Hálózatok biztonsága 2019 nappali

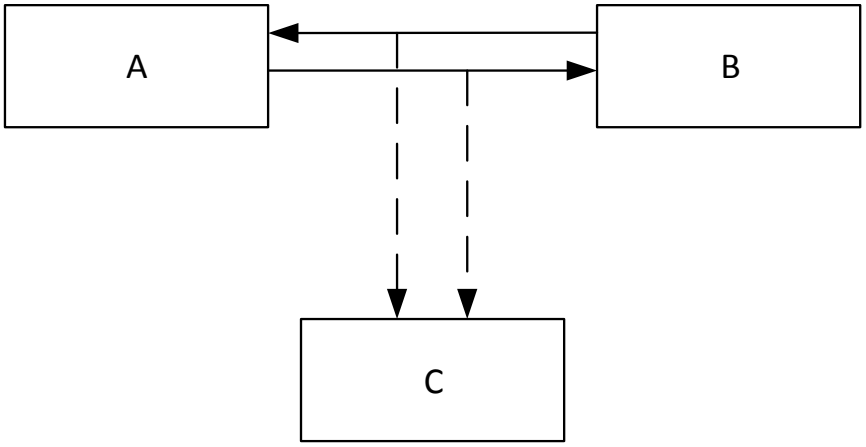
Dr. Répás Sándor

Támadások csoportosítása

- Passzív támadások
- Aktív támadások
- Csomag szintű támadások
  - IP spoofing
  - Smurf
  - SYN flood
  - Xmas, Ymas
- Hálózati szintű támadások
  - MAC flooding
  - ARP poisoning
  - ICMP redirect
  - Source IP route
  - DNS cache poisoning
- Social engineering támadások
  - DNS átregisztráció
  - Jelszó megkérdezés
  - Gyenge jelszavak

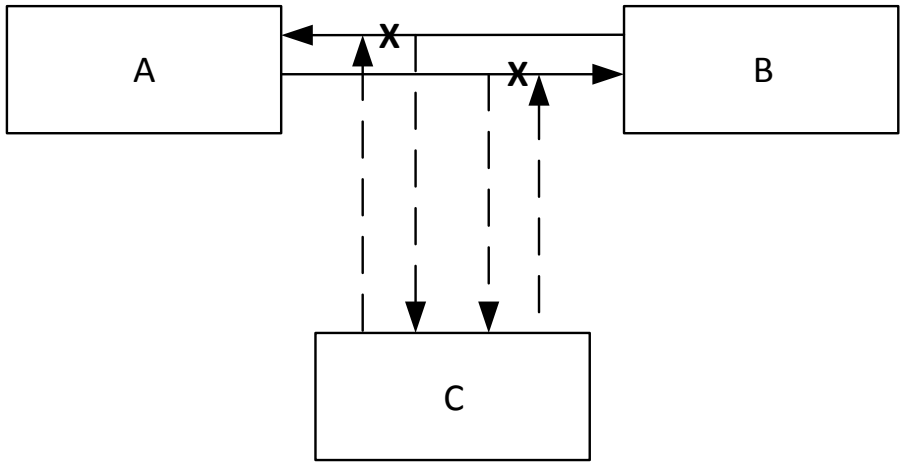
Passzív támadások

- Információ megszerzésére irányuló lehallgatás (evesdropping, wiretapping)
- Támadó nem módosítja az átviteli csatorna tartalmát
- Nagyon nehéz a detektálása
- Fontos kérdés: ki fér hozzá az átviteli közeghez?



Aktív támadások

- Támadó forgalmaz a csatornán
- Módszerek
  - Üzenetmódosítás
  - Megszemélyesítés
  - Visszajátszás
  - Szolgáltatás megtagadás

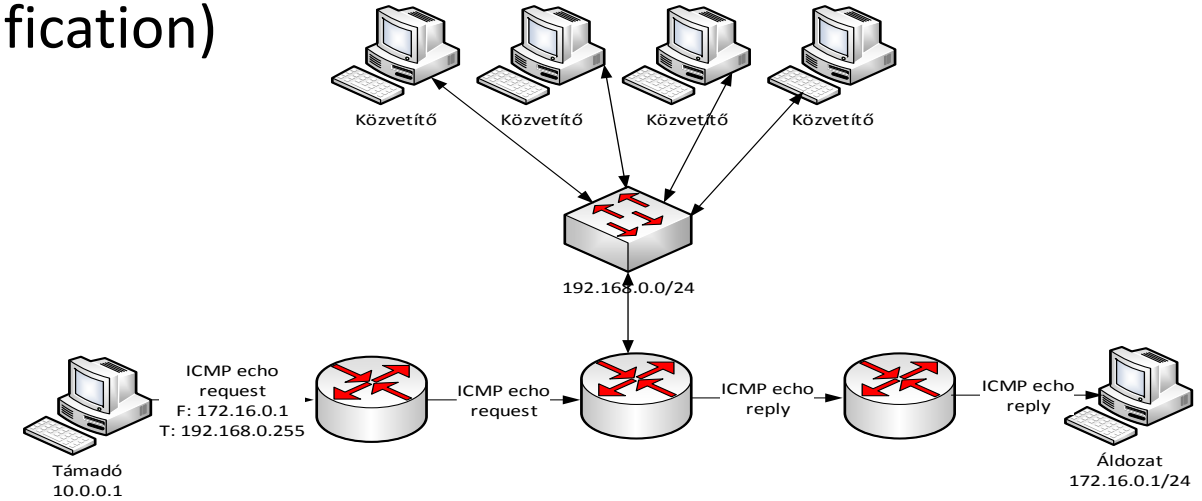


IP spoofing

- IP cím hamisítása
- Önmagában nem támadás, más támadásokhoz szükséges
- Ha mindenki betartaná a szabályokat, helyesen konfigurálna, nem/vagy nehezen megoldható lenne
- Jellemző célok:
  - IP címmel azonosított hoszt esetén jogosulatlan elérés
  - Szolgáltatás megtagadás (DoS/DDoS támadás)

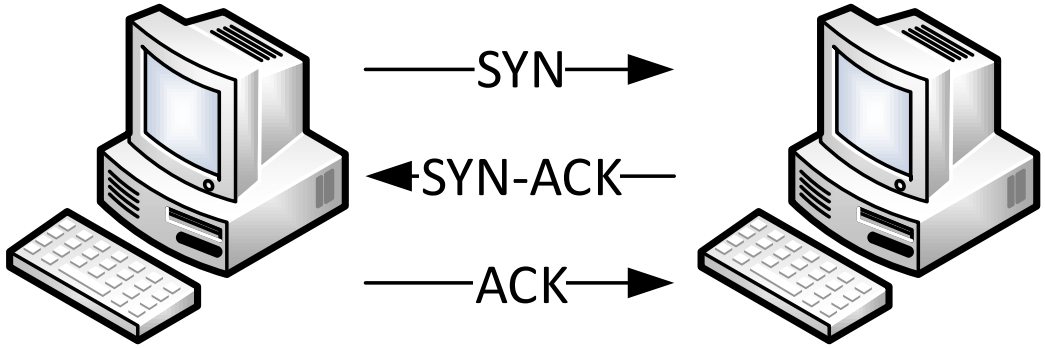
Smurf attack

- DoS támadás
- A támadó ICMP echo request (ping) üzeneteket küld
  - Forrás címnek az áldozat címét hamisítja
  - Célcímként egy broadcast címet ad meg
  - A közvetítők is „rosszul” járnak
  - Erősítés (amplification)



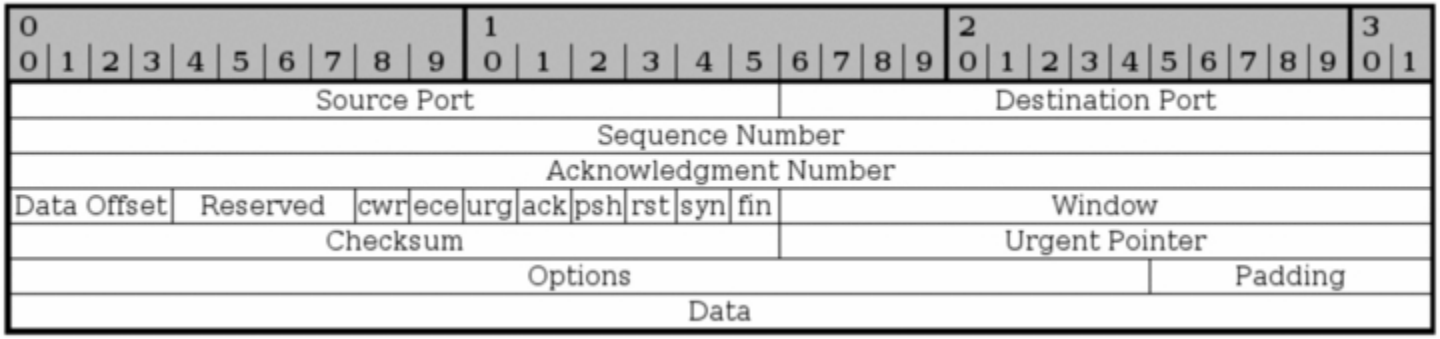
SYN flood

- DoS támadás
- TCP kapcsolatfelépítés 3 utas kézfogással
- A SYN érkezésekor struktúrát foglal le a kapcsolatot fogadó
- Sok SYN telíti a rendelkezésre álló memóriát
- Védekezés: mikrostruktúra, vagy SYN cookie (sorszám hash segítségével)



Xmas, Ymas

- CWR és ECE bit
- Eredetileg (RFC-3168) az ECN (Explicit Congestion Notification) mechanizmus céljára
- Korábbi TCP implementációk 0 értéket várnak
- 0-ától eltérő bitekkel a támadó információt szerezhet a TCP implementációról



MAC flooding

- Ethernet switch normál működés:
  - Beérkező unicast keretet csak arra a portra továbbít, ahol az adott hoszt található
    - Ha nem tudja, mely porton van, minden portra továbbítja
  - Ehhez táblázatot vezet, a beérkező keretek forrás címe és portja alapján
  - Ha a táblázat megtelik, akkor abból a korábbi adatokat eldobja
- Támadás:
  - Táblázat megtelítése, rengeteg hamisított forrás MAC című kerettel
  - Így minden keret minden portra kiküldésre kerül
    - Hálózat lassul
    - Forgalom lehallgatható

ARP poisoning

- IP címekhez fizikai (MAC) cím rendelése
- Támadás:
  - Hamis ARP válaszok küldése, melyben a megadott IP címhez saját MAC címét tünteti fel
  - Forgalom lehallgatható, eltéríthető

ICMP redirect

- ICMP Type 5
- A host értesítésére használható, hogy az elérni kívánt cím felé létezik egy (jobb) másik útvonal
- Az átjáró küldeti vissza a csomag küldőjének
- DoS támadás, csomagok eltérítése (lehallgatás), IP spoofing
- Védekezés:
  - Az elfogadása letiltható az operációs rendszerekben

IP source route

- Loose Source and Record Route (LSRR), IP option 3
- Strict Source and Record Route (SSRR), IP option 9
- A küldő host tudja megmondani, hogy a csomag milyen irányban legyen továbbítva
- Privát IP című hálózatok is elérhetőek az internet irányából
- Védekezés:
  - Az elfogadása letiltható a routereken

DNS cache poisoning
DNS spooofing

- A DNS szerverek cacheben tárolják a korábbi névfeloldások eredményeit
- Query:
  - UDP protokoll, src port: 53
  - 16 bit query ID, azonosítja a kérést (választ)
- Támadás:
  - Sok értelmetlen kérés küldése
  - Sok „válasz” küldése a hamisított IP címmel (hosszú TTL)
  - Pl: adathalászat, panki oldalak hamisítása
- Védekezés:
  - UDP source port randomization (UDP SPR)
  - Query ID randomiztaion

Social engineering

- Domain átregisztráció
- Jelszó megkérdezés
- Gyenge jelszavak kitalálása
- Védekezés:
  - Tudatossági képzés
  - Szabályzatok és oktatásuk
  - Házirendek

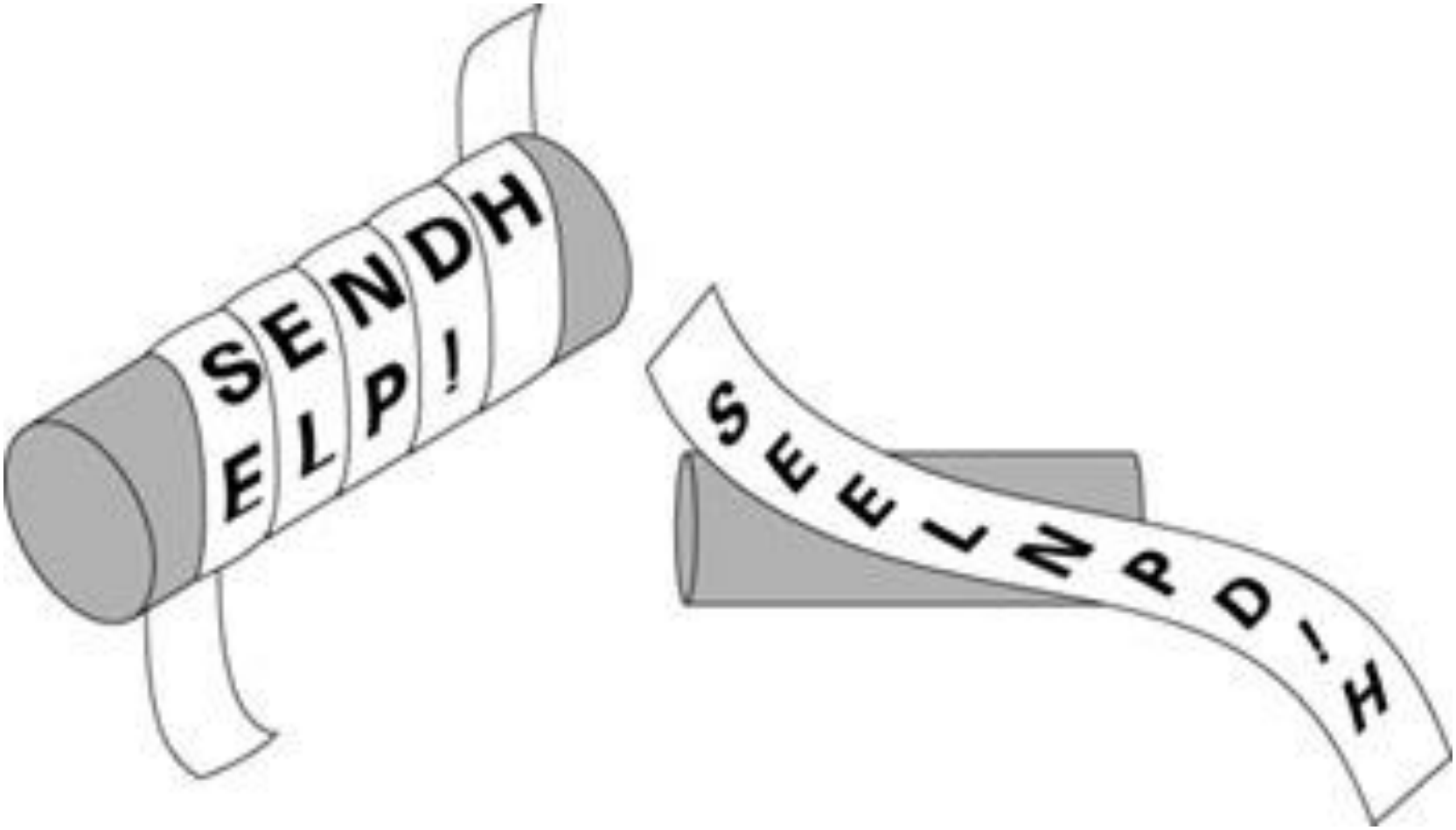
IFMMP

?????

Scytale

- Eredetileg a spártaiak használták katonai célokra
- A kutatások szerint feltalálója Archilochus költő ie. VII. században
- Rúdra tekert szíj belső oldalára írt üzenet
- Szíjat futárral elküldték a címzettnek
- Dekódolásához ugyanolyan vastag bot
- Transzpozíciós kódolás

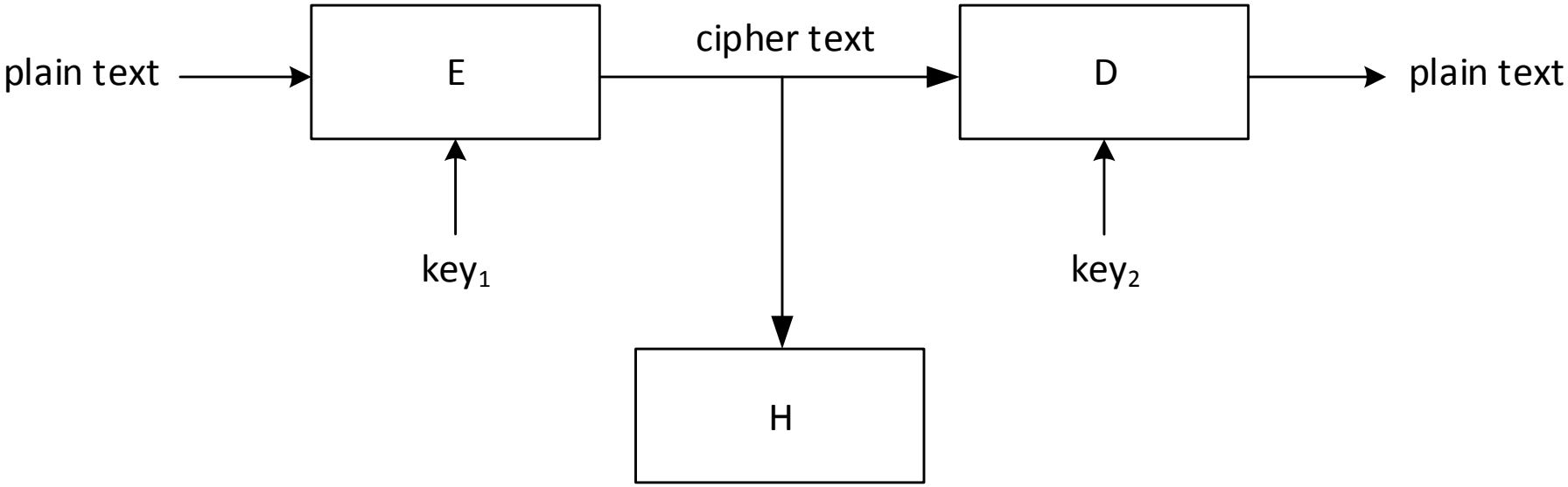
Scytale



Kriptológia

- Titkos kommunikációval foglalkozó tudomány
- Két fő ága:
  - Kriptográfia: titkosítás
  - Kriptoanalízis: titok jogosulatlan megfejtése
- Gyakorlati titkosság: az információ korábban váljon értéktelenné, mint a kor technikai színvonalán, a megfejtése

