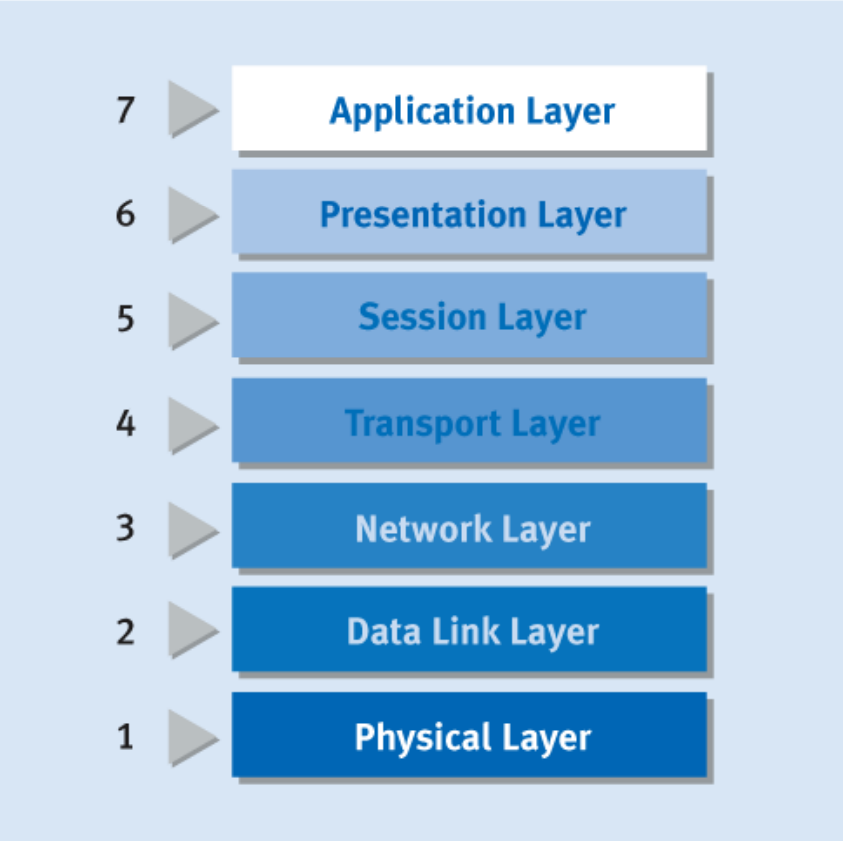
Olvasnivaló:

Kevin D. Mitnick – A legendás hacker (a behatolás művészete)

Kevin D. Mitnick – A legendás hacker (a megtévesztés művészete)

Támadások

Különböző támadásokat fogunk megnézni, az ISO/OSI modellen fogunk végighaladni, lentről felfelé.

