Az információs rendszerek biztonsága, Internet és az adatbiztonság

Bízhatunk-e a hálózatban és rendszerekben?

Mohácsi János <mohacsi@ik.bme.hu>

Tartalom

- Információs rendszerek biztonsága
- Bevezetés az adatbiztonságba
- Veszélyes-e az Internet?
- Leggyakoribb támadási fajták
- Eszközök az adatbiztonság megvalósítására
- Tennivalók, hogy védve legyünk
- Mit tegyünk, ha mégis baj történik?
- Algoritmikus módszerek

Információs rendszerek biztonsága

Mohácsi János
<mohacsi@ik.bme.hu>

Jelenlegi informatikai helyzet

- A gazdaság egésze jelentos mértékben a számítástechnikára épül
- Számítógépes rendszerek egyre bonyolultabbak egyre áttekinthetetlenebbek
- Adatok és programok széles körben hozzáférhetok
- stratégiai adatok - értékek

Az informatikai biztonság - adatvédelem

- informatikai rendszerek
  - hatékonyság
  - biztonság
  - titkosság
  - hitelesség
- informatikai szervezés
  - ellenorzés
  - adatbiztonság
  - adatvédelem

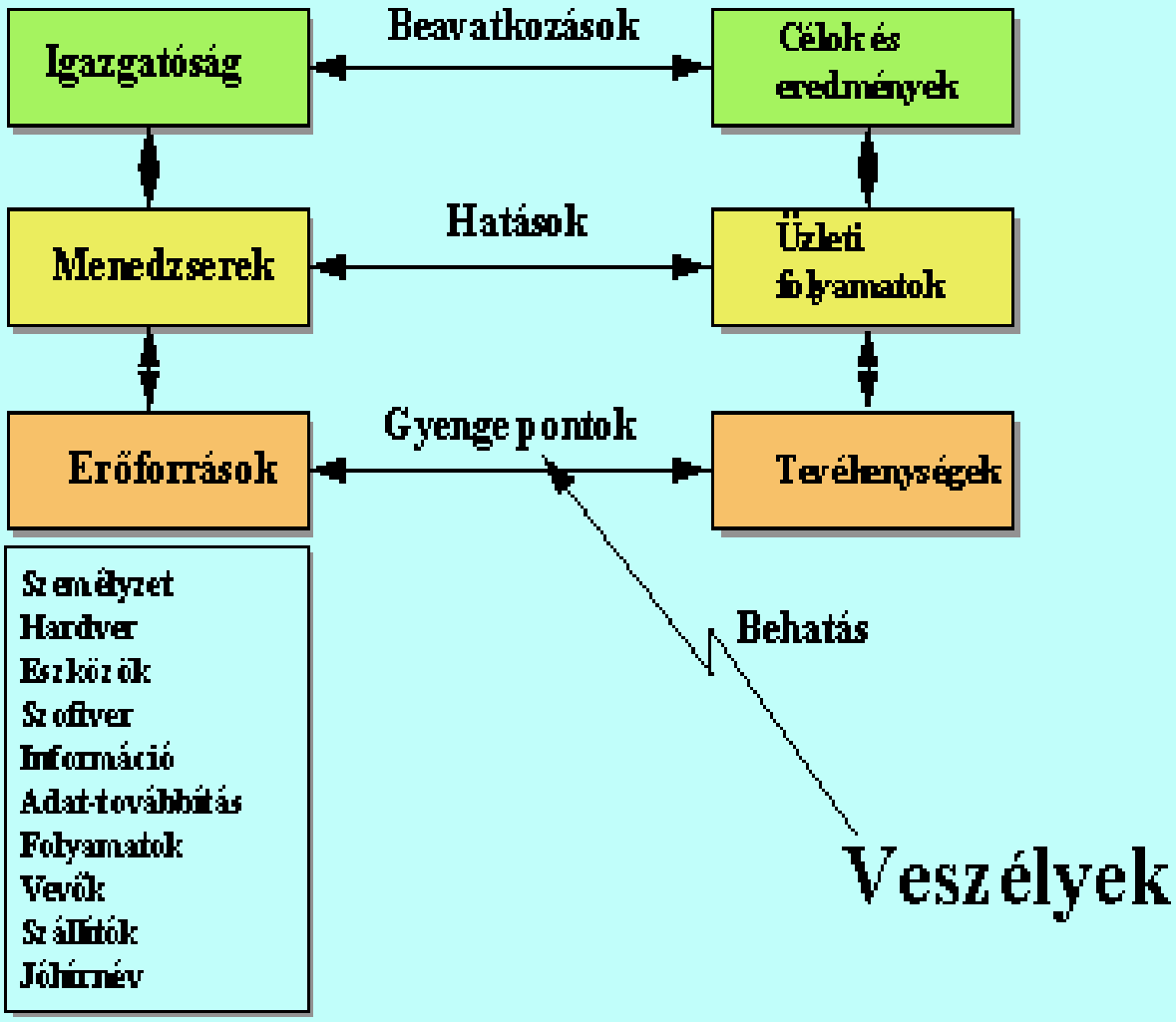
Az adatvédelem fo céljai

- PC-k, szerverek és a rajtuk lévo, vagy segítségükkel hozzáférheto adatok biztonsága (integritása, hozzáférhetosége és hitelessége - együtt).
- A kezelo személyek azonosítása, tevékenységük naplózása, környezetük biztonságának megteremetése és fenntartása.
- Az illetéktelen behatolás, hozzáférés és eltulajdonítás észlelése, megakadályozása.

Az adatvédelemi rendszerre vonatkozó követelmények

- Átlátszó legyen az összes jogosult használatra nézve
- Moduláris és skálázható legyen a környezetnek megfeleloen
- Összefüggo, egységes és egyenszilárdságú legyen
- Integrálható legyen az adott informatikai környezetbe
- Többszörös védelmi struktúrát alkosson
- A biztonságot érinto minden (beállított) eseményt naplózzon
- Biztosítsa a rendszer muködés alatti finom-beállítását és továbbfejlesztését
- Védje saját magát