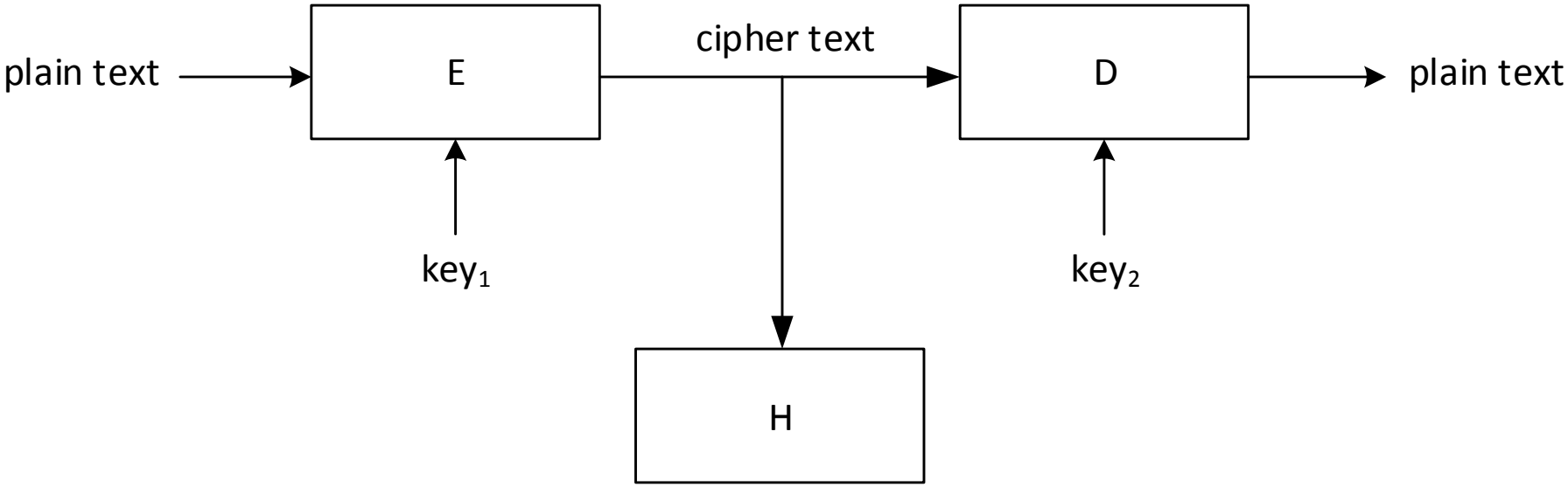
Titkosítás



One time pad (OTP)

- Véletlen átkulcsolásnak/Vernam cipher
- 1917 Gilbert Vernam (1890-1960)
- Kulcs:
  - Hossza megegyezik a kódolandó szöveggel
  - Minden esetben véletlenül generált
  - Feltörhetetlen
  - Gyakorlatban nem alkalmazható:
    - Kulcsgenerálás
    - Kulcs továbbítása

Titkosítás



Titkosítás

- key_1=key_2?
  - Szimmetrikus kulcsú titkosítás
  - Nyilvános kulcsú titkosítás
- Alapvetően
  - Transzpozíció (permutáció)
  - Helyettesítés
- Kulcskezelés
- Kulcscsere

Szimmetrikus kulcsú algoritmusok

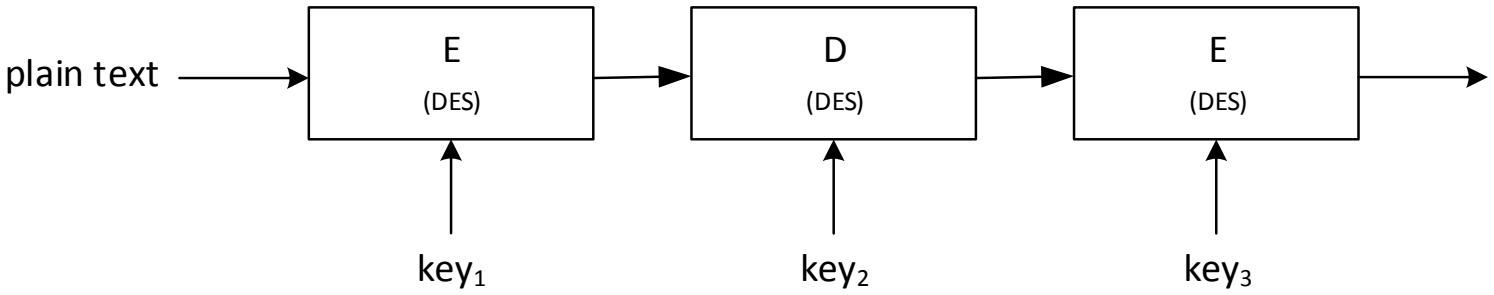
- (Titkos kulcsú blokkrejtjelezők)
- $key_1 = key_2$
- *k* bit hosszú kulcs
- Nyílt üzenetet *n* bit hosszúságú blokkokra
  - Csak n egész számú többszörösével megegyező hosszúságú nyílt üzenet titkosítása
  - Szöveg kiegészítése a megfelelő hosszra (padding)
- Probléma: A titkosító kulcs eljuttatása a címzett(ek)hez
- Ismertebb algoritmusok:
  - DES
  - 3DES
  - AES

DES

- Data Encryption Standard
- IBM 1970-es évek
- Blokkméret 64 bit
- Kulcsméret 56 bit (eredeti terv 128 bit, de NSA)
- Nem törhető fel, de:
  - Rövid kulcsméret
  - Mai technológiával kimerítő kulcskeresés hamar elvégezhető (brute force)

3DES

- Triple Data Encryption Standard
- Cél: Kulcshossz növelése
- Kompatibilitás egyszerű megőrzése a DES-re képes eszközökkel
- E-D-E, vagy D-E-D konfiguráció
- $key_1=key_2=key_3$: Normál DES
- key_1, key_2 és key_3 eltér: 3DES 3*56=168 bites kulcs



AES (Rijndael)

- Advanced Encription Standard
- National Institute for Standards and Technolgy (NIST) 1997-es projektje a DES lecserélésére
- 21 nevezés a pályázatra, 15-öt elfogadtak
- 5-öt választottak:
  - MARS
  - RC6
  - RIJNDAEL
  - SERPENT
  - TWOFISH
- RIJNDAEL győzött

AES (Rijndael)

- Blokk és kulcsméret:
  - 128 bit
  - 192 bit
  - 256 bit
- Hardveres támogatás:
  - Korszerűbb intel mikroprocesszorok AES-NI utasításkészlet
  - AMD esetén AES utasításkészlet
  - SoC-okban: Security System, Security Processor, vagy Crypto Engine

Blokkrejtjelezési módok

- Electronic Codebook (ECB)
  - Bemenet *n* bites blokkokra bontása
  - Blokkok külön-külön rejtjelezve
  - Adott kulcs mellett adott nyílt szöveg blokkhoz egyértelműen tartozik a titkosított párja:
    - Könnyen támadható
    - Blokkok beszúrhatóak, törölhetőek, sorrendjük felcserélhető
- Cipher Block Chaining (CBC)
  - Küldő a rejtjelezett blokkot megőrzi, és rejtjelezés előtt bitenkénti kizáró vagy művelettel hozzáadja a következő rejtjelezendő blokkhoz
  - Első blokkhoz az Inititalization Vectort (IV) adja hozzá
  - Láncolat képződik
  - Sérülés? Dekódolás?

Lenyomatképző algoritmusok

- Hash függvények célja a bemeneti szövegre (vagy egyéb információra) jellemző kimenet létrehozása („újlenyomat”)
- Szempontok:
  - Egyirányú (lenyomatból sosem állítható elő az algoritmus bemenete)
  - Nehéz legyen olyan szöveget előállítani, ami egy előre megadott újlenyomatot (DIGEST) eredményez (születésnap paradoxon)
    - Könnyen lehetne szöveget hamisítani meglévő aláíráshoz
  - Viszonylag rövid legyen a generált lenyomat
- MD5
- SHA1, SHA2, SHA3

MD5

- Message Digest 5 (MD5)
- Az MD4 javítása
- 128 bites lenyomat
  - Ez ma már túl rövid a születésnap paradoxonon alapuló támadásoknak
- Használata nem ajánlott, de számos esetben előfordul (Pl sok tanúsítványban is)

SHA

- Secure Hash Algorithm (SHA)
- SHA-1
  - 160 bites lenyomatot képez
  - NSA tervezte
  - 2005 óta nem tartják biztonságosnak
  - 2017-ben publikáltak azonos lenyomattal rendelkező PDF állományt
  - Alkalmazása nem ajánlott. Több rendszer nem fogadja el biztonságosnak.
- SHA-2
  - NSA tervezte
  - Lényegesen eltér az SHA-1-től, de más problémákkal rendelkezik
  - SHA-224
  - SHA-256
  - SHA-384
  - SHA-512(/224-256)

Üzenethitelesítés

- Címzett biztos lehessen:
  - Üzenet valóban attól származik, akinek tulajdonítja
  - Üzenetet pontosan az, amit a feladója küldött
- CBC-MAC
  - Utolsó blokk a MAC
- HMAC
  - Valamely lenyomatképző függvény
  - HMAC-MD5
  - HMAC-SHA1

Nyilvános kulcsú algoritmusok

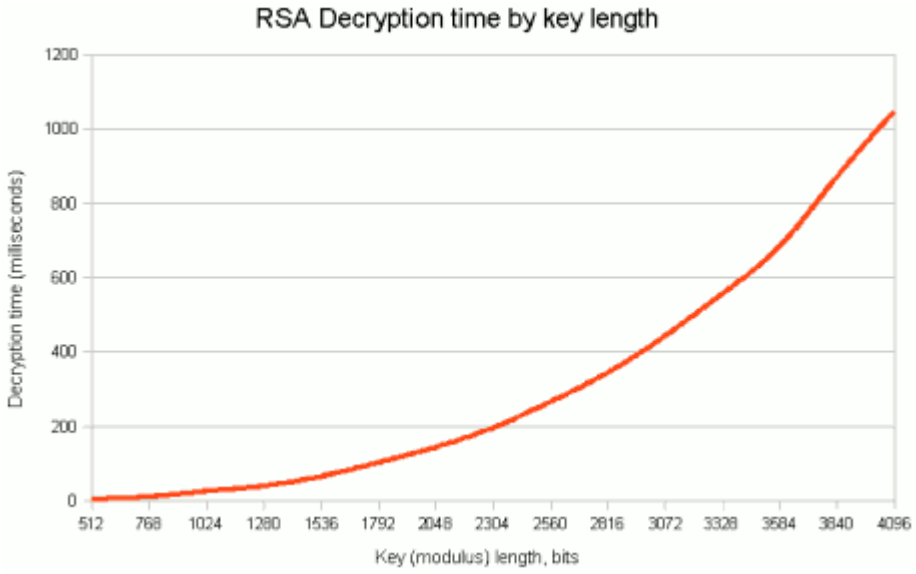
- $key_1 <> key_2$
- Amit az egyik kulccsal elkódolunk, az a másik kulccsal dekódolható
- Az egyik kulcsot titokban tartjuk: privát kulcs
- A másik kulcsot nyilvánosságra hozzuk: nyilvános kulcs
- RSA
- DSA
- EC

RSA

- 1976. Ron **R**ivest, Adi **S**amir, Leonard **A**dleman (RSA)
- 2000. szeptember 20-án lejárt a szabadalmi védelme
- Alapja:
  - Nagy számok faktorizációjának problémája:
    - Egy kellően nagy számról nehéz megállapítani annak prímtényezőit.
    - Jelenleg nem ismerünk az egész számok prímtényezős felbontására hatékony algoritmust
    - Ha egy szám két igen nagy prímszám szorzata, akkor annak prímtényezős felbontása nagyon gyors számítógépekkel is nagyon sokáig tart.
- A legelterjedtebb nyilvános kulcsú algoritmus
- 1994. Peter Shor: egy kvantumszámítógép elvileg végre tudja hajtani a faktorizációt polinom időn belül
- Ajánlott kulcshossz legalább 2048 bit:
  - Rövidebb kulcsok már nem biztonságosak
    - 2013 júliustól Google nem fogadja el biztonságosnak az 1024 bites, vagy rövidebb kulcsokat
  - Hosszabb kulcsoknál viszont problémák léphetnek fel
    - Eszköz kompatibilitás
    - Dekódolási sebesség

RSA dekódolás

- A kulcshossz duplázásával a dekódolási idő 6-7-szeresére nő
- 2GHz Pentium alapú számítógép dekódolási ideje:



Forrás: https://www.javamex.com/tutorials/cryptography/rsa_key_length.shtml

DSA

- Digital Signature Standard (DSS)
  - NIST FIPS 186-(1,2,3,4)
- Digital Signature Algorithm (DSA)
- Célja nem a titkosítás, hanem a digitális aláírás
- Sok helyen az RSA helyett használják (Pl. SSH)

Algoritmikus támadások

1. Rejtett szövegű támadás. Ez a módszer ugyanazon kulccsal titkosított rejtett szövegű üzeneteket használ fel. (ciphertext only attack)
2. Ismert nyílt szövegű támadás. Ismert, összetartozó nyílt szöveg – rejtett szöveg párokat használ fel. (known plain text attack)
3. Választott szövegű támadás. A támadónak lehetősége van megválasztani a nyílt szövegeket, amelyekhez tartozó rejtett szövegeket megkaphatja, vagy a rejtett szövegeket, amelyekhez való nyílt szövegeket megkaphatja. (chosen text attack)

- Az egyre nagyobb sorszámú támadás kategóriák egyre többet követelnek a támadótól

Kulcsmenedzsment

- A használt kulcsokat időnként cserélni kell:
  - Kommunikáció kezdetekor
  - Ne legyen túl sok azonos kulccsal titkosított szöveg
  - Kulcs kompromittálódik:
    - Kitudódás
    - Sérülés
- Kulcs archiválása
- Kulcsgenerálás:
  - Véletlen számok
- Kulcstárolás
- Kulcsok továbbítása

Digitális aláírás

- Letagadhatatlanság
- Sértetlenség
- Bizalmasságot nem biztosít!!!
- Aláírás folyamata:
  - Üzenet lenyomatának elkészítése
  - Lenyomat elkódolása küldő privát kulcsának segítségével
- Aláírás ellenőrzése:
  - Kapott üzenet lenyomatának elkészítése (aláírás nélkül)
  - Üzenettel érkezett aláírás elkódolása a feladó nyilvános kulcsának segítségével
  - Készített és kapott lenyomat összehasonlítása

Titkosított üzenet küldése

- Bizalmasság
- Sértetlenség?
- Titkosítás folyamata:
  - Szimmetrikus titkosításhoz kulcs generálása
  - Üzenet titkosítása szimmetrikus algoritmussal és a generált kulccsal
  - Szimmetrikus kulcs elkódolása címzett nyilvános kulcsával
  - Titkosított üzenet és a hozzá kapcsolódó titkosított szimmetrikus kulcs elküldése
- Üzenet visszafejtése:
  - Kapott üzenetben szereplő szimmetrikus titkosító kulcs dekódolása a címzett privát kulcsával
  - A kapott üzenet visszafejtése a szimmetrikus kulcs segítségével

Tanúsítvány

- Certificate
- Hogyan kezeljük a nyilvános kulcsokat?
- Honnan tudhatjuk, hogy kinek mi a nyilvános kulcsa?
- Honnan tudhatjuk, hogy a nyilvános kulcs tényleg azé, akit gondolunk?
- Mi történjen a kompromittálódott kulcsokkal?
- …

Ötlet

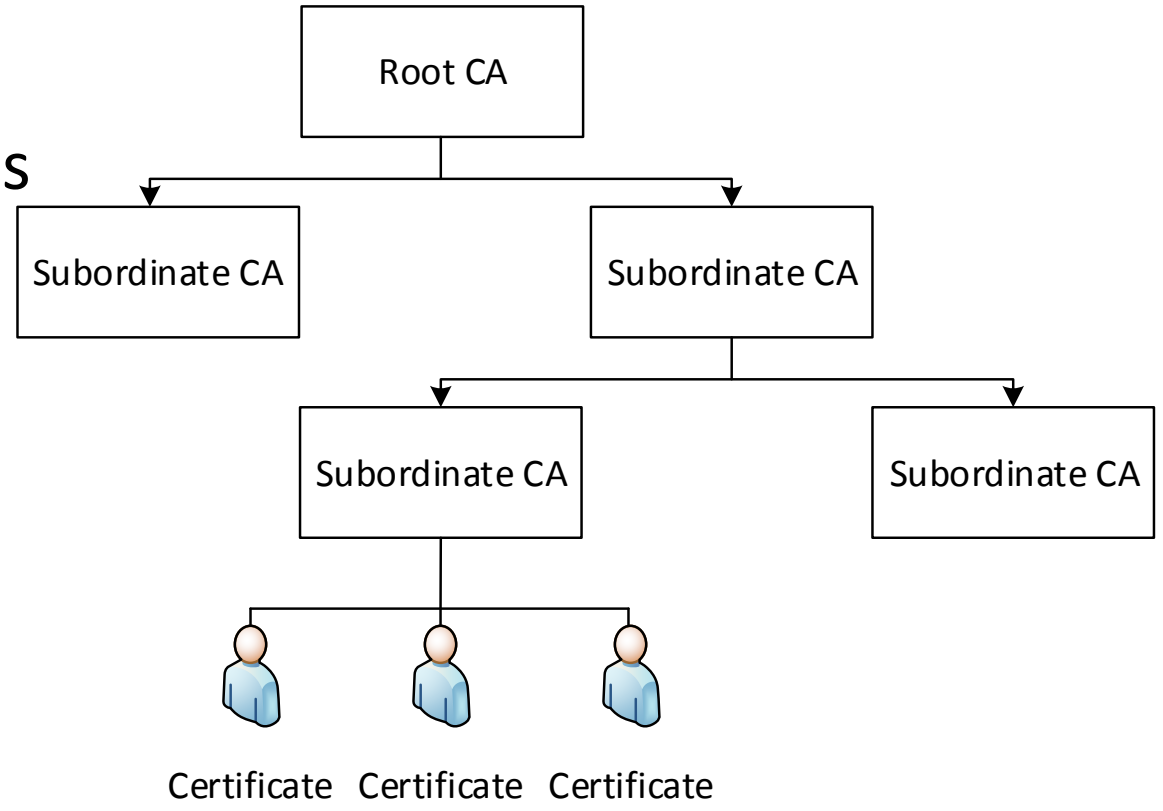
- Valakinek a kulcsában már megbízunk
- Az illető hitelesítse (írja alá) mások kulcsát (és a hozzá tartozó tulajdonságokat)→tanúsítvány
- Két elterjedt megoldás:
  - X.509
  - PGP

X.509

- Trusted root CA
  - Önaláírt tanúsítvány
  - Hosszú érvényesség
  - Az operációs rendszer/böngésző gyártó beépíti, de a felhasználó is telepíthet
- Subordinate CA
  - A felette lévő CA hitelesíti a tanúsítványát
  - Rövidebb, de még mindig hosszú érvényességi idő
  - (Azonos szinten is aláírhatják egymás tanúsítványát)
- Többszintű láncolat is kialakítható
- Az egyes CA-k különböző célokra oszthatnak tanúsítványt

