Hálózati szolgáltatások

Titkosítás, hitelesítés

Informatikus
(rendszerinformatikus)

1

Titkosítás, hitelesítés

- *Titkosítás*: a jelfolyam értelmezése harmadik fél számára nem lehetséges (elfogadható erőforrás-ráfordítás árán!)
- *Hitelesítés*: a kommunikáló felek bizonyítottnak tekinthetik a másik azonosságát
- *Sértetlenség*: a kommunikálók ugyanazzal a jelfolyammal találkoznak!

2

Titkosítás, hitelesítés

- Hagyományos titkosítási eljárásnál egyazon kulcsot kell ismernünk az üzenet kódolásához és dekódolásához.
- Ez a szimmetrikus titkosítás.
- Az egykulcsos rendszer a titkosított kommunikációt *megelőzően* kulcscserét feltételez.
- Ehhez biztonságos csatorna kell!

3

Titkosítás, hitelesítés

- A kulcs-csere egy megoldása: a Diffie - Hellman kulcscsere: két vagy több résztvevőre is alkalmas.

4

Titkosítás, hitelesítés

- Nyilvános kulcsú (aszimmetrikus) titkosításnál minden egyes felhasználóhoz két kulcs tartozik:
  - egy titkos (*private*)
  - és egy nyilvános (*public*)
- Fontos, hogy a privát kulcsból könnyen elő lehet állítani a nyilvános kulcsot,
  azonban ez fordítva már nem, vagy nagyon nehezen lehetséges.

5

Titkosítás, hitelesítés

- A titkos és a nyilvános kulcs szerepe szimmetrikus. Ha
  - N jelöli a nyilvános kulcs alkalmazását,
  - T a titkos kulcsét, és
  - x egy kódolandó információ
- akkor:

$$N(T(x))=x \text{ és } T(N(x))=x$$

6

Titkosítás, hitelesítés

Titkosítás, hitelesítés

- Minden felhasználónak generálnia kell a maga részére egy nyilvános/titkos kulcs párt.
- A nyilvános kulcsot minél szélesebb körben ismertté kell tenni,
- a titkos kulcsra értelemszerűen vigyázni kell.

7

Titkosítás

- A titkosítottan továbbítani kívánt üzenetet
  - a feladó
  - a címzett
  - nyilvános kulcsával

  kódolja.
- Az így kódolt üzenet már csak a címzett titkos kulcsával való visszafejtéssel válik olvashatóvá!

8

Titkosítás

- Az aszimmetrikus titkosítás nagy előnye a szimmetrikus megoldással szemben, hogy itt nincs szükség védett csatornán történő előzetes kulcsegyeztetésre.
- Hátránya, hogy sebessége jóval lassabb mint a szimmetrikus megoldásé, így nagy mennyiségű adat védelmére egyelőre nem használják.

9

Hitelesítés

- Magába foglalja
  - Az üzenet feladójának és címzettjének hitelesítését és
  - az üzenet tartalmának a hitelesítését

10

Hitelesítés

- Az üzenetből a feladó képez egy, az üzenetből származó de annál lényegesen rövidebb számot.
- Ez az üzenet ellenőrző összege vagy újlenyomata.
- Ez az újlenyomatot kódolja a feladó a saját titkos kulcsával!

11

Hitelesítés

- A címzett az üzenet újlenyomatát a feladó nyilvános kulcsával dekódolja.
- Az üzenetből ugyanazon algoritmussal a címzett is képezi ezt az újlenyomatot!
- A címzett e két újlenyomat egybevetésével hitelesít:

12

Titkosítás, hitelesítés

Hitelesítés

- Az egyezés azt jelenti, jó kulcsot használt (ez a feladó személyét hitelesíti),
- illetve azt jelzi, hogy a két újlenyomat-képzés között az üzenet nem változott, azaz hiteles a tartalma is!
- (Az üzenet ekkor nincs feltétlen kódolva a kommunikáció során!)

13

RSA, algoritmus

- Az RSA algoritmus *Fermat* kis tételén alapul:
  - ha p és q különböző prímszámok,
  - és a-nak egyik sem osztója,
  - akkor mind p, mind pedig q
  - osztója $a^{(p-1)(q-1)}-1$-nek.

14

RSA, algoritmus

- Mivel p és q különböző prímek, ezért a szorzatukkal is osztható $a^{(p-1)(q-1)}-1$
- Legyen $n=qp$
- Ekkor $a^{(p-1)(q-1)}+1$ pont a maradékot ad n-nel osztva, ha a kisebb, mint n.