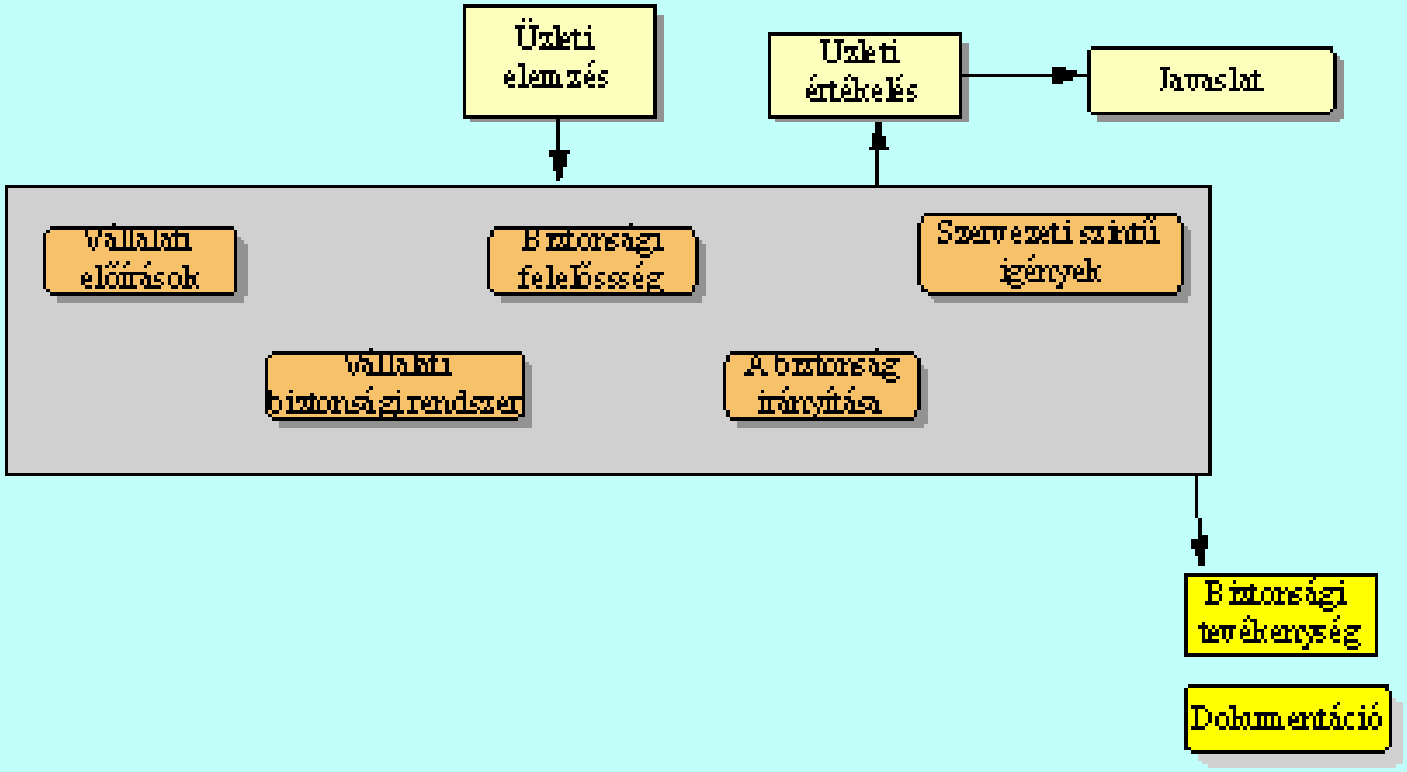
A biztonsági modell



Az adatvédelem tervezése és megvalósítása

- meglévo biztonsági helyzet elemzése
  - funkcionális, strukturális, vagy analitikus módszerek
  - veszélyességi tényezok és súlyuk
  - védendo funkciók, adatok és szervezetek
  - kritikus pontok
- Minosítés: hol, mit és milyen formában kell alkalmazni

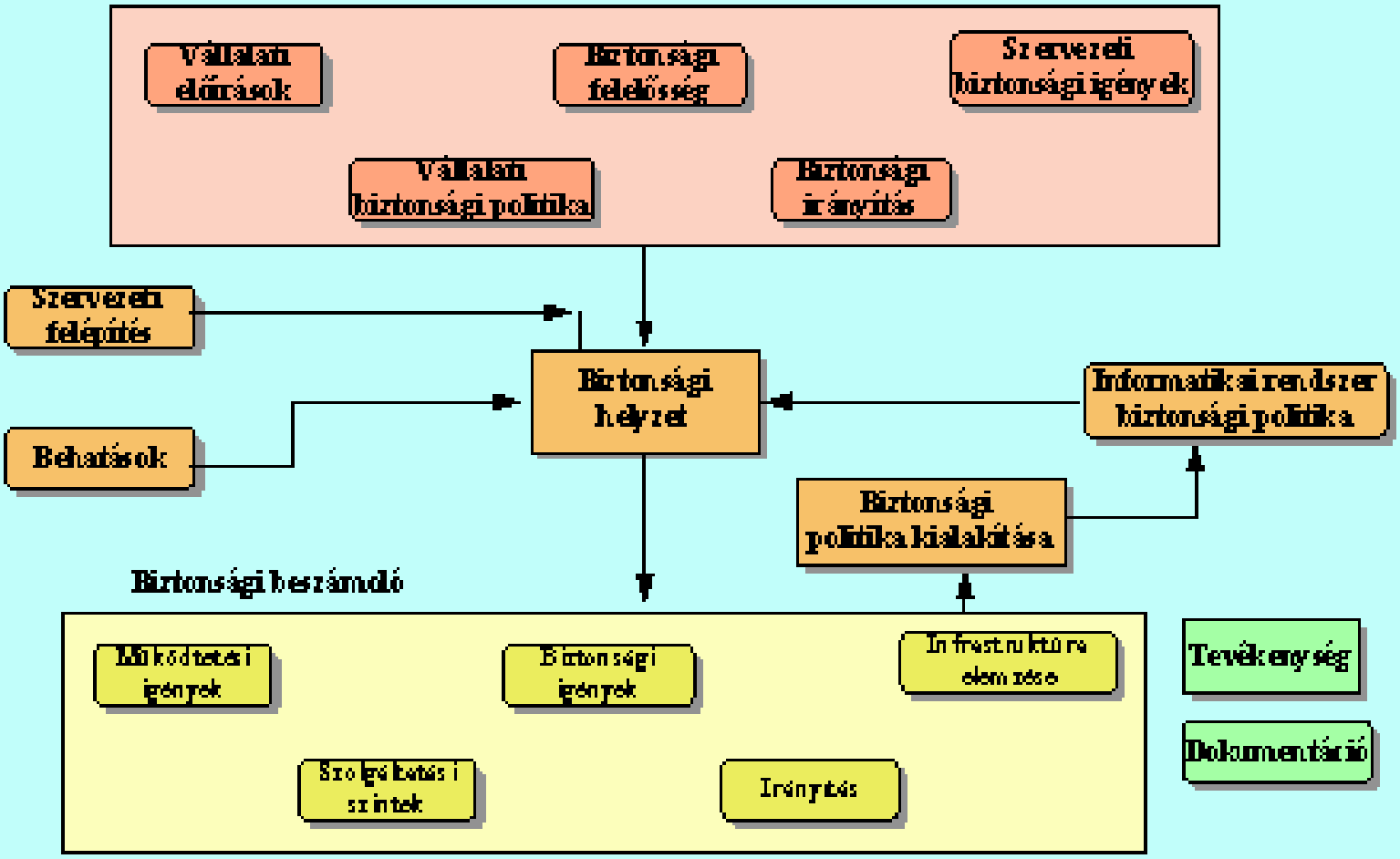
Vállalati szintű elemzés



A biztonsági politika

- alapveto védelmi elvek rögzítése
- általános biztonsági feladatok és felelosök
- az adatvédelem ellenorzésének feladatai és felelosei
- a biztonság továbbfejlesztésének kritériumai
- biztonsági feltételek és tevékenység veszélyhelyzetben

A biztonsági helyzet



Az adatvédelem megvalósítási folyamata

- elokészítési terv : vállalatvezetés és a menedzserek felkészítése és oktatása
- muszaki megvalósítási terv készítése
- személyi képzési és oktatási terv készítése
- elozetes ütemterv készítése vállalati szervezeti szinten
- finanszírozási és beruházási terv készítése
- mintarendszer (pilot) létesítése - célokkal és ütemtervvel, tesztelés
- a mintarendszer tapasztalatainak kiértékelése és a kritikus pontok elemzése
- részletes muszaki és személyi terv elkészítése a szervezeteken belül
- részletes megvalósítási ütemterv készítése az egyes szervezetekre