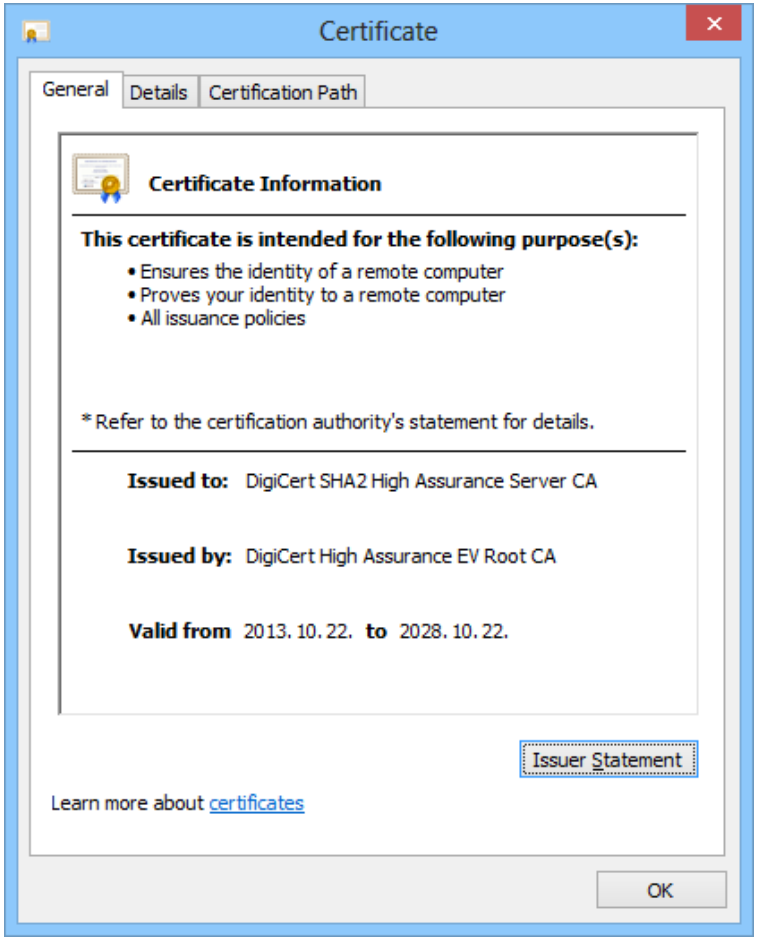
CA láncolat

- Root CA
- Subordinate/Intermediate CA
- Issuing CA
- Clients certificates



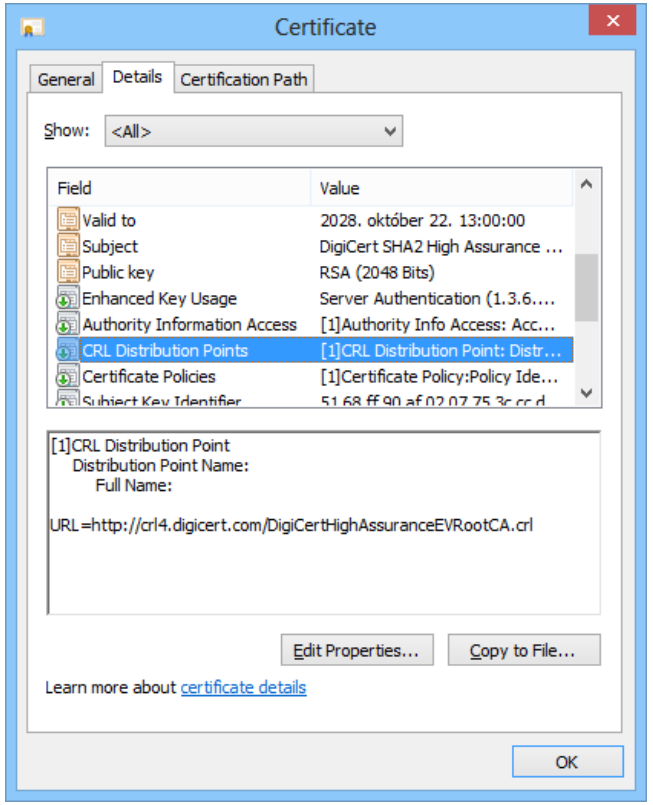
Tanúsítványok néhány tulajdonsága

- Sorozatszám
- Ki kapta
- Ki tanúsította
- Érvényesség kezdete
- Érvényesség vége
- Visszavonási lista elérhetősége
- Mire használható
- Verzió szám
- **A nyilvános kulcs**



CRL

- Certificate Revocation List (CRL)
- A kompromittálódott kulcsú tanúsítványokat vissza kell vonni
- Lista a visszavont tanúsítványokról:
  - Sorozatszámok
  - Általában HTTP URL
  - Természetesen digitálisan aláírva



PKI

- Public Key Infrastructure (PKI)
- Szerepkörök, eljárások, szabályzatok melyek a digitális tanúsítványok:
  - menedzseléséhez,
  - kiosztásához,
  - használatához,
  - tárolásához,
  - visszavonásához szükségesek
- Például:
  - CA szervezete (Pl dolgozók)
  - CA szabályzata
  - Tanúsítványok

PGP

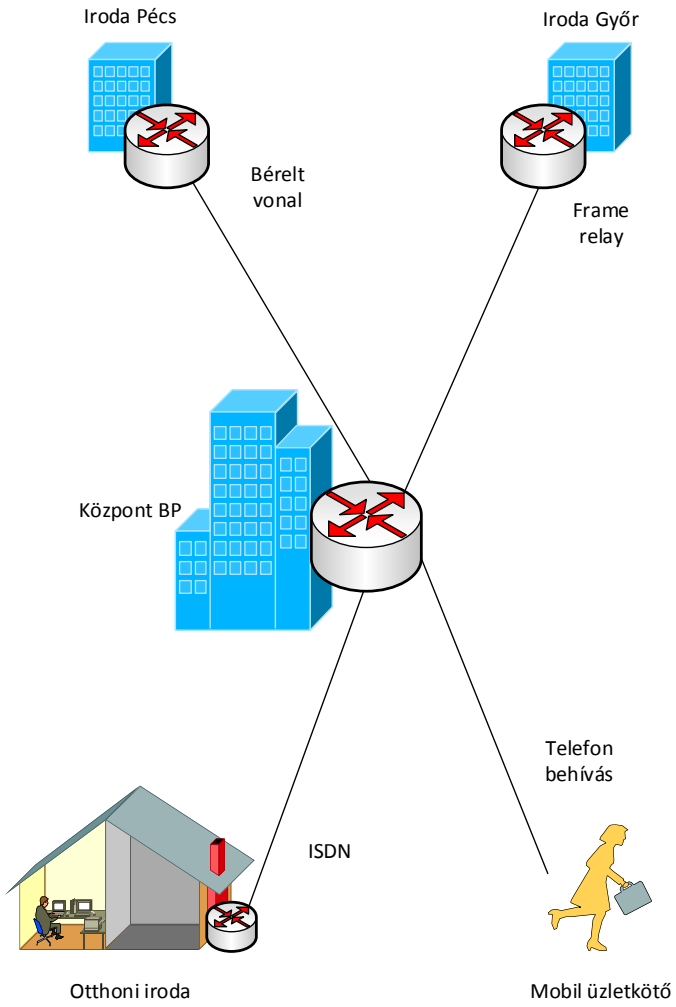
- Pretty Good Privacy (PGP)
- Első verzió: 1991. Philip R. Zimmermann
  - (1993 februárjában meggyanúsították az USA exportszabályainak megsértéséért)
  - 2010-ben a Symantec megvette a PGP-t
  - 1997 júliusban OpenPGP, jelenleg RFC 4880
  - 1997. szeptember 7-én a Free Software Foundation (FSF) kiadta saját OpenPGP kompatibilis programját: GNU Privacy Guard (GnuPG, GPG)
- Web of trust
  - Egymás tanúsítványait írhatják alá, hitelesíthetik

GnuPG

IP VPN

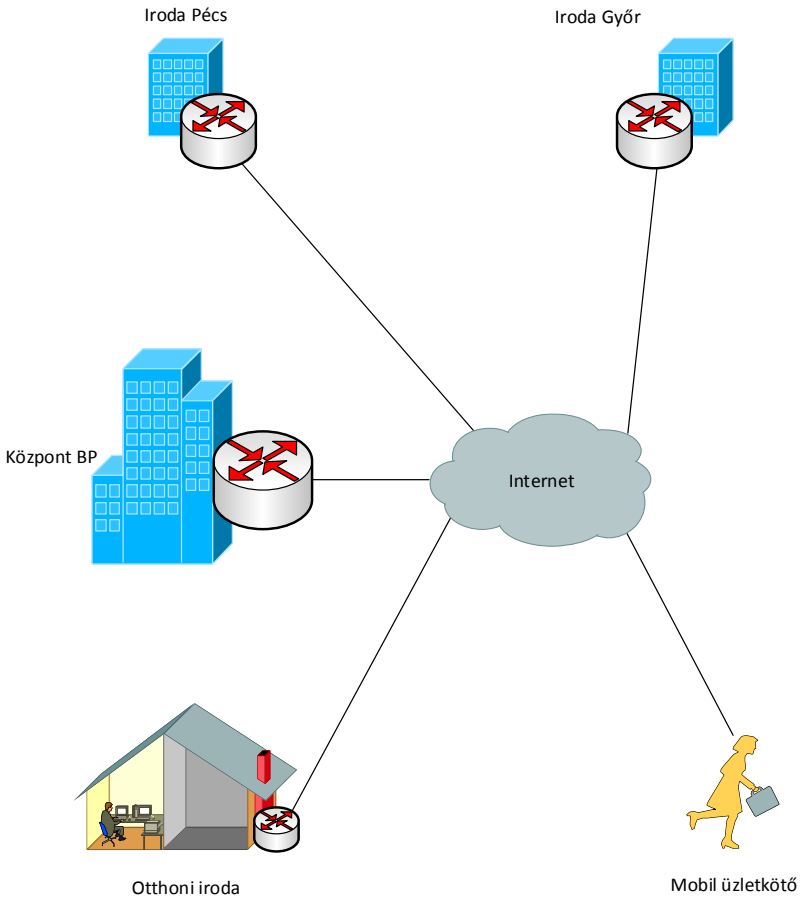
Hagyományos hálózat kialakítása

- Állandó sávszélesség
- Nehézkes kiépítés, bővítés
- Speciális eszközök
- Magas költségek



IP VPN hálózat kialakítása

- Virtual Private Network (VPN)
- Kommunikáció (titkosított) tunnelekben
- Folyamatosan változó sávszélesség
- Egyszerű, gyors kiépítés
- Alacsony költségek
- Egyszerű bővítés
- Site to Site, vagy Remote-Access VPN



Site to Site VPN

- A hagyományos WAN hálózatok továbbfejlődése
- Bérelt vonal, Frame Relay helyett
- A telephelyi LAN-ok közti kapcsolatot biztosító tunnelt egy hálózati eszköz (pl VPN router, tűzfal) építi ki
- A felhasználók számítógépei nem is „tudnak” a VPN igénybevételéről

Remote Access VPN

- A hagyományos betárcsázós, ISDN-es kapcsolatok helyett
- Egy felhasználó részére teszi lehetővé a távoli hálózathoz való csatlakozást
- A VPN kliens általában a felhasználó számítógépére kerül telepítésre és nem külön eszközön
- Általában a felhasználás időtartamára kerül csak kiépítésre a VPN csatorna

IP VPN protokollok

VPN Protokoll	Protokoll, port	Tulajdonság	Szabvány
PPTP	TCP 1723, GRE (IP 47)	Elterjedt, egyszerűen telepíthető, nem biztonságos, elavult.	RFC 2637
L2TP	UDP 1701	Nincs titkosítás	RFC 2661 (3931)
IPsec	UDP 500, 1701, 4500, ESP (IP 50), AH (IP 51)	Framework. „Pilótavizsga” Tanúsítvány és PSK is használható hitelesítésre. Mindkét irányú hitelesítés.	RFC 6071
L2TP/IPsec	UDP 500, 1701, 4500, IP protokoll 50	IPsec segítségével titkosított L2TP. „Egyszerű” konfigurálás, magas biztonság. Mindkét irányú hitelesítés.	RFC 3193
SSTP	TCP 443	SSL/TLS csatorna. Tűzfalakon egyszerűen átjut.	Microsoft
IKEv2	UDP 500	Security Association (SA) létrehozásához: titkosító algoritmus, kulcsok, egyéb paraméterek.	RFC 7296
OpenVPN	UDP 1194, TCP 443	TUN, vagy TAP működés. Tanúsítvány, PSK, felhasználónév/jelszó is használható hitelesítésre. Mindkét irányú hitelesítés. Nem egyszerű beállítás.	OpenVPN Inc.

IPsec

- Nyílt szabványok algoritmus független keretrendszere
- Hitelesítheti és védheti az IP csomagokat
- Biztosít:
  - Bizalmasságot
  - Integritást
  - Hitelesítést
  - Visszajátszás elleni védelmet

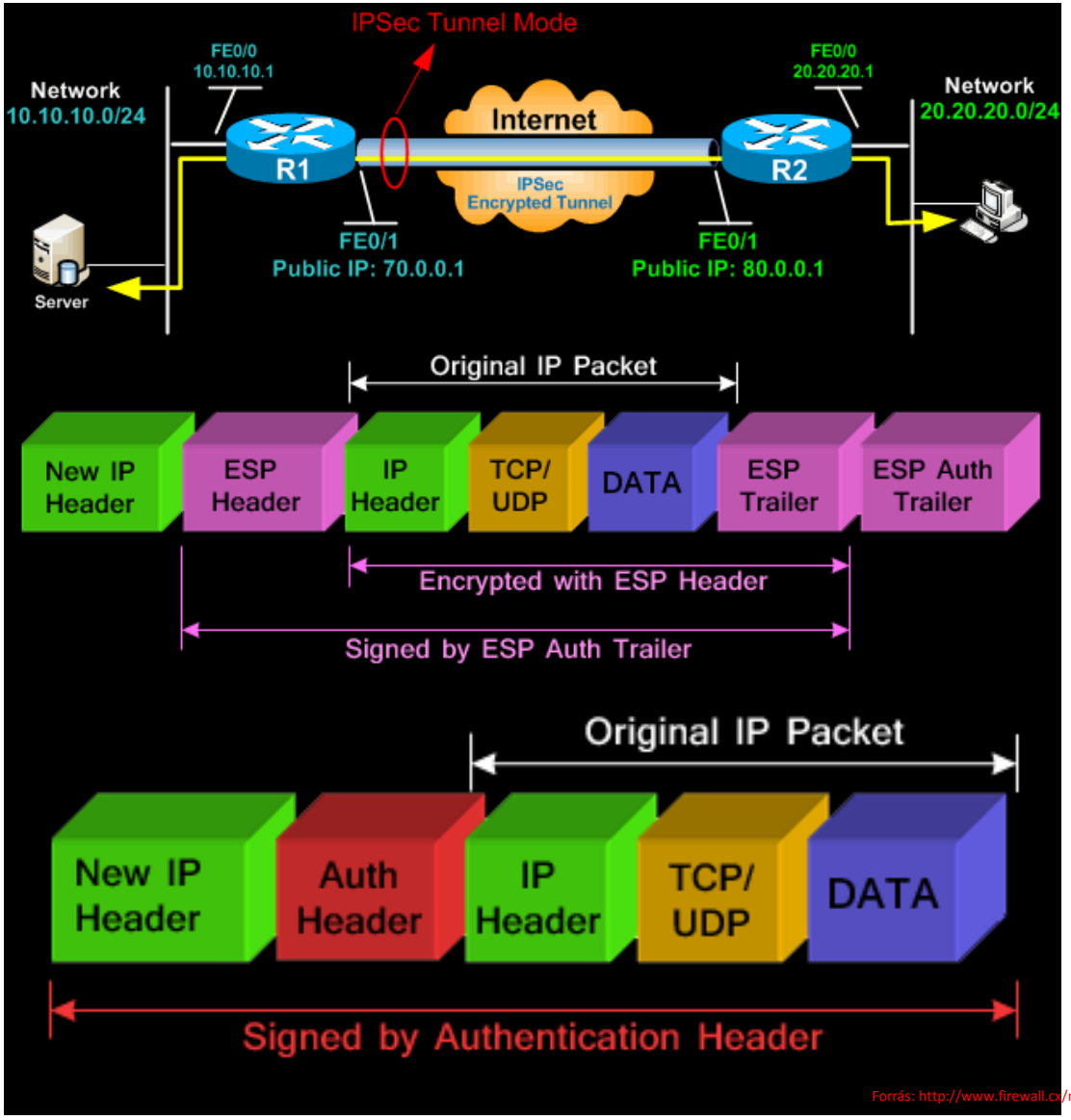
IPsec protokollok

- Authentication Header (AH)
  - Hitelesítés
  - Integritás
- Encapsulation Security Payload (ESP)
  - Titkosítás
  - Hitelesítés
  - Integritás