15

RSA, algoritmus

- Legyen $ef=(p-1)(q-1)+1$ szorzat alakban felírva;
- Ekkor a fentiek alapján: $a^{ef} \bmod n = a$ (mod a maradékképzés)

16

RSA, algoritmus

- Legyen a nyilvános kulcs az e,n számpáros, a titkos kulcs pedig az f szám.
- A kódolás során az üzenetet először számokká alakítjuk olyan módon,
- hogy a számok mindegyike kisebb legyen mint n

17

RSA, algoritmus

- Ezután az egyes m számokat az

  $$M=m^e \bmod n$$

  képlettel kódoljuk előállítva a rejtjelezett M üzenetet.
- Az üzenetet dekódolni a

  $$m=M^f \bmod n$$

  képlet alapján lehet dekódolni.

18

Titkosítás, hitelesítés

RSA, algoritmus

- A felhasznált számoknak olyan nagyoknak kell lenniük,

  hogy az n számot ne lehessen prímtényezőkre bontani.
- Ha ugyanis az n számot fel tudjuk bontani ***n***=***qp*** alakra,

  akkor ***e*** alapján egy osztással meg lehet határozni ***f***-et.

19

RSA, algoritmus

- A prímtényezős felbontásra pillanatnyilag nem áll rendelkezésre hatékony algoritmus, bár az sem bizonyított, hogy ilyen algoritmus nem létezik.
- A ***p*** ás ***q*** tipikus mérete általában bithosszban van megadva, és többnyire kettő hatványa.
- Ha ***n*** 1024 bit hosszú, azt általában katonai célokra is megfelelőnek tartják.

20

Digitális aláírás

- A nyilvános kulcsú titkosítás lehetővé teszi, hogy az információk titkosítása mellett elektronikus aláírásokat is használjunk.
- Az elektronikus aláírás az üzeneteket nem rejtjelezi,
- célja az, hogy a címzett meggyőződhessen arról, hogy a neki küldött információ valóban a feladótól származik, és azt más nem módosíthatta. (Lsd. hitelesítés)

21

Digitális aláírás

- A nyilvános kulcsú titkosítási eljárások használatakor fontos, hogy a titkosított üzenet küldése előtt megbizonyosodjunk arról: valóban a címzett nyilvános kulcsát használjuk-e.
- Erre használható a digitális tanúsítvány (*certificate*).

22

Digitális aláírás

- Ez az elektronikus tanúsítvány a következő információkat kell tartalmazza:
  - Az adott személy/szervezet nyilvános kulcsa;
  - Az adott személy/szervezet adatai: pl. neve, lakhelye, munkahelye, vagy más adatai;
  - Egy, vagy több digitális aláírás: azoknak a szervezeteknek és/vagy személyeknek az aláírása, akik igazolják a fentiek valódiságát.

23

Digitális aláírás

- Az információk valódiságát, helyességét, eredetiségét, sértetlenségét igazolhatják
  - egymás között maguk a felhasználók (*web of trust*)
  - egy szervezet, melyben a tanúsítványt felhasználók közössége megbízik.

    Ez a szervezet a Hitelesítési Szolgáltató, *Certification Authority*, CA.

24

Titkosítás, hitelesítés

Digitális aláírás

- 2001. évi XXXV. törvény
- Fajtái:
  - Egyszerű elektronikus aláírás: az aláíró egy elektronikus szöveg végére odaírja a nevét.
  - Fokozott biztonságú elektronikus aláírás

25

Digitális aláírás

- A fokozott biztonságú aláírás megfelel az alábbiaknak:
  - alkalmas az aláíró azonosítására és egyedülállóan hozzá köthető,
  - olyan eszközzel hozták létre, mely kizárólag az aláíró befolyása alatt áll,
  - a dokumentum tartalmához olyan módon kapcsolódik, hogy minden - az aláírás elhelyezését követően az iraton, illetve dokumentumon tett - módosítás érzékelhető.

26

Digitális aláírás

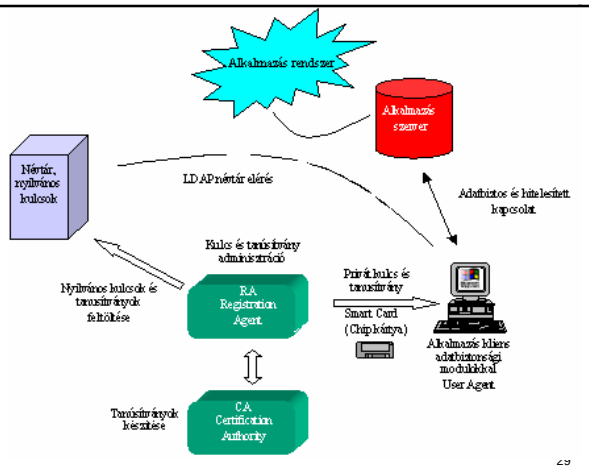
- Minősített elektronikus aláírás: olyan - fokozott biztonságú - elektronikus aláírás, amely biztonságos aláírás-létrehozó eszközzel készült, és amelynek hitelesítése céljából minősített tanúsítványt bocsátottak ki.