ITSEC és TCSEC kritériumok

CC, TCSEC és ITSEC áttekinto táblázat	KÖZÖS KRITÉRIUMOK	SZINT	USA TCSEC ORANGE KÖNYV KÖVETELMÉNYEK	SZINT	EU ITSEC KÖVETELMÉNYEK	
EAL0	Nem minosített	D	Minimális védelem	E0	Nem minosített	
EAL1	Funkcionálisan tesztelt	D	Minimális védelem	E0	Nem minosített	
EAL2	Strukturálisan tesztelt	C1	Szeparált, vagy egyedi védelem	E1	Gyártó által minosített	
EAL3	Módszertanilag tesztelt és ellenorzött.	C2	Ellenorzött hozzáférési védelem	E2	Függetlenül kiértékelt	
EAL4	Módszertanilag tervezett, tesztelt és felülvizsgált.	B1	Célorientált védelem	E3	Függetlenül kiértékelt és minosített	
EAL5	Részben formálisan tervezett és tesztelt..	B2	Strukturált védelem	E4	Srtuktúrálisan szilárd	
EAL6	Ellenorzött módon, részben formálisan tervezett és tesztelt	B3	Biztonságos védelem	E5	Szigorúan tervezett	
EAL7	Ellenorzött módon, formálisan tervezett és tesztelt	A1	Ellenorzött tervezés	E6	Minosítetten tervezett	

Adatbiztonság

- Az elektronikusan tárolt információ különleges tulajdonságai:
  - Sokféle információ típust képviselhet
  - Könnyen továbbítható
  - Minoségromlás nélkül másolható
  - Többszörös hozzáférésu
  - Nyom nélkül módosítható

Adatbiztonsági alapelvek

- A védelem ne kerüljön többe, mint a védendo információ
- A védelemnek olyannak kell lennie, hogy ellenálljon a feltörési kísérleteknek addig, amíg a védendo információ értékes

Védelem alapjai

- Fizikai védelem
  - Az adathordozó védelme
- Adminisztratív védelem
  - A hozzáférés korlátozása adminisztratív eszközökkel
- Algoritmikus védelem
  - Titkosítási módszerek

Fizikai védelem

- Érzékeny adatok ellopásának legegyszerubb módja, ha az adatot hordozó vagy továbbító eszközhöz férünk hozzá : sokkal egyszerubb ellopni a számítógépet, mint távolról feltörni
- Az eszközök értéke = saját értékük + rajtuk keresztül elérheto információ értéke
- Az eszköz pótolható, az információ nem

Adminisztratív védelem

- Egyes felmérések szerint az adatbiztonsági problémáknak 90%-a adminisztratív eszközökkel elkerülheto lett volna
- A leggyakoribb hibák emberi mulasztásból következnek be
- Ez csak megfeleloen kidolgozott adminisztratív szabályozással kerülheto el

Adminisztratív védelem

- Ki kell dolgozni a biztonsági eloírásokat és ügyviteli szabályokat
- Össze kell fognia a fizikai és az algoritmikus védelmet egy egységbe
- Szigorúan betartandó, mert megsértése súlyos következményekkel járhat

Algoritmikus védelem

- A fizikailag nem védheto információt, pl.: a nyilvános telefonvonalon keresztül haladót megfelelo algoritmikus módszerekkel védeni kell
- Ezek a módszerek csak a másik két védelmi móddal együtt hoznak eredményt

Algoritmikus védelem céljai

- Lehallgatás elleni védelem (titkosítás)
  - Harmadik személy az adatátviteli vagy adattároló eszközhöz való hozzáférés esetén se jusson hozzá az információhoz
- Adatintegritás védelem
  - Harmadik személy ne legyen képes megváltoztatni az átvitt vagy tárolt információt észrevétlenül

Algoritmikus védelem céljai

- Partnerazonosítás
  - Illetéktelen ne adhassa ki magát másnak, mint aki, azaz a kommunikáló felek biztosak lehessenek abban, hogy valóban egymással vannak kapcsolatban
- Letagadhatalanság
  - Az üzenetet küldo ne tudja letagadni az üzenet elküldésének tényét (pl. banki átutalás)

Információvédelmi eszközök

- Olyan hardver vagy szoftvereszközök, amelyek segítségével az elobbi célok megvalósíthatóak
- Csak megfelelo körülmények között és csak megfelelo célokra alkalmazhatók
- Nem szabad vakon bízni bennük

Az Internet biztonsága

- 1995 - nincs
- 1996 - kezdemények
- 1997 - bizonyos problémákra van megoldás
- 1998 - körvonalazódik egy általános biztonsági architektúra
- 1999-2000 - összemérheto vagy jobb, mint a jelenleg használt más eszközöké

Mi hozta elo a gondokat?

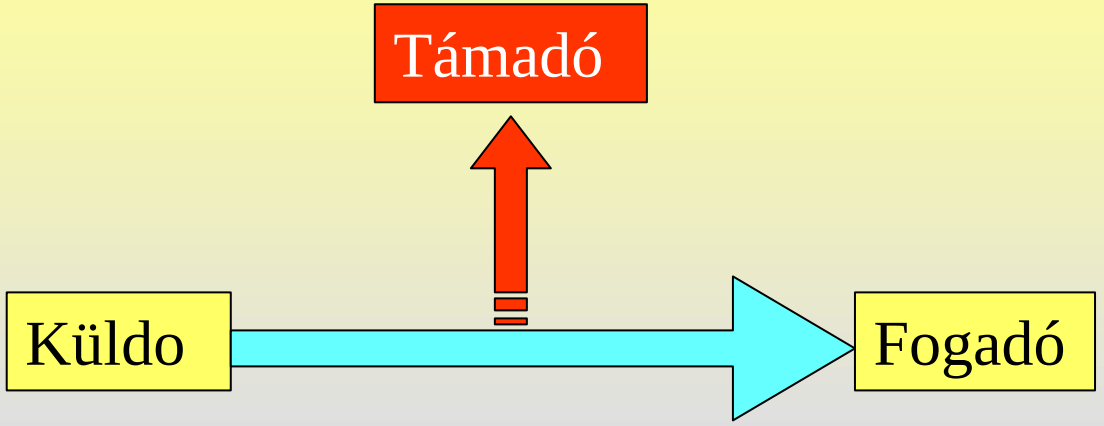
- Megváltozott biztonsági igények
- Megváltoztak a felhasználók
- Megváltozott a hálózat muködtetése
- Megváltoztak a „veszélyes” eszközök

Kell-e félni?

- NEM! , de csak akkor, ha betartunk néhány szabályt.
- Sok tévhit kering: vírusok terjedése, betörés, lehallgatás
- Ezek nagy része (pl. vírusok terjedése) nem az Internet hibája

