

Hálózatok építése és üzemeltetése

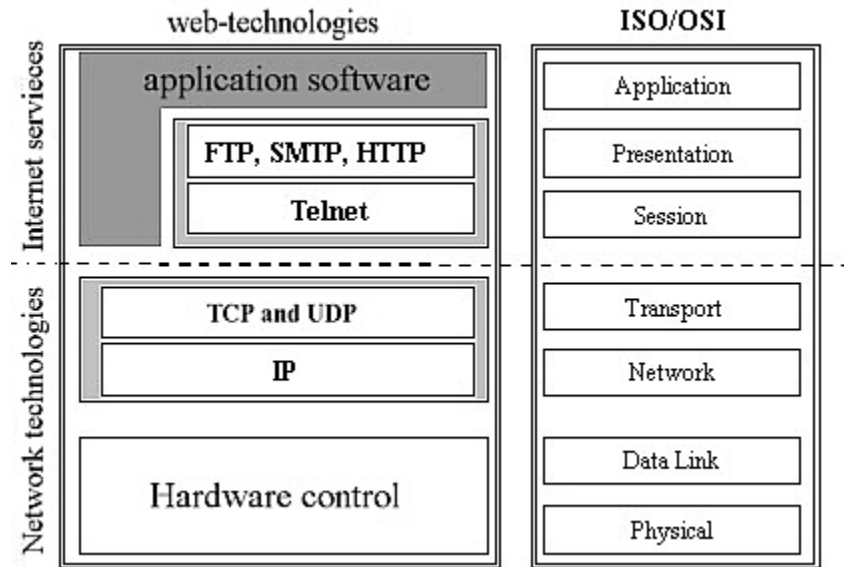
Hálózatbiztonság 1.

Biztonság az 1. és 2. rétegben

Emlékeztető a rétegekre

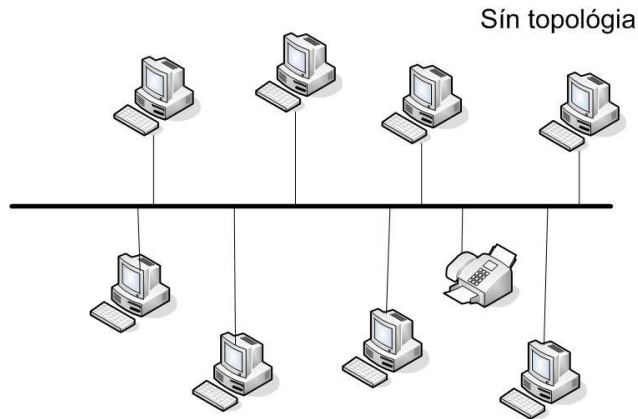
▶ ISO/OSI 1983

- ▶ International Standards Organization Open Systems Interconnection Basic Reference Model

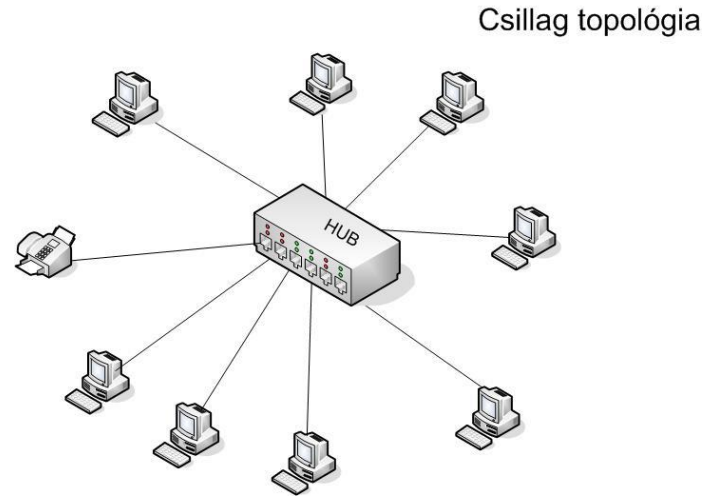


Hálózati alap topológiák

► Sín-, csillagtopológia



Minden forgalom látható



Elkülönített felhasználók

Egyéb topológiák: gyűrű, háló (mesh)