27

PKI: fogalmak

- PKI: (*Public Key Infrastructure*), olyan alkalmazás környezetet ami lehetővé teszi a törvények által elfogadott kétkulcsú harmadik személyes hitelesítési és adatbiztosítási eljárások használatát a számítógépes alkalmazások számára.

28



29

PKI: fogalmak

- *Certification Authority*, CA:
  - RSA kulcs-párok generálása
  - X.509 tanúsítványok kibocsátása (a CA által aláírva)
  - nyilvános kulcsok személyekhez kötése
  - tanúsítvány visszavonási listák generálása (*Certificate Revication List*)
  - adatbázisok és névtárak kezelése
  - master kulcsok kezelése

30

Titkosítás, hitelesítés

PKI: fogalmak

- *Registration Agent*, RA:
  - felhasználó azonosító generálása
  - felhasználó kulcs kérése, fogadása CA-tól, fájlban vagy kártyán tárolása
  - tanúsítvány visszavonás kérése a CA-tól, stb

31

PKI: fogalmak

- *User Agent*: olyan alkalmazás, amely a végfelhasználó gépén kerül installálásra,

  és a felhasználó kulcsokkal tanúsítványokkal és chip kártyákkal kapcsolatos műveleteket tesz lehetővé.
- Feladatok:
  - digitális aláírás képzés
  - kódolás, dekódolás
  - kulcs megújítás kérelmek (jogosultság esetén)…

32

PKI: fogalmak

- X.500: ez a névtár szolgáltatás lehetővé teszi, hogy a nyilvános kulcsokat X.509 formában az X.500 névtár szolgáltatásba helyezzük, lehetőséget adva arra, hogy az X.400-as levelek titkosításánál és digitális aláírásánál a nyilvános kulcsterjesztés és kezelés egyszerűvé váljon.

33

Tanúsítvány

- X.509: olyan kommunikációs szabvány, mely az elektronikus tanúsítványok szerkezetére, felépítésére, tartalmára ad előírásokat.
- Az ennek megfelelő tanúsítvány tartalmazza pl.:
  - a tanúsítvány verziószámát,
  - egyedi sorozatszámát
  - a Hitelesítő Hatóság által az aláíráshoz használt algoritmus azonosítóját, stb.

34

Tanúsítvány

- *Személyes hitelesítés*: azt szavatolja, hogy azok vagyunk, akiknek mondjuk magunkat.
- *Helyhitelesítés, szervertanúsítvány*: azt igazolja, hogy az adott Web-hely biztonságos és valódi.

  A böngészőben a hiteles Web-helyeket nem az egyszerű HTTP protokollon keresztül, hanem az SSL titkosítást használó HTTPS protokollon nyitunk meg.

35

Tanúsítvány

- *Programkészítői hitelesítés, szoftvertanúsítvány*: azt igazolja, hogy egy az éppen gépünkre telepítendő programhoz gyártója a nevét adja, és az ő személyazonosságát, a program eredetiségét és sértetlenségét egy megbízható harmadik fél tanúsítja.

36

Titkosítás, hitelesítés

Tanúsítvány

- Tanúsítvány osztályok (*class*): Tanúsítvány és tanúsítvány között nagy különbségek lehetnek.
- Például:
  - Expressz (C, leggyengébb),
  - Üzleti (B),
  - Közjegyzői (A)

37

Tanúsítvány

- Visszavonási lista (*CRL, Certificate Revocation List*): Bár a tanúsítványoknak létezik érvényességi ideje, szükség lehet arra, hogy a lejárat előtt visszavonásra, felfüggesztésre kerüljenek a kibocsátó által.
- A visszavonás oka pl.:
  - a titkos kulcs kompromittálódását (a kompromittálódás gyanúját),
  - a tulajdonos nevének megváltozása, stb.

38

Hitelesítési eljárások: CHAP

- **CHAP**: Kihívásos-kézfogásos hitelesítési protokoll (*Challenge-Handshake Authentication Protocol*)
- ISP-hez bejelentkezett felhasználó autentikálására (hitelesítésre) tervezett protokoll.
- Az RFC 1994 vonatkozik rá.

39

Hitelesítési eljárások: CHAP

- A felhasználó hitelesítését periodikus ellenőrzéssel végzi.
- Az azonosítási folyamat vázlata:
  - A hitelesítő a kapcsolat kiépülése után egy CHALLENGE üzenetet küld az ügyfélnek;
  - Az ügyfél válasza, RESPONSE az üzenetnek egy egyutas (*hash*) algoritmussal készített összege (pl. MD5 módszer);

40

Hitelesítési eljárások: CHAP

  - A hitelesítő maga is elkészítve ezt az értéket összeveti a kapottal. Ha egyezik, akkor a hitelesítés rendben, üzenet SUCCESS, ha nem akkor bontja a kapcsolatot, FAILURE!
- A hitelesítő véletlenszerű időközönként megismétli a CHALLENGE üzenet küldését ill. a vázolt hitelesítési folyamatot.

