1. Nagyvállalati hálózatok, követelmények a nagyvállalati hálózatokkal szemben, rendelkezésreállás

CISCO Enterprise Campus

- Számítástechnikai infrastruktúra része
  - Hálózati szolgáltatások elérése
- Egy adott helyen elérhető hálózat
  - Lehet egy emelet vagy akár több épület is
- Nagy sebességű L2 és L3 rétegek
- Integrált elemek, amelyek szolgáltatások megvalósítását teszik lehetővé olyan felhasználók és eszközök között, akik ugyanazon a nagysebességű hálózathoz tartoznak
  - Vezetékes és vezetéknélküli adattovábbítás
  - Forgalom azonosítás és irányítás (biztonság)
  - Forgalom figyelés és menedzsment
  - Rendszer menedzsment

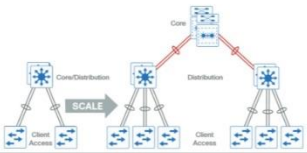
4 Hálózatok építése, konfigurálása és működtetése, BME-TMIT

CISCO Enterprise Campus

- Campus hálózat követelmények
  - Globális elérhetőség
    - ötkilences rendelkezésre állás, valós idejű interaktív alkalmazások, gyors hibaelhárítás
    - Kevesebb, központosított adat. Hálózati elérés minden üzleti folyamatban
    - 7x24x365-ös működés
  - Együttműködések, valós idejű kommunikáció
  - Védekezés a támadások ellen
  - Gyors változáskövetés
    - Az eszközöket adaptálni kell a változásokhoz
    - Gyorsabb, egyszerűbb frissítések, módosítások
    - Új hálózati protokollok (pl. IPv6 megjelenése)
  - Következő generációs alkalmazások növekvő igényei
    - Multimédia, interaktív HD video
  - Heterogenitás
    - Partner és vendég hálózatok
    - Különböző eszközök támogatása

Campus hierarchia

- 3 szintű hierarchia
  - Lehet kevesebb is és több is
- **Access/hozzáférési réteg**: Felhasználók és eszközök közvetlen hálózat elérése
- **Distribution/elosztási réteg**: Access rétegek aggregációja, szolgáltatások elérhetősége
- **Core/központi réteg**: Nagy hálózatokban a distribution rétegek összekapcsolása

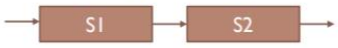


Rendelkezésreállás

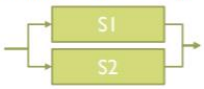
- MTBF: Mean Time Between Faliure
- MTTR: Mean Time to Repair
- Rendelkezésre állás (Availability): $\frac{MTBF}{MTBF+MTTR}$

SLA: Service Level Agreement

- Soros esetben (mindkét komponensre szükség van)
  - A_S: $A_1 \times A_2$



- Párhuzamos esetben (Csak akkor áll, ha mindkettő áll)
  - A_S: $1-(1-A_1) \times (1-A_2)$



Part Number	Maximum Rated Power (W)	Rated MTBF (Hours)
WS-C4503-E	60	1,064,279
WS-C4506-E	120	710,119
WS-C4507R+E	135	248,630
WS-C4510R+E	200	179,714

120 év

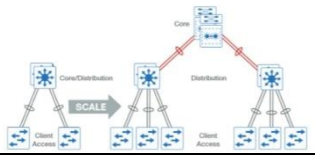
Defects per Million (DPM)

- A hiba hatása a felhasználó szemszögéből
  - Felhasználói élmény mérése
  - DPM: $\frac{\sum(\text{érintett felhasználók száma} \times \text{kiesett idő})}{\text{Összes felhasználó} \times \text{teljes szolgáltatási idő}} \times 10^6$
- Szintén fontos metrika, a maximális kiesés mértéke

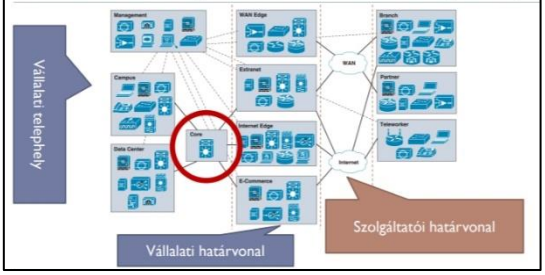
2. Nagyvállalati hálózatok felépítése. Hierarchia és modularitás. Campus hierarchia

Campus hierarchia

- 3 szintű hierarchia
  - Lehet kevesebb is és több is
- **Access/hozzáférési réteg**: Felhasználók és eszközök közvetlen hálózat elérése
- **Distribution/elosztási réteg**: Access rétegek aggregációja, szolgáltatások elérhetősége
- **Core/központi réteg**: Nagy hálózatokban a distribution rétegek összekapcsolása

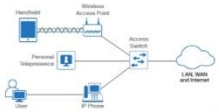


CISCO Enterprise Architecture (CEA)



Access (hozzáférési) réteg

- **Felhasználó gépek, végpontok csatlakozása**
- Vezetékes vagy vezetéknélküli kapcsolat
  - Nagy sávszélességű kapcsolat
  - Több alhálózat (logikai szétválasztás)
    - Teljesítmény, biztonság, menedzsment
- Biztonságos, hibatűrő működés
  - Magas rendelkezésreállás
  - Védekezés az emberi hibák és rosszindulatú támadások ellen
  - Hitelesített szolgáltatások és felhasználók
- Megkülönböztetett forgalmak



Hozzáférési réteg feladatai

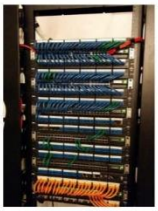
- A legszélesebb funkciókínálatot mutató réteg
  - Konfigurálás, feltérképezés
  - Biztonsági szolgáltatások
  - Hálózati azonosítás
  - Alkalmazás felismerő szolgáltatások
  - Intelligens hálózat irányítási szolgáltatások
  - Fizikai infrastruktúra szolgáltatások (PoE)
- A hálózat és az eszközök határa
  - Biztonság, QoS, házirend feladatok

Hozzáférési réteg eszközei

- Felhasználói eszközök
  - Munkaállomások, VoIP berendezések, hozzáférési pontok, kapcsolók
- Gigabit Ethernet switch
  - Biztonsági megoldások, monitorozás, PoE
  - „Stackable"
  - 2-5 Gpbs sebesség
  - Pl: Cisco Catalyst 2960-X, Catalyst 3850, HP 5500

Hozzáférési réteg eszközei

- Rack szekrény



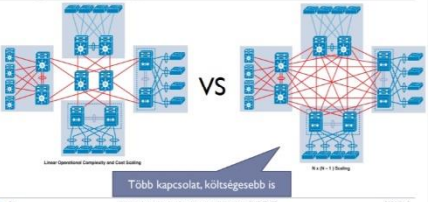
Core (központi) réteg

- **Állandó összeköttetés az egész campus számára**
- A legegyszerűbb, de egyben a legkritikusabb réteg
  - Always-on, 7x24x365
- Nagyon szűk szolgáltatáskör
  - Nincsenek felhasználók
  - Nincsenek házirendek
  - Kizárólag Layer 3 kapcsolatok! (Nincs switching)

Központi réteg

- REDUNDANCIA! Nagyon fontos, hogy bármely eszköz kiesése esetén maradjon a működés
  - Tervezett bővítések, cserék
- Feladata, hogy a campus más moduljainak aggregálása

Központi réteg nélkül



Központi réteg eszközei

- 10/40/100 Gb Ethernet
- Redundancia
- Pl: Cisco Nexus 7700, Catalyst 6800, HP 7500

Distribution (elosztási réteg)

- Irányítási határ
- Szolgáltatás és szabályozás réteg a hozzáférési és a központi réteg között
  - Kapcsolódás a hozzáférési réteghez
    - Aggregálja a hozzáférési pontok forgalmát
  - Kapcsolódás a központi réteghez
- Szabályozás
  - A helyi forgalom maradjon a helyi hálózaton
  - Forgalomszűrések, forgalomfelügyelet
    - Hozzáférés vezérlés
    - Támadás, hiba esetén hibatartomány korlátozás

Komplexitás, rendelkezésreállás

- A hozzáférési réteg
  - Csökkenti a komplexitást
    - Kapcsolatok számának csökkentése
    - Konfigurálás komplexitásának csökkentése
  - Növekedő rendelkezésreállás
    - Redundancia. Redundáns táp, modulok
    - Másodperc közeli helyreállás

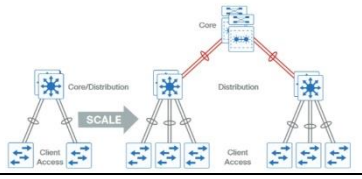
Elosztási réteg eszközei

- Cisco Catalyst 3850, Catalyst 4500 sorozat
  - Többszáz Gbps
  - Magas szintű rendelkezésre állás képesség
  - Skálázhatóság
  - Intelligens szolgáltatások vezetékes és vezeték nélküli hozzáféréshez

3. Hibakezelés 3 rétegű modellben

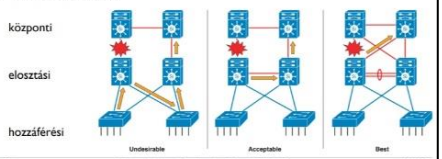
3 szintű hierarchia

- Lehet kevesebb is és több is
- **Access/hozzáférési réteg**: Felhasználók és eszközök közvetlen hálózat elérése
- **Distribution/elosztási réteg**: Access rétegek aggregációja, szolgáltatások elérhetősége
- **Core/központi réteg**: Nagy hálózatokban a distribution rétegek összekapcsolása



Hibakezelés a 3 rétegű modellben

- Meghatározott funkciók a rétegekben
- Pl. hiba kezelés



FHRP: First-hop redundancy protocol

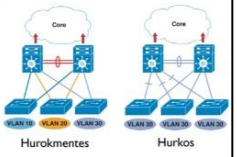
- Rendelkezésreállás növelése
  - Beugrás a kieső router helyére (de nem csak router)
- Hot Standby Router Protocol (HSRP)
  - Prioritások szerinti ARP válasz
- Virtual Router Redundancy Protocol (VRRP)
  - A hoszt alapértelmezett routere egy csoportból kerül ki (virtuális router)
- Gateway Load Balancing Protocol (GLBP)
  - Terhelésmegosztásos IP cím megosztás (súlyozás)
  - Az ARP válaszoknál különböző virtuális MAC címek kerülnek vissza
- Common Address Redundancy Protocol (CARP)
  - Egy IP cím megosztása több gép között (master/slave)
  - Terhelésmegosztás is lehetséges

Hozzáférési-elosztási réteg

- Gyakorlati megvalósítása
  - Többlépcsős (multi-tier) megoldás
  - „routed access"
  - Virtuális kapcsoló
- Minhárom megoldásnál a topológia azonos, a kábelezés hasonló
  - Különböző beállítások, képességek

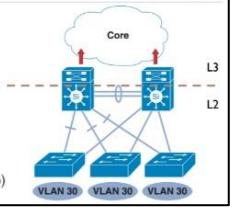
Többlépcsős variációk

- Hurokmentes (V) és hurkos változatok
  - A hurok eltávolítása előnyös
    - Terhelésmegosztás
    - STP függőség csökkentése



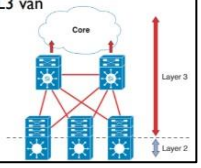
Többlépcsős hozzáférési-elosztási réteg

- Hozzáférési réteg: L2
- Elosztási réteg: L2 & L3
- VLAN trönkök
  - Akár több switchen keresztül
- FHRP
  - First-hop redundancy protocol
  - Konvergencia: 900ms-9mp
- STP protokoll
  - Hurokmentesítés
  - Lassú konvergencia (akár 50 mp)



Routed access

- A hozzáférési rétegben már elérhető a L3
- Az elosztási rétegben már csak L3 van
- Az elosztási réteg funkciói a hozzáférési réteghez kerülnek
  - Alapértelmezett átjáró, VLAN
  - Nincs szükség az FHRP protokollokra, lokális átjárók

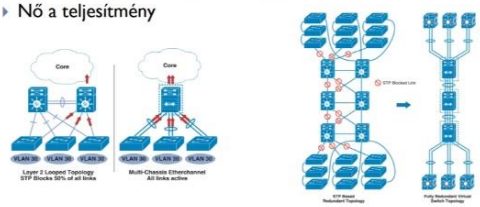


Routed access előnyök, hátrányok

- Routing protokollok
  - Konvergencia: < 200ms
  - Reroute hiba esetén
- Könnyebb hibakeresés, ismert szerszámok
  - Ping, traceroute, ip route
- Egyetlen kontroll protokoll, nincs FHRP
- Ugyanakkor vannak korlátok is
  - A VLAN nem terjedhet át másik kapcsolóba

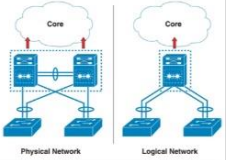
Virtuális kapcsolók vs. STP

- Nő a teljesítmény



Virtuális kapcsoló (Virtual Switch System - VSS)

- Régi megközelítés:
  - Redundáns elosztási réteg kapcsolók és protokoll, amely meghatározza az aktívat és vált hiba esetén
- Új megközelítés:
  - A redundáns elosztási réteg kapcsolók egyetlen logikai kapcsolót alkotnak



Virtuális kapcsoló előnyök

- **Nincsenek hurkok a (logikai) kapcsolatban**
  - STP maradhat, mint tartalék megoldás
- Egyszerűsödik a topológia
- Terhelésmegosztás flow alapon
- Hiba esetén gyors váltás, nincs szükség megvárni az STP-t, vagy hasonló protokollt
- A VLAN több hozzáférési kapcsolóra is kiterjedhet
- A technológia nincs korlátozva csak a hozzáférési / elosztási rétegre

Összehasonlítás

	Többlépcsős Multitier Access	Routed Access	Virtual Switch
Protokollok	STP	Routing, pl: OSPF	(PAgP, LACP)
STP szükség	Szükséges	Nincs	Nincs, de tartaléknak jó
Hibaelhárítás	STP és FHRP	Re-routing	Multichassis EtherChannel (MEC)
VLAN átívelése kapcsolón	Támogatott, de nem ajánlott	Nincs	Támogatott
L2 és L3 határa	Elosztási réteg	Hozzáférési rétes	Elosztási réteg (akár hozzáférési réteg is)

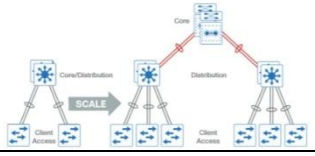
Összehasonlítás folyt.