A támadási formák

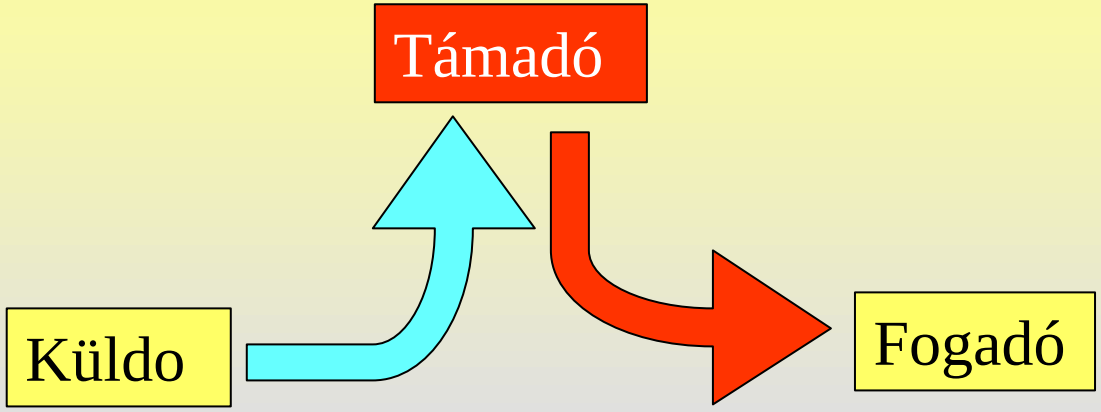
Adatok ellopása



A támadó hozzájut az átvitt információhoz

A támadási formák

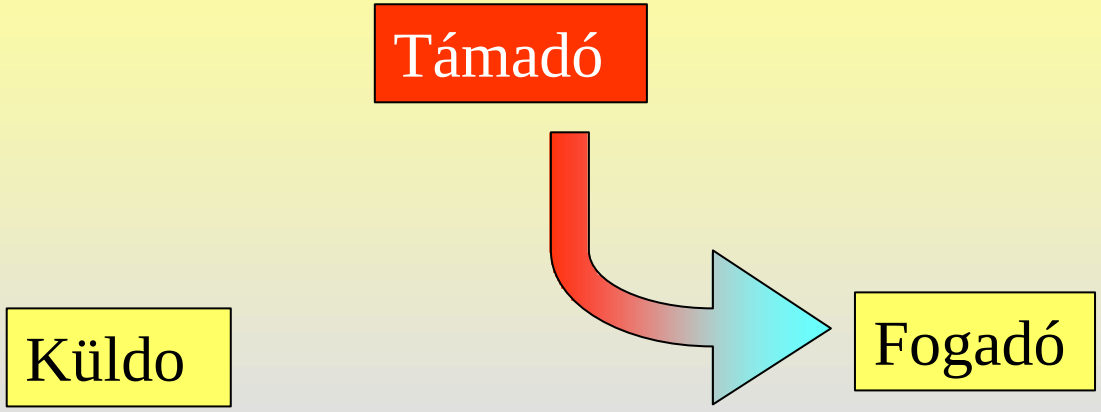
Adatok módosítása



A támadó módosítja az átvitt információt

A támadási formák

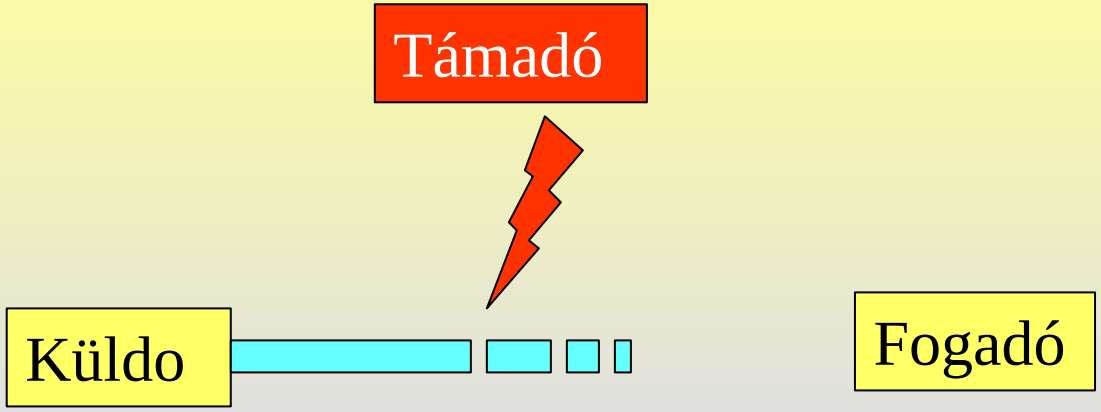
Megszemélyesítés



A támadó másnak adja ki magát

A támadási formák

Szolgáltatás meghiúsítása
Denial of Service (DoS)



A támadó valamilyen szolgáltatást meghiúsít

A védekezés

- Fobb védekezési módok
  - Lopás: fizikai, adminisztratív, algoritmikus
  - Változtatás: algoritmikus
  - Megszemélyesítés: algoritmikus,
  - DoS: adminisztratív, algoritmikus, fizikai
- A védelem csak komplex rendszerként képzelheto el

Eszközök

- Titkosítás: az információt más számára értelmezhetetlenné tenni
- Összetevok:
  - nyílt szöveg : nem titkosított
  - titkos szöveg: titkosított szöveg
  - titkosítási algoritmus: a két szöveg közti átalakítást végzi
  - kulcs: a titkosítás vezérléséhez, mérete

Titkosítási eljárások

- Titkos kulcsú titkosítás:
  - a küldo és a fogadó birtokában van ugyanannak a kulcsnak. A küldo titkosítja a kulccsal, a vevo csak ennek a kulcsnak a birtokában tud nyílt szöveget képezni
  - A kulcs nem kerülhet harmadik személy birtokába, biztonságos úton kell szétosztani

Titkosítási eljárások

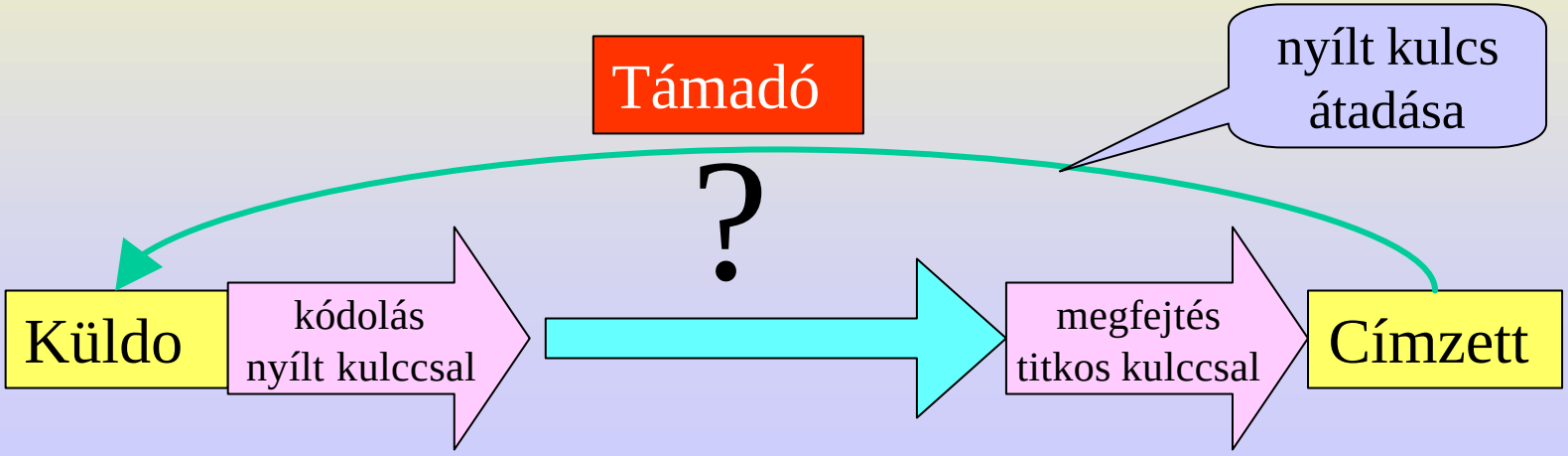
- Nyílt kulcsú titkosítás
  - A küldo és a vevo külön kulccsal (kulcspár) rendelkezik
  - Amit egyik kulccsal titkosítottak, azt a másikkal lehet megfejteni
  - Az egyik kulcs birtokában a másik nem határozható meg
  - Egyszerusíti a kulcsszétosztást

A nyílt kulcsú titkosítás

- A küldo létrehoz egy kulcspárt: titkos kulcs és nyilvános kulcs
- A titkos kulcsot biztonságban tartja
- A nyilvános kulcsot nyilvánosságra hozza, ezzel a kulcsszétosztás problémája megoldódik, hiszen nem kell titkosan átvinni a kulcsot