41

Hitelesítési eljárások: CHAP

- A CHAP védelmet nyújt a jelszó-visszajátszások (jelszólopások) ellen, mivel egy mindig változó, kihívó értéket használ.
- Mivel a kihívás egyedi és véletlenszerűen választott, a kapott kivonat szintén egyedi és véletlenszerű lesz.
- Az ismételt felkéréseknek az a célja, hogy korlátozza azokat az időintervallumokat, amíg a hívott ki van téve egy támadásnak.

42

Titkosítás, hitelesítés

Hitelesítési eljárások: PAP

- PAP: Jelszó hitelesítéses protokoll (*Password Authentication Protocol*)
- Kétfázisú kézfogással egyszer eljárást biztosít a távoli állomás azonosságának megállapításához.
- Az RFC 1334 vonatkozik rá.

43

Hitelesítési eljárások: PAP

- Miután a PPP kapcsolatelépítési fázisa befejeződött,
- a távoli állomás egy felhasználónév/jelszó párt küldözget mindaddig,
- amíg meg nem érkezik a hitelesítési nyugta,
- vagy le nem zárul a kapcsolat.

44

Hitelesítési eljárások: PAP

- A PAP nem egy erős hitelesítési protokoll!
- A jelszavakat az összeköttetésen keresztül egyszer szövegként továbbítja.
- Azok ellopása és visszajátszása, illetve próbálgatással történ kitalálása ellen nem biztosít védelmet.

45

Hitelesítési eljárások: MS-CHAP

- A Microsoft által megvalósított CHAP hitelesítési protokoll: MS-CHAP.
- A protokoll két változatban létezik:
  - MS-CHAPv1, RFC 2433
  - MS-CHAPv2, RFC 2759 (A Windows 2000-rel jelent meg)

46

Hitelesítési eljárások: MS-CHAP

- Az MS-CHAP és a CHAP eltérései:
  - LCP (*Link Control Protocol*, kapcsolatkezelő protokoll) beépítésével a küldő és fogadó eszköz azonosítása;
  - a hitelesítő által ellenőrzött jelszóváltási mechanizmus;
  - A hitelesítő által ellenőrzött megismételt hitelesítési mechanizmus;
  - hibakódok a FAILURE üzenetben.

47

Hitelesítési eljárások: EAP

- EAP: bővített hitelesítő protokoll (*Extensible Authentication Protocol*)
- Általános hitelesítési mechanizmus, mely általánosan használt a vezeték nélküli hálózatokban illetve PPP (pont-pont, *point-to-point*) kapcsolatokban.

48

Titkosítás, hitelesítés

Hitelesítési eljárások: EAP

- Az EAP hitelesítési keretrendszer, nem egy konkrét hitelesítési módszer.
- Az EAP tartalmaz közös függvényeket és a közel 40 féle hitelesítési mechanizmus ezeket hívja meg.

49

Hitelesítési eljárások: EAP

- Fontosabb EAP eljárások:
  - LEAP (*Lightweight Extensible Authentication Protocol*) a Cisco Systems EAP megvalósítása.
  - EAP-TLS a vezeték nélküli hálózatok eredeti hitelesítési protokollja. (TLS: *Transport Layer Security*, az SSL protokoll utódja) Ezt használják PKI rendszerek illetve RADIUS szolgáltatások is.

50

Hitelesítési eljárások: EAP

- EAP-MD5: IETF (*Internet Engineering Task Force*) szabvány, mely minimális biztonságot is nyújt.
- EAP-TTLS (*Tunneled Transport Layer Security*) széles körben használt kereszt-platformos hitelesítési eljárás, magas biztonsági szolgáltatásokkal.
- EAP-SIM: mobil kommunikációs eszközök (GSM) számára kidolgozott hitelesítési és munkamenet azonosító cserére való módszer

51

Hitelesítési eljárások: RADIUS

- RADIUS: (*Remote Authentication Dial In User Service*) az IETF egyik szabványa.
- A RADIUS protokoll hitelesítési, engedélyezési és számlázási szolgáltatások biztosítására szolgál.
- Kapcsolódva az ISP-hez, meg kell adni felhasználói nevet és jelszót.
- Ezek átadásra kerülnek RADIUS protokollal egy RADIUS szervernek.

52

Hitelesítési eljárások: RADIUS

- A RADIUS-kiszolgáló hitelesíti és engedélyezi a RADIUS-ügyfél kérelmét,
- és egy RADIUS-válaszüzenetet küld vissza.
- A RADIUS-ügyfelek RADIUS-számlázási üzeneteket is küldenek a RADIUS-kiszolgálóknak.