IPsec módok

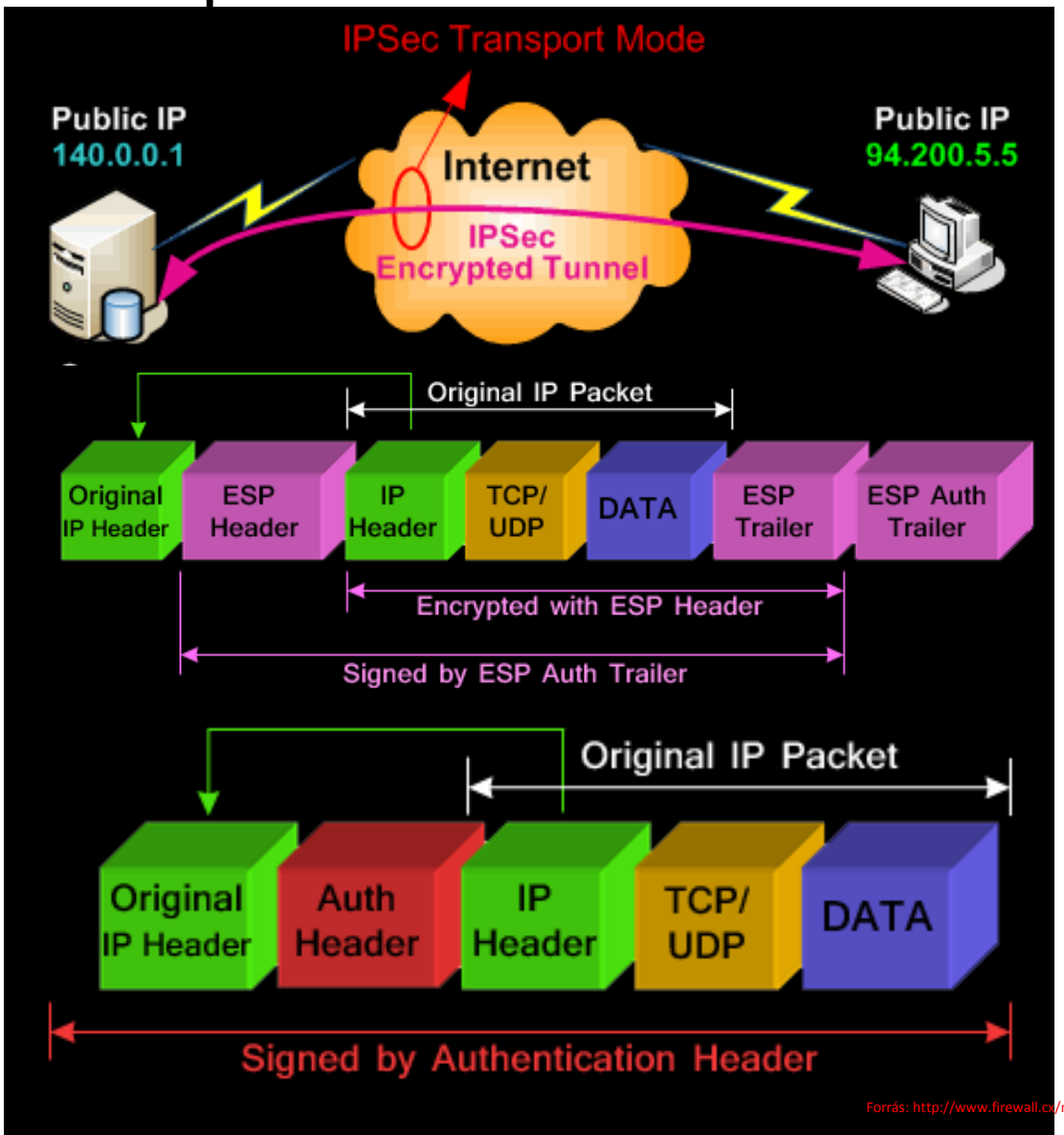
- Tunnel mód
- Transport mód

IPsec tunnel mód



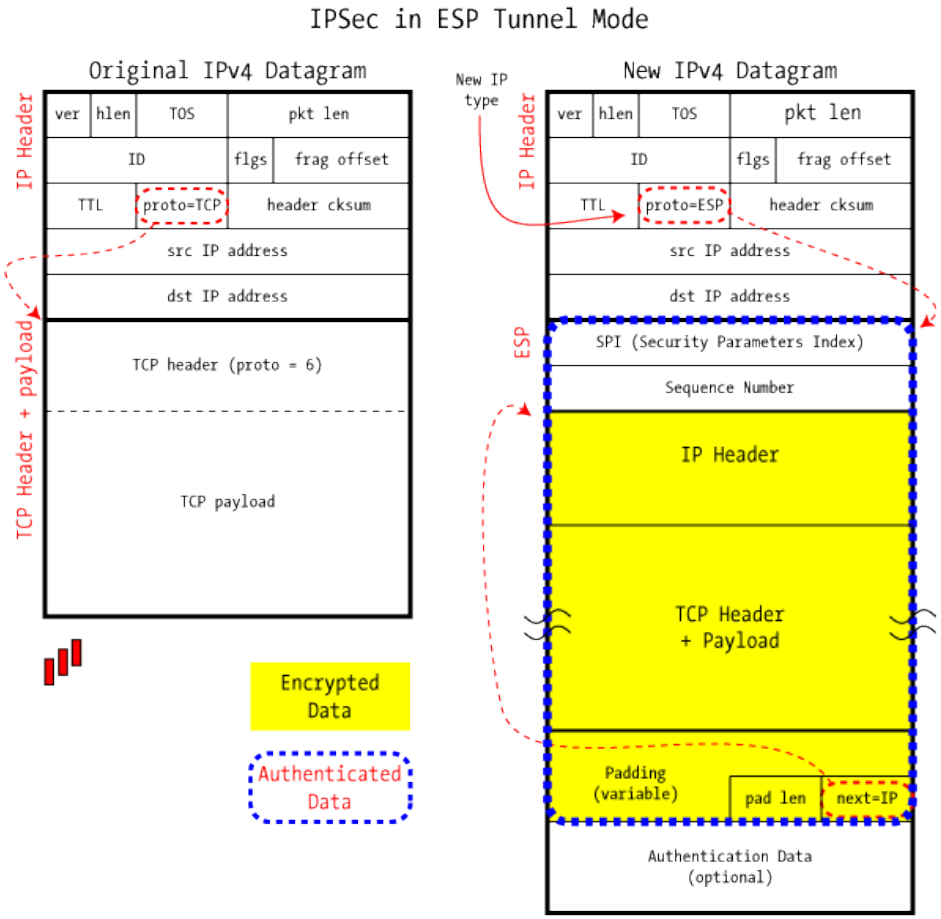
Forrás: http://www.firewall.cx/networking-topics/protocols/870-ipsec-modes.html

IPsec transport mód



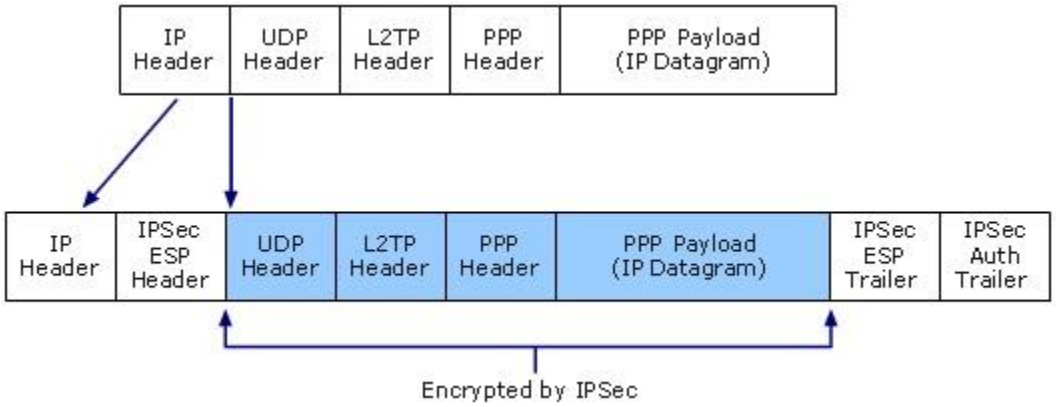
Forrás: http://www.firewall.cx/networking-topics/protocols/870-ipsec-modes.html

IPsec ESP tunnel mód fejléc



Forrás: http://www.unixwiz.net/techtips/iguide-ipsec.html

L2TP/IPsec fejléc



Hitelesítő eszközök

- Password
  - PAP (Password Authentication Protocol)
  - CHAP (Challange-Handshare Authentication Protocol) (MS-CHAP)
  - Preshared key
- One-Time Password (OTP):
  - HOTP (HMAC-based One-time Password)
  - TOTP (Time-based One-time Password)
  - OCRA (OCRA: OATH Challenge-Response Algorithm, Open Authentication)
  - (Software)
- Certificate:
  - File
  - Smartcard
  - USB Token
- EAP

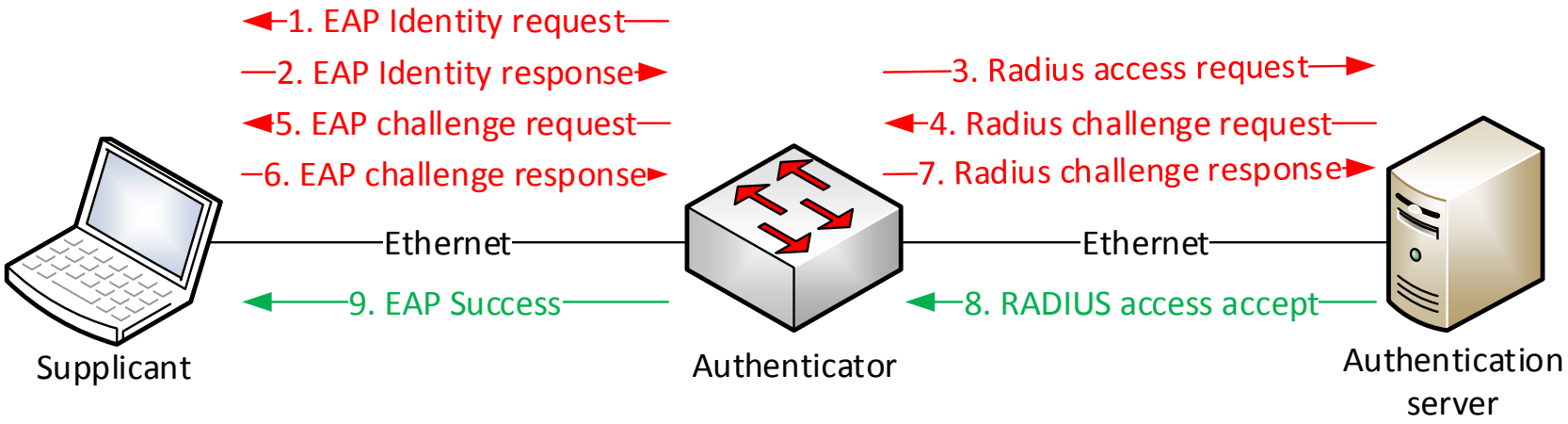
Extensible Authentication Protocol (EAP)

- PEAP (Protected EAP)
  - Szerver oldali tanúsítványokat használ. Védett tunnelben továbbítja az adatokat.
- EAP-MSCHAPv2
  - Szerver oldali tanúsítvány, míg a kliens hitelesítéséhez MSCHAPv2 protokoll.
- EAP-GTC (Generic Token Card)
  - Egyszer használatos jelszavakkal, titkosítatlan hitelesítés.
  - RFC 2284
- EAP-MD5
  - A jelszó MD5 lenyomatát ellenőrzi.
  - RFC 2284
- EAP-TLS (Transport Layer Security)
  - A felhasználók tanúsítvánnyal hitelesítik magukat.
  - RFC 5216
- EAP-TTLS (Tunneled Transport Layer Security)
  - A szerver tanúsítványt, míg a felhasználók jelszavakat alkalmaznak.
  - RFC 5281
- EAP-SIM (Subscriber Identity Module)
  - GSM SIM alapú hitelesítés. Hálózat is hitelesítve.
  - RFC 4186
- És még: EAP-AKA (RFC 4187), EAP-POTP (RFC 4793), EAP-TLV, ZLXEAP, EAP-FAST (RFC 4851), LEAP, …

Forrás: https://www.arubanetworks.com/techdocs/ArubaOS_63_Web_Help/Content/ArubaFrameStyles/802.1x/Overview_of_802_1x_Authe.htm

EAP – Radius

- Enterprise WiFi
  - WPA-Enterprise
  - WPA2-Enterprise
- 802.1X



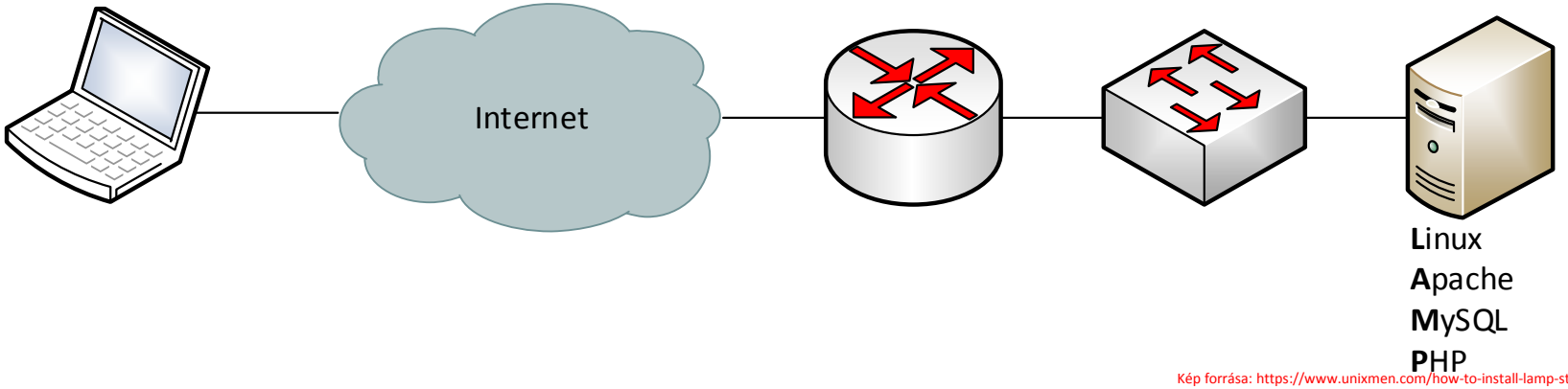
Multifaktoros authentikáció

- Erős hitelesítés
- Two Factor Authentication (2FA)
- Legalább kettő egyidejű alkalmazása a következőkből:
  - Tudok valamit
    - Jelszó
    - PIN kód
  - Rendelkezem valamivel
    - Tanúsítvány
    - Token
    - Mobil telefon
  - Van valamilyen tulajdonságom
    - Retina
    - Véna
    - Arc
    - Újlenyomat

Web alkalmazások biztonsága

LAMP architektúra

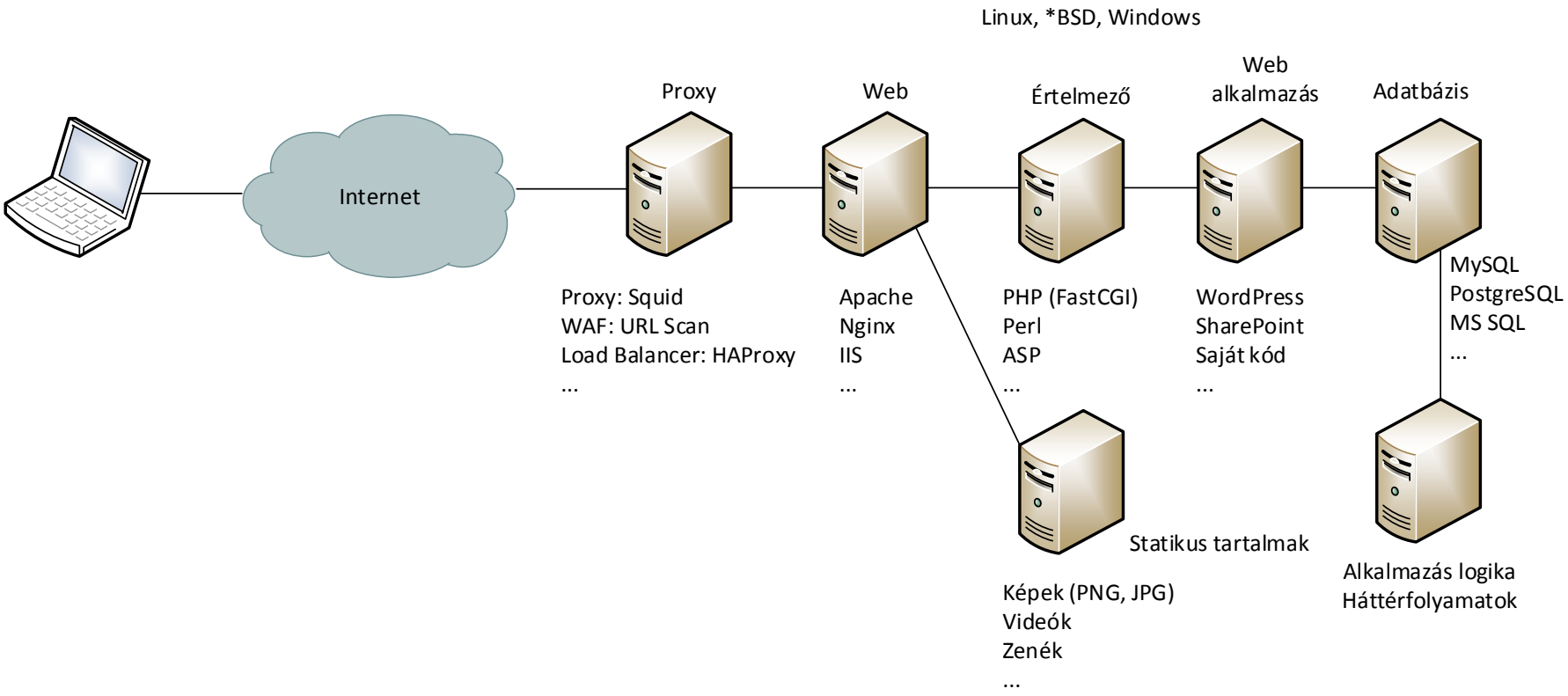
- Rengeteg webes szolgáltatás alapja
- Célpont lehet:
  - (Hálózati eszközök)
  - Linux
  - Apache
  - PHP (értelmező, feldolgozó)
  - **CMS (Content Manamenet System) és pluginjei**
  - Saját PHP kód
  - MySQL
- Természetesen az egyes komponensek külön gépeken is elhelyezhetőek



Kép forrása: https://www.unixmen.com/how-to-install-lamp-stack-on-mageia-5/

Web alkalmazás architektúra

- Ez csak egy példa! Sok eltérés lehetséges (Node.js, Ruby, …)
- Rengeteg komponens(réteg)→támadási lehetőségek



OWASP

- Open Web Application Security Project (OWASP)
- https://www.owasp.org
- 2001.12.1-e óta elérhető
- 2004.4.21-én alakult meg az USÁ-ban nonprofit szervezetként
- „OWASP is an open community dedicated to enabling organizations to conceive, develop, acquire, operate, and maintain applications that can be trusted.”

OWASP Top 10

- A WEB alkalmazások legkritikusabb biztonsági kockázatai
- Rendszeresen frissítésre kerül
- Biztonsági szakértők véleménye alapján kerül összeállításra
- „Adopting the OWASP Top 10 is perhaps the most effective first step towards changing the software development culture within your organization into one that produces secure code.”