	Többlépcsős Multitier Access	Routed Access	Virtual Switch
Protokollok	STP	Routing, pl: OSPF	(PAgP, LACP)
FHRP	Szükséges	Nincs	Nincs
Terhelésmegosztás	Alhálózat vagy hoszt alapon	Flow alapon	Flow alapon
Konvergencia	900ms-50mp	50-600ms	50-600ms

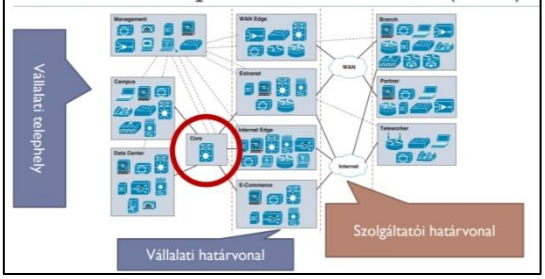
4. Nagyvállalati hálózat architektúra. Modulok, határvonalak

Campus hierarchia

- 3 szintű hierarchia
  - Lehet kevesebb is és több is
- **Access/hozzáférési réteg**: Felhasználók és eszközök közvetlen hálózat elérése
- **Distribution/elosztási réteg**: Access rétegek aggregációja, szolgáltatások elérhetősége
- **Core/központi réteg**: Nagy hálózatokban a distribution rétegek összekapcsolása



CISCO Enterprise Architecture (CEA)



Intranet Data Center

- A kritikus alkalmazások és adatok zöme
  - Jellemző a virtualizáció
  - Az egyik alapvető követelmény a biztonságos tervezés
- Biztonság
  - Elszigetetlés (Isolation)
    - Tűzfalak, hozzáférési listák, VLAN-ok, virtualizáció, fizikai elszigetelés
  - Házirendek (Policy Enforcement)
  - Felügyelet (Visibility)

Data Center Access

- L2 kapcsolat a szerverfarmhoz
- Skálázhatóság a legalapvetőbb kritérium
- L2-re fókuszált védelem
  - VLAN technológia az adatutak szétválasztására
  - Hozzáférési listák (ACL) a jogosultságok ellenőrzésére
  - ARP-DHCP forgalom felügyelete
  - Port elárasztások megakadályozása
- Virtuális hozzáférési réteg
  - Logikailag a hozzáférési réteggel egyező

Catalyst Integrated Security Features (CIFS)

Enterprise Campus – hozzáférési réteg

- A nagyvállalati felhasználók csatlakozása
  - Heterogén eszközök (munkaállomás, laptop, printer, VoIP telefon, …)
    - Nehezen karbantartható megfelelő biztonság (sérülékenységek, vírusok)
    - Hordozhatóságból adódóan vállalathoz bejutó problémák
      - A felhasználók hozzák be a támadást
  - Veszélyeztetik az egész nagyvállalatot

Enterprise Campus – elosztási réteg

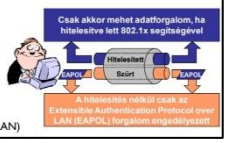
- Infrastruktúra védelme
- Végpontok védelme
- Behatolás felismerő rendszerek (IDS/IPS)
  - Adatútba helyezve (inline)
    - Azonnal hatás, a forgalom szűrése
    - Teljesítmény szempontjából kritikus
  - Lehallgató módban (promiscous)
    - Távoli szenzorok küldenek adatot (Switched Port Analyzer – SPAN, RSPAN)
  - Terhelésmegosztással is dolgozhatnak
    - Akár virtuális kapcsolók esetén is

Network Access Control (NAC)

- A hálózati elérés szabályozása
  - Különböző jogosultságú felhasználók
    - Dolgozó, szerződéses külsős, partner, vendég, …
  - A hálózat elérhető az egész campus területén
    - Ma már NEM a fizikai védelem (nincs hálózat) a jellemző
  - Személyes vagy szerepkör szerinti azonosítás
  - Megfelelés a biztonsági előírásoknak
    - Megfelelő biztonsági szoftverek, patchek
    - A nem megfelelő eszközök karanténba helyezése

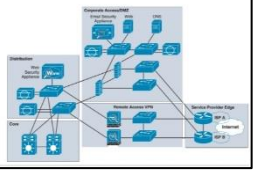
Végpontok csatlakozása

- Csatlakozás hitelesítése
  - IEEE 802.1X – Port-based Network Access Control
    - Felhasználó hitelesítése különböző módszerekkel
  - MAB - MAC Authentication Bypass
    - Hitelesítés MAC cím alapján
  - WebAuth
    - HTTP alapú kommunikáció
    - Hitelesítő oldal megjelenítése
- Hitelesítési sorrend (probléma esetén)
  - 802.1X -> MAB -> WebAuth
  - Változtatható, tilthető
- Újrahitelesítés lehetősége
- Hitelesítés nélkül külön hálózatra kerülhet (VLAN)



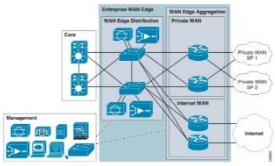
Enterprise Internet Edge

- Kapcsolódás az Internethez
- Gyakran tartalék a WAN eléréshez
- Szolgáltatói határ (SP Edge)
  - Router a szolgáltató felé
  - Redundáns
- Corporate Access/DMZ
  - A vállalat elérése
  - Szolgáltatások az Internet felhasználóknak
    - Demilitarizált övezet
    - WWW, FTP
- Távoli elérés (Remote access)
  - A vállalat elérése távoli dolgozók részére
- Határ elosztási réteg (Edge Distribution)
  - Interfész a nagyvállalati hálózathoz



Enterprise WAN Edge

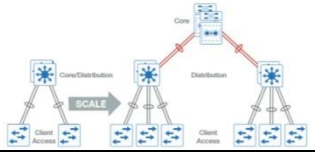
- Telephelyek összekötése
  - Üzleti alkalmazások
  - Együttműködés
- WAN határ aggregáció
  - Site-to-site VPN
- WAN határ elosztás
  - Hozzáférés a központi réteghez



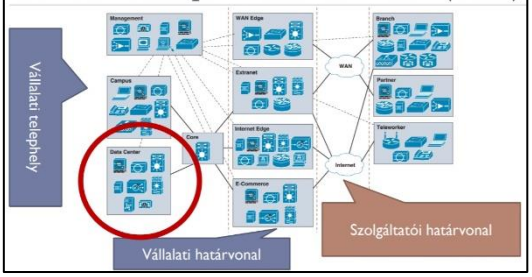
5. Nagyvállalati hálózat architektúra. Adatközpont

Campus hierarchia

- 3 szintű hierarchia
  - Lehet kevesebb is és több is
- **Access/hozzáférési réteg**: Felhasználók és eszközök közvetlen hálózat elérése
- **Distribution/elosztási réteg**: Access rétegek aggregációja, szolgáltatások elérhetősége
- **Core/központi réteg**: Nagy hálózatokban a distribution rétegek összekapcsolása



CISCO Enterprise Architecture (CEA)



Intranet Data Center

- A kritikus alkalmazások és adatok zöme
  - Jellemző a virtualizáció
  - Az egyik alapvető követelmény a biztonságos tervezés
- Biztonság
  - Elszigetelés (Isolation)
    - Tűzfalak, hozzáférési listák, VLAN-ok, virtualizáció, fizikai elszigetelés
  - Házirendek (Policy Enforcement)
  - Felügyelet (Visibility)

47 Hálózatok építése, konfigurálása és működtetése, BME-TMIT 2020/21

Data Center Core

- Belépési pont az adatközpontba
  - Routing feladatok
  - Az adatközpont aggregációs rétegek kapcsolása
- Védekezés routing támadások ellen
  - Az összekötött eszközök (peer) hitelesítése
  - Routing szűrések
  - Naplózás

50 Hálózatok építése, konfigurálása és működtetése, BME-TMIT 2020/21

Data Center Services

- Webes alkalmazások biztonsága
  - Tűzfal – Web Application Firewall (WAF)
    - Védelem a megszemélyesítés, adatlopás, szolgáltatás megtagadás, csalás ellen
    - Támadások: XSS (Cross Site Scripting) támadás, SQL injektálás, Buffer overflow, Cookie tampering, DoS
  - Működés, mint reverse proxy
- Behatolás jelző rendszerek – Intrusion Prevention System
  - DPI – Deep Packet Inspection
  - Anomáliák figyelése

53 Hálózatok építése, konfigurálása és működtetése, BME-TMIT 2020/21.2

Data Center támadások

- Kiszolgálás főleg a belső hálózat felé
  - De védekezés kívülről jövő támadások ellen is
  - Főleg alkalmazási rétegben lévő támadások (HTML, SQL, XML, …)
- Támadási vektorok
  - Jogosulatlan hozzáférés (eszközhöz vagy adatokhoz)
  - Szolgáltatás megakadályozás
  - Adatvesztés
  - Adat módosítás

48 Hálózatok építése, konfigurálása és működtetése, BME-TMIT 2020/21

Data Center Aggregation

- Virtual Device Context (VDC)
  - Síkok (vezérlés, adat, menedzsment) virtualizációja
  - Logikai szétválasztás
- Tűzfalak
  - Megfelelő hely a tűzfalak elhelyezésére
    - Nagy teljesítményű tűzfalak (10 Gbps forgalom megfigyelése)
    - Állapotok figyelése, Layer 2 forgalom
  - A tűzfal szintén virtualizálható, több logikai tűzfalra

51 Hálózatok építése, konfigurálása és működtetése, BME-TMIT 2020/21

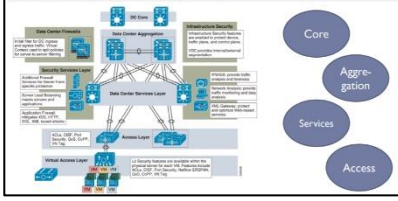
Data Center Access

- L2 kapcsolat a szerverfarmhoz
- Skálázhatóság a legalapvetőbb kritérium
- L2-re fókuszált védelem
  - VLAN technológia az adatutak szétválasztására
  - Hozzáférési listák (ACL) a jogosultságok ellenőrzésére
  - ARP-DHCP forgalom felügyelete
  - Port eláraszt ások megakadályozása
- Virtuális hozzáférési réteg
  - Logikailag a hozzáférési réteggel egyező

Catalyst Integrated Security Features (CIFS)

54 Hálózatok építése, konfigurálása és működtetése, BME-TMIT 2020/21.2

Data Center felépítése



Data Center Services

- Skálázhatóság
- Biztonság
- Védelem
  - Alkalmazás tűzfalak, tűzfalak
  - Behatolás jelző/megelőző rendszerek (Intrusion Detection/Prevention System)

A titkosított adatforgalom nem megfigyelhető, ezért itt már nincs titkosítás: SSL-proxy

ARP-DHCP felügyelet

- DHCP snooping
  - A nem megfelelő DHCP forgalom eldobása
  - Összerendelések: MAC cím – IP cím - VLAN
- Dynamic ARP inspection
  - A nem megfelelő ARP forgalom eldobása
  - Statikus konfiguráció vagy DHCP snooping
- IP Source Guard
  - IP cím hamisítás (IP spoofing) ellen
  - Statikus konfiguráció vagy DHCP snooping

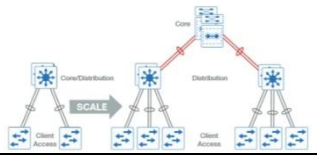
Virtuális hozzáférési réteg

- Virtuális gépek
  - Adott esetben a forgalom nem hagyja el a gazda gépet
    - Elszigetelés és megfigyelés nehézségei
  - Virtuális kapcsolók
    - Virtuális felügyelet és hálózati interfész
    - Házirend profilok az egyes virtuális interfészeknek
    - Beágyazott távoli port analizátor - Encapsulated Remote Switched Port Analyzer (ERSPAN)
      - Virtuális IDS/IPS szenzorok
      - Forgalom tükrözése forgalom analízis céljából

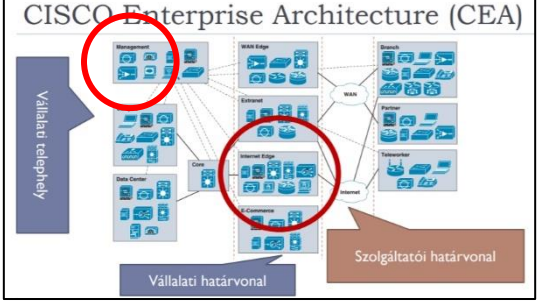
6. Nagyvállalati hálózat architektúra. Vállalati és szolgáltatói határvonal

Campus hierarchia

- 3 szintű hierarchia
  - Lehet kevesebb is és több is
- **Access/hozzáférési réteg**: Felhasználók és eszközök közvetlen hálózat elérése
- **Distribution/elosztási réteg**: Access rétegek aggregációja, szolgáltatások elérhetősége
- **Core/központi réteg**: Nagy hálózatokban a distribution rétegek összekapcsolása

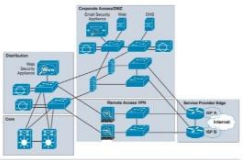


CISCO Enterprise Architecture (CEA)



Enterprise Internet Edge

- Kapcsolódás az Internethez
- Gyakran tartalék a WAN eléréshez
- Szolgáltatói határ (SP Edge)
  - Router a szolgáltató felé
  - Redundáns
- Corporate Access/DMZ
  - A vállalat elérése
  - Szolgáltatások az Internet felhasználóknak
    - Demilitarizált övezet
    - WWW, FTP
- Távoli elérés (Remote access)
  - A vállalat elérése távoli dolgozók részére
- Határ elosztási réteg (Edge Distribution)
  - Interfész a nagyvállalati hálózathoz



Fenyegetések

- Interfész a nyilvános hálózat felé
  - Támadások az Internetről
    - DoS és DDoS támadások
    - Alkalmazás, email, webes spyware, malware, adware, virus, spam, phishing
    - Alkalmazási réteg támadások
      - XSS

Védekezések

- Szolgáltatói határ
  - Védekezés redundanciával
    - Több router, több szolgáltató
  - Forgalom optimalizálása, terhelésmegosztás
- Vállalati elérés/DMZ
  - Demilitarizált övezet (DMZ)
    - Minden olyan forgalom, ami nem mehet be a nagyvállalati hálózatba
    - Csak a nyilvánosan elérhető szolgáltatások (WWW, FTP, email, DNS, …)
  - Tűzfalak
    - Kapcsolat megfigyelés (Connection tracking)
    - Deep Packet Inspection (DPI)
    - Web application firewall (WAF)

Védekezések 2.

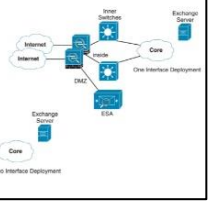
- Távoli elérés
  - Különböző VPN megoldások
    - SSL VPN: Csak bizonyos HTTP szolgáltatások elérése
  - Hitelesítés, jogosultság kezelés
  - Általában külön tűzfal (nem osztozik a vállalati tűzfallal)
- Határ elosztási réteg
  - Aggregált forgalom, szolgáltatások védelme
  - IDS/IPS megoldások
  - Cisco WSA (Web Security Appliance)
    - Tartalom szűrés
    - URL szűrés, malware és spyware blokkolása
    - Házirendek

Email és Web biztonság

- ESA: Email Security Appliance
- WSA: Web Security Appliance
- Az email és web forgalom figyelése
  - Globális küldési nagyságrendek, spamtrap accountok, DNS feloldás sikere, fekete listák, open-proxy, URL a vírusos levelekben
  - Pontozás különböző faktorok alapján, majd szűrés pontszám alapján (reputation score)

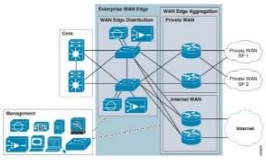
Email és Web biztonság 2.