53

Hitelesítési eljárások: RADIUS

- Ezenkívül a RADIUS szabvány a RADIUS-proxyk használatát is támogatja.
- A RADIUS-proxyk a RADIUS protokollt támogató számítógépek között RADIUS-üzeneteket továbbító számítógépek.

54

Titkosítás, hitelesítés

Hitelesítési eljárások: RADIUS

- A RADIUS-üzenetek UDP-üzenetekként továbbítódnak.
- A RADIUS protokoll hitelesítési üzenetei az 1812-es UDP-portot,
- a RADIUS-számlázási üzenetek az 1813-as UDP-portot használják.

55

Hitelesítési eljárások: Kerberos

- A '80-as évek közepén kifejlesztett Kerberos az egyik legszélesebb körben elterjedt általános célú hitelesítési protokoll, amely számos ingyenes és kereskedelmi termékben kerül felhasználásra.
- RFC 1510, de-facto szabvány

56

Hitelesítési eljárások: Kerberos

- Kidolgozásánál a fő célkitűzés, hogy egy heterogén, esetleg ellenséges hálózaton legyen egy megbízható harmadik fél (*third-party*), azaz a Kerberos, mely segítségével a használók megbízhatnak egymásban.
- A rendszer biztosítja a felhasználók számára a különböző hálózati szolgáltatásokhoz történő hozzáférések valós-idejű autentifikálását.

57

Hitelesítési eljárások: Kerberos

- A Kerberos nem tételez fel biztonságot a saját szerverén kívül egyik fél részéről sem.
- A Kerberos protokoll szimmetrikus vagy titkos kulcsú kriptográfián (*Symmetric or Secret Key Cryptography*) alapul.

58

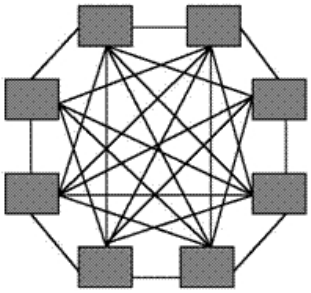
Hitelesítési eljárások: Kerberos

- A titkos kulcsú rendszerek nagy hátránya a kulcsmenedzsment.
- Ahány féllel szeretnénk kommunikálni annyi titkos kulcsra, van szükségünk.
- Ez viszont egy bonyolult hálózat esetén a kezelendő kulcsok száma a résztvevők számával négyzetes arányos.

59

Hitelesítési eljárások: Kerberos

- A kulcsok száma:



60

Titkosítás, hitelesítés

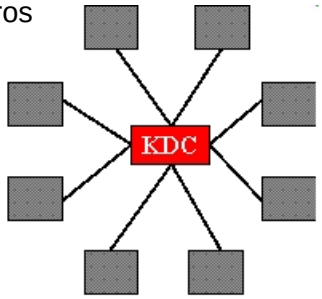
Hitelesítési eljárások: Kerberos

- A Kerberos esetén bevezettek egy ún. harmadik félt.
- Ez a kulcselosztó központot (*Key Distribution Center* - KDC)
- Ennek segítségével az ügyfél és a kívánt szolgáltatás egymásra találhat.
- A KDC egy megbízható, biztonságos kiszolgálón fut.

61

Hitelesítési eljárások: Kerberos

- Kulcskezelés Kerberos esetén:



62

Hitelesítési eljárások: Kerberos

- A KDC és az ügyfél az egymás közti kommunikációjuk során az ügyfél hosszú távú kulcsát (*long-term key*) használják.
- Ezt az első bejelentkezéskor a felhasználó jelszavából állítanak elő DES-CBC-MD5 kódolással.
- A KDC minden felhasználónak ismeri a hosszú távú kulcsát.

63

Hitelesítési eljárások: Kerberos

- Ha egy ügyfél kapcsolatot szeretne kiépíteni egy kiszolgálóval először fel kell venni a kapcsolatot a KDC-vel!
- Ezt az ügyfél hosszú távú kulcsával teheti meg.
- Ha a KDC hitelesnek állapítja meg az ügyfelet, akkor generál neki egy ún. kapcsolati vagy szakaszkulcsot (*session ticket*)

64

Hitelesítési eljárások: Kerberos

- A kapcsolati kulcsot az ügyfél hosszú távú kulcsával titkosítja a KDC.
- Az ügyfél ezt a kiszolgálónak is elküldi, az említett titkosítással.
- A szakaszjegyek élettartama általában 8 óra, ezután újra kell igényelni egy új szakaszkulcsot.

65

Hitelesítési eljárások: Kerberos

- A KDC feladata ebből a szempontból kettős:
  - a hitelesítési feladatok (*Authetication Service*) ellátása
  - a jegykiszolgáló (*Ticket-Granting Service*) feladatok ellátása

66

Titkosítás, hitelesítés

Hitelesítési eljárások: Kerberos

- A Kerberos protokoll három al-protokollból áll;
- Az első két protokoll az ügyfél és a KDC közötti kapcsolatról szól.
- A harmadik az ügyfél és az őt kiszolgáló gép kapcsolatáról.
- Az összes protokoll lényegében kérésekből (Kerberos_xxx_Request) és válaszokból (Kerberos_xxx_Reply) tevődik össze.