OWASP Top 10 - 2017

- A1 Injection
- A2 Broken Authentication
- A3 Sensitive Data Exposure
- A4 XML External Entites
- A5 Broken Access Control
- A6 Security Misconfiguration
- A7 Cross Site Scripting (XSS)
- A8 Insecure Deserialization
- A9 Using Components with Known Vulnerabilities
- A10 Insufficient Logging & Monitoring

(https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf)

CVE

- Common Vulnerabilities and Exposures (CVE)
- Különböző szoftverek nyilvánosságra került sebezhetőségeit tartalmazza
  - Elnevezés
  - Azonosító
  - CVSS (súlyosság)
  - Érintett termék
  - Leírás
  - Következmény
  - Védekezési lehetőségek
  - Példák:
    - https://cve.mitre.org/
    - https://www.kb.cert.org/vuls/
    - https://www.cvedetails.com/
    - https://vuldb.com
    - http://www.cnnvd.org.cn/

CVSS

- Common Vulnerability Scoring System (CVSS)
  - https://www.first.org/cvss/
  - Szabad és nyílt szabvány a sebezhetőségek súlyosságának meghatározására
  - 0-10-es skála, 10 a legsúlyosabb
  - A jelenleg használt CVSSv3.0, 2015 júniusában jelent meg

SQL Injection

- Az egyik legelterjedtebb, legfontosabb támadás
- Egy SQL kód bejuttatási technológia
- Szinte minden oldalon van beviteli mező
  - Akár felhasználónév, jelszó megadásához
  - A támadó nem a kért adatokat adja meg, hanem, egy megfelelően formázott SQL statementet
- Védekezés
  - A beviteli mezőkben megadott értékek megfelelő ellenőrzése

SQL Injection példa

- 1=1 ☺
- Programozó kódja:

```
SELECT * FROM Users WHERE UserId = beviteli mező értéke;
```

- Támadás:
  - A beviteli mezőbe:
    - 105 OR 1=1
  - A végrehajtott kód:

```
SELECT * FROM Users WHERE UserId = 105 OR 1=1;
```

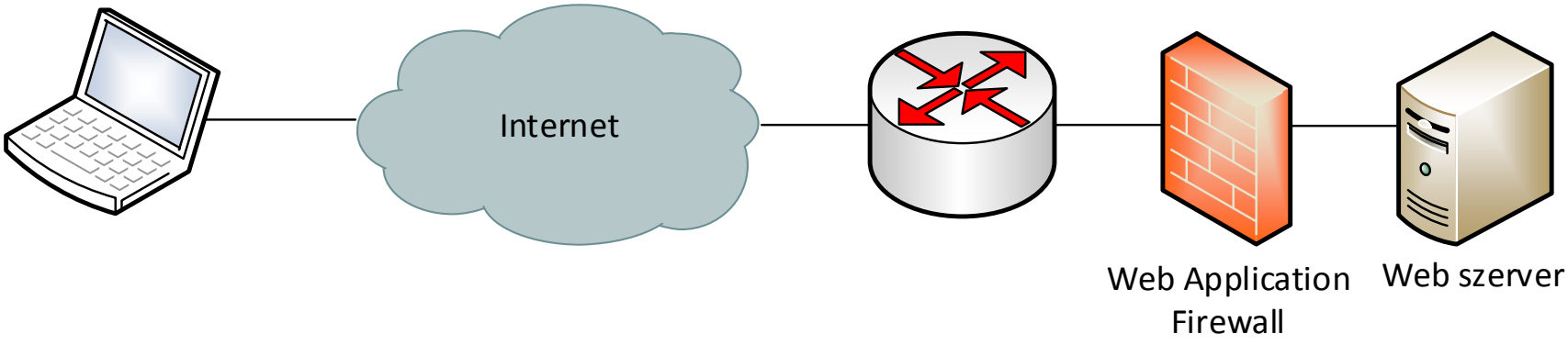
- Ez csak egy nagyon egyszerű példa!
- Próbáljuk ki: https://tech.io/playgrounds/154/sql-injection-demo/sql-injection

Web Application Firewall

- A WEB szerver felé és/vagy felől
  - Monitorozza,
  - Szűri,
  - Blokkolja a forgalmat.
- Típusai, néhány termékkel:
  - Szoftver
    - TrustWave Modsecurity (Apache, Nginx)
    - BitNinja WAF 2.0
    - Microsoft URLScan
    - (Akár azonos hoszton a webszerverrel)
  - Appliance
    - Fortinet Fortiweb
    - Barracuda Networks WAF
  - Felhős (Cloud)
    - Akamai Kona Site Defender
    - Amazon Web Services WAF
    - F5 Silverline WAF

Web Application Firewall

- Leginkább egy reverse proxyra hasonlít, amin mindenféle szabályok hozhatóak létre
- Megvédhet a programozói hibáktól, akár Zero day sebezhetőségek esetén is
- Kérdés, hogy a HTTPS-t hol végződtetjük
  - Bele kell „látnia” a forgalomba
  - Nagy terhelést okozhat a ki/be titkosítás
  - Csökkenhet a biztonság



HTTP

- HyperText Transfer Protocol (HTTP)
- Kérés-válasz alapú
- Állapot nélküli
- Plain-text
- HTTP/1.0 RFC 1945 (1996)
- HTTP/1.1 RFC 2616 (1999)
- HTTP/2.0 RFC 7540 (2015)
- TCP 80 port

HTTPS

- Hypertext Transfer Protocol Secure (HTTPS)
- Titkosított HTTP kapcsolat
  - SSL vagy TLS
  - Lehallgatás, közbeékelődés, egyéb támadások ellen
- TCP 443 port
- RFC 2818 - HTTP Over TLS (2000)

SSL/TLS

- Nagyon nem ajánlottak (biztonsági problémák):
  - SSL 1.0
  - SSL 2.0 (1995)
  - SSL 3.0 (1996)
- TLS 1.0 RFC 2246 (1999)
  - Kivezetése folyamatban
- TLS 1.1 RFC 4346 (2006)
  - CBC támadások elleni védelmek
- TLS 1.2 RFC 5246 (2008)
  - MD5 helyett SHA-1 és SHA-256, és más korszerűsítések
- TLS 1.3 RFC 8446 (2018)
  - Még csak korlátozott támogatása van
- Külön (TCP) porton „figyel” a szerver (80→443, 110→995), vagy parancs (pl: STARTTLS)
- Szerver oldalon (megbízható CA által aláírt) tanúsítvány
- Az adatátvitelhez szimmetrikus kulcsú titkosítás
  - Szimmetrikus kulcsot a kliens elküldi a szervernek annak privát kulcsával titkosítva (megszűnt)
  - vagy Diffie–Hellman algoritmussal megbeszélik (biztonságos, forward secrecy!) a kommunikáció elején

X.509 web szerver tanúsítvány

- A HTTPS-hez szükség van megbízhatónak tartott szerver tanúsítvány alkalmazására
- Típusok:
  - Single domain
  - Multiple domain (Subject Alternative Name, SAN)
  - Wildcard domain (*.domain)
- Generálhatunk magunknak (privát CA)
  - Intraneten megfelel, sőt bizonyos esetekben jobb is lehet
  - A gyökértanúsítványt telepíteni kell a kliensekre (Trusted root CA)
- Vehetünk Magyarországon vagy az EU-ban
  - Itthon csak kettő maradt:
    - Microsec Zrt. (https://www.microsec.hu/, https://e-szigno.hu)
    - NETLOCK Kft. (https://netlock.hu)
  - https://webgate.ec.europa.eu/tl-browser/#/
- Vehetünk EU-n kívüli kibocsátótól
  - Nem mindig szerencsés
- Ingyen is kaphatunk

X.509 web szerver tanúsítvány bizonyossági szintek

- Domain Validated (DV)
  - CABF OID 2.23.140.1.2.1
  - Domain feletti rendelkezés ellenőrzése (Pl: admin e-mail cím, fel tudunk-e valamit másolni a webszerverre.)
  - Általában automatikus folyamat, vagy önkiszolgáló portál
- Organization Validated (OV)
  - CABF OID 2.23.140.1.2.2
  - Igénylő szervezet egyszerű ellenőrzése
  - A domain név az igénylő szervezeté-e
  - Az eljáró személynek joga van-e eljárni a szervezet nevében
- Extended Validation (EV)
  - CABF OID 2.23.140.1.1
  - Igénylő szervezet ellenőrzése, működő szervezet-e
  - A domain név az igénylő szervezeté-e
  - Az eljáró személynek joga van-e eljárni a szervezet nevében
  - Meg kell feleljen a folyamat a CA/Browser forum Extended Validation Guideline-nak!
  - Wildcard nem igényelhető
- Qualified Website Authentication Certificate (QWAC)
  - Pénzügyi szolgáltatóknak kötelező az EU-ban
  - eIDAS megfelelőség

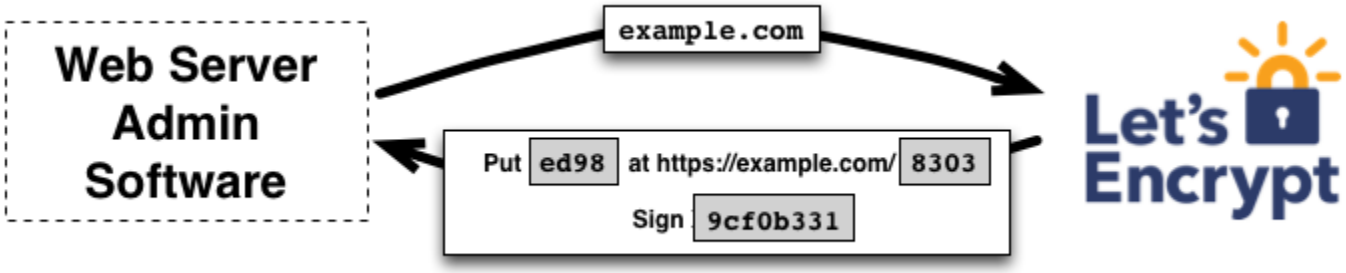
Let’s Encrypt

- Internet Security Research Group (ISRG) által üzemeltett nonprofit CA
- Rengeteg szponzor szervezet
- Célja, hogy a webes kommunikáció lehet minden esetben titkosított legyen, ezáltal előzve meg a visszaéléseket
- 90 napig érvényes tanúsítványokat bocsát ki:
  - DV
  - Ingyenes
  - Automatikus folyamat
    - ACME (Automated Certificate Management Environment) és ACMEv2 protokoll
    - Challenge-Response
    - Minden elterjedt operációs rendszerhez letölthető, nyílt eszközök
  - 2018 márciustól wildcard is
- 2014. november 14-én alakult meg
- 2016. április 2-án indult a tanúsítás

Kép forrása: https://letsencrypt.org/trademarks/

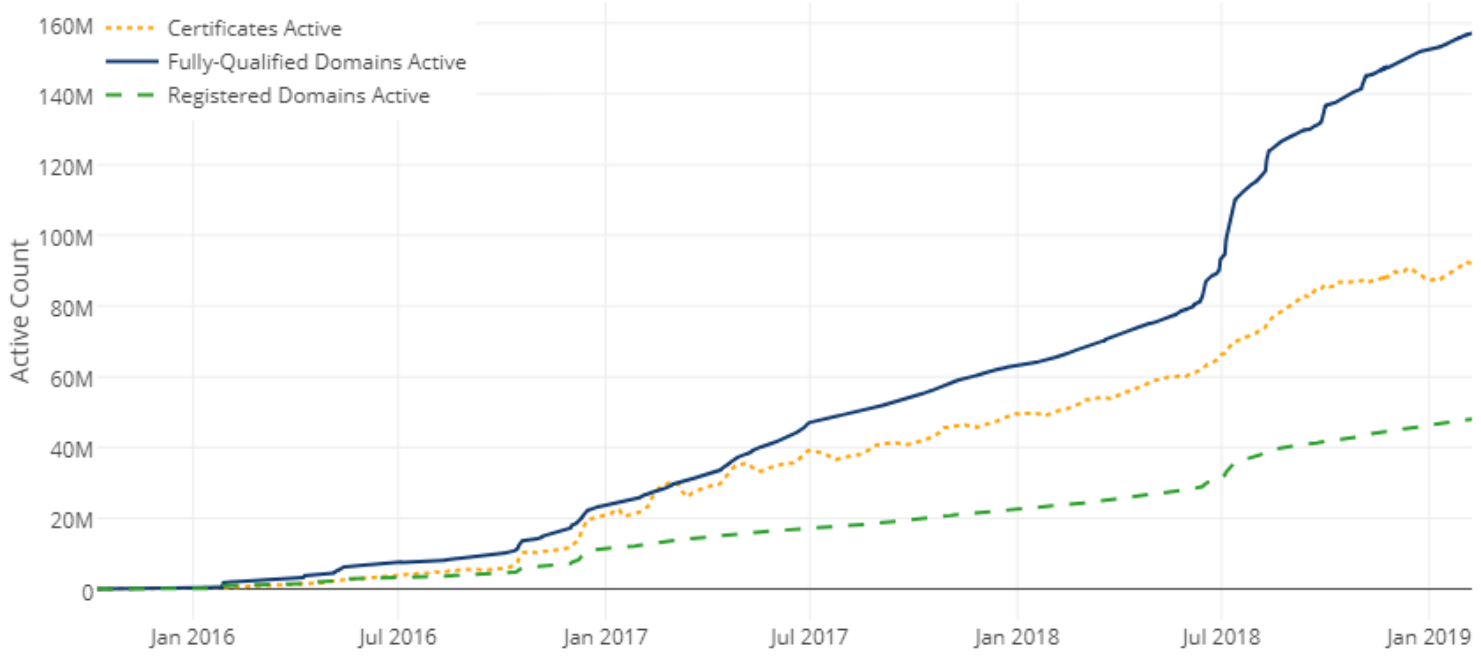
Let’s Encrypt működése

- Csak a domain feletti jogosultságot ellenőrzi:
  - Egy DNS rekord lekérdezésével, vagy
  - Egy állománynak a webszerverről letöltésével
  - Ezek paramétereit a CA adja meg (Név, aláírandó kódszó)



Kép forrása: https://letsencrypt.org/how-it-works/

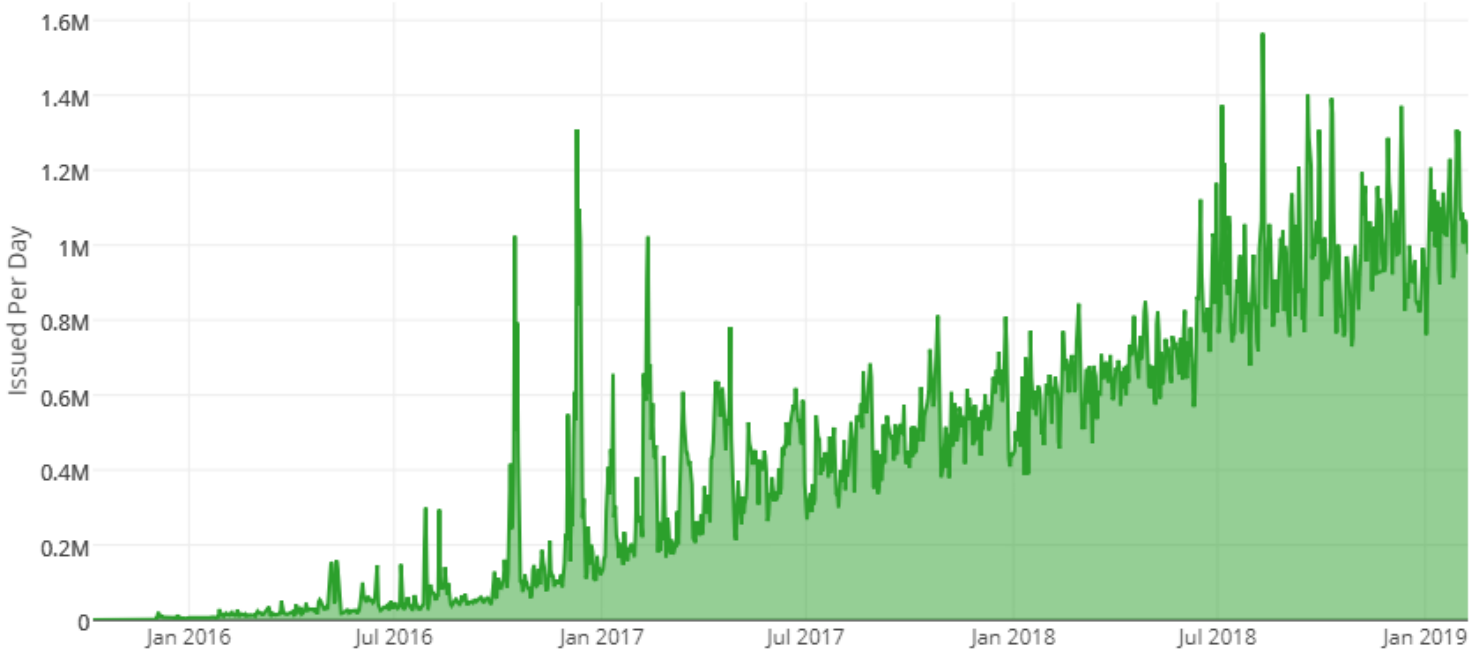
Let’s Encrypt terjedése



2019. 3. 31-i állapot

Forrás: https://letsencrypt.org/stats/

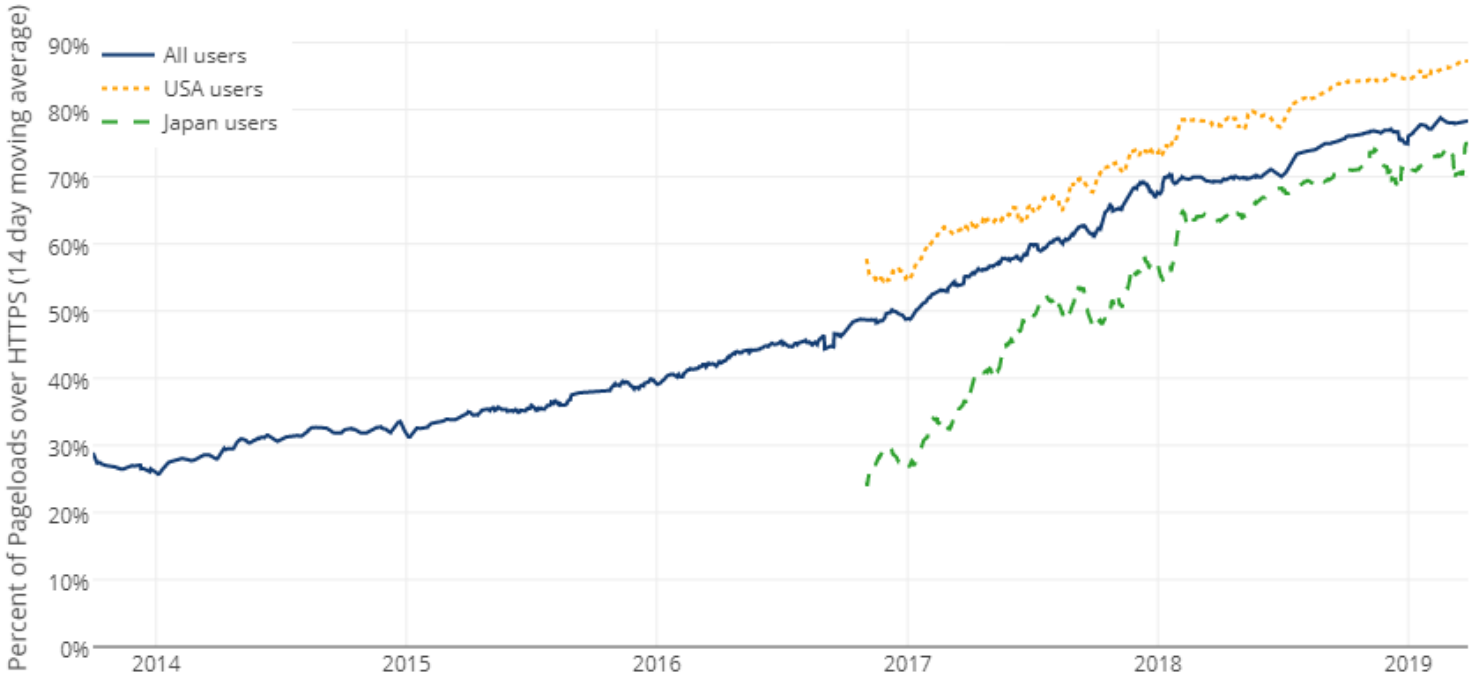
Naponta kiosztott tanúsítványok



2019. 3. 31-i állapot

Forrás: https://letsencrypt.org/stats/

HTTP/HTTPS aránya az internetes forgalomban



2019. 3. 31-i állapot

Forrás: https://letsencrypt.org/stats/

Biztonsági eszközök

Biztonsági eszközök

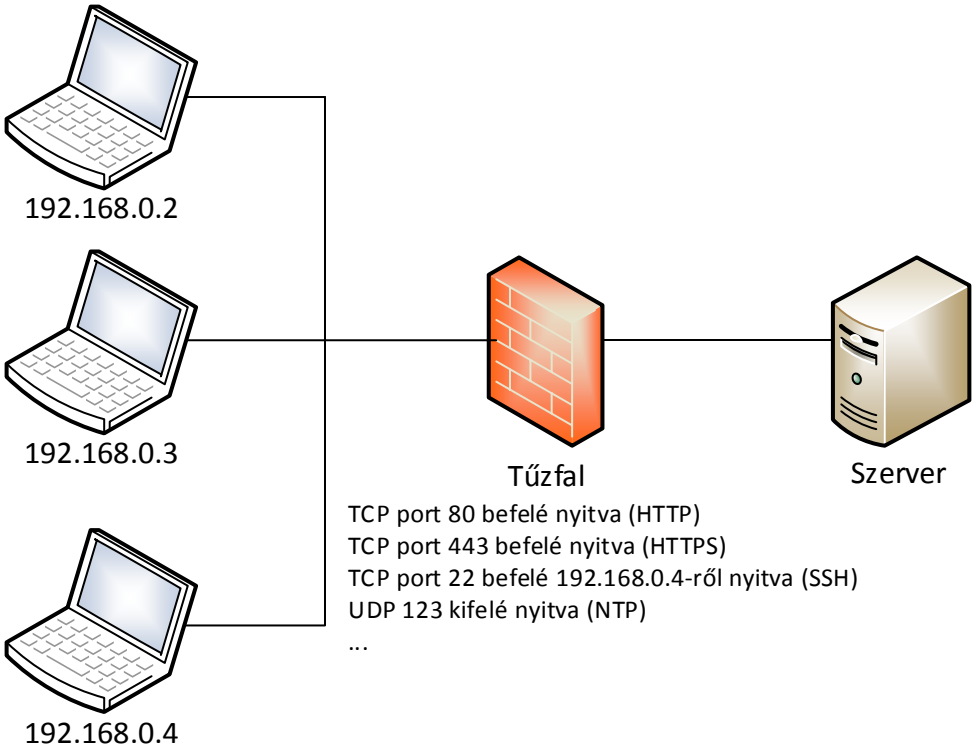
- Tűzfal
  - Access Control List (ACL)
  - Állapotmentes (stateless)
  - Állapottartó (stateful)
  - Host alapú
  - Hálózat alapú
  - Demilitarizált zóna (DMZ), Perimeter network, Screened subnet
- Proxy
- Honeypot
- Log szerver
- Idő szerver
- Hitelesítő szerver
- Intrusion Detection System (IDS)
- Intrusion Prevention System (IPS)

ACL

- Access Control List (ACL)
- Routeren létrehozva
- Engedélyezi, vagy tiltja a csomagok áthaladását a routeren
  - ACL nélkül minden csomag továbbításra kerül
- Standard ACL
  - Csak forrás IP cím
- Extended ACL
  - Forrás/cél IP cím és port, protokoll (TCP/UDP/ICMP)
- Több célra is:
  - NAT
  - Engedélyezi, vagy tiltja a router virtuális terminál elérését (vty)

Firewall, Tűzfal

- Két vagy több eltérő biztonsági szintű hálózat határán elhelyezett (határ)védelmi/forgalomkorlátozó eszköz.