Tipikus mai helyi hálózatok

▶ Ethernet

- ▶ Olcsó és gyors
- ▶ Csillag topológia (de korábban sín volt!)
- ▶ Hálózati kapcsolók (switch) a forgalom irányítására
 - ▶ Korábban: repeater, bridge, hub

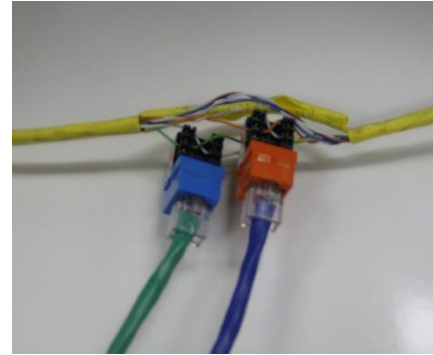
▶ WiFi

- ▶ Olcsó és gyors és vezeték nélküli
- ▶ Logikai csillag topológia (de valójában egy broadcast rádió)
- ▶ Hálózati hozzáférési pontok

Támadások az 1. és 2. rétegben

▶ Fizikai hozzáférés a hálózathoz

- ▶ Lehallgatás
- ▶ Kábel rongálás, jamming



▶ Identitás lopás

- ▶ MAC cím, mint egyedi azonosító
 - ▶ Általában gyárilag rögzített, de megváltoztatható
- ▶ MAC cím klónozás

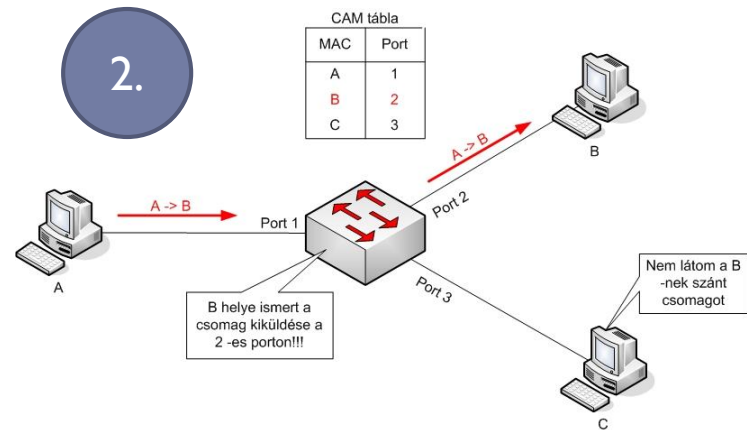
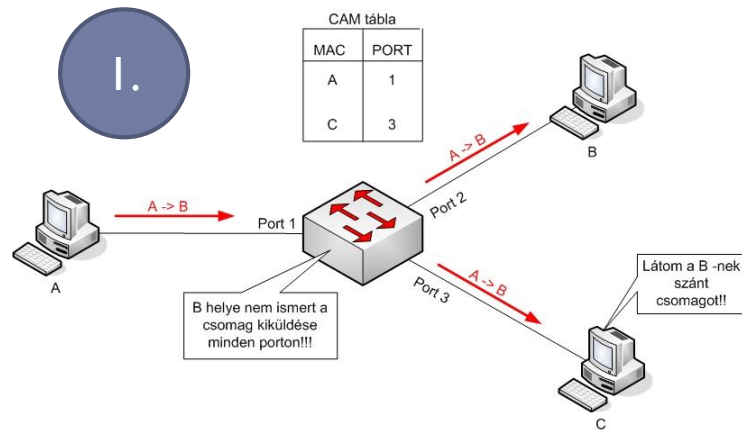
wrietap