67

Hitelesítési eljárások: Kerberos

- A Kerberos rendszer három al-protokollja:
  - **Hitelesítő Szolgáltatás** (*Authentication Service*, AS): A felhasználók azonosítása a Kerberos szerveren még a szolgáltatás igénylése előtt. Ha az azonosítás rendben, akkor egy speciális jegyet (Ticket-Granting Ticket, TGT) ad. E jeggyel lehet további, szolgáltatásokra szóló un. *Ticket-Granting Service*, TGS jegyet igényelni…

68

Hitelesítési eljárások: Kerberos

  - **Jegykiadó Szolgáltatás** (Ticket Granting Service, TGS): A felhasználók által igényelt szolgáltatásokhoz bocsát ki jegyeket. A felhasználók a jegyekkel azonosítják, hogy valóban jogosultak-e az illető szolgáltatás használatára.
  - **Kliens/szerver üzenetváltás** (Client/server Exchange, CS): Az ügyfél és a kiszolgáló közötti hitelesítés a TGS-től kapott szakaszjegy alapján

69

VPN: fogalmak

- VPN: virtuális magánhálózat (*Virtual Private Network*): nyilvános hálózaton (például Interneten) keresztül megvalósított, titkosított hálózati kapcsolat.
- Távolról intézményi hálózat elérése (régebbi megoldás): *Routing and Remote Access Service* (RAS) telepítése és elérése.

70

VPN: fogalmak

- Alternatíva: VPN; egy, az Interneten keresztül kiépített titkosított csatorna; a felhasználók a VPN kiszolgálón keresztül csatlakozhatnak a belső hálózatra.

71

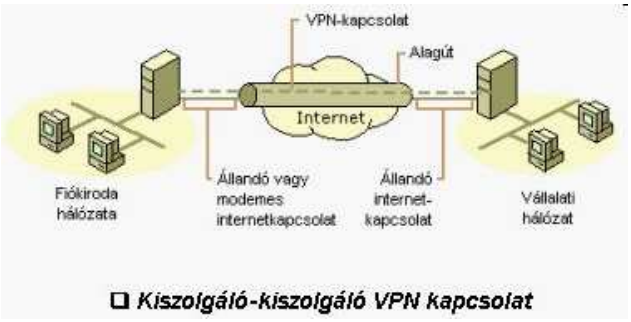
VPN: ügyfél-kiszolgáló

❑ *Ügyfél-kiszolgáló VPN kapcsolat*

72

Titkosítás, hitelesítés

VPN: kiszolgáló-kiszolgáló



❑ *Kiszolgáló-kiszolgáló VPN kapcsolat*

73

VPN

- A nyilvános hálózaton keresztüli biztonságos kommunikáció érdekében a hálózati forgalmat titkosítani kell.
- Többféle protokoll használatos:
  - *Point-to-Point Tunneling Protocol* (PPTP): Az RFC 2637-ben definiált alagútprotokoll
  - *Layer 2 Tunneling Protocol* (L2TP): Az RFC 2661 definiálja. A protokoll saját titkosítást nem tartalmaz, ezért az *L2TP over IPSec* használatos.

74

VPN: PPTP

- Virtuális magánhálózati technológia két számítógép között végzett adatcsere védelmére.
- A PPTP a PPP protokoll Microsoft által készített továbbfejlesztése.

75

VPN: PPTP

- Jellemzői:
  - könnyű kliens-oldali telepíthetőség, rugalmasság;
  - PPTP kapcsolat egyszerű TCP csatornán keresztül közlekedik;
  - a kapcsolat NAT-olható. vagyis egy címfordítást végző tűzfalon is átvihető;
  - az összeköttetés biztonsága viszonylag alacsony biztonsági szintű (bár ma már 128 bites titkosítást is képes kezelni);

76

VPN: IPSec

- Az IPSec-protokollok oly módon biztosítják az egyes IP-csomagok adat- és azonosító-védelmét, hogy saját biztonságiprotokoll-fejlécükkel látják el az egyes csomagokat.
- Módok:
  - *Tunnel* (bujtatott)
  - *Transport* (szállítási)

77

VPN: IPSec, *Transport* mód

- Az IPSec alapértelmezett üzemmódja az átviteli üzemmód.
- A hálózat két pontja közötti kommunikációra használható (például ügyfél és kiszolgáló közötti kommunikációra).
- Az átviteli üzemmód használatakor az IPSec csak az IP-tartalmat titkosítja.

78

VPN: IPSec, *Tunnel* mód

- Az IPSec bújtatási üzemmódban az IPSec az IP-fejlécet és az IP-tartalmat is titkosítja.
- A bújtatási mód egy teljes IP-csomag védelmét biztosítja.