- Email
  - SMTP (Simple Mail Transfer Protocol)
- Külső és belső emailek elkülönítése
  - Egy interfészes elrendezés
  - Két interfészes elrendezés
- ESA redundancia
  - DNS esetén tartalék MX címek
  - Terhelésmegosztás



Enterprise WAN Edge

- Telephelyek összekötése
  - Üzleti alkalmazások
  - Együttműködés
- WAN határ aggregáció
  - Site-to-site VPN
- WAN határ elosztás
  - Hozzáférés a központi réteghez



Fenyegetések

- Telephelyekről induló támadások
  - Trójai, vírus, botnet
- WAN hálózatban támadások, közbeékelődéses támadás (MITM)
- Jogosulatlan hozzáférés, jogosultság emelés
- DoS

Védekezés

- WAN kapcsolat védelme
  - WAN forgalom elkülönítése
    - Hitelesítés, integritás védelem
    - VPN segítségével, MPLS segítségével
    - IPSec
  - WAN hozzáférés hitelesítése
    - Erős hitelesítés
      - PKI alapon
  - WAN forgalom titkosítása
    - Erős titkosítás (pl.: AES)

WAN határ elosztási réteg

- IPS/IDS megoldások
  - Inline vagy promiscuous mód
  - Skálázhatóság
  - Kétirányú forgalom figyelése!
    - Másolás, egyetlen kapcsoló, forgalomirányítás, 'sticky' terhelésmegosztás
- Forgalomirányítás biztonsága
  - Szomszédok hitelesítése
  - Naplózás

7. WiFi hozzáférésvédelem. Rossz és jó megoldások

Wireless Fidelity

Vezetéknélküli hálózatok – miért is?

- Előnyök a korábbi vezetékes hálózatokkal szemben
  - Felhasználók
    - Az Intranet és Internet elérése vezetékek nélkül (vezetékes telefon és vezetéknélküli telefon)
    - Csatlakozás a frekventált helyeken (HOTSPOT)
      - Reptéri terminálok
      - Kávézók, szórakozóhelyek
      - Szállodák
  - Adminisztrátorok
    - Könnyen üzembe helyezhető
    - Olyan helyekre is elvihető, ahova vezetékeket nehezen lehet kihúzni
  - Üzleti szempont
    - Hosszútávon olcsóbb üzemeltetni, beruházás is olcsóbb lehet
    - HotSpot esetében a felhasználók fizetnek a szolgáltatásért
    - **WiFi offload – Tehermentesíteni más (mobil) hálózatokat**

Vezetéknélküli hálózat elemei

- Vezetéknélküli hálózati kártya
  - Leginkább könnyen mozgatható eszközökhöz Laptop, PDA és TablePC
    - De ma már fényképezőgép, videójáték, mobiltelefon …
  - Beépített eszközök, PCMCIA, CF kártya, USB eszköz, stb..
  - Egyedi MAC cím
- Hozzáférési pont (Access Point – AP)
  - A vezetéknélküli eszközök rádiókapcsolatban vannak a hozzáférési ponttal

Vezetéknélküli hálózatok kihívásai

- Legfőbb kihívások
  - Rádióhullámok (csatornák) interferenciája
    - Több hozzáférési pont elhelyezése
    - Egymást zavaró adások/zajok
    - Tereptárgyak hatásai
  - Eszközök tápellátása (részben vezetékes..)
    - Tápfelhasználás optimalizálása
  - Mozgás a hozzáférési pontok között
    - AP váltás, szolgáltató-váltás, technológia váltás
  - Biztonság

8 Hálózatok építése, konfigurálása és működtetése, BME-TMIT

Vezetéknélküli hálózatok biztonsága

- Vezetékes hálózat esetében az infrastruktúrához való hozzáférés sok behatolót megállít
- Vezetéknélküli hálózat esetén azonban megszűnik ez a korlát
  - A fizikai közeg nem biztosít adatbiztonságot, a küldött/fogadott adatokat mindenki észleli
  - A támadó nehézségek nélkül és észrevételenül hozzáfér a hálózathoz
  - Sokszor a hálózat eljut az lefedni kívánt területen kívülre is

9 Hálózatok építése, konfigurálása és működtetése, BME-TMIT

Vezetéknélküli hálózatok biztonsága 2.

- Felmerülő biztonsági kérdések
  - Hálózat elérésének korlátozása
  - Hitelesítés
    - A felhasználó hitelesítése
    - A szolgáltató hitelesítése
  - Sikeres hitelesítés után az adatok védelme
  - Infrastruktúra védelme
  - Anonimitás (jelenleg nem cél)

Hitelesítés problémái

- Kihívás-válasz alapú hitelesítés
  - Vezetékes környezetben jól működik
    - A felhasználó általában bízhat a vezeték épségében
  - Vezetéknélküli környezetben már nem tökéletes
    - A támadó könnyen megszerezheti a kihívást és a választ is
    - Gyenge jelszavak (és protokollok) eseték egyszerű a szótáras támadás

12 Hálózatok építése, konfigurálása és működtetése, BME-TMIT 2020/21.2

Szolgáltatásbiztonság problémái

- Hamis hozzáférési pontok (rogue AP)
  - Könnyű elrejteni – egy SD kártya is lehet AP!
  - Lehet falakon kívül is (irányított antennák)
  - A felhasználó nem feltétlenül ismeri Pl.: HOTSPOT környezet
  - Segítségével közbeékelődéses (man-in-the-middle) támadások
- Szolgálatmegtagadás DoS
  - Szolgálatmegtagadás elárasztással egy vezetékes eszközről
  - Fizikai akadályoztatás (jammer)

13 Hálózatok építése, konfigurálása és működtetése, BME-TMIT 2020/21.2

Hozzáférés vezérlés – MAC szűrés

- Hozzáférés szűrése MAC címek alapján
  - A hozzáférési pontnak listája van az engedélyezett kártyákról (vagy tiltott kártyák)
  - Nem biztonságos, mert:
    - A MAC címek lehallgathatóak a hálózaton és felvehetőek egy másik eszköz által
    - Az eszközök megszerzése már hozzáférést biztosít
    - Több hozzáférési pont menedzsmentje nehéz
- Sajnos ma is ez van a sok „biztonságos" helyen

BME

Hozzáférés vezérlés – SSID tiltás

- A hozzáférési pontok elrejtése
  - A hozzáférési pont nem közli a saját azonosítóját (Service Set ID - SSID)
  - Csak azok a készülékek csatlakozhatnak, akik ismerik ezt
    - PROBE request
  - Lehallgatással felderíthető!

www.wifidetective.com

TOP 10 ESSID (hálózatnév)	darabszám
SPIC	1274
linksys	1013
default	1003
TP-LINK	500
NETGEAR	437
belkin	337
belkin54g	322
GIGABYTE	213
WIBRA	195
WLAN	150

15 Hálózatok építése, konfigurálása és működtetése, BME-TMIT 2020/21.2

Hozzáférés vezérlés - WEP

- Hitelesítés és adatkommunikáció védelem a WEP protokollal
  - Wired Equivalent Privacy
    - Kitűzött cél: Pont olyan védett, mintha vezetékes lenne
- Hitelesítés és titkosítás
  - Hitelesítés: az eszköz ismeri a WEP kulcsot
    - Nem a felhasználót hitelesítjük, hanem az eszközt
  - RC4 titkosító használata (gyors!)
  - CRC32 hibajelző kód (gyakran használjuk)
    - Cyclic Redundancy Check
    - Titkosítjuk a hibajelző kimenetét
- Kihívás – válasz alapú hozzáférés vezérlés

16 Hálózatok építése, konfigurálása és működtetése, BME-TMIT 2020/21.2

WEP törések

- 2002
  - „Using the Fluhrer, Mantin, and Shamir Attack to Break WEP, A. Stubblefield, J. Ioannidis, A. Rubin"
    - Gyenge WEP IV-k
    - 4.000.000 – 6.000.000 csomag
- 2004
  - KoReK, fejlesztett FMS támadás
    - 500.000 – 2.000.000 csomag (104 bites WEP)
- 2006
  - KoReK, Chopchop támadás
    - Az AP segítségével a titkosított CRC miatt bájtonként megfejthető a titkosított üzenet
- 2007
  - PTW (Erik Tews, Andrei Pychkine and Ralf-Philipp Weinmann), még több korreláció
    - 60.000 – 90.000 csomag (104 bites WEP)

WEP hibák

- HIBA 1:
  - Az titkos kulcs és a publikus IV egyszerűen csak illesztve van. Ennek segítségével az RC4 kimenetéből kiszámítható a titkos kulcs!!!
- HIBA 2:
  - A titkos kulcs kezdetben túlságosan rövid, mindössze 40 bit. Ma 104 bit.
- HIBA 3:
  - Az IV túlságosan rövid (24 bit) és nincsen egyértelmű utasítás hogyan alkalmazzuk. A megismételt sorszám felfedheti a titkosított adatot. Sok eszköz mindig nullázta az IV-t induláskor. Szülinapi paradoxon miatt, amúgy is ütközés 2^12 véletlen sorszám után
- HIBA 4:
  - A titkosított CRC32 kód nem véd. Az értéke kiszámítható a változás ismeretében
- **Hamis biztonságérzet!**

18 Hálózatok építése, konfigurálása és működtetése, BME-TMIT 2020/21.2

Adatszerzés WEP töréshez

- Hamisított csomagok
  - De-authentication
  - ARP response kicsikarása
    - Módosított ARP request / Gratuitous ARP üzenet
    - WEP esetén könnyen módosítható a titkosított ARP is (rossz integritás védelem)
- „Caffé latte" támadás
  - Nem szükséges a WEP hálózatban lenni
    - A PC/smartphone tárolja a WEP kulcsokat, a hamis AP megtévesztheti
    - Hamis ARP üzenetekkel 90.000 csomag gyűjtése
    - 6 perces támadás

19 Hálózatok építése, konfigurálása és működtetése, BME-TMIT 2020/21.2

WEP patch

- Nagy kulcsok
- Gyenge IVk elkerülése
- ARP filter
- WEP Chaffing
  - Megtévesztő WEP csomagok injektálása. Hatására a WEP törésnél hibás adatok alapján számolódik a kulcs
  - A törő algoritmusok javíthatóak..

WPA - Wi-Fi Protected Access

- Wi-Fi Allience a WEP problémáinak kijavítására (2003)
  - Szabványokon alapuló
  - Erős biztonság
  - Hitelesítés és adatbiztonság
  - **ssssss**
  - A meglévő eszközökön csak SW frissítés
  - Kompatibilis a közelgő 802.11i szabvánnyal
- A fokozott biztonság mellett cél a gyors elterjedés is!

22 Hálózatok építése, konfigurálása és működtetése, BME-TMIT 2020/21.2

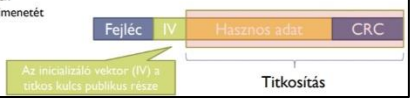
WPA - TKIP

- A WEP összes ismert hibájának orvoslása, megőrizve minél több WEP blokkot
- Titkosítás: Temporal Key Integrity Protocol (TKIP)
  - Per-packet key mixing (nem csak hozzáfűzés)
  - Message Integrity Check (MIC) - Michael
  - Bővített inicializáló vektor (48 bit IV) sorszámozási szabályokkal
  - Idővel lecserélt kulcsok (Nem jó, de muszáj)
- Hitelesítés: 802.1x és EAP
  - A hitelesítés biztosítása
    - Kölcsönös hitelesítés is (EAP-TLS)
  - A hitelesítés változhat a környezettől függően (SOHO <> Enterprise <> HOTSPOT)

8. WEP – WPA1 – WPA2 protokollok. Problémák és javítások

Hozzáférés vezérlés - WEP

- Hitelesítés és adatkommunikáció védelem a WEP protokollal
  - Wired Equivalent Privacy
    - Kitűzött cél: Pont olyan védett, mintha vezetékes lenne
- Hitelesítés és titkosítás
  - Hitelesítés: az eszköz ismeri a WEP kulcsot
    - Nem a felhasználót hitelesítjük, hanem az eszközt
  - RC4 titkosító használata (gyors!)
  - CRC32 hibajelző kód (gyakran használjuk)
    - Cyclic Redundancy Check
    - Titkosítjuk a hibajelző kimenetét
- Kihívás – válasz alapú hozzáférés vezérlés



WEP patch

- Nagy kulcsok
- Gyenge IVk elkerülése
- ARP filter
- WEP Chaffing
  - Megtévesztő WEP csomagok injektálása. Hatására a WEP törésnél hibás adatok alapján számolódik a kulcs
  - A törő algoritmusok javíthatóak..

Hitelesítés problémái

- Kihívás-válasz alapú hitelesítés
  - Vezetékes környezetben jól működik
    - A felhasználó általában bízhat a vezeték épségében
  - Vezetéknélküli környezetben már nem tökéletes
    - A támadó könnyen megszerezheti a kihívást és a választ is
    - Gyenge jelszavak (és protokollok) eseték egyszerű a szótáras támadás

WPA - Wi-Fi Protected Access

- Wi-Fi Allience a WEP problémáinak kijavítására (2003)
  - Szabványokon alapuló
  - Erős biztonság
  - Hitelesítés és adatbiztonság
  - SSSSSS
  - A meglévő eszközökön csak SW frissítés
  - Kompatibilis a közelgő 802.11i szabvánnyal
- A fokozott biztonság mellett cél a gyors elterjedés is!

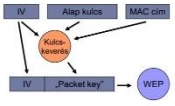
	WEP	*TKIP*	*CCMP*
Titkosító	RC4, 40 vagy 104 bites kulcs	RC4, 128 és 64 bites kulcs	AES, 128 bites kulcs
Kulcs élettartama	24 bites IV	48 bites IV	48 bites IV
Csomagkulcs	Összefűzés	TKIP kulcskeverés	nem szükséges
Fejléc integritása	nincs védve	Michael: Forrás és cél MAC	CCM
Adatok integritása	CRC-32	Michael	CCM
Visszajátszás védelem	nincs védelem	IV szabályok	IV szabályok
Kulcs-menedzsment	nincs	IEEE 802.1X	IEEE 802.1X

WPA - TKIP

- A WEP összes ismert hibájának orvoslása, megőrizve minél több WEP blokkot
- Titkosítás: Temporal Key Integrity Protocol (TKIP)
  - Per-packet key mixing (nem csak hozzáfűzés)
  - Message Integrity Check (MIC) - Michael
  - Bővített inicializáló vektor (48 bit IV) sorszámozási szabályokkal
  - Idővel lecserélt kulcsok (Nem jó, de muszáj)
- Hitelesítés: 802.1x és EAP
  - A hitelesítés biztosítása
    - Kölcsönös hitelesítés is (EAP-TLS)
  - A hitelesítés változhat a környezettől függően (SOHO <> Enterprise <> HOTSPOT)

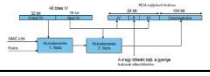
TKIP

- Per Packet Keying
- Az IV változásával minden üzenetnek más kulcsa lesz
- Minden terminálnak más kulcsa lesz, akkor is, ha az alap kulcs véletlenül egyezne
- A packet kulcsot használjuk az eredeti WEP kulcs helyett



TKIP – kulcs keverés

- 128 bites ideiglenes kulcs
- Csomagkulcs előállítása 2 lépésben
  - Feistel alapú kódoló használata (Doug Whiting és Ron Rivest)
  - 1. lépés
    - A forrás MAC címének, az ideiglenes kulcsnak és az IV felső 32 bitjének keverése
    - Az eredmény ideiglenesen tárolható, 2^{16} kulcsot lehet még előállítani. Ez javítja a teljesítményt
  - 2. lépés
    - Az IV és a kulcs függetlenítése