Ethernet kapcsolók támadása

▶ CAM tábla

- ▶ Drága, kicsi, fix méret



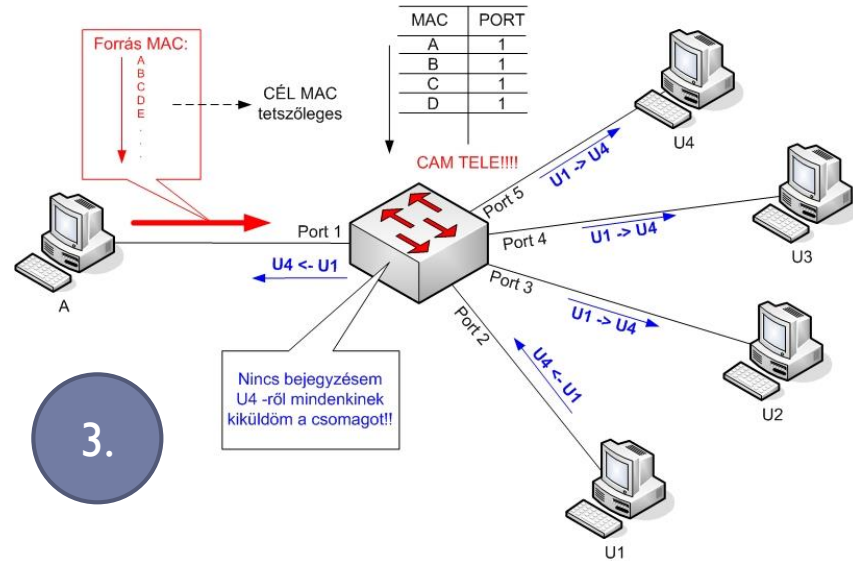
Ethernet kapcsolók támadása 2.

▶ CAM elárasztás / MAC áradat

- ▶ A CAM tábla megtelik hamis címekkel, felülíródnak a valódi címek
- ▶ A kapcsoló ismét mindenkinek küldi a beérkező keretet

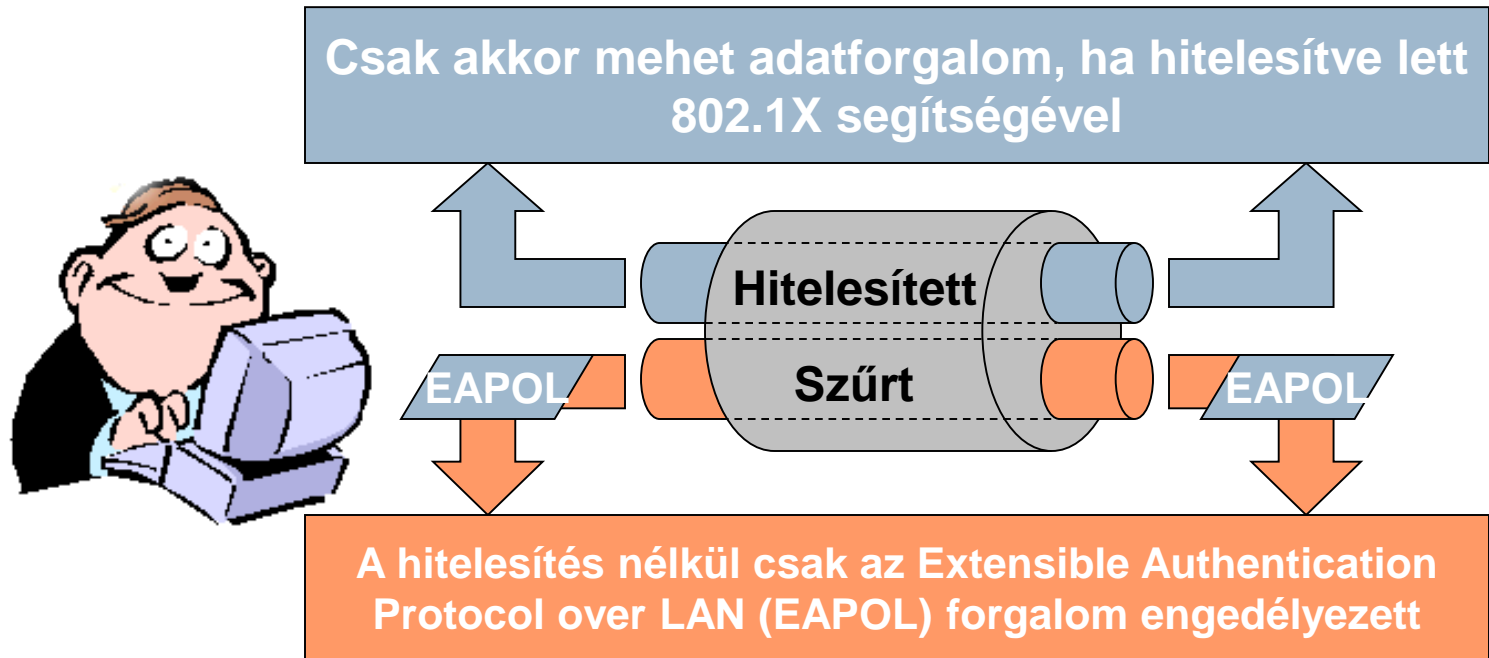
▶ Védekezés?