79

VPN: IPSec, *Tunnel* mód

- A bújtatási móddal egy teljes IP-csomag beágyazása történik egy kiegészítő IP-fejléccel.
- A külső IP-fejléc IP-címei az alagút végpontjai, a beágyazott IP-fejléc címei pedig az eredeti forrás- és célcímek.

80

VPN: IPSec, *Tunnel* mód

- Az IPSec bújtatási üzemmódja különösen hasznos a hálózatok közötti forgalom védelmére, ha ez a forgalom egy közvetítő, nem megbízható hálózaton megy keresztül.

81

Címtárak

- Címtár: olyan, mint egy adatbázis, de arra törekszik, hogy magába foglaljon egy részletesebb, tulajdonság alapú információkezelést.
- A címtár, *directory service* egy olyan speciális adatbázist takar, mely keresésre van optimalizálva.

82

Címtárak

- Akkor célszerű ilyet használni, ahol kevés a módosítás, és nagy számú, gyors lekérdezésekre van szükség.
- Az információ egy faszerű szerkezetben tárolódik.
- Minden csúcsában bejegyzések (*entry*) szerepelnek.

83

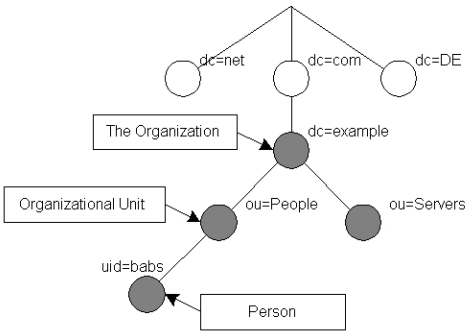
Címtárak

- Egy bejegyzésnek van típusa, amely meghatározza, hogy milyen attribútumai lehetnek.
- Minden egyes ilyen bejegyzésre egyértelműen hivatkozhatunk a bejegyzés DN-jével (*Distinguished Name*), mely lényegében a fában a csúcshoz vezető utat írja le.

84

Titkosítás, hitelesítés

Címtárak



85

Címtárak, LDAP

- LDAP (*Lightweight Directory Access Protocol*): kliens-szerver protokoll, címtár szolgáltatás eléréséhez.

86

Címtárak, LDAP

- Az LDAP címtárszolgáltatás kliens-szerver modellen alapul.
- Egy vagy több LDAP szerveren tárolt adatból épül fel az LDAP fa vagy LDAP háttér adatbázis.
- Az LDAP kliens egy LDAP szerverhez csatlakozik, és teszi fel a kérdéseit.

87

Címtárak, LDAP

- A szerver megválaszolja a kérdést, vagy egy mutatót ad vissza, hol talál több információt a kliens (tipikusan egy másik LDAP szerver).
- Mindegy, hogy a kliens melyik LDAP szerverhez csatlakozik:
- Ugyanazt a címtárat látja, ugyanaz a név az egyik címtár szerveren ugyanazt az adatot jeleníti meg, mint a másikon.

88

Címtárak, LDAP

- LDAP műveletek:
  - Keresés
  - Módosítás
  - Új bejegyzés
  - Törlés

89

Címtárak, LDAP

- Egy LDAP keresés megadásához a következő információkat kell megadni:
  - a keresés kezdetét (*base*): egy DN ahol a keresést kezdeni kell, a lehetőségek:
    - *base*: csak a *base* DN által megadott objektum
    - *one*: a *base* DN által meghatározott bejegyzés, és az egy szinttel lejjebb lévő bejegyzések
    - *sub*: a *base* DN által meghatározott teljes részfa
  - a keresés hatáskörét (*scope*),
  - egy keresési szűrőt (*filter*): a kereséshez megadható szűrő.

90

Titkosítás, hitelesítés

Tűzfal

- Szükséges, hogy az Internet felől érkező nem kívánatos tevékenységet távol tartsuk a belső hálózattól. A védelem első lépcsőfoka a tűzfal.

91

Tűzfal

- Tűzfal technológiák:
  - csomagszűrő (*packet filter*)
  - állapottartó csomagszűrő (*stateful packet filter*)
  - Állapottartó betekintő (*stateful inspection filter*)
  - Socks
  - Alkalmazás szintű (*application layer gateway*)

92

Tűzfal

- Csomagszűrés:
  - Az áthaladni kívánó csomagok fejlécét vizsgálja;
  - Ezt előre meghatározott szabályokkal (*rules*) hasonlítja össze;
  - Egyezés esetén a szabályhoz rendelt döntést (tovább engedik, blokkolják, stb.) végrehajtják;
  - A vizsgálatot a forrás és a cél IP címmel kezdik;

93

Tűzfal

  - A legtöbb implementáció a következő, az adatkapcsolati réteget is kiértékeli: eben az esetben lehetőség van a forrás és a cél portokra való szűrésre is!
  - A fejléc opciós bitjeit is ki szokás értékelni!
- A csomagszűrés összetett igények kielégítésére nem alkalmas!
- A szabályok mennyisége átláthatatlanná növekedhet.