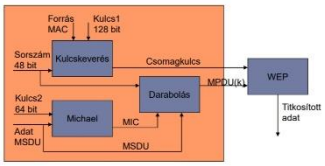
IV sorszámozás

- IV szabályok
  - Mindig 0-ról indul kulcskiosztás után
    - Ellentétben a WEP-pel, itt ez nem gond, mert úgy is más kulcsunk lesz minden egyeztetésnél
  - Minden csomagnál eggyel nő az IV
    - Ha nem, akkor eldobjuk az üzenetet
- A 48 bites IV már nem merül ki
  - Ha mégis, akkor leáll a forgalom

MIC

- Message Integrity Code
- Michael algoritmus (Neils Ferguson)
  - 64 bites kulcs 64 bites hitelesítés
  - Erőssége: kb. 30 bit, azaz a támadó 2^{31} üzenet megfigyelésével képes egy hamisat létrehozni
    - Nem túl erős védelem
    - De egy erősebb (HMAC-SHA-1 vagy DEC-CBC-MAC) már nagyon rontaná a teljesítményt
    - + védelem: ha aktív támadást észlel, akkor azonnal megváltoztatja a kulcsot + 1 percig nem enged újra változtatni
  - Már nem csak az adatot védjük, hanem a forrás és cél MAC címeket is!
  - Nincs külön sorszámozás, a visszajátszás elleni védelem úgy van biztosítva, hogy a MIC értéket titkosítjuk (itt van sorszám)

TKIP működése

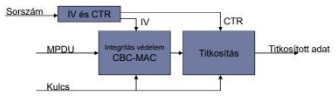


802.11i (WPA2)

- IEEE - 2004 –ben jelent meg
  - WPA +
    - Biztonságos IBSS
    - Biztonságos gyors hálózatváltások
    - A hitelesítés biztonságos feloldása
    - Új titkosító protokollok: AES-CCMP, WRAP
  - Már szükséges a HW módosítása is
    - Lassabb elterjedés, de mára már elterjedt

CCMP

- Counter Mode CBC-MAC Protocol
- Az AES használata



CBC-MAC

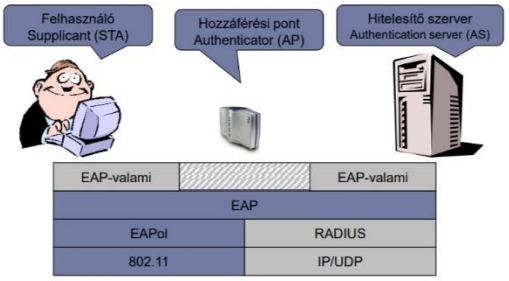
- Cipher Block Chaining Message Authentication Code
- Módszer
  - 1. Az első blokk titkosítása
  - 2. Az eredmény és a következő blokk XOR kapcsolat, aztán titkosítás
  - 3. A második lépés ismétlése
- Szükséges a kitöltés (padding)!

CCMP előnyök:

Egy kulcs elég, AES (párhuzamosítható, nagy biztonság, előre számolható), szabadalom mentes.

9. IEEE 802.1X protokoll feladata és működése

802.1x protokollok



802.1x

- IEEE specifikáció a (W)LAN biztonság javítására (2001)
  - Protokollok a hitelesítés és az adatok védelmére
    - RADIUS (de facto)
      - Hitelesítés a hozzáférési pontokon túl
      - Széles körben elfogadott és alkalmazott hitelesítési módszer
    - EAP és EAPoL (EAP over Lan)
      - Transzport protokoll a biztonság (hitelesítés és adatvédelem) egyeztetésére
      - EAP-MD5 Challange, EAP-TLS, LEAP (EAP-Cisco Wireless), PEAP
    - Nagyon jól illik WLAN környezetbe:
      - Felhasználó alapú hitelesítés
      - A hozzáférési pont nem ismeri a hitelesítést (egyszerű és olcsó)
      - Központosított hitelesítés

802.1x és WEP

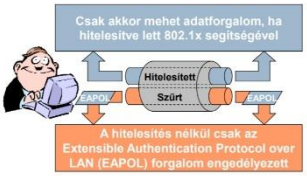
- Nem célja, hogy javítsa a WEP hibáit!
  - Az adatok biztonságát továbbra is a WEP biztosítja (így persze nem ér semmit)
  - De a 802.1x képes kulcsot egyeztetni az adattitkosítás számára is
- Új protokollok a WEP javítására
  - TKIP, CCMP, WRAP
  - Együttműködnek a 802.1x protokollal

EAPoL (EAPoW)

- EAP over LAN: EAP adaptáció a port alapú (802.1X) környezethez
- EAPoL kerettípusok:
  - EAP keret
    - Beágyazott EAP keret
  - EAPoL-Start
    - A kliens küldi, hogy elindítsa az EAP kommunikációt. Hatására EAP-Request/Identity jön
  - EAPoL-Logoff
    - Port lezárása
  - EAPoL-Key
    - Kulcscsere
  - EAPoL-Encapsulated-ASF-Alert
    - Riasztások engedélyezése az adott porton. (Pl. SNMP trap)

Hozzáférés szűrés

- Kezdetben csak EAPoL forgalom



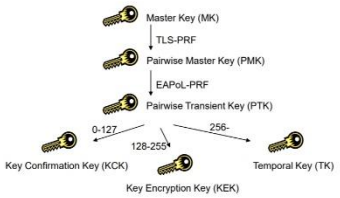
Kulcsok

- Master Key (MK)
  - A viszony alatt fennálló szimmetrikus kulcs a felhasználó (STA) és a hitelesítő szerver között (AS)
  - Csak ők birtokolhatják (STA és AS)
  - Minden más kulcs ebből származik
- Pairwise Master Key (PMK)
  - Frissített szimmetrikus kulcs a felhasználó (STA) és a hozzáférési pont (AP) között
  - A felhasználó (STA) generálja a kulcsot MK alapján
  - A hozzáférési pont (AP) a hitelesítő szervertől (AS) kapja

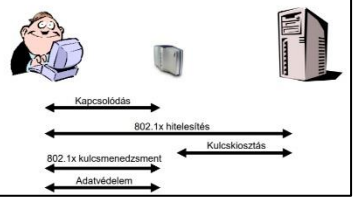
Kulcsok (folyt.)

- Pairwise Transient Key (PTK)
  - A felhasznált kulcsok gyűjteménye
  - Key Confirmation Key (PTK bitek 1-128)
    - A PMK ismeretének bizonyítása
  - Key Encryption Key (PTK bitek 129-256)
    - Más kulcsok terjesztése
  - Temporal Key (TK) (PTK bitek 257-..)
    - Az adatforgalom biztosítása

Kulcs hierarchia



802.1x működési fázisok



802.1x működési fázisok (folyt.)

- Kapcsolódás
  - A kommunikáló felek megállapítása (STA és AP)
  - A hozzáférési pont (AP) képességeinek ismertetése
- 802.1x hitelesítés
  - Központosított döntés a hitelesítő szervernél (AS)
  - A felhasználó (STA) eldönti, hogy kíván-e csatlakozni
  - A felek (STA és AS) kölcsönös azonosítása
  - Master kulcs (MK) és Pairwise Master kulcs (PMK) generálása

802.1x működési fázisok (folyt.)

- Kulcskiosztás
  - A Pairwise Master kulcs (PMK) mozgatása a hozzáférési ponthoz (AP)
- 802.1x kulcsmenedzsment
  - A PMK hozzárendelése a felekhez (STA és AP) + ellenőrzés
  - Friss kulcsok generálása (PTK) és szétosztása

Kapcsolódás

- Kapcsolódás (authentication + association)

Kapcsolódás lépései

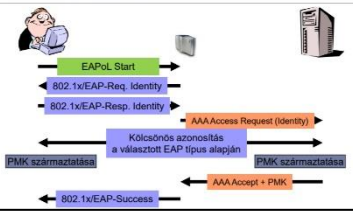
1. Beacon vagy Probe (próba) küldése és válasz
   - Az AP tulajdonságai:
     - SSID: Az hozzáférési pont azonosítása
     - Támogatott hitelesítések
     - Támogatott unicast/multicast titkosítások
   - Biztonság szempontból nem számít, bár néha elhagyják az SSID-t
     - „nem látható hálózatok"

Képesség felderítés lépései (folyt.)

2. 802.11 nyílt azonosítás
   - Kompatibilitás miatt tartották meg
   - Semmi biztonság nincs benne
   - Létezik közös titok alapú hitelesítés is, ez a WEP alapján működik (hamisítható)
3. Kapcsolódás (asszociáció) kérelem/válasz
   - A hozzáférési pont által hirdetett hitelesítés kiválasztása

- Itt még nincs biztonság semmilyen szinten!
- A felek készek a hitelesítésre és a kommunikációra

802.1x hitelesítés



802.1x hitelesítés lépései

- A hitelesítést a felhasználó indítja, de a hitelesítő szerver (AS) választja meg a módszert
  - A hitelesítő legtöbbször RADIUS szerver
    - Tapasztalatok, fejlesztések
  - A hitelesítő módszer legtöbbször EAP-TLS, EAP-TTLS vagy PEAP
    - Több kell, mint kihívás alapú hitelesítés
    - Privát/publikus kulcsok használata
- Sikeres hitelesítés esetén a hozzáférési pont (AP) megkapja a Pairwise Master Key (PMK) –t is
- Otthoni és ad-hoc környezetben nem szükséges hitelesítő központ
  - Pre-shared Key (PSK) használta PMK helyett
  - Az otthoni felhasználó ritkán kezel kulcsokat..

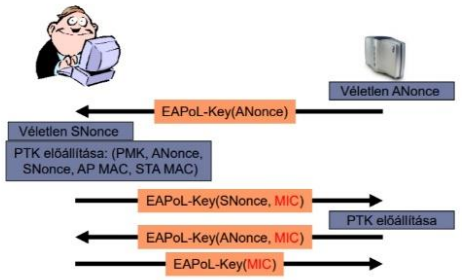
802.1x hitelesítés gondok

- Az EAP nem biztosít védelmet
  - Hamisított AAA-Accept üzenetek
- RADIUS
  - Statikus kulcs a hozzáférési pont (AP) és a hitelesítő szerver (AS) között
  - A hozzáférési pont minden üzenettel együtt egy kihívást is küld
    - Hamisított üzenetekre a RADIUS szerver gond nélkül válaszol
  - Megoldást a DIAMETER hitelesítő jelenthet
    - Sajnos úgy látszik ez sem fogja tökéletesen megoldani a problémát

802.1x kulcsmenedzsment

- A Pairwise Master Key (PMK) segítségével a felhasználó (STA) és a hozzáférési pont (AP) képes előállítani a Pairwise Transient Key (PTK) –t
  - A PMK kulcsot (ha a hitelesítő szerverben (AS) lehet bízni, akkor csak ők ismerik
  - A PTK kulcsot mindketten (STA és AP) származtatják (nem utazik a hálózaton!) és ellenőrzik, hogy a másik fél valóban ismeri
    - 4 utas kézfogás
  - A többi kulcsot vagy egyenesen a PTK –ból származtatják (megfelelő bitek) vagy a KEK segítségével szállítják a hálózaton (pl. Group TK)

4 utas kézfogás



4 utas kézfogás lépései

- MIC: Az üzenetek integritásának védelme
- Man-in-the-middle támadások kizárása
  - A 2. üzenet mutatja, hogy
    - A felhasználó (STA) ismeri PMK –t
    - A megfelelő ANonce –t kapta meg
  - A 3. üzenet mutatja, hogy
    - A hozzáférési pont (AP) ismeri PMK –t
    - A megfelelő SNonce –t kapta meg
- A 4. üzenet csak azért van, hogy teljes legyen a kérdés/válasz működés

Adatvédelem

- A TK (multicast esetén Group Transient Key - GTK) felhasználható az adatok tikosítására
  - A kulcsot a hitelesítés mellett egyeztetik (melléktermék)
- Felhasználható titkosítások:
  - TKIP
  - CCMP
  - WRAP (Patent gondok, nincs a szabványban)

10. RADIUS / EAP protokollok és főbb hitelesítő metódusok

RADIUS

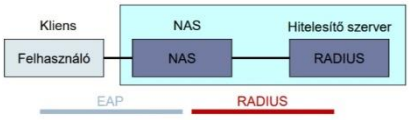
- Remote Authentication Dial In User Service
  - Eredetileg a betárcsázós felhasználóknak (Merit Networks és Livingston Enterprises)
  - Ma már széleskörű használat
    - Azonosítás nem csak dial-in felhasználáskor
    - xDSL felhasználó azonosítás
    - Nagyvállalalti WiFi
    - Távközlésben számlázáshoz
- AAA szolgáltatás nyújtása
  - Authentication - Hitelesítés
  - Authorization - Jogosultság kezelés
  - Accounting - Számlázás

RADIUS tulajdonságok

- Legfőbb tulajdonságok
  - UDP alapú (kapcsolatmentes)
    - 1812 –es port
    - Hálózati hiba kezelése a RADIUS részéről
  - Állapotmentes
    - Multithread támogatás
  - Hop by hop biztonság
- Hiányosságok
  - End to end biztonság támogatása
  - Skálázhatósági problémák (főleg torlódás esetén)

RADIUS kapcsolat

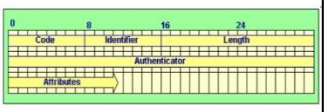
- Kliens - NAS - RADIUS



- Sok esetben a kliens és a hitelesítő szerver kommunikál (hitelesít)
  - A NAS csak továbbítja az üzeneteket
- De van RADIUS – RADIUS kapcsolat is (proxy)

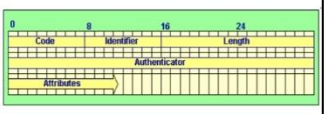
RADIUS üzenetek

- Kérés/válasz üzenetek



- Code
  - 1: acces-request, 2: acces-accept, 3: access-reject
  - 4: accounting-request, 5: accounting-response
  - 11: access-challenge
  - 12: status-server, 13: status-client
  - 255: reserved
- Identifier
  - Üzenetváltás azonosítója
    - A kérés válasz összerendelése
  - Egyszerre csak max. 256 üzenetváltás
- Length
  - Üzenet hossza: 20 – 4096 bájt

Radius üzenetek (folyt.)



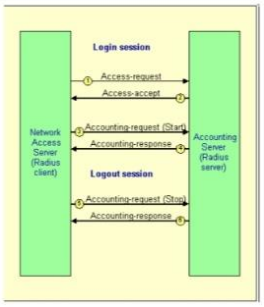
- Authenticator
  - 16 bájt hitelesítés
  - Request authenticator:
    - Hitelesítés kérés: 16 bájt véletlen érték
    - Lehet egyben a CHAP kihívás is
    - Jelszó elrejtése
  - Response authenticator:
    - Hitelesítés válasz: MD5(Code, ID, Length, hit. kérés, AVs, közös titok)
    - Hitelesítés és integritás védelem

RADIUS üzenetek - AVP

- Attribútum-érték párok (AVP)
  - Attribútum (1 bájt) – hossz (1 bájt) - érték mezőhármas
  - Az attribútum csak számmal jelölve
    - Típusok:
      - Integer, Enumeration, IP Address, String, Date, Binary
    - Előre definiált attribútumok
    - 26:Vendor-specific attribute
      - VSA mező, hasonló az AVP –hez
      - Gyártó – típus – hossz - érték
- Attribútumok:
  - User-Name, User-Password, CHAP-Password, NAS-IP-Address, NAS-Port, Service-Type, …
  - Szótár az attribútum név és száma (típus) megfeleltetéséhez

RADIUS üzenetváltás

- Kérdés-válasz típusú
- Hitelesítés esetén
  - Kérés:
    - access-request
  - Válasz:
    - acces-accept
    - access-reject
    - access-challenge
- Számlázás esetén
  - késedelmi idő
  - viszony idő
  - küldött és fogadott bájtok, csomagok
  - magyarázat a bontásra



Extensible Authentication Protocol (EAP)

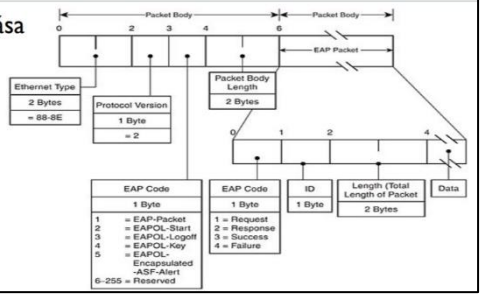
- Hitelesítő keretprotokoll, mely egy konkrét metódus alapján hitelesí
  - Plusz információk kicserélésének lehetősége
- A NAS szerepe
  - Nem hitelesít, továbbítja az EAP hitelesítési üzeneteket
    - EAP beágyazása RADIUS üzenetekbe
  - A NAS nem feltétlenül ismeri az azonosítás módját
    DE: Muszáj ismerni, hogy sikerült-e vagy sem!
- Hitelesítési lehetőségek (metódusok)
  - Pl.: MD-5 kihívás, egyszeri jelszavak (OTP), nyilvános kulcsok
  - Bővíthető!