- ▶ Fix MAC tábla?
 - ▶ Hibaforrás
- ▶ Port letiltása elárasztás esetén
- ▶ IEEE 802.1X



Mi az a 802.1X ?

► Port-based Network Access Control (PNAC)



Biztonság a 2. és 3. rétegben

MAC címek (@L2) és IP címek (@L3)

▶ MAC címek hamisíthatóak?

- ▶ Forrásként és célként tetszőleges MAC cím beállítható

▶ IP címek hamisíthatóak?

- ▶ Forrásként tetszőleges IP cím beállítható
- ▶ Célként az adott alhálózaton belül tetszőleges IP cím beállítható
 - ▶ Inkább csak vak támadásokhoz jó (nem látszik az áldozat válasza)

▶ Védekezés

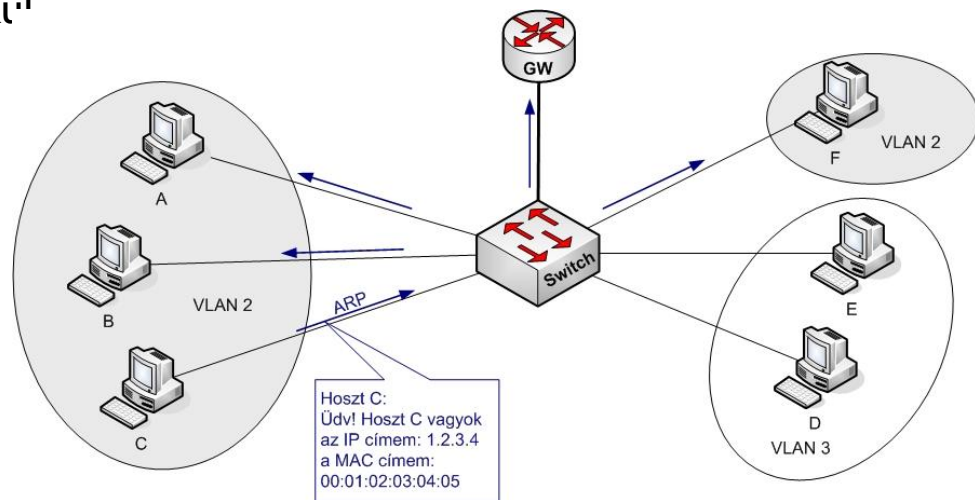
- ▶ IP: a kimenő forgalom szűrése.
 - ▶ Költséges, nem használják.

Átjárás MAC és IP világ között

- ▶ ARP – Address Resolution Protocol
 - ▶ IP alapján MAC címet mond. Kérdésre válaszol.
 - ▶ (MAC alapján IP cím: BOOTP, DHCP)
 - ▶ Gratuitous ARP
 - ▶ MAC cím hirdetés kérés nélküli
 - ▶ Konfliktus keresés
 - ▶ Azonnali váltás új címre