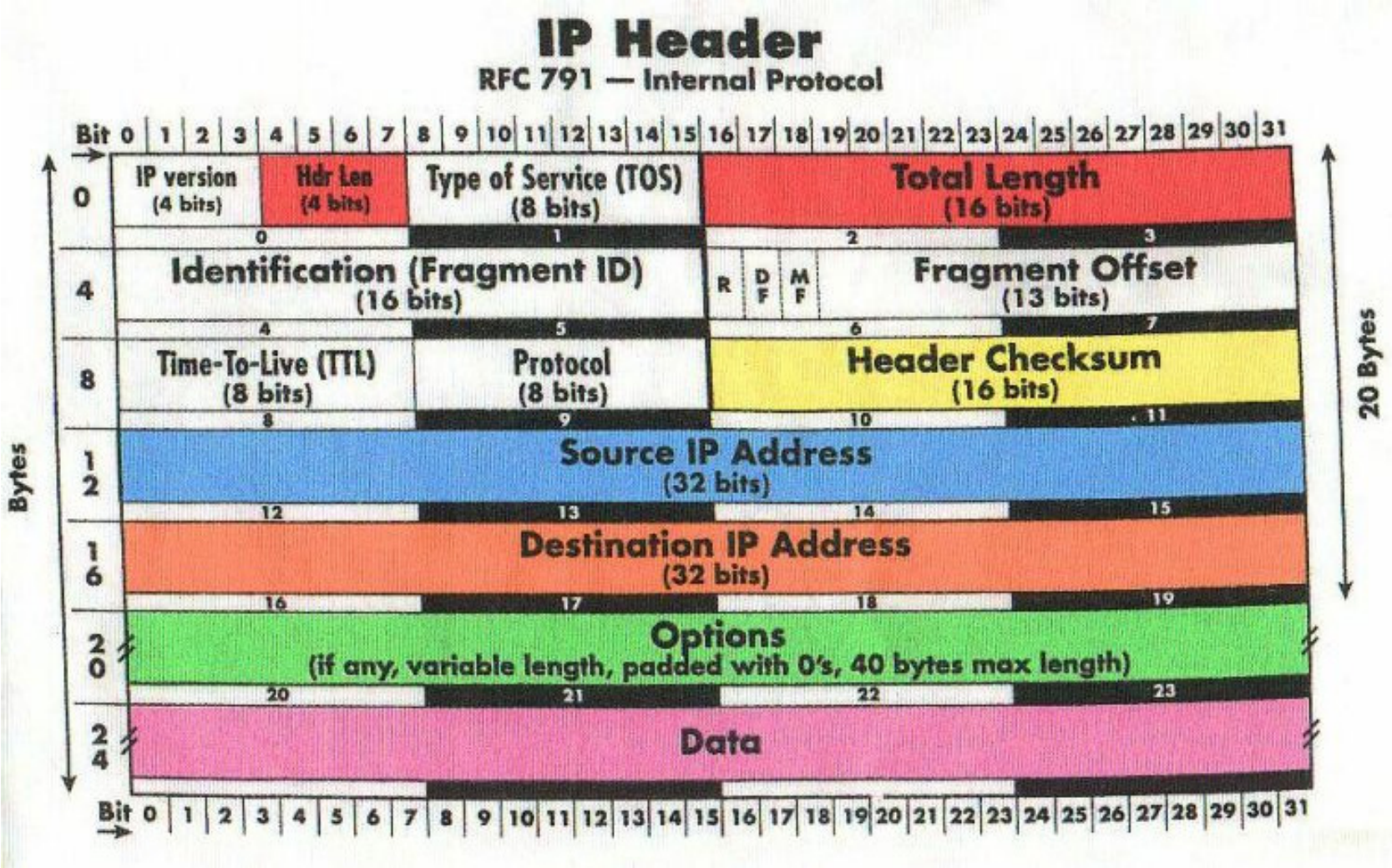


Támadások

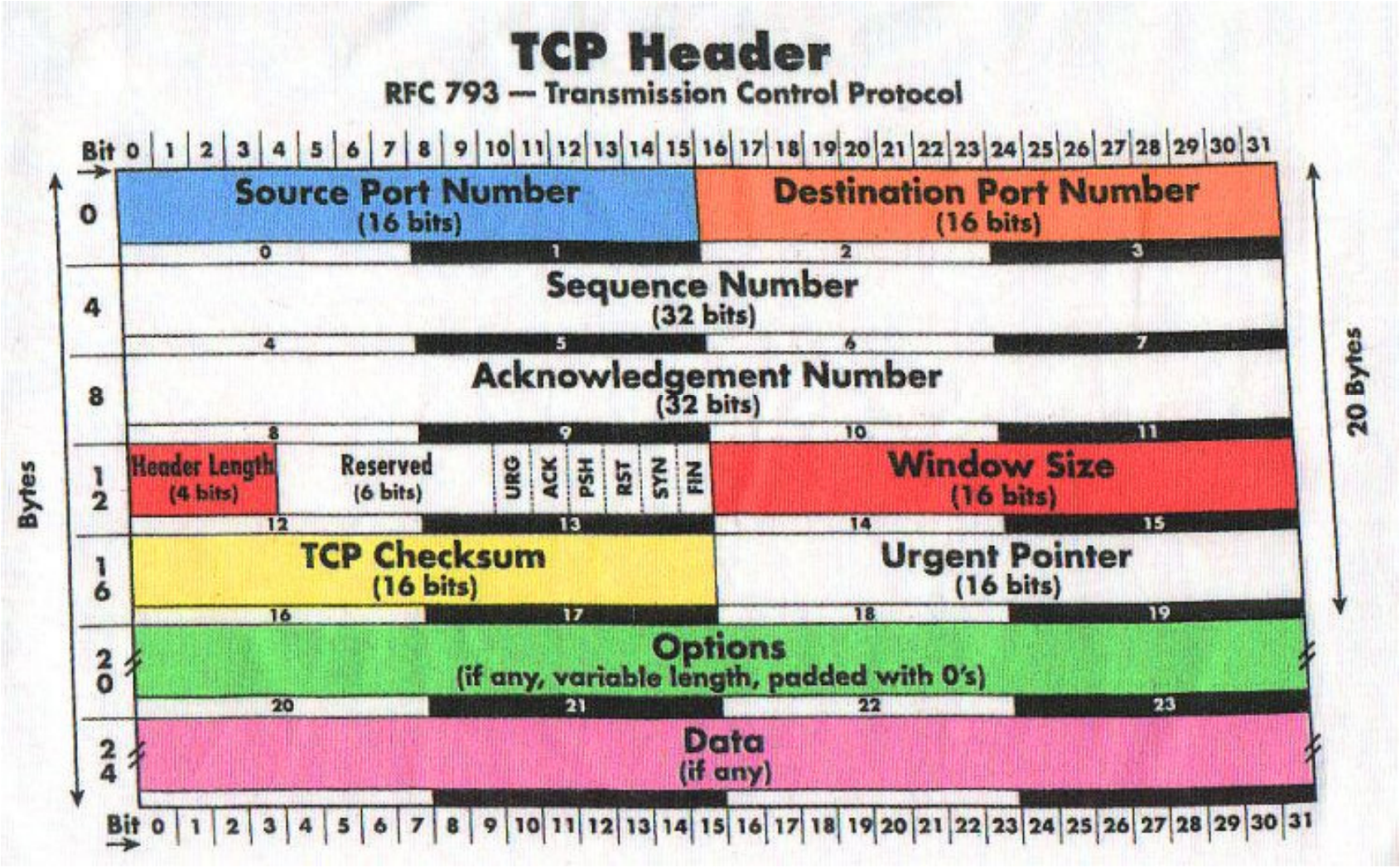
Nézzük meg, hogyan működnek a következő támadások:

- Fizikai rétegbeli lehallgatás
- Fizikai rétegbeli zavarás
- MAC Spoofing
- ARP Spoofing
- IP Spoofing
- Land attack
- Teardrop támadás
- Smurf támadás
- Ping of Death
- SYN flood
- DNS poisoning

Emlékeztető (IP fejléc)



Emlékeztető (TCP fejléc)



Kérdések?

KÖSZÖNÖM A FIGYELMET!

Híradástechnikai Tanszék

Szabó Sándor
Lendvai Károly
BME Híradástechnikai Tanszék
szabos@hit.bme.hu