EAP tulajdonságok

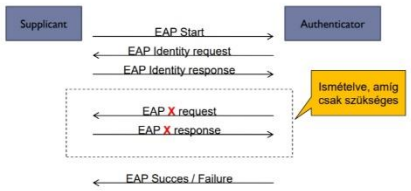
- Duplikált üzenetek elnyomása és újraküldés szükséges
  - Elhelyezkedhet a lokális linken és az AAA stackjében is
- Az alsóbb rétegnek kell biztosítania az üzenetek hitelességét
  - Pl.: Hamis EAP-Success üzenetek veszélye

EAPoL – EAP a linken

- EAP szállítása

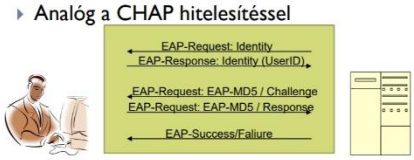


EAP üzenetciklus



EAP-MD5

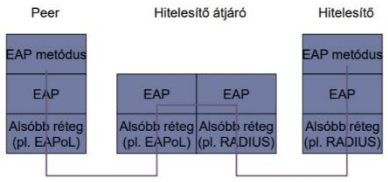
- IETF RFC 3748
- Analóg a CHAP hitelesítéssel



	EAP-MD5	EAP-TLS	EAP-TTLS	PEAP
Kliens hitelesítés	MD5	Tanúsítvány	Bármi	EAP
Szerver hitelesítés	-	Tanúsítvány	Tanúsítvány*	Tanúsítvány*
Hitelesítés iránya	Kliens hitelesítése	Kölcsönös	Kölcsönös	Kölcsönös
Felhasználó identitásának védelme	Nincs	Nincs	TLS	TLS

Hitelesítő EAP segítségével

- Nem a NAS végzi a hitelesítést!



EAP üzenetek

- Több kérdés és válasz ciklus
  - Az authenticator kérdez, supplicant válaszol
  - Egyszerre csak 1 aktív kérdés
  - Egy viszonyban csak egyetlen hitelesítési mód
- A kérdések ismételve, ha nem érkezik válasz
  - Kivéve sikeres és sikertelen üzenetek
- Kérés (request) és válasz (response)
  - Code (1 byte) – Azonosító (1 byte) – Hossz, beleértve a fejlécet is (2 byte) – Adat/hitelesítő típus (1 byte) – Adatok a megadott hosszúságban
- Sikeres és sikertelen üzenet
  - Code (1 byte) – Azonosító (1 byte) – Hossz (2 byte)
  - A hossz itt 4 bájt

EAP code, type

- Code
  1: kérés, 2: válasz, 3: siker, 4: sikertelen, 5: Inicializálás, 6: Befejezés
- Type
  - 1: Identitás (Identity)
    - A végpont identitásának lekérdezése
  - 2: Figyelmeztetés (Notification)
    - Megjelenítendő üzenet
  - 3: Elutasítás (Nak)
    - Érvénytelen vagy értelmezhetetlen típus
    - Csak válasz esetén

EAP hitelesítő típusok

- 4: MD5-Challenge
  - A CHAP megfelelője
- 5: Egyszeri jelszó (One-Time Password - OTP)
  - OTP kihívás és válasz
- 6: Általános jelkártya (Generic Token Card)
  - üzenet és válasz

…

- 13: EAP-TLS
- 21: EAP-TTLS
- 25: PEAP, Protected EAP
- 26: MS-EAP-Authentication (EAP/MS-CHAPv2)

EAP-TLS

- TLS – Transport Layer Security
  - Kölcsönös azonosítás
    - Certificate: Nyilvános kulcsú azonosítás
    - Kliens és szerver tanúsítványok
  - Integritás védelem
  - Kulcscsere
- EAP-TLS
  - IETF RFC 2716
  - A TLS funkcióinak átültetése PPP hitelesítéshez
  - Csak a „handshake" funkció, nem a titkosítás!

EAP-TTLS

- EAP-TTLS
  - Tuneled Transport Layer Security
  - IETF draft: Funk, Meetinghouse
- Hitelesítés
  - 1. lépés: Titkos csatorna felépítése (TLS)
    - Csak a szerver azonosítja magát
  - 2. lépés: Aktuális hitelesítés
    - AVP üzenetek, a RADIUShoz hasonlóan
  - Támogatott hitelesítések:
    - EAP módszerek, PAP, CHAP, MS-CHAP, MS-CHAPv2

PEAP

- PEAP
  - Protected EAP
  - IETF draft: Microsoft (+ Cisco és RSA)
- Hitelesítés
  (hasonlóan az EAP-TTLS-hez)
  - 1. lépés: Titkos csatorna felépítése (TLS)
    - Csak a szerver azonosítja magát
  - 2. lépés: Aktuális hitelesítés
  - Támogatott hitelesítések:
    - Csak EAP módszerek + MSCHAPv2
    - EAP esetén az üzenetek beágyazva EAP-TLV –be (type-length-value)

11. SSO és Kerberos

Single Sign On környezet

- Alap helyzet:
  - Sok gép, sok szolgáltatás, emberek jönnek - mennek
  - Sok jelszó, amit fejben kell tartani, gyakran kéne cserélni. Általában leírják őket
  - Gyorsan új accountok létrehozása, régi jogok törlése

SSO

- Megoldás
  - Single Sign On, avagy Egyszeri belépés
  - csak 1 bejelentkezés, csak 1 jelszó!
- SSO Előnyök
  - Egyetlen jelszó mindenhez: Nem kell fejben tartani, nem kell leírni, nem okoz gondot a sűrű csere
  - Egyetlen adatbázis, könnyebb és gyorsabb adminisztráció. Pl. mi van ha valaki elhagyja a céget...

SSO megközelítések

- Bróker alapú
  - A bróker azonosít és kioszt egy tanúsítványt, amit a szolgáltatásnak be lehet mutatni.
  - Pl.: KERBEROS, SESAME (Secure European System for Applications in a Multi-vendor Environment)
    - Az alkalmazásokat a brókerhez kell igazítani. (Kerberized alkalmazások)
    - Központosított adminisztráció, de mi van, ha megsérül
    - Nagyon sok múlik az azonosításon

SSO megközelítések 2.

- Ügynök alapú
  - Egy ügynök automatikusan azonosít minden alkalmazásnak. (Jelszó listák vagy kulcsok)
    - Pl.: SSH ügynök
  - Előnyök és hátrányok
    - Az alkalmazásokat nem kell módosítani, működik a régiekkel is
    - Nem támogatja az adminisztrációt, sőt még az ügynökök miatt is aggódni kell
    - Az ügynököket biztonságosan kell tárolni

SSO megközelítések 3.

- Token alapú
  - Egy fizikai eszköz egy egyszer használatos kódot szerez, és ezt használja fel.
    - A fizikai eszköz csak plusz komplikáció
    - De biztonságosabb azonosítás
- Átjáró alapú
  - A szolgáltatások egy biztonságos területen vannak elhelyezve. A hozzáféréshez egy „tűzfalon" kell átjutni.
    - Hasonlít a bróker alapú megoldásra
    - Sok átjáró esetén szinkronizáció kell
- Ügynök és Bróker alapú
  - Egyesíti a két megoldás előnyeit. A felhasználó felé broker alapú, az alkalmazások felé ügynök alapú

Kerberos 5

- Kerberos és a jogosítványok
- A felhasználó egy szolgáltatást szeretne igénybe venni egy meghatározott szerveren. Létezik egy azonosítást végző központ, aki azonosítani tudja a szolgáltatást és a felhasználót is. Feladat, hogy a felhasználó azonosítsa magát a szolgáltatásnál.
- De CSAK „Kerberized" alkalmazások!
- MIT fejlesztés
  - 1988 október - Kerberos 4
  - 1993 szeptember - RFC 1510: Kerberos 5

Kerberos azonosítás

- Biztonság
  - Nincsenek nyílt jelszavak (DES titkosítás használata, a jelszó mint kulcs)
  - A szolgáltatás nem tartja nyilván a felhasználókat
  - A jelszó megszerzése csak 1 felhasználót vagy szolgáltatást tesz kiszolgáltatottá
  - Egyetlen jelszó az összes szolgáltatáshoz (regisztrációnál egyeztetve)

Ticket Granting Server (TGS)

- Cél, hogy a felhasználónak ne kelljen minden szolgáltatáshoz jelszavát ismételten megadnia: SSO
- A TGS egy olyan szolgáltatás, amely megszerzi helyette a kívánt viszonykulcsot. Kvázi egy „guest ID" amivel egy vendég bemegy egy épületbe
- TGT: Ticket Granting Ticket, az amit a TGS ad. Ez csak limitált ideig érvényes azonban!
- A TGS külön egység, de sokszor az AS melltett található (együtt: KDC - Key Distribution Center)

Kerberos előnyök

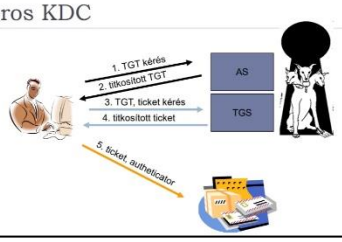
- Teljes SSO megvalósítás
- A hitelesítés állapotmentes
  - Kiesés esetén a szolgáltatást más Kerberos kiszolgáló tudja folytatni
  - Elosztott Kerberos szolgáltatás
    - Egyetlen „master" adatbázis, a többi kiszolgáló tükrözi és csak olvasható módon használja

Azonosítás kellékei

- AS - Authentication Server
- TGS - Ticket Granting Server
- Kulcsok
  - A felhasználó kulcsa (jelszó)
  - A szolgáltatás kulcsa (biztonságos)
  - Az ideiglenes viszonykulcs
- Üzenetek
  - "Ticket"
  - "Authenticator"

KDC: Key Distribution Center

Kerberos KDC



(Cross Realm) Tartományok közötti azonosítás

- A hálózat növekedésével az AS és TGS szerverek nem bírják a tempót
- Megoldás a hálózat tartományokra (realm) osztása
- Realm: felhasználók, szolgáltatások, KDC
- Minden tartomány egy saját TGS-t regisztrál a másik tartományokban. (RTGS - Remote TGS) és ezen keresztül éri el a tartományon belüli szolgáltatásokat
  -> Ez viszont nem jó, mert rosszul skálázható
- Az RTGS egységek hiearchikusan is felépíthetőek

12. Virtuális magánhálózatok (VPN). IPSec

Virtuális magánhálózatok

- Telephelyek összekapcsolása
  - WAN (Wide Area Network)
  - Lehet elkülönítve az Internet forgalomtól
    - Kapcsolatminőségi védelem
    - De ettől még védeni kell a forgalmat
  - Nagyvállalati környezetben: WAN Edge
- Távmunkások bekapcsolása
  - Interneten keresztül lehetséges
  - Nagyvállalati környezetben: Internet Edge

Magánhálózat kialakítás

- Hálózat fizikai elkülönítése
  - Elkülönítésre alkalmas hálózati technológia alkalmazása
    - Bérelt vonal
    - Optikai kábel esetén különböző hullámhossz
- Adatcsomagok elkülönített irányítása
  - IP hálózatokban, adott szolgáltatón belül
    - Multiprotocol Label Switching – MPLS
      - A forgalom meg van címkézve, amint beér a hálózatba
      - A címkék rögzített útvonalon közlekednek
      - Opcionálisan erőforrás-foglalás is (Minőségi garancia)
- Elkülönítés titkosítással
  - IP szintű titkosítás
  - Adatkapcsolat szintű alagutak

Virtuális!

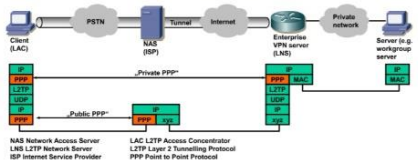
Gyakorlatban a legnagyobb biztonság

Elkülönítés titkosítással

- A magánhálózat adata a többi forgalommal együtt halad
- A titkosítás biztosítja, hogy illetéktelen személy nem férhet hozzá
  - Nem tudhatja meg tartalmát
  - Nem módosíthatja
  - Nem hozhat létre új (valós) csomagokat
  - De törölheti (rombolás)
- Nincsen prioritásos kezelés, nincs minőségi garancia
  - Best effort Internet
  - Más protokollokkal kiegészíthető
- Független a hordozó hálózat biztonságától

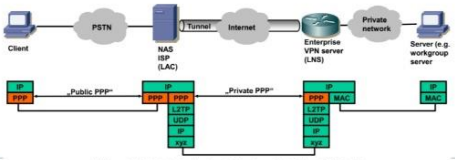
VPN típusok

- Kliens által indított VPN
  - A VPN kliens a felhasználó gépén
  - L2 tunneling, a felhasználó vállalati IP címet kap
  - A VPN felállításáról a felhasználó dönt



VPN típusok

- NAS által kezdeményezett VPN
  - A NAS a felhasználó számára indít VPN kapcsolatot
  - A hozzáférési rész nem védett!
  - A VPN felállításáról a NAS dönt

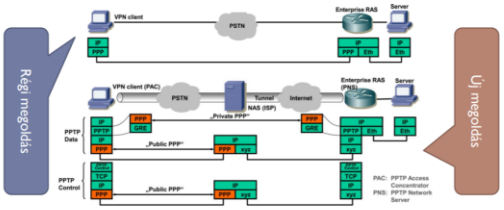


VPN típusok

- Intranet / Extranet VPN
  - A VPN egy tunnlet állít fel a két helyszín között
  - A két helyszín egy hálózatba kerül (L2 vagy L3 kapcsolat)

Tunneling protokollok - PPTP

- PPTP – Point to Point Tunneling Protocol (RFC2637)

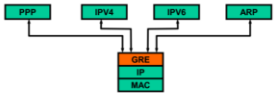


PPTP - Point to Point Tunneling Protocol

- PPTP
  - PPP: Point to Point Protocol
    - Hitelesítés (PAP, CHAP, MSCHAP, EAP), titkosítás és tömörítés
  - GRE: Generic Routing Encapsulation
    - Multiprotokoll beágyazás. Bármi (L2 és L3) átvihető, az alkalmazás számára teljesen transzparens
  - PPTP Control
    - A PPTP tunnel felállítására szolgál
    - TCP felett. Nincs védelem a protokoll számára.
- A korai időszakban a legelterjedtebb VPN protokoll a kliens csatlakozására