- ▶ **Működése:**

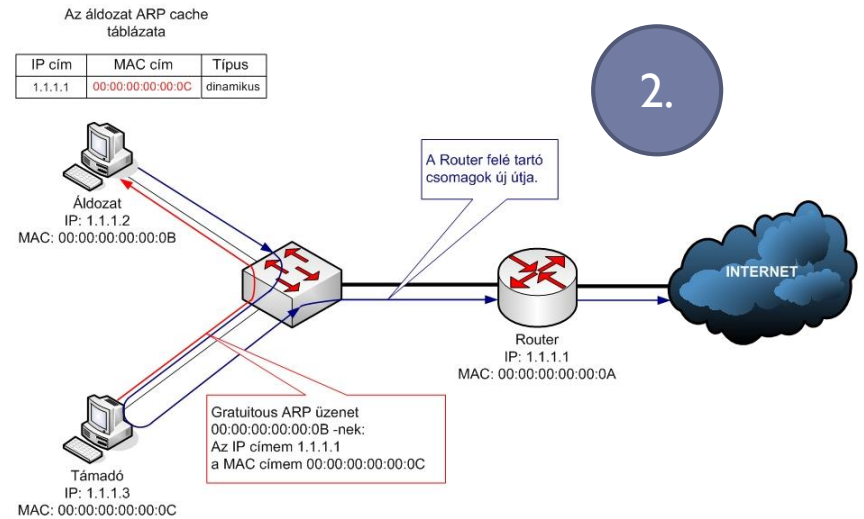
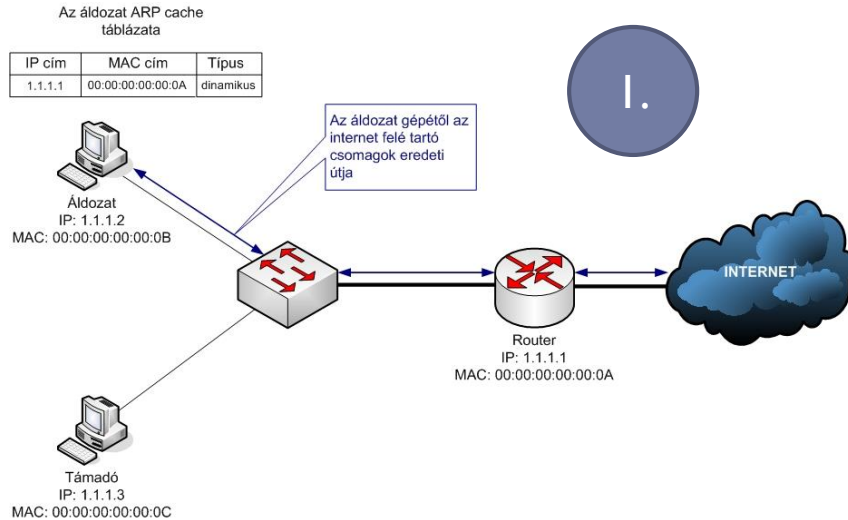
- ▶ Az adott hoszt látja a felé intézett kérdéseket és válaszol rájuk



ARP mérgezés

▶ ARP poisoning

▶ MiM – Man in the Middle támadás



ARP védekezés

▶ ARP forgalom

- ▶ Kicsi, fix méretű csomagok, jól kiszámítható tartalommal
 - ▶ ARP üzenet példa (28 bájt): | HW MAC | proto type (Eth=1) | Proto addr.Type (IP=0x800) | MAC size | IP size | operation (1=request, 2=reply) | SRC MAC | SRC IP | DST MAC | DST IP |

▶ Védekezés

- ▶ ARP forgalom megfigyelése, hamis forgalom szűrése (Dynamic ARP inspection)
 - ▶ A hálózat végzi, nem a végpontok

DHCP támadások

▶ Működése (ismétlés)

- ▶ DHCPDISCOVER -> DHCPOFFER -> DHCPREQUEST
- ▶ Több szerver is lehet
- ▶ Kliens broadcast címre küld, unicast válasz érkezik

▶ Támadás

- ▶ Kiéheztetés és hamis DHCP szerver
 - ▶ Az összes pool cím elkérése (MAC hamisítással)
 - ▶ Az új kéréseket már csak a hamis szerver tudja kiszolgálni

DHCP támadás nyertesei

- ▶ **Miért jó a DHCP szervernek?**
 - ▶ DHCP options:
 - ▶ Időzóna, **router cím**, idő server, **DNS server**, alapvető szerverek címei (levelezés, böngészés, IRC), TFTP server és frissítés fájl

- ▶ **Védekezés**
 - ▶ MAC címek portonkénti korlátozása
 - ▶ IEEE 802.1X használata
 - ▶ Hiteles konfigurációs fájlok

Biztonság a 3. és 4. rétegben

ICMP

- ▶ **Protokoll az IP hálózati funkciók segítésére**
 - ▶ Tesztelés, hibajelzés, segítség forgalomirányításnál
- ▶ **Internet Control Message Protocol**
 - ▶ Echo
 - ▶ Destination Unreachable
 - ▶ Router Advertisement
 - ▶ Traceroute
 - ▶ ...