94

Tűzfal

- A csomagok kiértékelése egymástól független, azaz pl. nem dönthető el, hogy egy csomag egy kérés vagy egy válasz része-e.

95

Tűzfal

- Állapottartó csomagszűrő:
  - A csomagok fejléce kerül kiértékelésre;
  - Nem csak különálló csomagok kerülnek kiértékelésre, hanem kapcsolatok is.
  - Ezáltal pl. TCP kapcsolat esetében megkülönböztethető a kapcsolat kiépülését végző csomagot a kapcsolat megszakítását végzőtől.
  - Adott csomag csak adott helyen szerepelhet.

96

Titkosítás, hitelesítés

Tűzfal

- Állapottartó betekintő:
  - A hagyományos állapottartó technológia kiegészítése;
  - Nem csak a csomag fejlécét, hanem a csomag tartalmát is analizálja;
  - Bizonyos protokollok jellemzőit is figyelheti: a nem ismert vagy illegális parancsokat tartalmazó csomagokat eldobhatja.
  - Többcsatornás protokollok kezelésére alkalmas.

97

Tűzfal

- Socks:
  - A kliens gépre települ egy program modul, ami minden hálózati kapcsolat kezelését átveszi az eredeti operációs rendszertől.
  - Amikor egy program hálózati kapcsolódást kezdeményez, a kapcsolódási kérést e modul kezeli;
  - Hálózati szempontból nem, de a program szempontjából transzparens.

98

Tűzfal

- Alkalmazás szintű:
  - A kliensek és a kiszolgáló között nem épül fel közvetlen kapcsolat;
  - mindketten a tűzfalon futó proxy alkalmazással kommunikálnak;
  - A proxy egyik hálózati csatolójával a hálózati kiszolgálóhoz, másikkal a helyi klienshez kapcsolódik.
  - Kivédi a csomagszintű támadásokat, ill. mély-protokoll elemzésre alkalmas

99

Proxy

- A böngészés során meglátogatott oldalakat *cach*-eli, amivel a meglévő sávszélesség jobban hasznosítható.
- Az Internet-es forgalom egy része megy csak át a proxy-n:
  - a böngészőben nincs beállítva;
  - bizonyos protokollok esetén semmiképp sem használható a proxy: pl. smtp es pop3…

100

Tartalomszűrés

- Szoftveres vagy hardveres és szoftveres megoldás arra, miként lehet az Internet nemkívánt tartalmú forgalmát a helyi hálózat felé vagy onnan megakadályozni.
- Két alapvető mód:
  - Cím (URL) alapján történő szűrés
  - Tartalom (kulcsszó) alapján való szűrés

101

Források:

- Ronald L. Rivest **http://theory.lcs.mit.edu/~rivest/**
- Leonard Adleman **http://www.usc.edu/dept/molecular-science/fm-adleman.htm**

102

Titkosítás, hitelesítés

Források:

- RSA
  http://www.muppetlabs.com/~breadbox/txt/rsa.html
  http://peter.verhas.com/cript/rsadef.htm

103

Források:

- Titkosítás
  http://www.cryptox.hu/crypto04.php
  http://galantai.inno.bme.hu/computing/titkositas_majdnem_mindenkinek.html
  http://ecdlweb.uw.hu/m7-15.html

104

Források:

- Kriptoprotokollok:
  http://nws.iif.hu/ncd2001/docs/eloadas/42/index.htm
- PKI:
  http://www.ediport.hu/szakmaioldalak.html

105

Források:

- X.400, X.500:
  http://www.itb.hu/ajanlasok/a17/html/a17_5-2.htm
- CHAP:
  http://en.wikipedia.org/wiki/Challenge-handshake_authentication_protocol

106

Források:

- Kerberos:
  http://pcforum.hu/cikkek/112/A+Kerberos+hitelesitesi+protokoll/oldal/1.html
- VPN:
  http://szamitogep.hu/show/read.php?id=14777

107

Források:

- PPTP:
  http://www.sulinet.hu/tart/fcikk/Kaaal/0/26071/1
- IPSec:
  http://www.microsoft.com/technet/prodtechnol/windowsserver2003/hu/library/ServerHelp/cef71791-bcf2-4f0f-9a56-db1682cf8a24.mspx

108

Titkosítás, hitelesítés

Források:

- Címtár, LDAP:
  http://padre.web.elte.hu/ldap.html
- Tűzfalak:
  portal.delta.hu/apic/tuzfalak.pdf

109

Források:

- xxx:
  xxx
- xxx:
  xxx

110