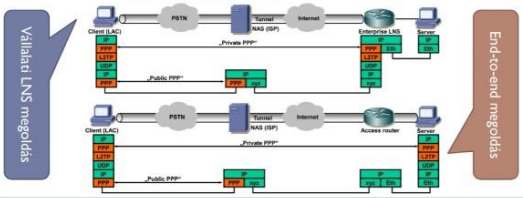
GRE – Generic Routing Protocol

- GRE
  - Tetszőleges protokoll beágyazása
  - Megszűnteti a "valami in valami" protokollok burjánzását
- Sorszámok
- Kis overhead
- Multicast támogatás
- Nincs titkosítás
- NAT-on átjutáshoz segítség kell



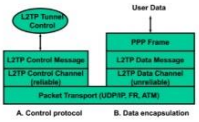
L2TP - Layer 2 Tunnelling Protocol

- L2TP - Layer 2 Tunnelling Protocol (RFC2661)



L2TP - Layer 2 Tunnelling Protocol

- L2TP
  - A. Controll protokoll tunnelek felállítására és bontására
    - Megbízható transzport protokoll szükséges hozzá
  - B. Adat beágyazás a tunnelekben
    - Nem szükséges megbízható transzport protokoll



L2TP - Layer 2 Tunnelling Protocol

- L2TP tulajdonságok
  - L2TP bármi felett (nem csak IP)
  - LNS és végpont – végpont összeköttetés is
    - Tetszőleges számú összeköttetés két végpont között
  - Egyetlen csomag formátum mind a kontroll, mind az adat számra
  - Felhasználó és tunnel azonosítás is
    - A tunnel az L2TP-vel, a felhasználó a PPP-vel hitelesít
  - Tűzfalon átjutáshoz IP/UDP használat
- De NINCS teljes titkosítás!!!
  - A PPP titkosít, de csak a payload részt, mást nem
  - Ezért szükséges, hogy más protokoll biztosítsa a védelmet (IPSec)

SSL VPN alapok

- A böngésző, mint univerzális kliens
  - HTML alapú alkalmazások (Application delivery platform)
  - Böngésző bővítmények használata (Java, ActiveX, …)
  - VPN portal és VPN tunnel
- A HTTPS a biztonság alapja
  - IPSec –cel azonos biztonsági szint (hasonló mechanizmusok, algoritmusok)
    - De ezt biztonságosabbnak tartják
  - Mindig működik!
    - NAT, proxy problémák kikerülése

SSL VPN architektúra

- Böngészőn keresztül azonosítás, végpont védelem
- HTTPS (TLS) használata a biztonságos kommunikációhoz

L7 VPN

Kliens nélküli (böngésző)

Web appok
- Fájl műveletek
- Web Mail
- Csapatmunka

L4 VPN

Vékony kliens (port forward)

Előkészített alkalmazások
- RDP, VNC
- X Windows
- Citrix, …

L3 VPN

Bővítmények segítségével

Teljes hálózati hozzáférés
- TLS kapcsolat

Könnyű telepítés

IPSec – IP Security

- IPSec (RFC2401)
  - Szabványos protokoll az Internetes adatforgalom biztonságára
- IPSec tulajdonságai
  - Hozzáférés védelem
    - Mások nem láthatják az adatforgalmat
  - Integritásvédelem
    - Az adatforgalmat nem lehet megváltoztatni
  - Hitelesítés
    - Bizonyosság, hogy valóban a küldő fél küldte az adatokat
    - A kapcsolatban lévő felek ismerik egymást
  - Védelem a visszajátszások ellen
    - Az adatforgalmat nem lehet ugyanazokkal az IP csomagokkal megismételni később

Security Association

- SA – Security Association
  - Logikai kapcsolat két kommunikáló pont között
  - Leírja a kapcsolat biztonsági szolgáltatásait
    - Üzemmód
    - Algoritmusok
    - Kulcsok
  - Egy SA: egyetlen kapcsolat
    - Duplex esetben két SA szükséges
    - Kombinált üzemmódok esetén szintén több SA

SAD – SA adatbázis

- Az aktív SA-k tárolása
  - Külső IP cím, protokoll, Paraméter index (SPI)
  - Paraméterek
    - Hitelesítési algoritmus és kulcs, Titkosító algoritmus és kulcs, élettartam, protokoll üzemmód, visszajátszás elleni sorszámok, biztonsági házirend hivatkozás

SPD – Biztonsági házirend adatbázis

- Minden egyes csomagra megvizsgálj a házirendet (szabályok)
- Csomag és házirend azonosítása
  - Cél IP cím, forrás IP cím, név (falhasználó vagy rendszernév), transzport protokoll, forrás és cél portok.
- Házirend
  - Csomag eldobás, átengedés, IPSec alkalmazás
  - IPSec esetén
    - Biztonsági protokoll és üzemmód
    - Engedélyezett műveletek (visszajátszás ellen, hitelesítés, titkosítás)
    - Algoritmusok
  - Hivatkozás az SAD-re

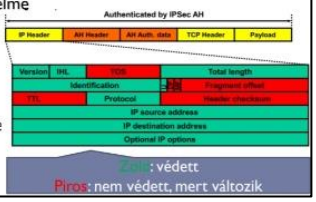
IPSec protokollok

- Hitelesítés – Authentication Header (AH)
  - IP protokoll (51)
  - Az adat (IP fejléc és magasabb rétegek) eredetének hitelesítése
    - Hash függvény segítségével a továbbítás közben nem változó mezők tartalma
  - Integritás védelem
  - Védelem a visszajátszás ellen
  - Nincs titkosítás
- Titkosítás – Encapsulating Security Payload (ESP)
  - IP protokoll (50)
  - Az adatok titkossága
  - Plusz hitelesítés és integritásvédelem
    - De csak ESP adatok + tartalom, IP fejléc nem hitelesített
  - Visszajátszás elleni védelem

- Titkosítás és hitelesítés AH + ESP
  - Titkosított tartalom és a hitelesítés kiterjed az IP fejlécekre is

IPSec – AH – Authentication Header

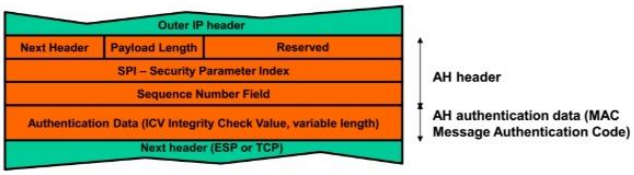
- IPSec AH
  - Hitelesítésre használják
    - Adat (payload) integritás védelme
      - Sorrend védelme
      - Visszajátszás elleni védelem
      - Nem visszavonható
    - Végpont hitelesítése
    - Külső IP fejlécmezők védelme
      - Csak azok, amelyek nem változnak az átvitel során



Zöld: védett
Piros: nem védett, mert változik

IPSec – AH – Authentication Header

- AH fejléc
  - Security Parameter Index
    - Kapcsolat paramétereinek azonosítása
  - Sequence Number Field
    - Sorszám a védelemhez (sorrend, visszajátszás ellen)

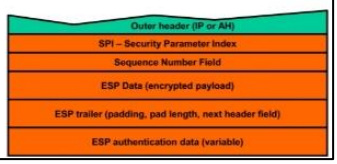


AH + ESP módok

- Szerepek elkülönítése
  - AH: hitelesítés
  - ESP: titkosítás
- Vannak esetek, amikor a hitelesítés elégséges és a titkosítás vagy túl költséges vagy szabályokba ütközik
- Az ESP is csinál hitelesítés, de vannak különbségek
  - AH: külső mezők hitelesítése is
  - ESP: csak a payload hitelesítése
- Az AH és ESP tetszőlegesen kombinálható

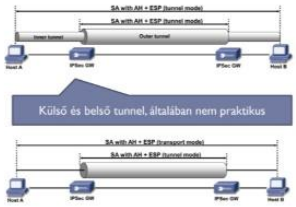
IPSec – ESP – Encapsulating Security Payload

- IPSec ESP
  - Titkosításra használják
    - Adat integritásának ellenőrzése
      - Visszajátszás elleni védelem
      - NINCS külső IP fejléc hitelesítés
    - Végpont hitelesítése (opcionális)
      - Amennyiben AH-val együtt van, felesleges



IPSec üzemmódok

- Szállítási (Transport) üzemmód
  - Védelem az IP réteg feletti protokolloknak
  - IPSec host
- Alagút (Tunnel) üzemmód
  - Az egész IP csomag védelme
  - IPSec gateway



AH és ESP összehasonlítása

	AH	ESP	AH+ESP
Encryption	No	Yes	Yes
Sender and receiver authentication	Yes	Yes (IPSec tunnel mode only)	Yes
Data integrity	Yes	Yes	Yes
Replay protection	Yes	Yes	Yes
Sender and receiver confidentiality	No	Yes (IPSec tunnel mode only)	Yes (IPSec tunnel mode only)

IPSec építési szabályok

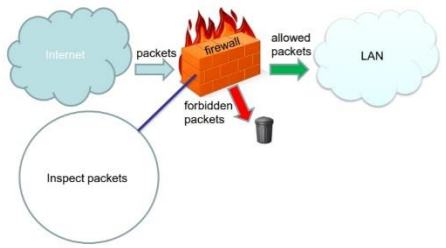
- Ha az egyik végpont GW, akkor a tunnel mód előnyösebb
- Ha mindkét pont végpont, a transzport mód előnyösebb
- Ha szükséges a teljes védelem, akkor tunnel mód. Ez még az eredeti fejlécet is rejti, védi
- Ha AH és ESP kombináció van, akkor a külső az AH a belső az ESP protokoll (integritás hiba esetén nem kell ESP-t dekódolni)
- AH és ESP kombináció esetén mindkét protokoll ugyanabban az üzemmódban (vagy transport vagy tunnel)

13. Tűzfal és behatolás felismerés (IDS)

Tűzfalak

- Mi a tűzfal?
  - Építészet: Fal, amely a tűz terjedését gátolja
  - Számítógép hálózatok
    - Egy rendszer (software, hardware, mindkettő vagy egyik sem) amely „access-control policy" –t valósít meg két hálózat határán (Intranet Firewalls; Fuller, Pagen; 1997)
- Mire jó?
  - Meggátol más hálózatokból érkező támadásokat
  - Biztonsági házirend: Csak az engedélyezett szolgáltatások használhatóak
    - Veszélyes szolgáltatások
    - A nyílt internet veszélye

Packet filters



Tűzfal feladatok

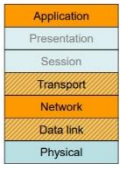
- A hálózatok határán!
  - Intranet és Internet – Belső és külső hálózat
  - Lokális hálózat szegmentációja
- Védelem
  - Forgalomfigyelés
  - Kívülről jövő támadások megállítása
    - Hosztok egyéni védelme nem szükséges (mert drága is)
  - A tűzfal elrejti a belső hálózatot
    - Sérülékenységek elrejtése
    - Topológia elrejtése

Packet filters

- Available information in a router
  - Source and destination port of the router
- Inspected header fields
  - IP addresses: source and destination
  - Protocol type (IPv4, ICMP, IP/TCP, IP/UDP)
  - TCP, UDP source and destination port
    - Identify services. Example: port 80 -> web service
  - TCP flags
    - SYN, ACK bit (TCP connection initiation, packet acknowledgement)
      - Theoretically easy to decide, whether a packet is a new connection or already part of an ongoing session, as SYN and SYN-ACK is for a specific direction.
  - Size of the packet
  - Fragmentation
    - The correct assembly of the fragments can be a problem

Tűzfal típusok

- Alkalmazás réteg
  - Application gateway
  - Proxy firewall
- Hálózati réteg (IP)
  - *Packet Filter*
  - *Screening Router*
    - Stateless – Állapot nélküli
    - Stateful - Állapottároló



Packet filtering control

- ACL - Access Control List
  - Block by default (whitelist)
    - If there is no rule for a packet then block it
    - Allowed services are listed

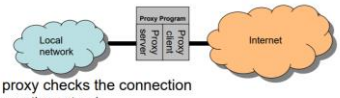
    or
  - Allow by default (blacklist)
    - If there is no rule for a packet then allow it
    - Blocked services are listed

The action after the packet filter

- Possible actions
  - ACCEPT - Send packet to the destination
  - BLOCK - Drop packet without notification
  - Drop packet with notification (ICMP): host/network <administratively> unreachable
  - Log the packet
  - Generating alert
  - Modify packet
  - Send packet to an other destination
  - Modify the filtering rules

Application firewall

- There is no direct connection between client and server



- The proxy checks the connection
  - Knows the protocol
- Other traffic is blocked
  - Ca not be avoided

Packet filter configuration

- Configuration example

Source IP	Source port	Dest. IP	Dest. port	Action
Any	Any	Web server	80 (Web)	Accept
Outside	Any	Inside	139 (Netbios)	Block
Outside	Any	Inside	110 (POP3)	Block

Inspect — Do

Proxy function

- Client and server in one hand
  - Classical Proxy (Pl. HTTP, FTP)
    - The goal is to speed up the browsing
  - Firewall Proxy
    - Access control
- Connection setup
  1. The proxy receives the connection
  2. Connects to the desired server
  3. Investigate the traffic while forwarding the protocol

Application proxy attributes

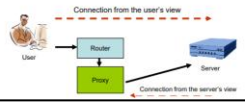
- Why it is good?
  - Looks inside the traffic
    - More powerful filtering (intelligent)
    - Content filtering
    - Powerful logging
  - User and application filtering is possible
  - Additional device between client and server
    - Fix broken protocol implementations

Dynamic packet filtering

- Inspecting whole sessions
  - TCP connection tracking
  - Necessary for UDP traffic
    - There are no connections here
- Advantages
  - More advanced filtering
  - Handling UDP traffic
- Disadvantages
  - More load on the firewall
  - DoS against firewall states
  - Sometimes it is unnecessary to store states

Transparent proxy

- Traditional proxy
  - Disadvantage that clients must be configured manually
- Transparent proxy
  - Hacking source/destination address at the firewall

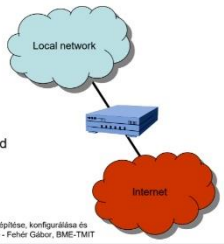


Application proxy attributes 2.

- Disadvantages
  - Continuous development
    - Changing protocols
    - New releases – even non public?
    - New attacks
  - Each service is a separate proxy
  - Performance problems
    - Server and client in one piece
    - Looks inside the packet payload
    - Two connections instead of one
  - Handling secret communication?
    - HTTPS

Firewall architectures 1.

- Screening Router architecture
  - Signe packet filter between Internet and local network



Using screening router

- Where to deploy?
  - String host security in the network
  - Small number of simple services
  - Performance counts
- Advantages
  - Simple
- Disadvantages
  - Same as the disadvantages of packet filters
    - Network can be discovered, complex configuration, application problems, …
  - If the packet filter is down the there is no more security

Firewall architectures 2.