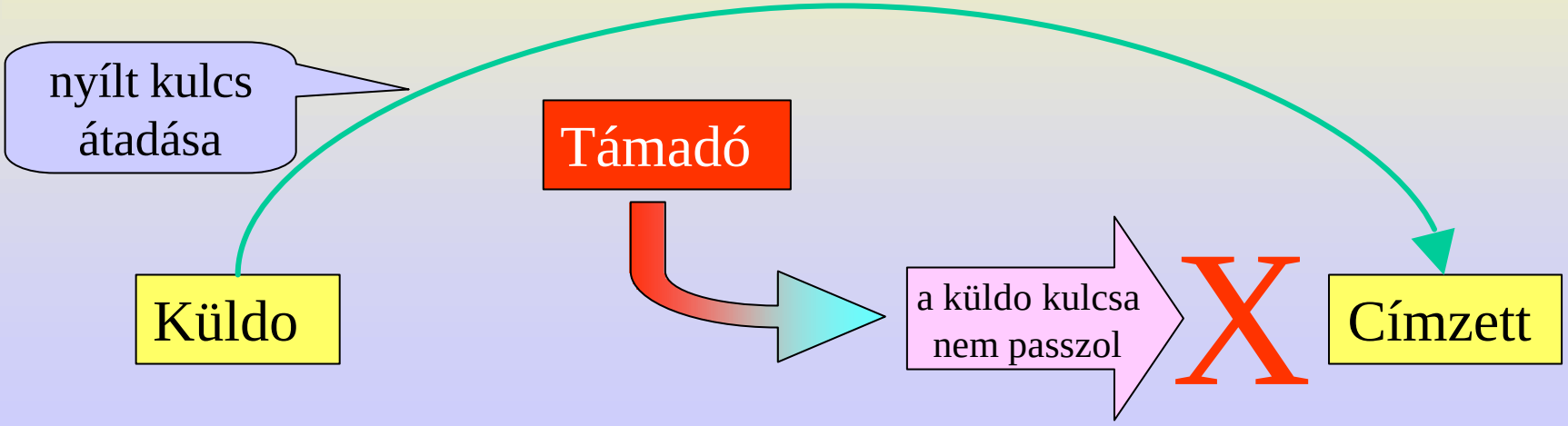
Lehallgatás védelem

- A küldo a címzett nyilvános kulcsával titkosítja az információt
- A titkos szöveget csak az tudja megfejteni, akinek megvan a nyílt kulcs párja: a címzett



Megszemélyesítés elleni védelem

- Küldo saját titkos kulcsával titkosít
- Ha a címzett a nyilvános kulccsal ki tudja kódolni, akkor csak az küldhette, akinek birtokában van a nyílt kulcs párja



Kulcshitelesítés

- A megszemélyesítés ellni védelemnél biztosnak kell lenni, hogy a nyílt kulcs azé, akinek mondja magát
- A kulcsot egy harmadik személy (CA - Certificate Authority), akiben megbízunk továbbítja:
  - a küldo a CA számára igazolja azonosságát
  - a kulcsot a CA-tol kapjuk meg
  - A CA-ben megbízunk

Megváltoztatás elleni védelem

- A küldo ellenorzo összeget számít a küldeményre:
  - Az ellenorzoösszeg megváltozik, ha az üzenet megváltozik
  - Nagyon nehéz úgy változtatni az üzenetet, hogy az ellenorzoösszeg ne változzon
- Az ellenorzoösszeget titkosítva küldi át
- A vevo is kiszámítja, ha nem egyezik, az üzenet megváltozott

Alkalmazások

- A nyíltkulcsú titkosítás elso alkalmazása a biztonságos email (PGP - Pretty Good Privacy)
- Szinte minden jelenlegi biztonsági eljárás alkalmazza a nyíltkulcsú elvet, gyakran a felhasználó számára észrevétlenül

A kulcsméret problémája

- Minden titkosítás feltörheto, ha kipróbáljuk az összes lehetséges kulcsot
- Minél nagyobb a variációk száma, annál tovább tart a törés
- A kulcsméretet a bitek számában mérik
- Minden egy bit növekedés megkétszerezi a variációk számát

A kulcsméret problémája

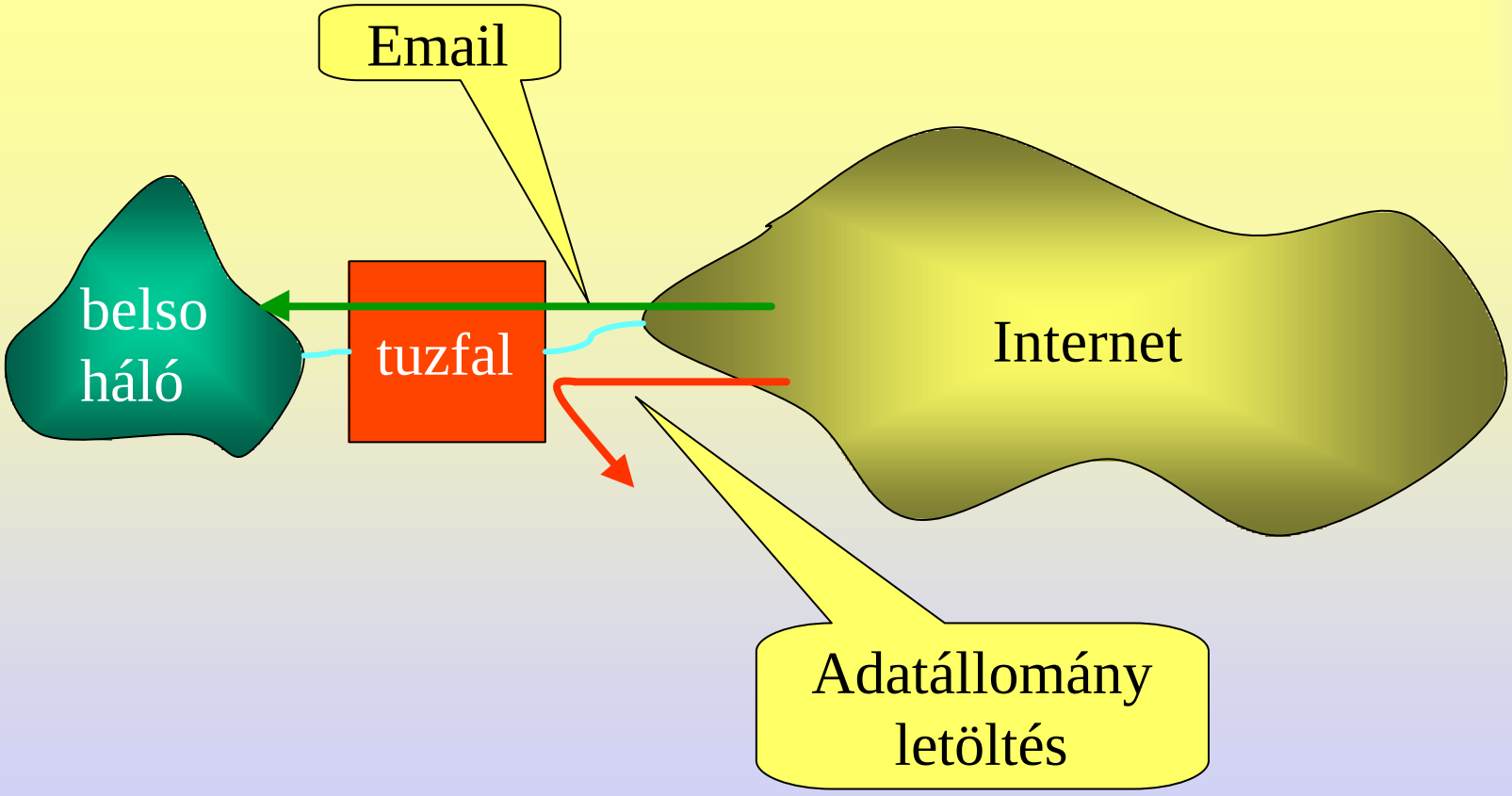
- Egy variáció kipróbálása 1 milliomod másodperc:

Bitek	Variációk	Törési ido
8	256	256 milliomod mp
16	65536	65 ezred mp
32	4,3 milliárd	71 másodperc
56	72 ezer billió	2341 év
64	18 trillió	600 ezer év

A tuzfal

- A tuzfal
  - Olyan eszköz, amely a helyi hálózat és az Internet között helyezkedik el
  - Minden szolgáltatás csak ezen keresztül érheto el, ha a tuzfal jól védett, csak egy pontra kell figyelni
  - Csak kívülrol jövo támadások ellen véd
  - Nem csodaszer, de hasznos

A tuzfal



Admisztratív szabályozás

- Minden szervezetnek rendelkezni kellene biztonsági szabályozással (Security Policy)
- A helyi viszonyok alapján kell kialakítani
- Bármely tevékenység csak ennek alapján végezheto
- Megsértését szankcionálni kell

A Security Policy

- Eldöntendo kérdések:
  - Mit akarunk védeni (Információ besorolása érzékenység szerint)
  - Mennyire akarjuk védeni (mindent 100%-os védelmben részesíteni lehetlen!)
  - Kik férhetnek mely adathoz
  - Milyen eszközök állnak rendelkezésünkre

A Security Policy

- Szabályozandó:
  - Felhasználók azonosítása
  - Ki, mikor, mihez, hogyan férhet hozzá
  - Tevékenységek naplózása
  - Felelosség
  - Eljárások a biztonság fenntartására
  - Eljárások különleges esetekben
  - Eljárások vész esetén

Mire van még szükség?

- Megfeleloen kiképzett és gyakorlott üzemelteto személyzetre
  - „A jó rendszergazda kicsit paranoiás, a nagyon jó rendszergazda nagyon paranoiás”
  - A rendszergazda bizalmi állás!
- Felhasználók felvilágosítása és betanítása
  - Megfelelo útmutatók elkészítése
  - Rendszeres tájékoztatás a változásokról

Ha baj történik

- Megelozés jobb:
  - rendszeres mentés (elengedhetetlen)
  - megfelelo biztonsági rendszerek
- Legyünk felkészülve
- Minél elobb fedezzük fel
- Nincs jelentéktelennek tuno támadás

Ha baj történik

- Jelentsük az esetet (CERT, levelezési listák stb.), lehet, hogy mások tudnak segíteni
- Mérjük fel a kárt (naplózás fontossága!)
- A „lukat” meg kell találni és be kell tömni (szoftverfrissítés, konfiguráció kijavítása, stb.) nem elég a támadót kizárni
- A nyomozás és bizonyítás nehéz, magunkra vagyunk utalva

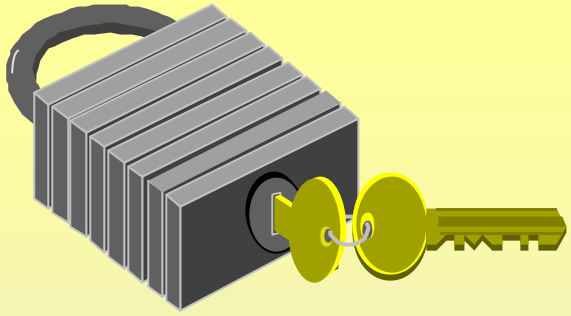
Összefoglalás

- Megfeleloen kialakított hálózat biztonságos
- A titkosítási módszerek csak egy részét jelentik a megoldásnak
- Csak komplett megoldás lehetséges
- Elengedhetetlen a megfelelo biztonsági politika és ennek betartatása
- Folyamatos felügyelet és fejlodés szükséges

Algoritmikus módszerek +

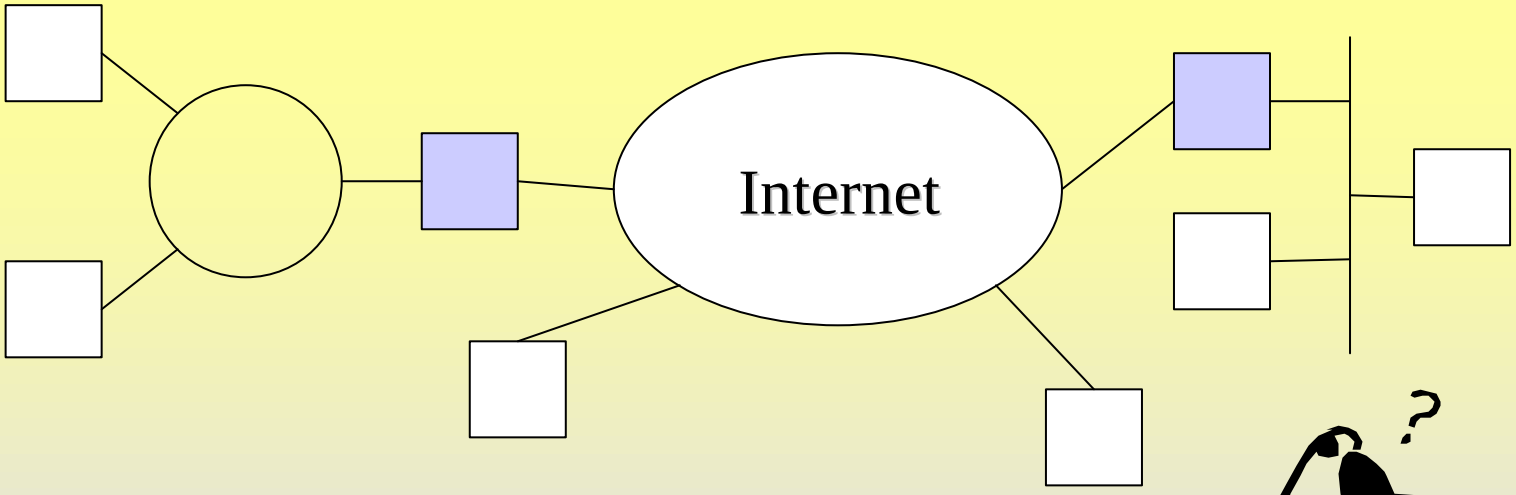
- IPSec és alternatívái
- PGP és alternatívái
- Tuzfalak
- SSL
- SSH

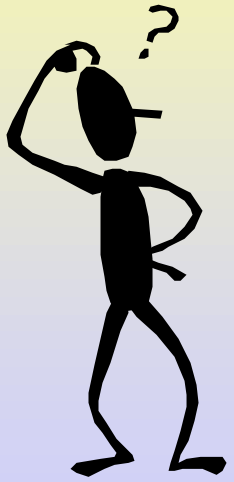
Az IPSec



Security Architecture for IPv6 and IPv4

Mivel van gondunk?



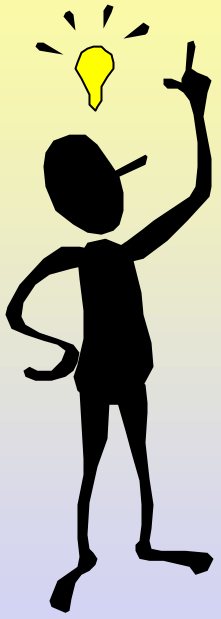


- Egy csoportba tartozó számítógépek
- **megbízhatatlan** hálózaton keresztül
- **bizalmas** adatokat cserélnek.