PING

ICMP támadásai

▶ SMURF

- ▶ DoS támadás ping segítségével broadcast IP cím segítségével
 - ▶ Védekezés 1.: Ne válaszolj a pingre! (főleg broadcast ping)
 - ▶ Védekezés 2.: A router nem továbbítja a ping csomagokat (főleg broadcast ping)
- ▶ SMURF sokszorozó – Hálózat, amely megsokszorozza a ping válaszokat egy megszemélyesített áldozathoz

▶ Hamisított ICMP üzenetek

- ▶ Hamis “Time exceeded”
- ▶ Hamis ”Destination unreachable”

▶ Ping of death

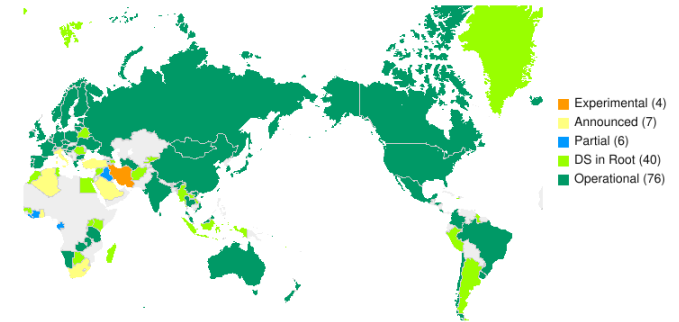
- ▶ Implementációs hiba az IP stackben
 - ▶ Túlméretezett ping csomag kékhalált okozott (Javítva 1998 óta)

DNS támadások

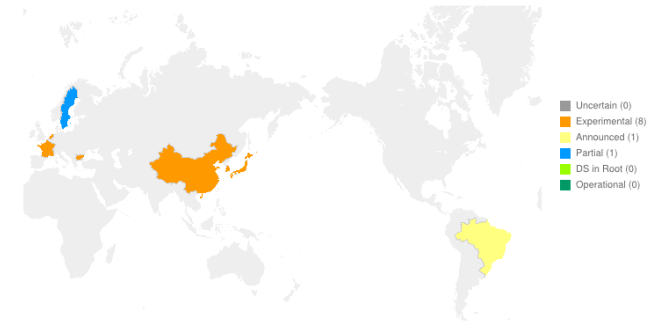
- ▶ **Biztonsági problémák**
 - ▶ A támadó bármit küldhet, akár az Internet másik feléről is
 - ▶ LAN lehallgatása
 - ▶ DNS hamis válasz (16 bit nonce & forrás port kitalálása)
 - ▶ Cache mérgezés
 - ▶ Hamis információ a DNS szerverben
- ▶ **DNSSEC**
 - ▶ DNS tranzakciók hitelesítése
 - ▶ DNS adatok eredetének igazolása
 - ▶ Adat integritás
 - ▶ Hitelesített nem létezés
 - ▶ Szép lassú elterjedés
- ▶ **DNS titkosítása?**
 - ▶ „Last mile” DNS biztonság

Nem erre
ad megoldást!

ccTLD DNSSEC Status on 2016-06-20

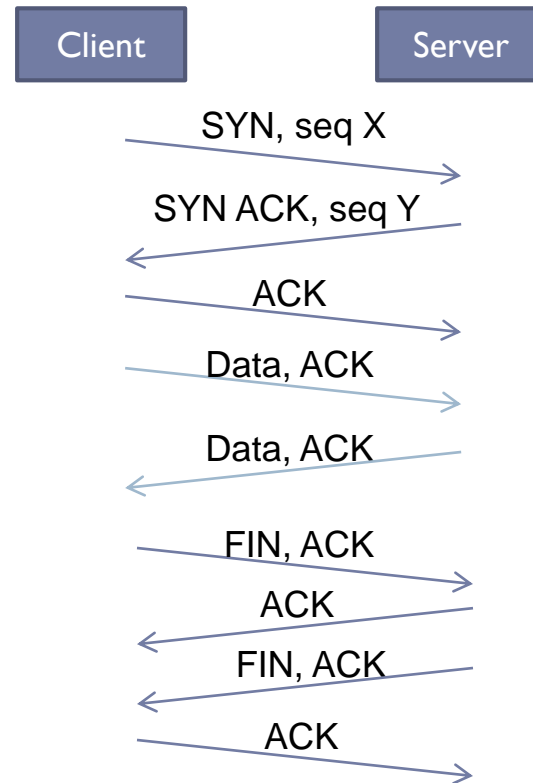


ccTLD DNSSEC Status on 2006-01-01



TCP kapcsolat (emlékeztető)