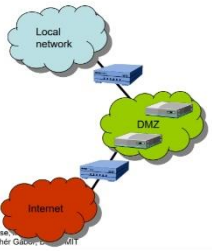
- Dual-Homed Host architecture
  - Separate interface for the local network and the Internet. No traffic forwarding!
  - Application gateway or login to the dual-homed host
- Often there are two different protocols on the ports of the dual-homed host
  - Example: NetBEUI (not exists today) and IP
- Internet packet in the local network: surely a security problem

Use of Dual-homed host

- Where to deploy?
  - Small amount of Internet traffic (due to the performance)
  - The traffic is not so critical in business view (for the case when the firewall is hacked)
  - No service for the Internet
- Advantages
  - Internet only sees the firewall, no more
- Disadvantages
  - Disadvantages of application firewalls
  - Not really comfortable without the proxy (but X windows)
  - If the firewall is down the there is no more security

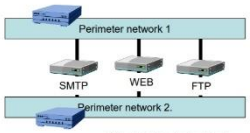
Firewall architectures 3.

- Screened Subnet architecture
  - Separate network with an inside and outside packet filter (DMZ)
  - Using application proxy within the DMZ
  - The packet filter protects the local network if DMZ would be hacked
  - Separating users and services



DMZ

- Demilitarized zone
  - Place for the servers
    - Servers are separated
    - DNS: Hiding names in the local network
  - There can be multiple DMZs



Use of screened subnet

- Where to deploy?
  - Everywhere ☺
  - Services for Internet users as well
    - Web and ftp server of the company in the DMZ
- Advantages
  - Very powerful
  - Separate service, separate zone
- Disadvantages
  - Usual firewall disadvantages

Firewall protection

- Protects against attacks, coming from outside using a know or unknown exploit
- No protection against worms or Trojans
  - We use other protections for them
- No protection against DoS
  - Moreover, firewalls are frequent victims

Firewall attacks

- Attacks from outside
  - IP source routing
    - Protection: disable source routing
  - ICMP Redirect, redirect the routing
    - Protection: ICMP traffic monitoring
  - Software errors in firewalls, OSs
    - Protection: frequent update, purchase a better product

Firewall tendencies

- More advanced packet filers (looks inside more and more)
  - Virus filtering
  - Content filtering
- More application proxies
  - Identifying the user
- Personal firewalls
  - Filtering between the local network and the host
- Managed firewalls
  - The security service provider manages the firewall
- Handling secure connections
  - The firewall terminates the secure connection and initiates a new one
  - User trusts the firewall

Intrusion detection and prevention

- Intrusion
  - Sequence of events that leads to a malicious operation
- Intrusion Detection System - IDS
  - Facilities and methods that helps to identify and report unacceptable activities
  - Passive
- Intrusion Prevention System - IPS
  - IDS + action to prevent damages
  - Reactive

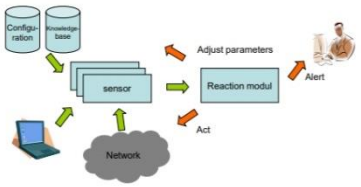
IDS types

- Network IDS (NIDS)
  - IDS in the network
  - Detecting attacks by monitoring the network traffic
    - Headers of the packets
    - Content of the packets
  - Protecting many resources at once
    - Resources connected to the network
- Host IDS (HIDS)
  - IDS on the host machine
  - Analyses log information produced by the host
    - Multihost IDS: Log from many host
  - Protects the host(s)

IDS types (cont.)

- File system IDS
  - IDS on the host machine
  - File and registry entry integrity
    - Using hash codes
  - Protects the host
- None of a single IDS type substitute the others
  - Hybrid IDS
    - Together IDSs are stronger

IDS architecture



Intrusion analysis

- Analysis phases
  - Preprocessing – Processing the information gathered from sensors
  - Analysis – Compare results to the knowledge base. Recognizing an attack or drop the information
  - Response – Alert or modification
  - Fine tuning – Adjusting the system based on previous intrusion alerts

Rule based detection

- Storing a rule set
  - Fitting rules to the information from sensors
  - Rules are maintained and continuously upgraded based on experiences (E.g.: CERT)
  - The rule set are periodically refreshed in IDSs
    - There are general rules that are need not be refreshed
- Two categories
  - Signature based detection: Signatures of known attacks
  - Specification based detection: Definition of the good behavior

Anomaly detection

- Intrusion means abnormal behavior
- Using statistical metrics to describe the behavior
  - Users, groups, files, resources, …
  - Profiles:
    - Information from past activities
    - Explicit values
  - Using a model (E.g.: Markov model)
- Examples for the abnormal behavior
  - Use resource out of the working time
  - Abnormal frequency of file access
  - Downloading extreme amount of data

NIDS sensors

- Sensors
  - Listening on the network capturing all the packets: promiscuous mode
  - Placing is important
    - Where can we see all the packets?
      - Switched network
      - SPAN port
    - First device after the router or firewall
    - Between two subnets (gateway)
  - Performance problem: heavy load

NIDS detection work

- The information is inside the packet
- Attacks that can be detected
  - Protocol errors
    - Examples: Ping of Death, SYN Flood
  - Implementation errors (bug)
    - Examples: Sendmail bug, CGI bugs, Buffer overflows
  - Confidential information stealing
    - Examples: „confidential" word, credit card number
  - Attacks in longer period
    - Example: Port scanning
    - However slow port scanning remains hidden!

IDS performance

- Attack and alert
  - Real attack and alert: true positive
  - No attack and no alert: true negative
  - Real attack, but no alert: false negative
  - No atatck, but alert: false positive
- Danger of false positives
  - Causing additional workload for the administrator
  - Flooding the network or other resources
    - No resource for the real attack
  - Decoy a real attack

14. Kis hatótávolságú IoT kommunikáció – Bluetooth LE

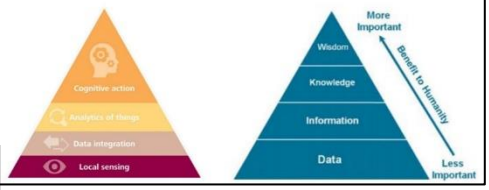
Mi is az IoT?

- A hagyományos Interneten is vannak tárgyak
  - A forgalmat a felhasználók generálják
  - Kommunikáció, dokumentum, fénykép, videó

- Mitől okos?
  - Szenzorok
  - Kommunikáció

IoT piramisok

- Adatból információ
- Információból tudás



IoT típusok

- Consumer IoT – pl.: okos otthon, asszisztensek
- Commercial IoT – pl.: egészségügy, közlekedés
- Industrial Internet of Things (IIoT) – pl.: ipar, mezőgazdaság
- Infrastructure IoT – pl.: okos városok
- Military Things (IoMT) – pl. harcászat

Bluetooth Low Energy (BLE)

- 1998-ban jelent meg, a standard Bluetooth alacsony energiafogyasztású változata
- A Bluetooth v4.0 része (v4.0 = legacy v3.0 + BLE)
- Marketing neve: „Bluetooth Smart"
- Standard BT:
  - 1600 ugrás/sec, 79 x 1MHz csatorna
  - 1, 2, 3 Mbps
- BLE:
  - 40 x 2MHz (megbízhatóbb nagyobb távolságra)
  - max 1 Mbps (bruttó = 260 kbps nettó)
  - 1 mW kimeneti teljesítmény, kb. 50 méter, kb 6 msec késleltetés

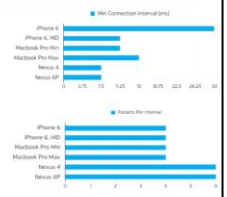
Bluetooth SMART

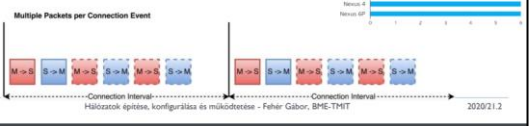
Bluetooth 4.0 Low Energy

16 Hálózatok építése, konfigurálása és működtetése - Fehér Gábor, BME-TMIT 2020/21.2

Bluetooth LE kommunikáció

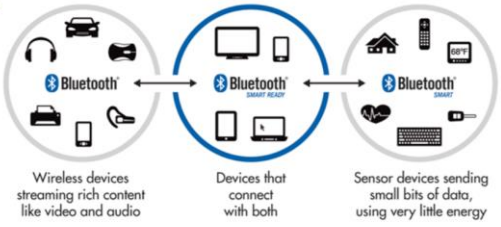
- Central (Master, client) – Peripheral (Slave, server)
  - Central pl.: Mobiltelefon, laptop
  - Peripheral pl.: fitness karperec, pulzusmérő
- Connection Interval
  - Minimum 7.5 ms !!! Növelhető 1.25 ms értékenként
- Communication Event
  - Amikor a kommunikáció történik
  - Central -> Peripheral minden esetben, még ha nincs is semmi





19 Hálózatok építése, konfigurálása és működtetése - Fehér Gábor, BME-TMIT 2020/21.2

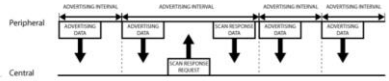
BLE



17 Hálózatok építése, konfigurálása és működtetése - Fehér Gábor, BME-TMIT 2020/21.2

Adatátviteli struktúrák

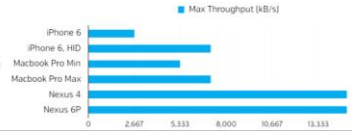
- Generic Access Profile - GAP
  - Kapcsolatok és hirdetés
- Hirdetés
  - Advertising Data
    - A peripheral egység folyamatosan hirdeti magát, hogy értesítse a central egységeket jelenlétéről. Fix csatornákon történik (3 különböző), maximum 31 bájt méret. KÖTELEZŐ!
    - Állítható időintervallum
  - Scan Response
    - A central egység további adatokat is kérhet a peripheral egységtől, ez a Scan Response.



20 Hálózatok építése, konfigurálása és működtetése - Fehér Gábor, BME-TMIT 2020/21.2

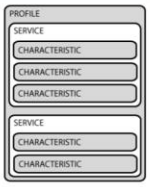
Bluetooth LE / Bluetooth Smart

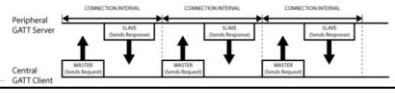
- Kis energia („fogyasztású"?) – Low Energy
  - Teljesen újratervezték, ez már nem a Bluetooth 2.0
- Gyors, olcsó
  - 2 Mbps ? – Csak a csúcs átvitel sebessége ennyi
  - Időréseket oszt, limitált kommunikáció
    - 2.5 KBps Iphone
    - 16 KBps Android Nexus 4
- Rövid hatótáv
- Hasonló technológia
  - Zigbee (pl. IKEA, Xiaomi, Philips Hue)
  - ANT+ (fitnesz eszközök)
  - Z-Wave, Wi-Fi HaLow, Thread



GATT - Generic Attribute Profile

- Adatok átvitele két eszköz között
  - Egy peripheral csak egyetlen central eszközhöz kapcsolódhat
    - GATT Server - Peripheral
    - GATT Client - Central
- Services
- Characteristics
- Attribute Protocol (ATT)





andraz2012 · 1 yr. ago

ESPNOW all the way. Bluetooth has a protocol and it's slow and awful. With espnow, you can just shoot the packets and that's it. I'm using espnow and light sleep. I can wake up, turn on wifi, send data, receive acknowledgement, turn off wifi and go back to sleep in less than 40ms (it can be done in way less time, but the overall consumption is higher that way). It will take longer if you plan on using deep sleep, but it's still pretty fast.

5 Reply Share Report Save

lastUsernameInReddit · 1 yr. ago · *edited 1 yr. ago*

ESPNOW is using around 120mA on connection and BLE is using 100mA. You can reduce current consumption of the BLE by decreasing CPU freq to 80MHz and decreasing transmission rate. I finally got 45mA on connection. However you always need to wait for BLE to initialize and pair with each other etc. So you need decide based on your application.

ESP-NOW is a kind of connectionless Wi-Fi communication protocol that is defined by Espressif.

- Custom Layer3, ONLY 3 layers!
- Mesh, self-healing, half-duplex, one/many-to-many/one sending
- CTR with CBC-MAC Protocol(CCMP) is used to protect the action frame for security.
- FAST!
- Can work on top of BLE etc.
- Responder <--ESP-NOW--> Initiator

15. Nagy hatótávolságú IoT kommunikáció – LoRaWAN és Sigfox

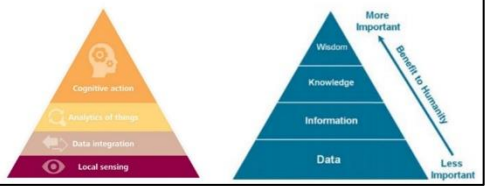
Mi is az IoT?

- A hagyományos Interneten is vannak tárgyak
  - A forgalmat a felhasználók generálják
  - Kommunikáció, dokumentum, fénykép, videó

- Mitől okos?
  - Szenzorok
  - Kommunikáció

IoT piramisok

- Adatból információ
- Információból tudás



IoT típusok

- Consumer IoT – pl.: okos otthon, asszisztensek
- Commercial IoT – pl.: egészségügy, közlekedés
- Industrial Internet of Things (IIoT) – pl.: ipar, mezőgazdaság
- Infrastructure IoT – pl.: okos városok
- Military Things (IoMT) – pl. harcászat

Sigfox

- Francia vállalkozás, 2009-ben alapították. „proprietary solution"
- LPWAN (= low-power WAN) megoldás, alacsony adatátviteli sebességgel
- ISM sáv (868 MHz Európában, 902, 928 MHz máshol)
- ultra keskenysávú (Ultra Narrow Band) LPWAN
- Csillag hálózati topológia, cellás (mobil) operátor hálózatával kiegészítve
- SIGFOX szabvány: 140 uplink üzenet naponta, 6-12 bájtos tartalommal + 4 downlink üzenet naponta fix 8 bájtos tartalommal
- Tipikus alkalmazási terület: okos mérők, távvezérlők, ...
- 30-50 kilométeres cellaméretek (városban kisebb)
- LOS (line-of-sight) üzenetek akár(*) **100 kilométerre is!** (*inkább 40 km)

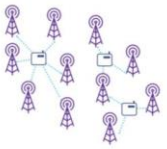
37 Hálózatok építése, konfigurálása és működtetése - Fehér Gábor, BME-TMIT 2020/21.2

Sigfox bázisállomások

- Egy adót egyszerre több vevő is fogad

Térbeli diverzitás

- Kétirányú kommunikáció
  - Az adó által küldött üzenet után 20 mp-cel nyílik a vevő ablak, ami maximum 25 mp-ig marad nyitva
  - A frekvencia az adó által először küldött + egy ismert eltérés

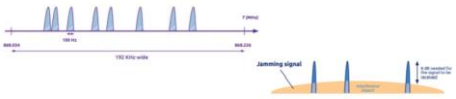


40 Hálózatok építése, konfigurálása és működtetése - Fehér Gábor, BME-TMIT 2020/21.2

Sigfox Ultra Narrow Band

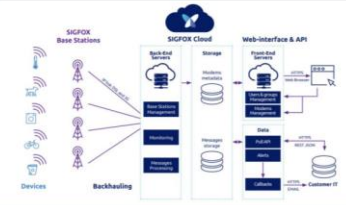
- 868 MHz (Európa), 192KHz, 100Hz D-BPSK
- Random access
  - 3x ismételt üzenet, különböző frekvenciákon
- 100bps ! 12 byte = 2.08 mp

Idő és frekvencia diverzitás



38 Hálózatok építése, konfigurálása és működtetése - Fehér Gábor, BME-TMIT 2020/21.2

Sigfox architektúra



41 Hálózatok építése, konfigurálása és működtetése - Fehér Gábor, BME-TMIT 2020/21.2

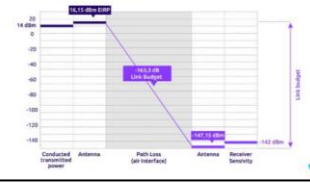
Sigfox

- 50 uW egyirányú módban
- 20 éves élettartam 2500 mAh elemről
- < 1 EUR modem ár
- 3 bázisállomás egy 1 milliós nagyvárosban elég
- Főleg Nyugat-Európában, de USA-ban és Szingapúrban is terjed rohamosan
  - 2018: 3.5 millió eszköz
  - 2019: 11.5 millió eszköz
  - 2020 (becslés): 15 millió eszköz (2023: 1 milliárd eszköz ?)