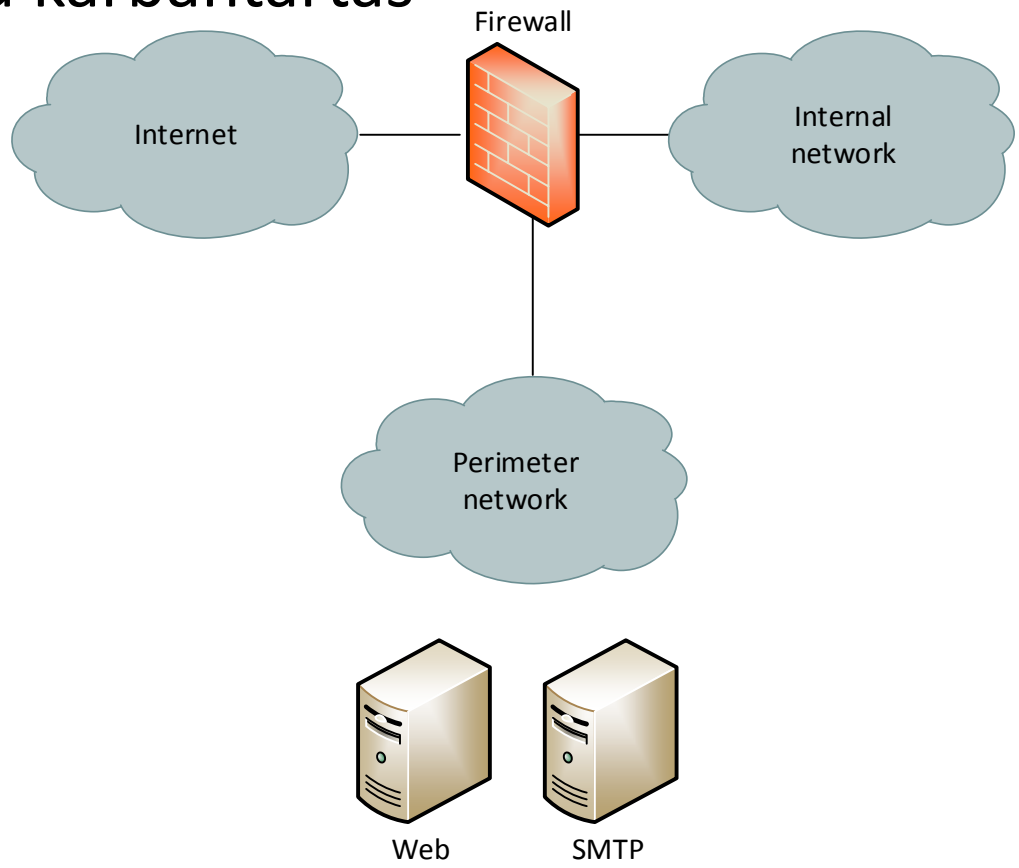


Típusok

- Állapotmentes (stateless)
- Állapottartó (stateful)
- Host alapú
- Hálózat alapú

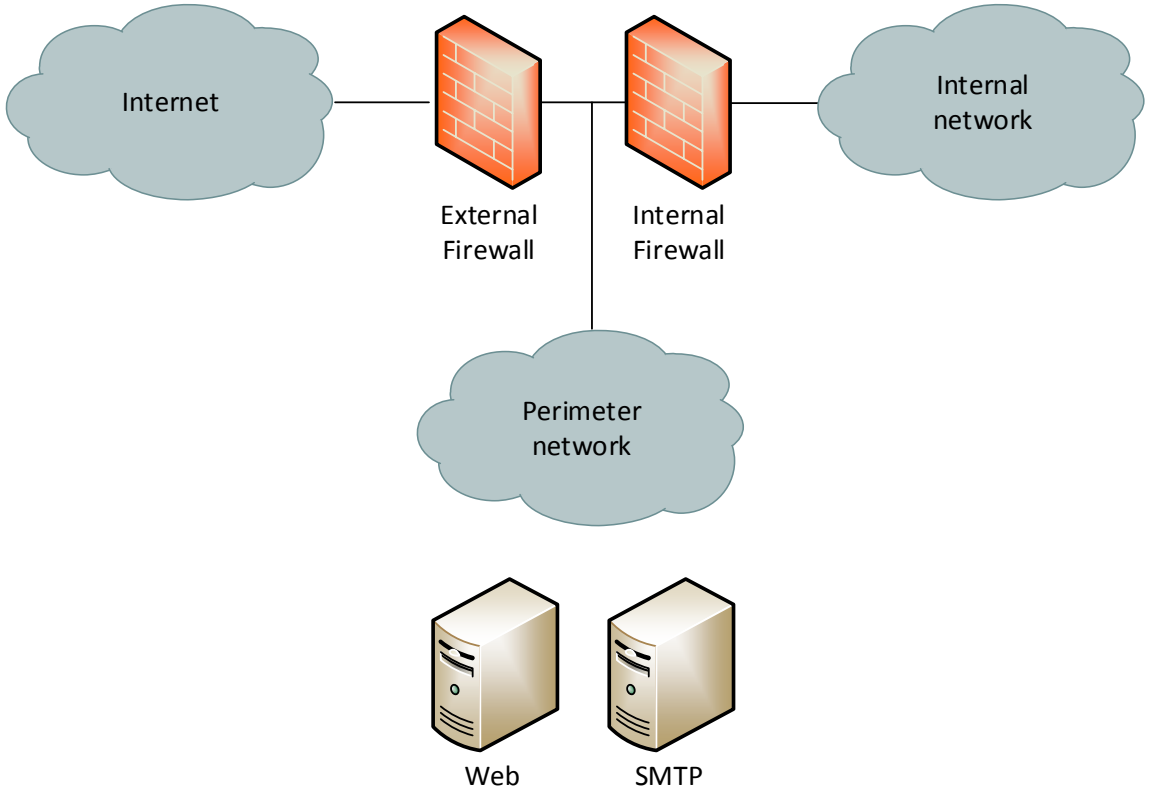
Single Firewall DMZ

- Olcsó kialakítás
- Egyszerű karbantartás

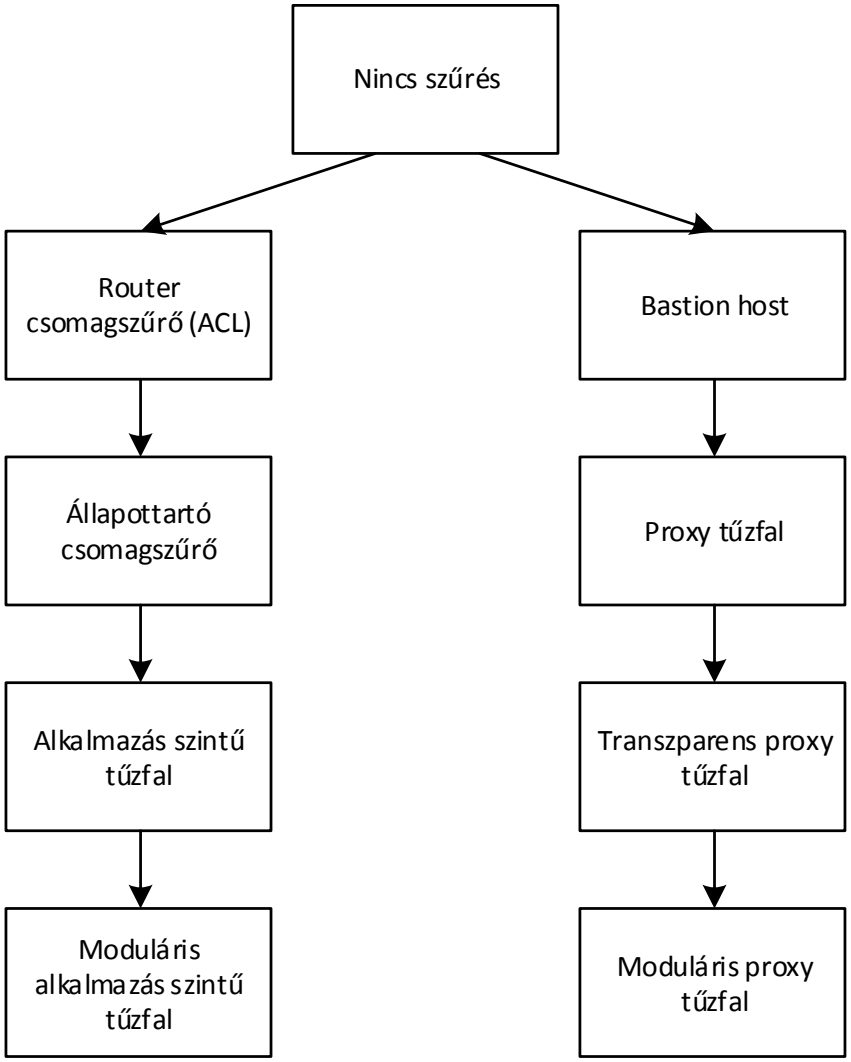


Dual firewall DMZ

- Két tűzfal
- Lehetőség szerint, eltérő gyártó és architektúra



Tűzfalak fejlődése



Proxy

- Kapcsolat szintű
- Alkalmazás szintű
- Reverse proxy
- Web Application Firewall
- Database Access Management

Syslog

- A rendszer eseményeinek távoli, vagy helyi rögzítésére, naplózására, „logolására”
- RFC 5424
- Hálózaton át: UDP 514, (TCP 6514)

Syslog facility

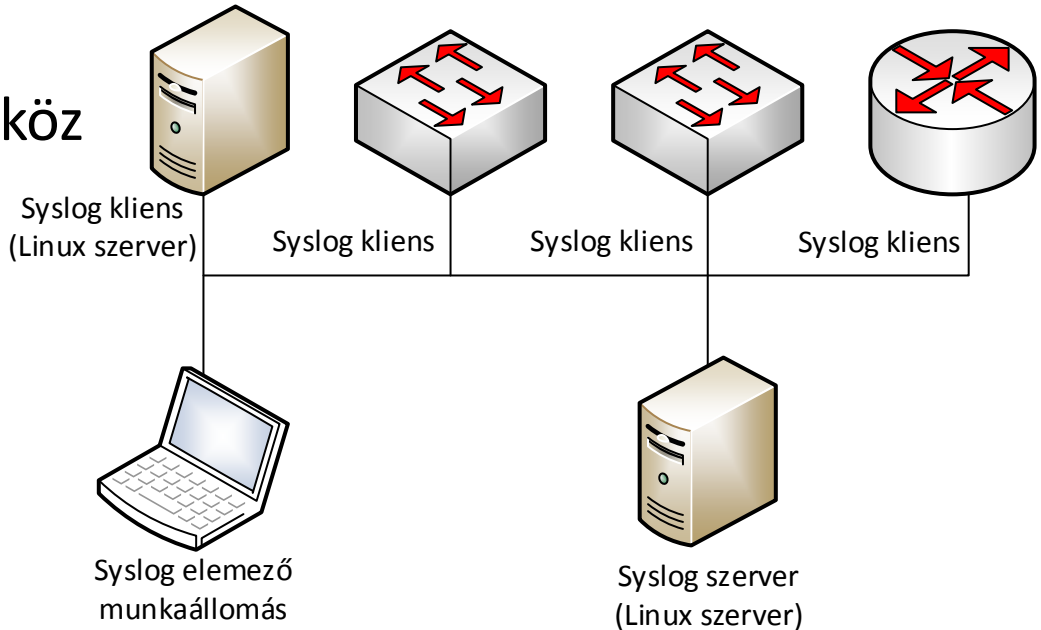
Facility code	Keyword	Description
0	kern	Kernel messages
1	user	User-level messages
2	mail	Mail system
3	daemon	System daemons
4	auth	Security/authentication messages
5	syslog	Messages generated internally by syslogd
6	lpr	Line printer subsystem
7	news	Network news subsystem
8	uucp	UUCP subsystem
9	cron	Clock daemon
10	authpriv	Security/authentication messages
11	ftp	FTP daemon
12	ntp	NTP subsystem
13	security	Log audit
14	console	Log alert
15	solaris-cron	Scheduling daemon
16–23	local0 – local7	Locally used facilities

Syslog severity/level

Value	Severity	Keyword	Description	Condition
0	Emergency	emerg (panic)	System is unusable	A panic condition.
1	Alert	alert	Action must be taken immediately	A condition that should be corrected immediately, such as a corrupted system database.
2	Critical	crit	Critical conditions	Hard device errors.
3	Error	err (eror)	Error conditions	
4	Warning	warning (warn)	Warning conditions	
5	Notice	notice	Normal but significant conditions	Conditions that are not error conditions, but that may require special handling.
6	Informational	info	Informational messages	
7	Debug	debug	Debug-level messages	Messages that contain information normally of use only when debugging a program.

Centralizált naplózás

- Syslog szerver:
  - A hálózat irányából érkező syslog üzeneteket tárolja (és dolgozza fel)
- Syslog kliens:
  - Naplóüzeneteket (syslog) készít és továbbít a syslog szerver irányába
  - Általában hálózati eszköz



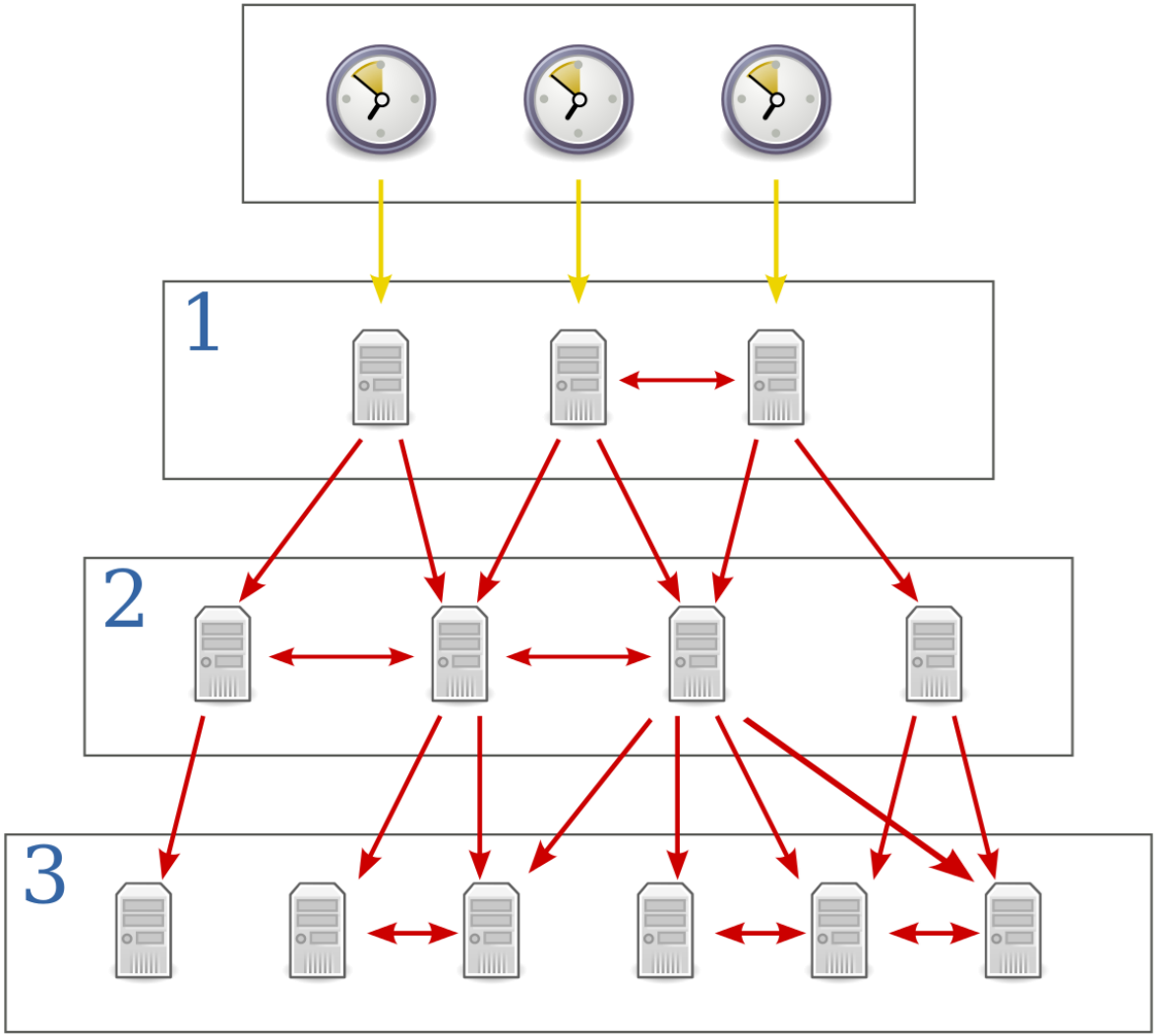
Centralizált naplózás

- Minden hálózati eszköz esetén központi szerverre naplózás
- Szerverek esetén központi szerverre naplózás
- (Eszközök és szerverek időszinkronizálása)
- Minden fontosabb esemény rögzítése
  - Konzol
  - Terminal
  - Interfész up/down
  - Konfigurálás
- Syslog szerver védelme tűzfalszabályokkal (ACL, iptables, stb.)