- ▶ SYN a kapcsolat indításához
 - ▶ Kezdeti sorszám (SEQ) inicializálás
 - ▶ Mindkét fél kitalál I-I -et
- ▶ ACK a nyugtázáshoz
 - ▶ Sorszám nyugtázás
- ▶ FIN az adás végére
 - ▶ Bárki kezdeményezheti
- ▶ Ha a sorszám nem stimmel (ablak) akkor az IP csomag nem a kapcsolathoz tartozik!
 - ▶ Védelem a kapcsolatnak



TCP viszonyrablás (session hijacking)

- ▶ **Beavatkozás egy már meglévő TCP kommunikációba**
 - ▶ Man-in-the-Middle technikák felhasználásával megoldható
 - ▶ Vak viszonyrablás távolról
 - ▶ Az egyik fél kiüthető, ha a küldött sorszám helyes
 - ▶ Sorszám találgatás
 - Néha nem teljesen véletlen
 - Win98: SEQ az aktuális időből
 - Kis ugrás az előző SEQ értékhez
 - IP ID használata (globális számláló)
 - ▶ Hamisított IP címmel csak egy irányban működik

TCP SYN támadás

- ▶ SYN elárasztásos DoS (SYN flooding)
 - ▶ SYN kérelmek küldése hamis (spoofed) IP címről
 - ▶ A szerver helyet foglal a kapcsolatnak (backlog)
 - ▶ A kapcsolat félig nyitott állapotba kerül (half open state)
 - ▶ A támadó sohasem nyugtázza a választ
 - ▶ Hamis IP esetén nem is tudja megtenni
 - ▶ A szervernél lévő memória tár véges (128, 1024, ...), A bejegyzések ideiglenesek, de percekre maradnak (ismétlések a feltételezett hiba miatt)
 - ▶ Amikor a memóriaterület betelik, a szerver nem tud több kapcsolatot fogadni
 - ▶ Sikeres támadás esetén nem senki sem tud TCP kapcsolatot kezdeményezni a szerverhez

- ▶ A hamis TCP SYN folyamnak nem is kell túl gyorsnak lennie

- ▶ **Megoldás**
 - ▶ Túlméretezés / TCP SYN proxy
 - ▶ SYN Cookie

SYN Cookies

Normál esetben

- ▶ A --- SYN ----> B
Állapot tárolás, kapcsolat
feljegyzése, várakozás az ACK
csomagra
- ▶ A <- SYN/ACK – B
Kapcsolat felépült
- ▶ A --- ACK ----> B
Kapcsolat felépült

SYN Cookies használata

- ▶ A --- SYN ----> B
Kapcsolat információ a Cookie-
ban
- ▶ A <- SYN/ACK – B
+ Cookie
Kapcsolat felépült
- ▶ A --- ACK ----> B
+ Cookie
Kapcsolat információ a
Cookie-ban

TCP SYN cookies

- ▶ TCP SYN cookie készítése (D. J. Bernstein)
 - ▶ Cél, hogy a SYN ACK állapotra emlékezzen a szerver, de ne tároljon semmit maga
 - ▶ A cookie-t visszaküldi a kliensnek, aki a kapcsolat nyugtázásánál újraküldi
 - ▶ TCP kompatibilis
 - ▶ Nincs szükség új TCP üzenetre, nincs szükség módosításra a kliensben
 - A kliensnek vissza kell küldenie az üzenetet akkor is, ha nem ismeri a cookie-t
- ▶ Cookies tárolása a sorszám helyén (SEQ)
 - ▶ 5 bit: Timestamp - $t \bmod 32$, t az idő számláló, 64 másodpercenként nő
 - ▶ 3 bit: MSS index - A leggyakoribb 8 Maximum Segment Size
 - ▶ 24 bit: Hitelesítés - MD5 és egy időfüggő kulcs
 - ▶ Bemenetek: SRC IP addr, port, DST IP addr, port, t + kulcs
- ▶ SYN cookie működés
 - ▶ Van hátrány is
 - ▶ Kliens által kezdeményezett TCP opciókat nem tud tárolni, így néhány TCP funkció nem működik (pl. large windows)
 - ▶ Nincs SYN-ACK újraküldés
 - ▶ Csak szükség esetén kell használni!