43 Hálózatok építése, konfigurálása és működtetése - Fehér Gábor, BME-TMIT 2020/21.2

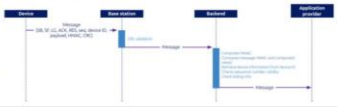
Sigfox link budget

Ultra Narrow Band brings Long-Range



Sigfox biztonság

- Titkosítás (AES), hitelesítés, integritás védelem, visszajátszás védelem
  - Az adat rész külön titkosítva, a felhasználó kulcsával!
  - Medium – high – very high level security, a kulcsok tárolásától függően
    - Legerősebb védelem Secure Element használatával



Sigfox

- Tervezési döntések

LoRa

- Nyílt szabvány: „carrier-grade IoT LPWAN" megoldás elemről üzemeltetett eszközökhöz
- LoRaWAN ≠ LoRa protokoll
- Hálózati topológia: „csillagok csillaga"
  - átjáró (gateway) elemek: standard IP a szerver felé, direkt (1-hop) rádiós link a végberendezéshez

49 Hálózatok építése, konfigurálása és működtetése - Fehér Gábor, BME-TMIT 2020/21.2

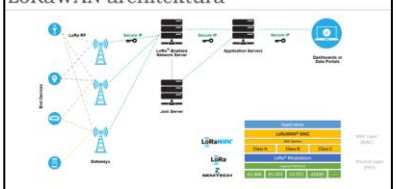
LoRa átviteli sebesség

- Mérések az eszközök által (szerver és kliens is)
  - EU leglassabb átvitel (DR0): 1 bájt, 1151 ms
  - EU gyors átvitel (DR5): 48 bájt, 112.9 ms

De már „csak" km távolság!

51 Hálózatok építése, konfigurálása és működtetése - Fehér Gábor, BME-TMIT 2020/21.2

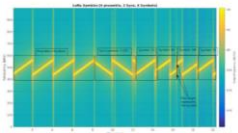
LoRaWAN architektúra



53 Hálózatok építése, konfigurálása és működtetése - Fehér Gábor, BME-TMIT 2020/21.2

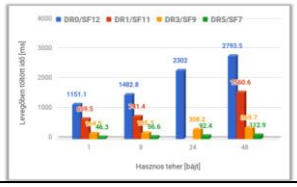
LoRa rádió

- Chirp Spread Spectrum
  - BW - Bandwidth: 125 – 250 – 500 kHz
    - Minél szélesebb csatorna, annál több adat
  - SF – Spreading Factor: 7-12
    - Hány chirp egy szimbólum: 2^{SF}
  - CR – Coding Rate: 4/5 – 4/8
    - FEC hibajavítás
    - hány bitet/hány biten
- Európai (ETSI) szabályozások
  - 1 % adó



LoRa levegőben töltött idő

- Levegőben töltött idő

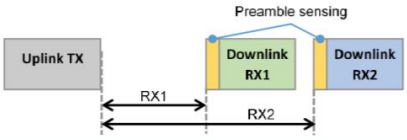


LoRaWAN

- Biztonságos, kétirányú kommunikáció, nyugtázott átvitel
- Lokalizációs szolgáltatások, mobilitás kezelése
- Adatsebességek: 0.3 kbps – 50 kbps
- ADR (Adaptive Data Rate): A szerver minden végberendezéshez egyenként határozza meg a RF kimenet paramétereit. („*Auto-magically manage SF for each end-device*" ☺)
- Különböző végberendezés osztályok: Class A, B, C

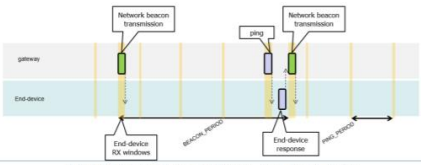
LoRaWAN osztályok

- Különböző végberendezés osztályok: Class A, B, C
  - Class A: elemről működtetett
    - kétirányú kommunikáció
    - végberendezés kezdeményez (uplink), downlink csak előzetes uplink esetén



LoRaWAN osztályok 2.

- Különböző végberendezés osztályok: Class A, B, C
  - Class B: kis késleltetésű
    - kétirányú kommunikáció ütemezett vételi ablakokkal
    - periodikus beacon a gateway-től (128 s)
    - szerver is kezdeményezhet átvitelt (ping slot)



LoRaWAN osztályok 3.

- Különböző végberendezés osztályok: Class A, B, C
  - Class C: real-time
    - unicast és multicast is
    - szerver kezdeményezhet bármikor átvitelt
    - a végberendezés folyamatosan kész a vételre

LoRaWAN kommunikáció

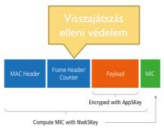
- Device Address
  - 32 bites, nem globálisan egyedi azonosító
    - Az adott hálózatban egyedi
    - Prefix címek. 7/14/22 bites hálózati cím
- Session keys
  - AppSKey: 128 bites privát kulcs az alkalmazáshoz
    - Titkosítás AES-CTR alapján
  - NwkSKey: 128 bites hálózati kulcs
    - Integritás ellenőrzéshez (MIC) AES-CMAC algoritmus alapján

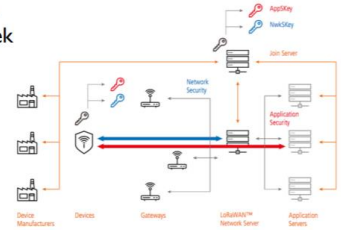
LoRaWAN beléptetés (commissioning)

- ABP (Activation By Personalization)
  - session kulcsok „beégetése" a gyártás során, adott hálózathoz kötötten. Nincs szükség OTTA-ra, az eszköz egyből kész a kommunikációra.
- OTAA (Over-the-Air Activation)
  - globális egyedi azonosítók alapján: Join Request – Join Accepts
  - DevAddr, AppSKey és NwkSKey dinamikus generálása
  - AppKey: 128 bites privát kulcs a többi kulcs generálásához
  - DevEUI és AppEUI 64 bites eszköz/alkalmazás azonosítók

LoRaWAN 1.0

- AppSKey átadása az applikáció szervernek





16. IP szintű IoT kommunikáció – MQTT és CoAP

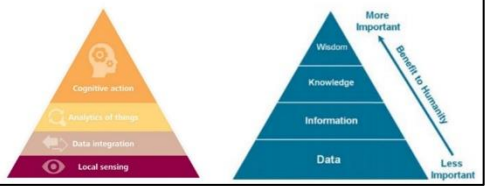
Mi is az IoT?

- A hagyományos Interneten is vannak tárgyak
  - A forgalmat a felhasználók generálják
  - Kommunikáció, dokumentum, fénykép, videó

- Mitől okos?
  - Szenzorok
  - Kommunikáció

IoT piramisok

- Adatból információ
- Információból tudás



IoT típusok

- Consumer IoT – pl.: okos otthon, asszisztensek
- Commercial IoT – pl.: egészségügy, közlekedés
- Industrial Internet of Things (IIoT) – pl.: ipar, mezőgazdaság
- Infrastructure IoT – pl.: okos városok
- Military Things (IoMT) – pl. harcászat

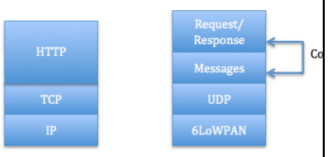
CoAP

- CoAP = RFC 7252 Constrained Application Protocol
- IETF ajánlás (CoRE Workgroup – Constrained RESTful Environment)
- Aka: „CoAP: The Web of Things Protocol"
- Alkalmazás réteg-beli protokoll: web (dokumentum) átviteli protokoll kis erőforrású (alacsony erőforrású) eszközök részére, veszteséges átvitelű („lossy") hálózatok felett.
- REST modell: A szerverek erőforrásokat tesznek elérhetővé URL-ek használatával. A kliensek elérhetik az erőforrásokat metódusok hívásával: GET, PUT, POST, és DELETE.

87 Hálózatok építése, konfigurálása és működtetése - Fehér Gábor, BME-TMIT 2020/21.2

CoAP kontra HTTP

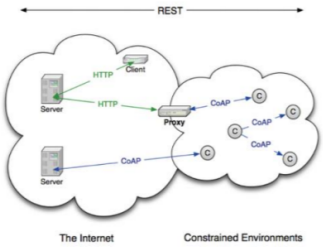
- Az alkalmazási rétegben tipikusan HTTP-t használunk web szolgáltatások eléréséhez.
- A HTTP...
  - komplex megoldás,
  - nagy energiafogyasztású,
  - kis adatsebességű.
- A CoAP...
  - HTTP-hez hasonlóan hálózat központú,
  - UDP-t használ (a komplex TCP helyett), optimalizált datagram mérettel.
  - REST architektúrán alapul,
  - lehetővé teszi az IP multicast-ot (IoT csoportos kommunikáció)



88 Hálózatok építése, konfigurálása és működtetése - Fehér Gábor, BME-TMIT 2020/21.2

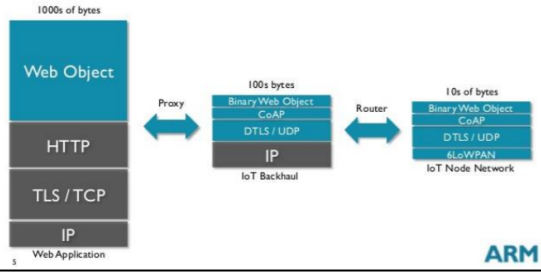
CoAP

- Beágyazott web transzport protokoll (coap://)
- Kompakt fejléc (4 byte)
- UDP, SMS támogatás (TCP is)
- Erős DTLS biztonság
- Aszinkron működés
- Multicast támogatás



89 Hálózatok építése, konfigurálása és működtetése - Fehér Gábor, BME-TMIT 2020/21.2

CoAP



ARM

MQTT

- MQTT = Message Queueing Telemetry Transport
- Nyílt, ingyenes
- publish/subscribe (one-to-many) modell
  - A küldő félnek semmit sem kell tudnia a vevő(k)ről
- Ideális kényszerekkel terhelt hálózatoknál
  - Pl. kis sávszélesség, nagy késleltetés, csomagvesztés, instabil kapcsolatok...
- Szűkös erőforrásokkal rendelkező eszközök számára
  - Kevés memória, kis teljesítményű processzor
- Cél: Megbízható üzenetküldés a lehető legegyszerűbb üzenet-formátumban

MQTT

- Publish-subscribe
  - A kliensek (*client*) feliratkoznak (*subscribe*) ún. *topic*-okra. Felratkozás után a topic-ra publikált (*publish*) összes üzenetet megkapják.
- Szolgáltatási szintek
  - 3 QoS szint definiált. Magasabb szolgáltatásminőség nagyobb megbízhatóságú üzenet célba juttatást valósít meg – ennek ára a nagyobb sávszélesség és/vagy késleltetés.
- Megőrzött üzenetek
  - A szerver meg is tartja az utoljára elküldött üzenetet. Egy új feliratkozó esetén egyből elküldi az utolsó üzenetet is a kliensek.

95 Hálózatok építése, konfigurálása és működtetése - Fehér Gábor, BME-TMIT 2020/21.2

MQTT

- Clean session flag
  - Amikor egy MQTT kliens csatlakozik a szerverhez, beállíthat egy ún. *clean-session* flag-et. Ha ez a beállítás „1"-es, a kliens összes feliratkozása törlődik, ha az eszköz lekapcsolódik a szerverről.
  - Ellenkező esetben a kliens előfizetése továbbra is élő marad mindaddig, amíg az vissza nem kapcsolódik. Eközben a magas QoS beállítás esetén érkezett összes üzenet eltárolódik, majd újracsatlakozás után elküldésre kerül.
- Végrendelet (Will)
  - Kérésre a szerver egy üzenetet küld a kliens által előre meghatározott topic-ba, ha a kliens váratlanul lecsatlakozik. (Pl. riasztás, ha egy érzékelő lecsatlakozik a hálózatról)

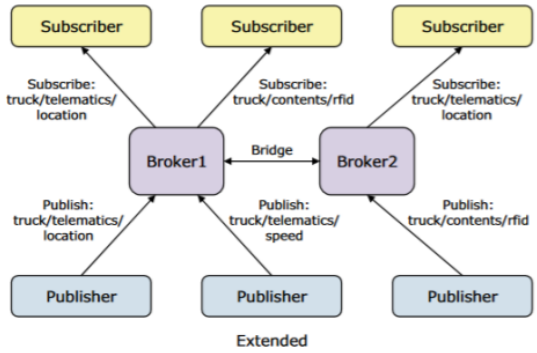
MQTT kliens

- Egy MQTT kliens (aka kliens alkalmazás)...
  - **adatokat gyűjt** egy telemetriai eszközről, csatlakozik egy MQTT szerverhez, majd egy topic string segítségével **publikálja** az információt, ÉS/VAGY
  - **feliratkozik** egy topic-ra, ahol **fogadja** a publikált adatokat, ÉS/VAGY
  - parancsok segítségével **vezérli** a telemetriai eszköz(öke)t.

MQTT bróker

- **MQTT bróker** = Egy szerver, amely implementálja az MQTT protokollt.
- Feladata: Közvetít az MQTT kliensek közötti kommunikációban.

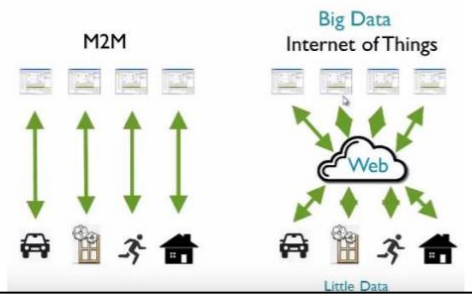
MQTT üzenetküldés



MQTT topikok, fák, sztringek

- topic
  - Az üzenetek osztályozását szolgálja, definiálja az üzenet tartalmát.
  - Pl: „truck”
- topic-tree
  - Tipikusan a topic-ok hierarchikusan szervezettek.
  - A „/” karakter használatával hozhatók létre al-topikok.
  - Pl: „truck/contents”, „truck/contents/rfid”
- topic-string
  - Egy karakterlánc, amely meghatározza az üzenet topikját. (wildcard használható!)
  - Pl: „truck/contents/#”, „truck/+”

MQTT és HTTP összehasonlítás

	MQTT	HTTP
Design orientation	Data centric	Document centric
Pattern	Publish/subscribe	Request/response
Complexity	Simple	More complex
Message size	Small, with a compact binary header just two bytes in size	Larger, partly because status detail is text-based
Service levels	Three quality of service settings	All messages get the same level of service
Extra libraries	Libraries for C (30 KB) and Java (100 KB)	Depends on the application (JSON, XML), but typically not small
Data distribution	Supports 1 to zero, 1 to 1, and 1 to *n*	1 to 1 only

M2M kommunikációtól az IoT felé