NTP

- Network Time Protocol (NTP)
- NTPv3 (RFC 1305), NTPv4 (RFC 5905)
- Számítógépek, hálózati eszközök időszinkronizálása
- UDP 123-as port
- Támogat hitelesítést preshared key, MD5 hash segítségével
- Hierarchikus felépítésű
- A hierarchiában alacsonyabb szinteken lévők egyre távolabb vannak a külső időforrástól:
  - Egyre pontatlanabbak
- Saját időszerver telepítése ajánlott, mely szinkronizálhat internetes szerverekhez, vagy hálózattól független időforráshoz (Pl. GPS)

Network Time Protocol Stratum



AAA

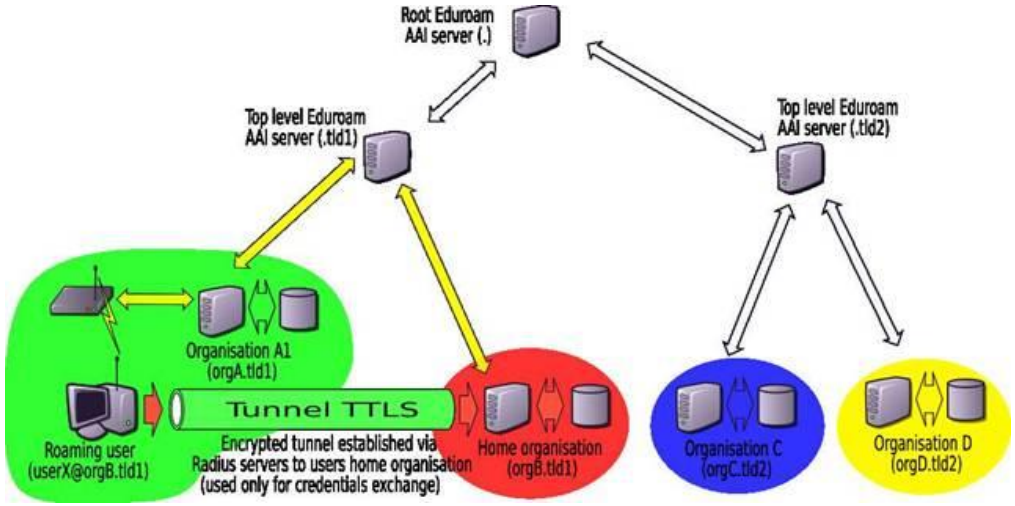
- Authentication
  - Hitelesítés
  - Melyik felhasználói fiók?
  - Ellenőrizni, hogy valóban az ő fiókja (Pl. felhasználónév/jelszó)
- Authorization
  - Feljogosítás
  - Mit csinálhat? (Pl. nyomtathat, FTP-zhet?)
  - Milyen erőforrásokat vehet igénybe?
- Accounting
  - Elszámolás, tevékenység rögzítése
  - Mikor, mit csinált?
    - Mennyit forgalmazott?
    - Mi volt az IP címe?
    - Honnan lépett be?
    - Stb.

AAA

- Adminisztratív hozzáférés
  - Ki léphet be a hálózati eszközre?
  - Mit csinálhat?
  - Megnézheti a konfigurációt
  - Módosíthat a konfiguráción
  - Stb.
- Hálózati szolgáltatások igénybevétele
  - Ki léphet be VPN-en?
  - Milyen szervereket érhet el?
  - Milyen protokollokat használhat?
  - Mely VLAN-ba kerül?
  - Stb.

RADIUS

- Remote Authentication Dial-In User Service (RADIUS)
- Livingston Enterprises (1991)
- Széles körben alkalmazott (szabványos)
  - PPPOE
  - VPN
  - WiFi
  - 802.1X
  - SIP
  - …
- RFC 2865 és RFC 2866
- UDP
- Alapesetben nem titkosított
- Skálázható (Proxy)
  - Realm (@ után)
  - Felfűzhetőek
  - Eduroam



Kép forrása: http://eduroam.sourceforge.net/

TACACS+

- Terminal Access Controller Access-Control System (TACACS+)
- RFC 927 TACACS (1980-as évek vége felé kezdte támogatni)
- XTACACS (1990) Cisco nem szabványos bővítése
- RFC 1492 (1993) TACACS+ Nem kompatibilis az előzőekkel
- Titkosított kommunikáció
- TCP, vagy UDP 49 port

Intrusion Detection System (IDS)

- Azonosítja a hálózatban a gyanús vagy kártékony aktivitásokat
- Észreveszi a rendszer normális működésétől eltérő tevékenységeket
- Naplózza, katalogizálja és osztályozza a rendszerfolyamatokat
- Szokatlan/gyanús események esetén képes valós idejű riasztásokat generálni
- Felépítése:
  - Szenzorok
  - Elemző
  - Szignatúra adatbázis
  - Felhasználói interfész és jelentés készítő
- Üzembe helyezést megelőzően „be kell tanítani”
- A hálózat változása esetén újabb beállítások:
  - Újabb típusú forgalmak jelennek meg
- A támadási módszerek változása miatt folyamatos frissítések és beállítások:
  - Újabb szignatúrák
- Csak riaszt!

Intrusion Prevention System (IPS)

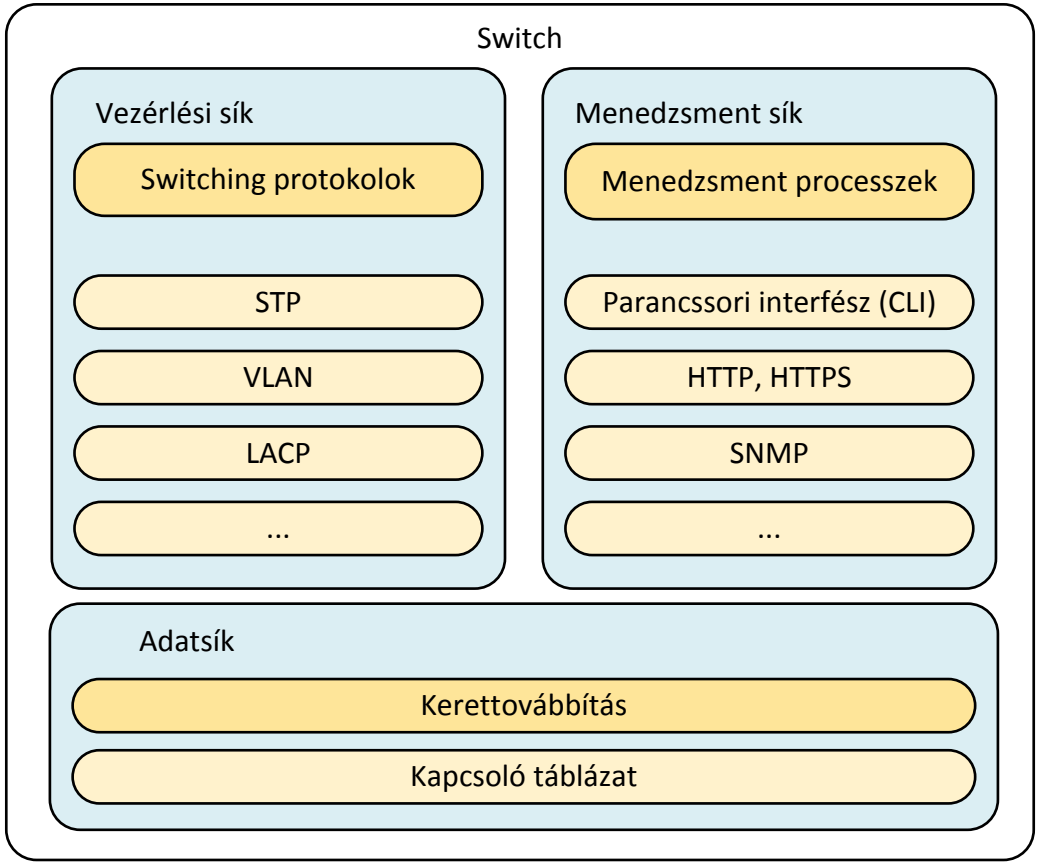
- Mindazt tudja, amit az IDS
- Képes ellenlépések megtételére is!
  - Adott IP cím letiltása
  - Adott port letiltása a switchen
  - Adott típusú forgalom letiltása
  - …
- Csak óvatosan!
  - Megakadályozhat legitim forgalmat is, ezáltal akadályozva a munkát

Hálózati eszközök biztonsága

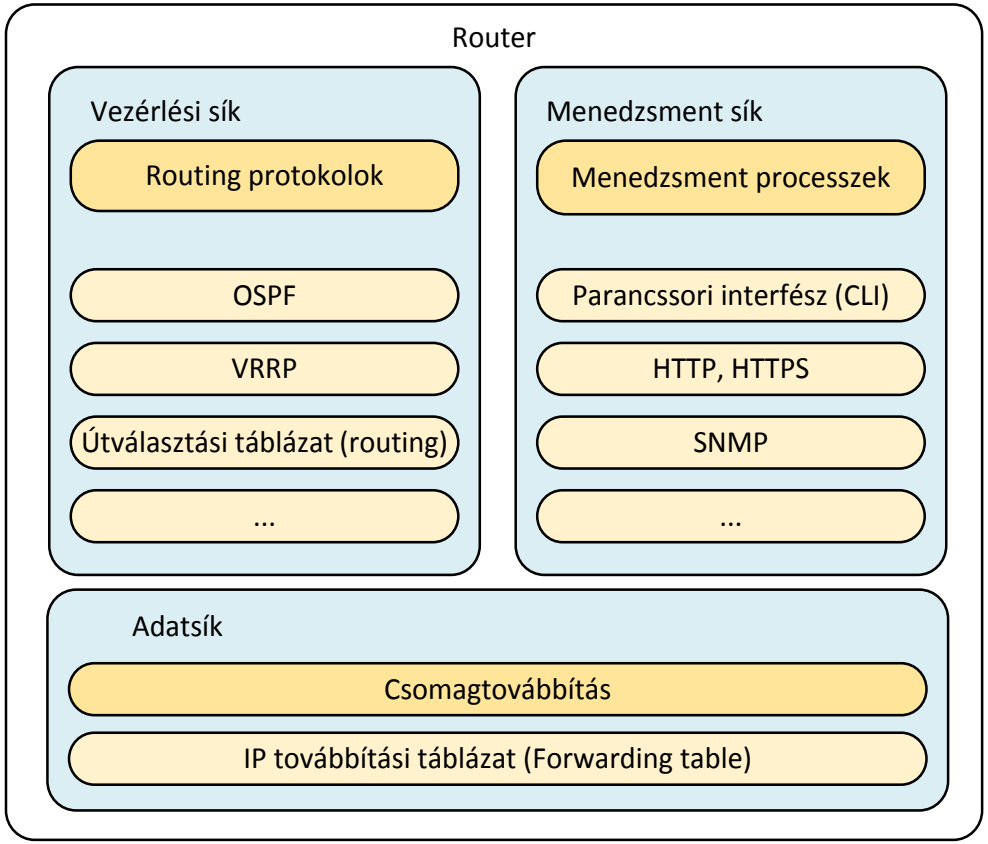
Hálózati eszközök, mint célpontok

- Jó célpontok:
  - Csak minimális mértékben tárolnak adatot, jellemzően a konfigurációs állományaikat, ezekben azonban jelszavak és titkosítási kulcsok is megtalálhatóak;
  - Nem futtatnak könnyen támadható alkalmazásokat, és nem telepítenek rájuk alkalmazásokat;
  - Rendszeresen nem dolgoznak segítségükkel, csak karbantartási, konfigurálási feladatokat;
  - Sokszor csak a telepítés során kerülnek konfigurálásra;
  - Sok esetben nem fordítanak elég figyelmet a megfelelő konfigurálás elvégzésére, csak a funkcionális elvárások teljesülését figyelik, tehát, hogy a hálózat jelenleg „működik”;
  - Nagyon ritka, sokszor elmarad a frissítések telepítése anyagi okok, vagy karbantartási hiányosságok miatt;
  - Naplózás, valamint naplóállományok figyelése sokszor nem megoldott;
  - Sok esetben közvetlenül az internetre csatlakoznak;
  - Eltérő biztonsági szintű hálózatokat választhatnak el egymástól;
  - Jól használhatóak további támadások kiindulópontjaként;
  - Minden adat „átmegy rajtuk”.

Ethernet switch



IP router


Router
Vezérlési sík
Routing protokolok
OSPF
VRRP
Útválasztási táblázat (routing)
...
Menedzsment sík
Menedzsment processzek
Parancssori interfész (CLI)
HTTP, HTTPS
SNMP
...
Adatsík
Csomagtovábbítás
IP továbbítási táblázat (Forwarding table)

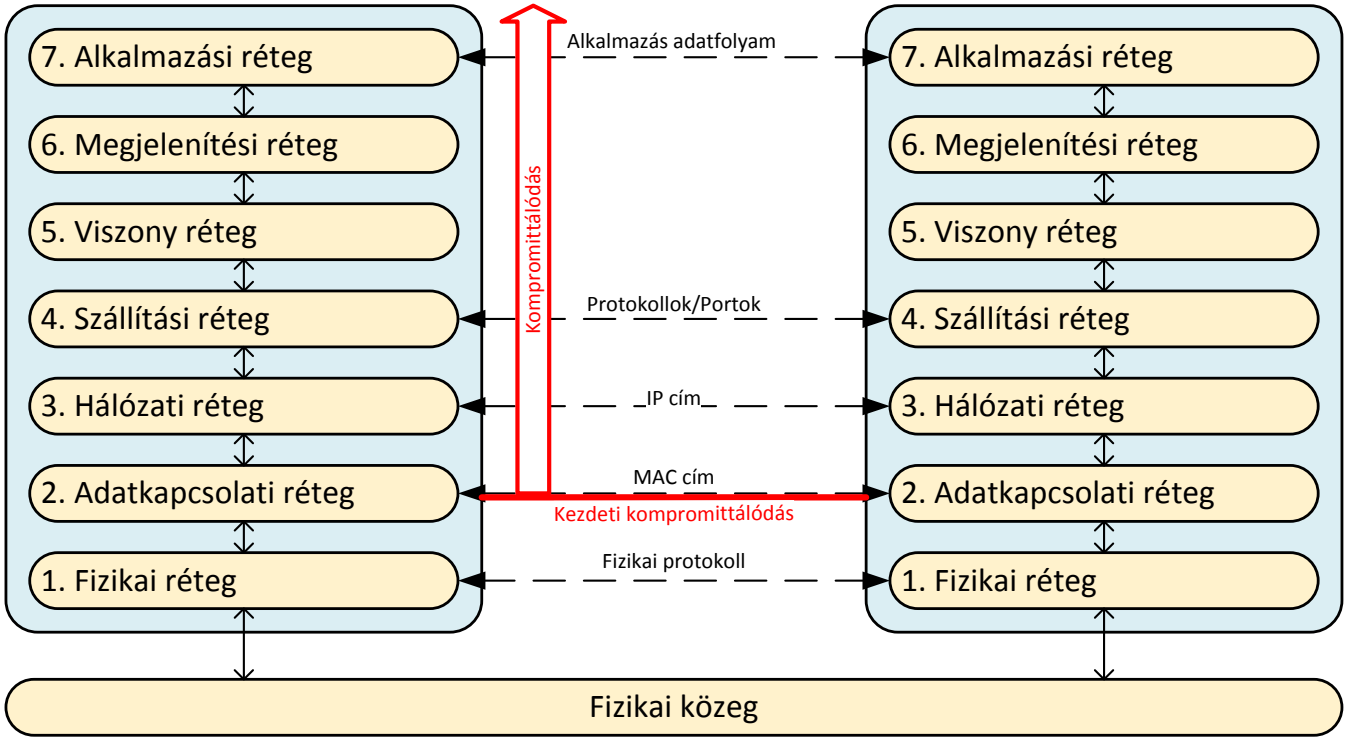
Támadások csoportosítása

- A célzott, vagy a támadás során kihasznált síkok alapján lehetnek:
  - vezérlési sík támadások;
  - menedzsment sík támadások;
  - adatsík támadások.
- A támadás módja alapján megkülönböztethetünk:
  - a protokoll hiányosságait kihasználó támadások;
  - az adott implementáció hibáit, programhibákat kihasználó támadások;
  - konfigurációs hibát kihasználó támadások;
  - egyéb támadások.
- A támadás végrehajtása:
  - az eszközhöz fizikai hozzáférést igényel;
  - a támadás távolról, hálózati kapcsolaton keresztül történik;
- Fontos kérdés az is, hogy a támadó a tényleges károkozást a megtámadott hálózati eszközben kívánja elérni, vagy azt csak kiindulási pontként felhasználja egy másik szervezet eszközei, hálózata elleni támadáshoz.

Támadások csoportosítása

- A támadás célozhatja:
  - a második, azaz az adatkapcsolati réteget;
  - a harmadik, azaz a hálózati (IP) réteget;
  - felsőbb rétegeket, esetlegesen a fizikai réteget.
- Ha egy alacsonyabb rétegben az adatok kompromittálódtak, úgy az a felsőbb rétegekre is kihatással van. Érvényesül a leggyengébb láncszem elve, és az adatkapcsolati réteg egy nagyon gyenge láncszem.