Mi lehet a megoldás?

A *megfelelo* megoldást az **IPSec** nyújtja:

- IP szintu védelem:
  - integritás és hitelesítés;
  - titkosítás;
  - tömörítés.
- Virtuális magánhálózatok (VPN)
- Alkalmazás-független
- Algoritmus-független

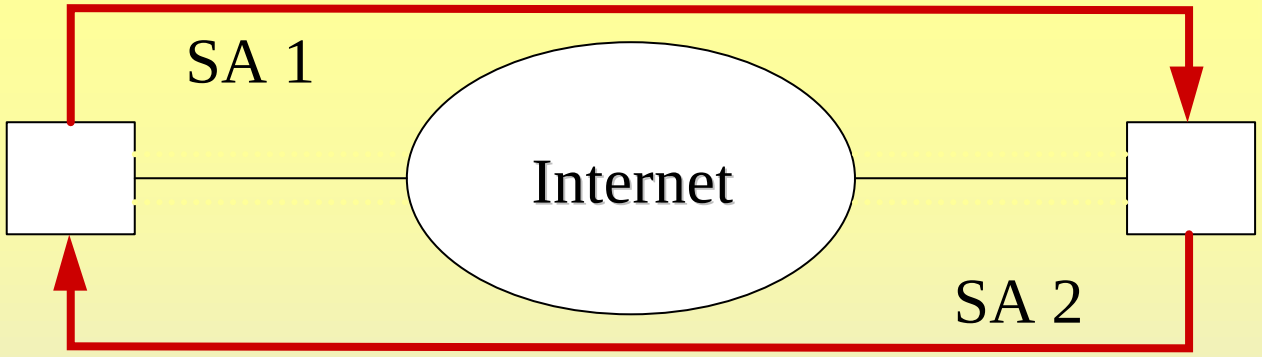


Security Associations

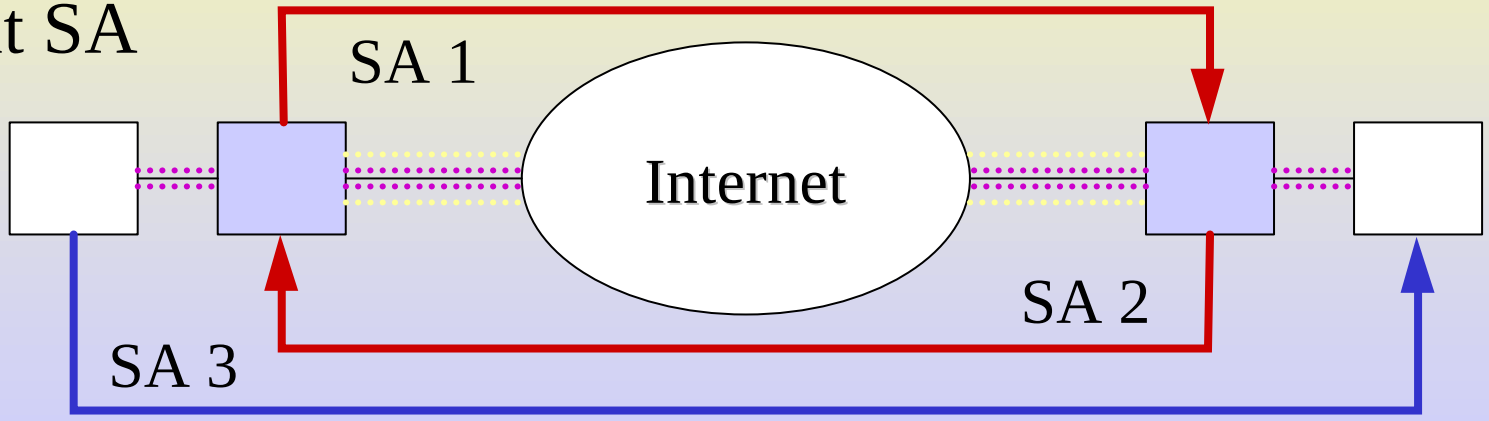
- SA = két fél közötti szerzodés
- Biztonságos kapcsolatot teremt
- Megadja a kapcsolat paramétereit:
  - biztonsági protokollok;
  - algoritmusok;
  - kulcsok;
  - stb.

Az SA-k típusai

Szállítási SA



Alagút SA



IPSec adatbázisok (Security Databases)

- Security Policy Database (SPD)
  - viszonyulás az egyes gépek felé irányuló forgalomhoz: védett, átengedett, tiltott;
  - hivatkozás egy SAD bejegyzésre.
- Security Association Database (SAD)
  - alkalmazott IPSec protokoll;
  - felhasznált algoritmusok;
  - kulcsok és egyéb paraméterek.

Kulcsgondozás

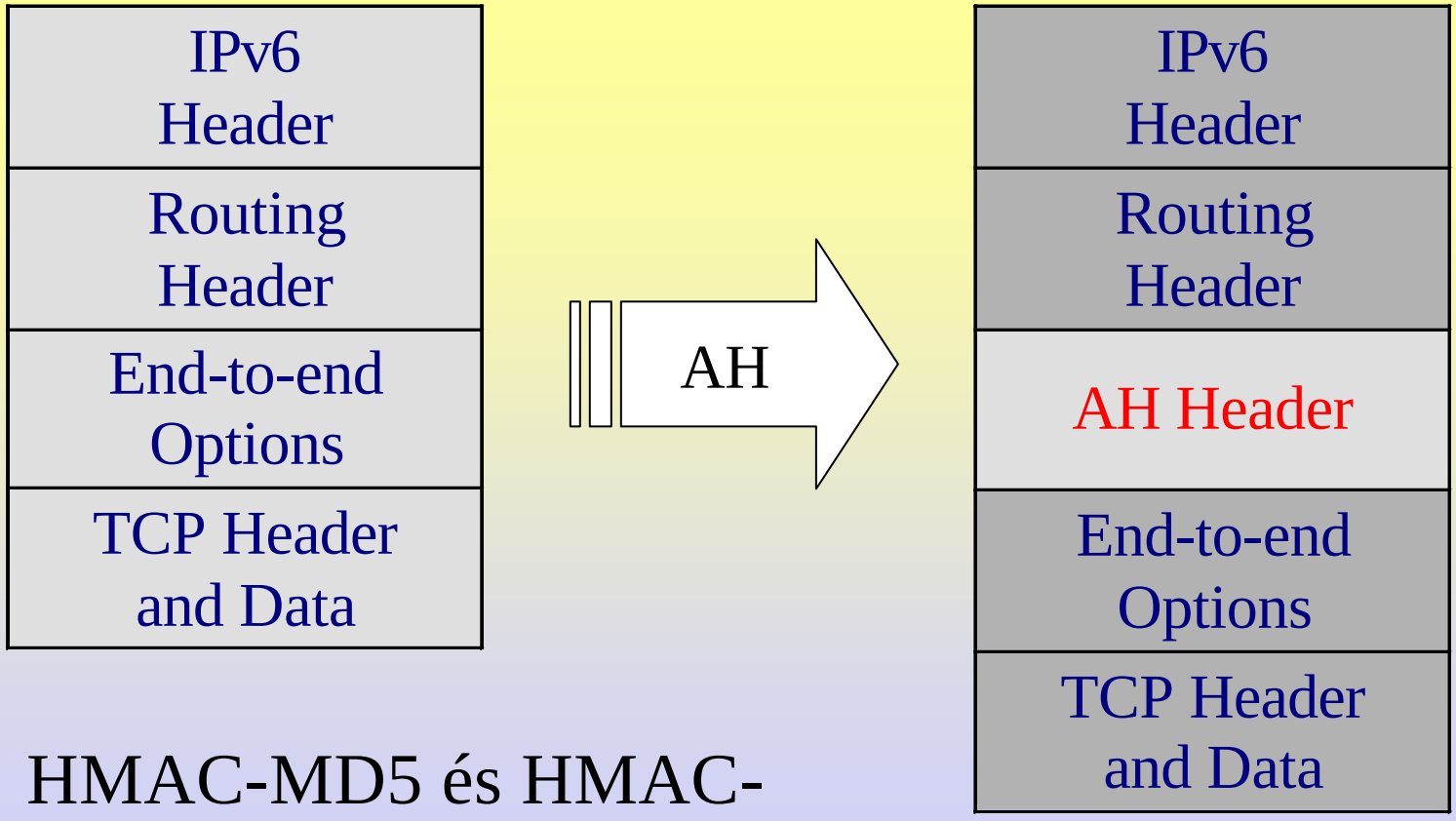
Az ISAKMP és az IKE lehetoséget nyújt:

- automatikus SA egyeztetésre;
- lejárt SA-k automatikus cseréjére;
- kulcsok generálására és biztonságos cseréjére.

Mindezt két fázisban végzi:

- ISAKMP SA létrehozása;
- akárhány és akármilyen IPSec SA egyeztetése.

Authentication Header (AH)



HMAC-MD5 és HMAC-SHA1

AH csomag feldolgozás

- Kifelé irányuló forgalom esetén:
  - Integrity Check Value (ICV) számítása az SA alapján
  - kitöltés (padding);
  - fragmentálás.
- Befelé irányuló forgalom esetén:
  - A csomag teljes helyreállítása a fregmesekbol;
  - SAD bejegyzés kikeresése;
  - ICV számítása.

Encapsulating Security Payload (ESP)

Példa: szállítási ESP

- Titkosítás: DES-CBC
- Hitelesítés: HMAC-MD5 és HMAC-SHA1

ESP csomag feldolgozás

- Kifelé irányuló forgalom esetén
  - közrezárás és kitöltés;
  - titkosítás és hitelesítés;
  - fragmentálás.
- Befelé irányuló forgalom esetén
  - A csomag teljes helyreállítása a töredékekbol;
  - SA bejegyzés kikeresése;
  - dekódolás.

Virtuális magánhálózatok (VPN)

- Földrajzilag szeparált gépek és alhálózatok csoportja,
- amelyek egyazon szervezethez tartoznak,
- de nyilvános hálózaton kapcsolódnak egymáshoz.

- Alhálózatonként egy gateway használ IPSec-et
- A többi gép hagyományos módon kommunikál
- Minden forgalom védett
- Mobil munkaállomások is bekapcsolódhatnak

IPSec értékelés

- Pozitív:
  - teljes IP szintu biztonság minden programnak;
  - könnyen bovítheto a közeljövoben;
  - általános, szabványos megoldás mindenkinek.
- Negatív:
  - összetett, bonyolult megvalósíthatóság;
  - nagy teljesítmény-igényu;
  - nehézkes beállítás.

IPSec algoritmusok

- Titkosítás
  - 3DES (kötelezo)
  - DES, CAST-128, Blowfish, AES
- Autentikáció
  - HMAC-MD5, HMAC-SHA1, HMAC-CRC32 :)
- Partner azonosítás
  - Publikus kulcs
  - osztott titok

IPSec implementációk

- Linux
  - FreeSWAN
- OpenBSD,FreeBSD, NetBSD - beépítve
  - FreeBSD és NetBSD esetén IPv6-on is
- Windows 2000 - beépítve

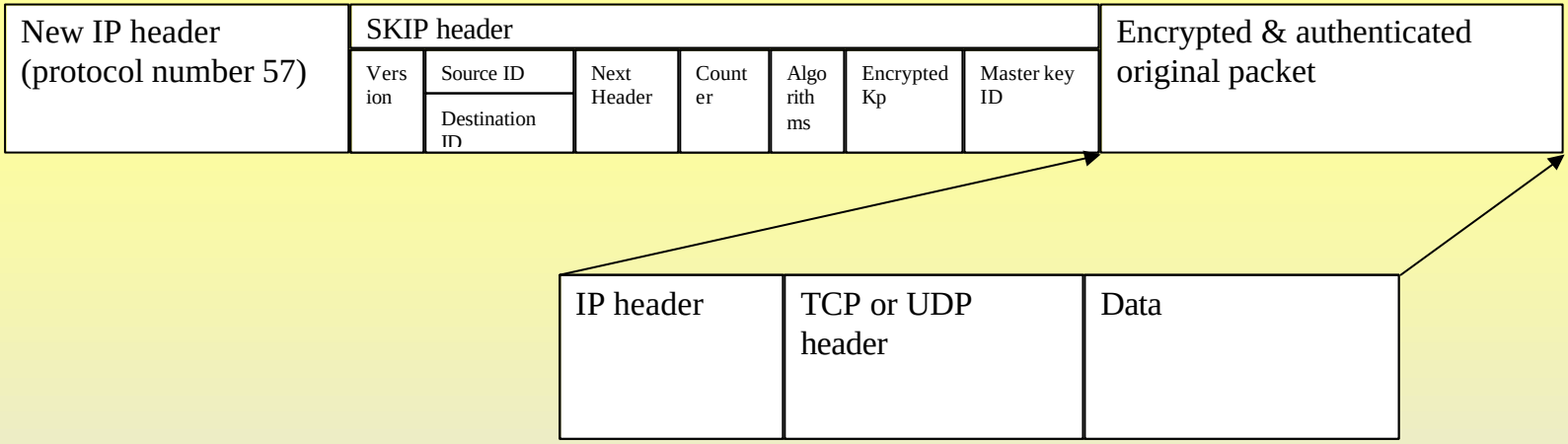
Alternatívák

- Simple Key Management for Internet Protocol (SKIP)
  - Nyitott szabvány
  - SUN Microsystems fejlesztette ki
    - Ashmar Aziz, Whitfield Diffie
- Secure Packet Shield
  - Zárt rendszer
  - Fortress Technologies fejlesztette ki

SKIP

- Hozzáférés szabályozás: ACL
- Autentikáció/hitelesítés: hashelt MD5
- Titkosság: 40 bites RC2,RC4, DES, 3DES, 128 bites safer
- Kulcscsere: Diffie-Hellman kulcscsere a mester kulcsokra.
  - Minden kommunikációs párnak van egy mester kulcsa, amit idonként frissítenek DH kulcscsere algoritmussal (kiindulási adatok directory servicebol (pl. X509) ból)

SKIP/2



- Kp random csomag kulcs. Minden csomagnál más és más
- Counter a visszajátszás megakadályozására és azonosításra

Összehasonlítás

Protocol	IPSEC	SKIP	SPS
Access Control	N	I	N
Authorisation	I	I	I
Auhentication	I	I	I
Encryption	I	I	I
Data Integrity	I	I	I
Non repudiation	csak az új	N	N
Algoritmus szabad választása	I	N	N
Overhead	nagy	nagy	közepes
sebesség	közepes	közepes	nagyobb
beállítás nehézsége	kulcscsere algoritmuson múlik	közepes	egyszeru
Flexibilitás	I	N	N
Együttmuködo képesség	I	korlátozott	N