Kompromittálódás kihatása



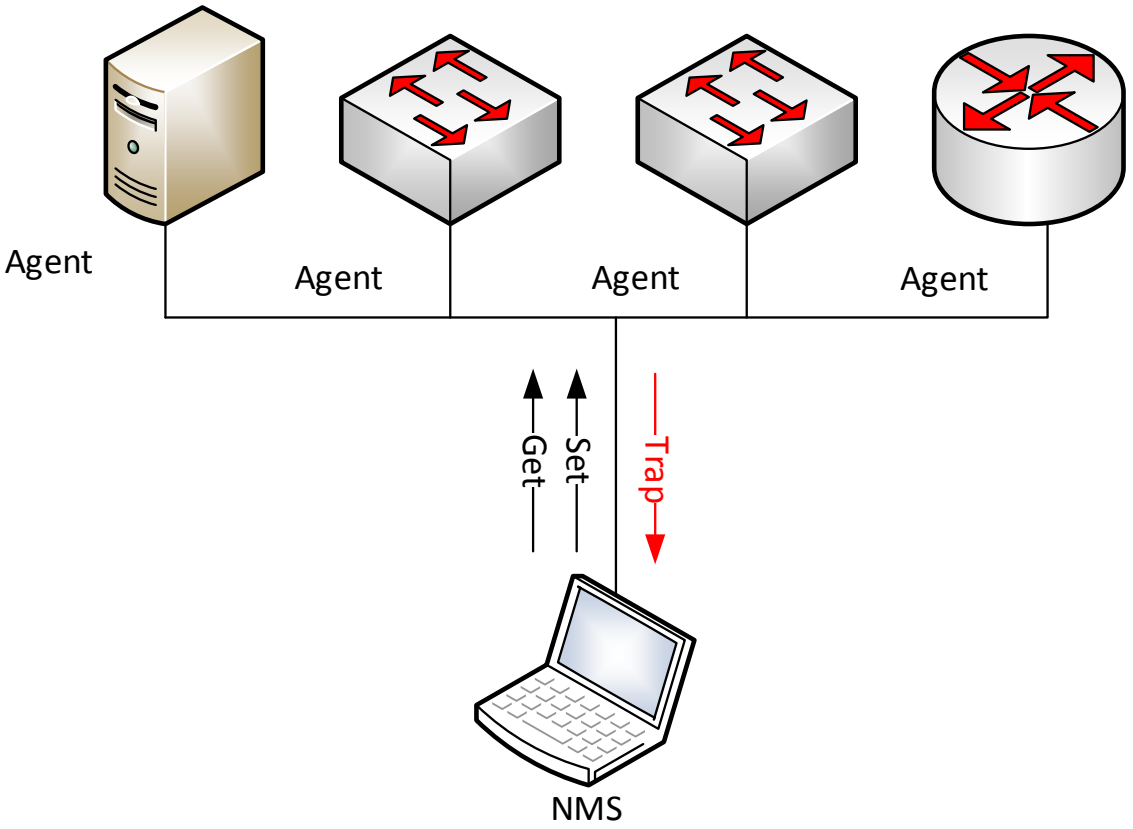
SNMP

- Simple Network Management Protocol (SNMP)
- Hálózati eszközök egyszerű, központi menedzsmentje
  - Adatgyűjtés
  - Konfiguráció módosítás
  - Riasztások fogadása
- UDP 161, Trap: UDP 162
- Network Management System(NMS)
  - A Management állomáson futó, az eszközöket felügyelő program
- Management Information Base (MIB)
  - Különböző információk hierarchikus gyűjteménye
  - A rendszer információinak leképezése egy szabványos formára
- Object Identifiers (OID)
  - A menedzselt objektumok egyedi azonosítója a MIB-ben

SNMP

- Managed device
  - SNMP segítségével felügyelt eszközök
  - Switch
  - Router
  - Szerver
  - Klíma
  - Hőmérő
- SNMP Agent
  - A Managed deviceon futó szoftver, mely fogadja az NMS üzeneteit, azokra válaszol, vagy SNMP Trapeket küld neki
- Get
  - Az NMS küldi az eszköznek (agentnek)
  - Állapotokat, beállításokat kérdezhet le
- Set
  - Az NMS küldi az eszköznek
  - Beállításokat végezhet el
- Trap
  - Az eszköz küldi az NMS részére, bizonyos események bekövetkezésekor
  - „riasztás”

SNMP



SNMP

```
user@NS1:~$ snmpwalk -v 2c -c PUBLIC 10.200.63.1
SNMPv2-MIB::sysDescr.0 = STRING: RouterOS RB433AH
SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.14988.1
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (1686692400) 195 days, 5:15:24.00
SNMPv2-MIB::sysContact.0 = STRING: root@domain.hu
SNMPv2-MIB::sysName.0 = STRING: Central-router
SNMPv2-MIB::sysLocation.0 = STRING: III.emelet
SNMPv2-MIB::sysServices.0 = INTEGER: 78
…
RFC1213-MIB::ipRouteNextHop.0.0.0.0 = IpAddress: 10.240.4.17
RFC1213-MIB::ipRouteNextHop.10.0.3.0 = IpAddress: 10.240.4.17
RFC1213-MIB::ipRouteNextHop.10.0.100.0 = IpAddress: 10.240.4.17
RFC1213-MIB::ipRouteNextHop.10.0.101.0 = IpAddress: 10.240.4.17
RFC1213-MIB::ipRouteNextHop.10.0.102.0 = IpAddress: 10.240.4.17
RFC1213-MIB::ipRouteNextHop.10.0.103.0 = IpAddress: 10.240.4.17
```

Community string

- Az SNMPv1 és v2c két szintű jogosultságot ismert
  - Csak olvasásra
    - Alapértelmezett community string: PUBLIC
  - Írásra és olvasásra
    - Alapértelmezett community string: PRIVATE
- Bárki, aki ismeri a community stringet elvégezheti az összes objektum lekérdezését/beállítását
  - Tűzfalszabályokkal, ACL-ekkel korlátozható az SNMP forgalom
- Nincsenek felhasználók, és az egyes objektumokhoz jogosultságok
- A teljes kommunikáció titkosítatlanul történik

SNMPv3

- Képes titkosításra
- NMS hitelesítésére (felhasználónév/jelszó)
- „View” alkalmazásával beállítható, hogy az NMS mely részeihez férjen hozzá az az SNMP MIB-nek
- A korábbi SNMP verziók helyett ennek alkalmazása ajánlott

Szabványok, ajánlások, bevált gyakorlatok

Szabványok, ajánlások

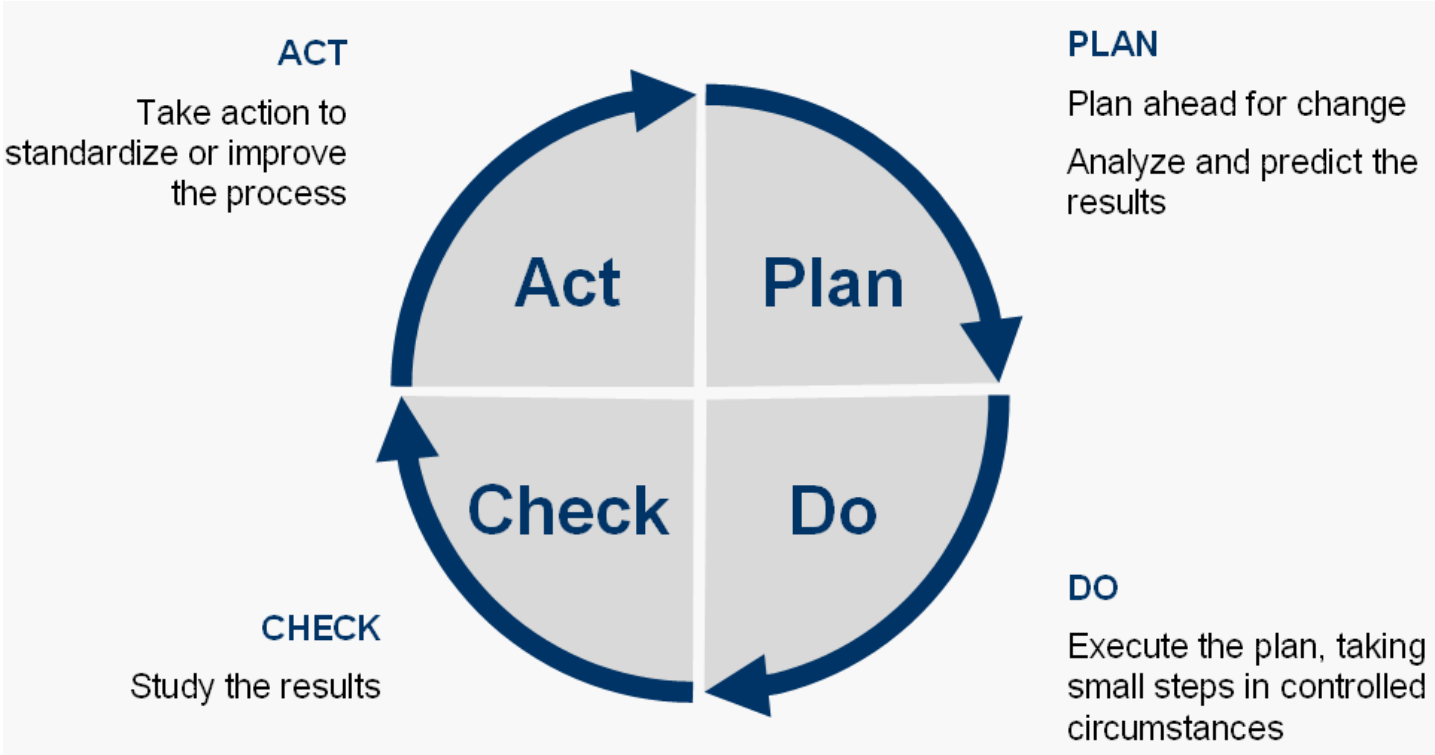
- ISO 27000 szabványcsalád
- COBIT (Control Objectives for Information and Related Technology)
- Common Criteria (ISO/IEC 15408)
- ITIL és ISO/IEC 20000 (IT Infrastructure Library)
- KIB 25. ajánlás (Közigazgatási Informatikai Bizottság)
- NIST Special Publication 800-53
- PCI DSS (Payment Card Industry (PCI) Data Security Standard)

Szabványok

- Termék
- Folyamat
- Szervezetek:
  - Magyar Szabványügyi Testület (www.MSZT.hu)
  - International Organization for Standardization (Nemzetközi Szabványügyi Szervezet, www.ISO.org)
  - International Electrotechnical Commission (Nemzetközi Elektrotechnikai Bizottság, www.IEC.ch)

Deming ciklus

- PDCA kör
- W. Edwards Deming, statisztikus
- Folyamatos fejlesztés (kontroll)



ISO 27000 szabványcsalád

- BS 7799 informatikai biztonsági követelmények
  - Az „Elől” (1995)
- ISO/IEC 27000:2012 Information security management systems – Overview and vocabulary (MSZ EN ISO/IEC 27000:2017)
- ISO/IEC 27001:2013 Information security management systems (MSZ ISO/IEC 27001:2014)
- ISO/IEC 27002:2013 Code of practice for information security controls (MSZ EN ISO/IEC 27002:2017)
- ISO/IEC 27005:2011 Information security risk management

  ISO/IEC 27007:2011 Guidelines for information security management systems auditing

COBIT (Control Objectives for Information and Related Technology)

- Information Systems Audit and Control Association (ISACA) és az IT Governance Institute (ITGI) 1992-ben
- COBIT 2019
- COBIT 5
- COBIT 4.1 verziója 34 magas szintű folyamatot,
  - 210 kontroll célkitűzést tartalmaz, amelyek négy szakterület köré csoportosulnak:
    - Tervezés és szervezés (Planning and Organization)
    - Beszerzés és megvalósítás (Acquisition and Implementation)
    - Szolgáltatás és támogatás (Delivery and Support)
    - Figyelemmel kísérés és értékelés (Monitoring and Evaluation)

Common Criteria

- 1996-ban elkészítették a Common Criteria for Information Technology Security Evaluation
- Informatikai biztonsági termékszabvány, amely ma az informatikai biztonság területén etalonnak tekinthető
- Az információk mozgását, tárolását szolgáló eszközök és rendszerek megbízhatóságának szabályozásával segítik
- 2.0-ás változatát az Informatikai Tárcaközi Bizottság 16. számú ajánlásaként magyar nyelven közreadta, majd az MSZ ISO/IEC 15408 jelzetű szabvány is lefordításra került.
- A szabványban a funkcionális követelmények, bizonyossági követelmények és értékelési bizonyossági szintek (EAL) mátrixaként határozhatóak meg az alkalmazandó biztonsági követelmények.
- Szabványcsalád tagjai:
  - ISO/IEC 15408-1:2009 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model
  - ISO/IEC 15408-2:2008 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 2: Security functional components
  - ISO/IEC 15408-3:2008 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 3: Security assurance components
  - ISO/IEC CD 15408-4 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 4: Framework for the specification of evaluation methods and activities (Készül)

ITIL és ISO/IEC 20000

- Elsősorban informatikai üzemeltetésére és fejlesztésére szolgáló módszertani gyűjtemény, folyamatszabvány
- Előírásaiban érinti a biztonsági területet.
- Nemzetközi legjobb gyakorlatként az IT szolgáltatások területén szolgál követelményhalmazként.
- Célja a jó minőségű, költséghatékony IT szolgáltatások támogatása, a minőségügyben ismert Plan-Do-Check-Act (PDCA) elv alkalmazásával.
- Öt kötete:
  - Szolgáltatás-stratégia (Service Strategy)
  - Szolgáltatás-tervezés (Service Design)
  - Szolgáltatás-létesítés és változtatás (Service Transition)
  - Szolgáltatás-üzemeltetés (Service Operation)
  - Állandó szolgáltatás-fejlesztés (Continual Service Improvement)

KIB 25. ajánlás (Magyar Informatikai Biztonsági Ajánlások)

- 25/1. Magyar Informatikai Biztonsági Keretrendszer (MIBIK)
- 25/1-1. kötet: Informatikai Biztonsági Irányítási Rendszer (IBIR)
- 25/1-2. kötet: Informatikai Biztonság Irányítási Követelmények (IBIK)
- 25/1-3. kötet: Az Informatikai Biztonság Irányításának Vizsgálata (IBIV)
- 25/2. kötet: Magyar Informatikai Biztonsági Értékelési és Tanúsítási Séma (MIBÉTS)
- 25/2-1. segédlet: MIBÉTS - Modell és Folyamatok
- 25/2-2. segédlet: MIBÉTS – Útmutató a Megbízók számára
- 25/2-3. segédlet: MIBÉTS – Útmutató a Fejlesztők számára
- 25/2-4. segédlet: MIBÉTS – Útmutató Értékelőknek
- 25/2-5. segédlet: MIBÉTS – Értékelési módszertan
- 25/3. kötet: Informatikai Biztonsági Iránymutató Kis Szervezeteknek (IBIX)

NIST Special Publication 800-53

- NIST 800-as sorozat a számítógépes biztonsággal foglalkozik
  - Iránymutatások
  - Ajánlások
  - Műszaki specifikációk
  - Éves jelentések

National Institute of Standards and Technology
U.S. Department of Commerce

- NIST SP 800-53: Security and Privacy Controls for Federal Information Systems and Organizations

ID	FAMILY	ID	FAMILY
AC	Access Control	MP	Media Protection
AT	Awareness and Training	PE	Physical and Environmental Protection
AU	Audit and Accountability	PL	Planning
CA	Security Assessment and Authorization	PS	Personnel Security
CM	Configuration Management	RA	Risk Assessment
CP	Contingency Planning	SA	System and Services Acquisition
IA	Identification and Authentication	SC	System and Communications Protection
IR	Incident Response	SI	System and Information Integrity
MA	Maintenance	PM	Program Management

PCI DSS (Payment Card Industry (PCI) Data Security Standard)

- Bankkártya kibocsátó és elfogadó szerveztek
- https://www.pcisecuritystandards.org

Control Objectives	PCI DSS Requirements
Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data
	2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data
	4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software on all systems commonly affected by malware
	6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need-to-know
	8. Assign a unique ID to each person with computer access
	9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data
	11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security

Néhány minősítés

- Information Systems Audit and Control Association (ISACA)
  - CISA (Certified Information Systems Auditor)
  - CISM (Certified Information Security Manager)
  - CRISC (Certified in Risk and Information Systems Control)
- International Information System Security Certification Consortium (ISC)²
  - CISSP (Certified Information Systems Security Professional)
- EC-Council
  - CEH (Certified Ethical Hacker)
- Offensive Security
  - OSCP (Offensive Security Certified Professional)

Jogszabályok

Jogszabályok hierarchiája

- Európai Unió
  - Rendeletek
    - Kötelező jogalkotási aktus, amely az EU egész területén teljes egészében alkalmazandó
  - Irányelvek
    - Valamennyi uniós ország számára kötelezően elérendő célkitűzés
    - A döntéshozatal módja az egyes országokra bízva
  - Határozatok
    - Csak a címzettjeit kötelezi (pl. egy tagállamot, egy vállalatot)
    - Közvetlenül alkalmazandó
  - Ajánlások
    - Nem kötelező
  - Vélemények
    - Kötelező erő nélküli nézőpont

- Magyarország

Jogforrási hierarchia

Jogszabályok elérhetősége

- Magyarországi jogszabályok
  - Nemzeti jogszabálytár
  - http://njt.hu/
- Európai Unió joganyaga
  - https://eur-lex.europa.eu

Fontosabb jogszabályok

- Az Európai parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet, GDPR)
- Az Európai Parlament és a Tanács 910/2014/EU rendelete (2014. július 23.) a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről (eIDAS)
- 2011. évi CXII. törvény az információs jogról és az információszabadságról
- 1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról
- 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról (Ibtv)
- ~~77/2013. (XII. 19.) NFM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint biztonságos információs eszközökre, termékekre vonatkozó, valamint a biztonsági osztályba és biztonsági szintbe sorolási követelményeiről~~
- 41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről
- 26/2013. (X. 21.) KIM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvényben meghatározott vezetői és az elektronikus információs rendszer biztonságáért felelős személyek képzésének és továbbképzésének tartalmáról
- 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről (Lrtv)

CERT/CSIRT

- Computer Security Incident Response Team (CSIRT)
- Computer Emergency Response Team (CERT)
- Tevékenysége:
  - Bejelentéseket fogad
  - Riasztásokat ad ki
  - Jelentéseket tesz közzé
  - Tudásbázist tart fenn
  - Gyakorlatokat tart
  - Védekezést összehangolja
  - Információkat cserél más CERT-ekkel
  - Tudatosság növelést végez
- Hun-CERT, Internet Szolgáltatók Tanácsának CERT-je (https://www.cert.hu/)
- Gov-Cert, Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (https://www.cert-hungary.hu/)
- Cert-EU, (cert.europa.eu)
- LRL IBEK, Létfontosságú Rendszerek és Létesítmények Informatikai Biztonsági Eseménykezelő Központja, (BM OKF LRLIBEK)

Adatbiztonság

A bölcsesség hierarchiája

- Adat
  - Az információs rendszer legalapvetőbb elemei. Szimbólumok, melyek tárgyak, események és környezetük tulajdonságait reprezentálják.
  - Önmagukban nem rendelkeznek jelentéssel.
  - Pl: piros, harminc, …
- Információ
  - Kontextusba helyezett adat.
  - Pl: Az autó piros. Harminc forint a kifli, …
- Tudás
  - Az egyének tudatában feldolgozott információk, és megokolt személyes meggyőződések, amelyek növelik annak képességét, hogy hatékonyan cselekedjünk. Az adat és az információ, szükséges a létrejöttéhez, de nem elégséges. Elengedhetetlen az emberi tényező. A tudás tartalmaz megértést és képességeket is.
  - Pl: A piros autó szép. A harminc forintos kifli drága.
- Bölcsesség
  - Olyan felhalmozott tudás összessége, mely lehetővé teszi, hogy megértsük, hogyan alkalmazhatók valamely területről származó fogalmak új szituációkban, vagy új problémák megoldására.

Forrás: http://tmt-archive.omikk.bme.hu/show_news.html?id=4954&issue_id=496

Adat tulajdonságai

- Bizalmasság
  - Confidentiality
  - Csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról
- Sértetlenség
  - Integrity
  - Az adat tartalma és tulajdonságai az elvárttal megegyeznek, ideértve a bizonyosságot abban, hogy az az elvárt forrásból származik (hitelesség) és a származás ellenőrizhetőségét, bizonyosságát (letagadhatatlanságát) is
- Rendelkezésre állás
  - Availability
  - Az arra jogosult személy számára elérhetőek és felhasználhatóak

Forrás: 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról

Adat értéke

- Információs társadalom
- Ipar 4.0
- „A ma elérhető adatok 90 százaléka az elmúlt 2 évben keletkezett”
- Mennyit ér?
  - Amennyibe az előállítása került
  - Amennyibe a pótlása kerül
  - Amennyiért el tudjuk adni
  - Amekkora kárt okoz az elvesztése
    - Elmaradt haszon
    - Jogszabálysértés
    - Hírnév sérülése
  - …

Vége