Hálózati szolgáltatások

SSL/SSH

Informatikus
(rendszerinformatikus)

SSL

- SSL: *Secure Socket Layer;*
- Célja a hálózati kommunikáció titkosítása: biztonságos kapcsolat létrehozatala két távoli TCP alkalmazás között

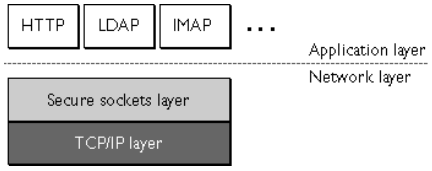
SSL

- Biztonságos adatátvitelt nyújt:
  - kölcsönös hitelesítést megengedve,
  - az egyedek digitális aláírásainak felhasználásával,
  - és az üzenet titkosításával.
- Tipikus alkalmazása: WEB szerver és kliens biztonságos kapcsolata

SSL

- A protokollt úgy tervezték, hogy többféle kriptográfiai, a kivonatolási (ujjlenyomat) és aláírási algoritmust támogasson.
- Az, hogy milyen algoritmust használnak egy kapcsolatban, akkor dől el, amikor a kliens és a szerver közötti kapcsolat kialakul.

SSL



SSL

- Eredetileg a Netscape fejlesztette ki;
- Közbenső réteg:
  - az összeköttetés alapú hálózati réteg protokollja (pl. TCP/IP)
  - alkalmazási réteg protokollja (pl. HTTP) között helyezkedhet el.
- Szabványosított (RFC 2246)

SSL/SSH

SSL

- Két sub-protokoll alkotja:
  - SSL *record protocol*: átviteli formátum
  - SSL *handshake protocol*: szerver – kliens üzenetváltás

7

SSL

- Az SSL kapcsolat egy párbeszéd alapján jön létre,
- amely a kliens és a szerver között zajlik.
- Ez a folyamat különböző lehet aszerint,
- hogy a szerver beállítása szerint a szerver biztosít egy szerver tanúsítványt,
- vagy igényel a klienstől egy kliens tanúsítványt.

8

SSL

- Ha egy SSL kapcsolat kialakult, akkor azt a szerver egyedi azonosítóval látja el.
- Ezért a kliens egy későbbi kapcsolatfelvétele esetén a kapcsolat időigényes kialakítása már nem szükséges, használható az azonosító (amíg az le nem jár)

9

SSL

- A kliens és a szerver közötti párbeszédben a következők történnek:
  - Megbeszélik és kiválasztják a kódkészletet (*Cipher Suite*), amit az adatátvitel alatt használni fognak.
  - Elfogadnak és megosztoznak egy kapcsolati kulcson a kliens és a szerver között.
  - Opcionálisan azonosítja a kliens a szervert.
  - Opcionálisan azonosítja a szerver a klienst.

10

SSL

- Az SSL-nek a titkosítás foka szerint két változata van: 40 bites és 128 bites, ami a titkosított tranzakció kulcsának hosszát jelenti.
- Minél hosszabb a kulcs, annál nehezebb feltörni a kódot.
- Az SSL az RSA nyilvános kulcsú kriptográfiai módszert használja a hitelesítéshez

11

A nyilvános kulcsú kriptográfia használata hitelesítéskor

- A hitelesítés az a folyamat, melynek során egy identitás oly módon kerül azonosításra, hogy az egyik entitás biztos lehet abban, hogy a másik entitás az, akinek ő hiszi. A következő példában két képzeletbeli személy András és Béla segítségével mutatom be a módszer működését.
- András hitelesíteni kívánja Bélát. Bélának van egy kulcspárja, azaz egy nyilvános és egy privát. Béla elárulja Andrásnak a nyilvános kulcsát. András ezután egy véletlenszerű üzenetet generál és elküldi Bélának.

12

SSL/SSH

A nyilvános kulcsú kriptográfia használata hitelesítéskor

- Béla privát kulcsa segítségével dekódolja az üzenetet, majd újra kódolja a saját privát kulcsával, és a kódolt változatot visszaküldi Andrásnak.
- András megkapja az üzenetet, dekódolja azt a Bélától kapott nyilvános kulccsal, és összehasonlítja az eredetileg elküldött üzenettel. Ha a két üzenet egyezik, akkor András tudja, hogy Bélával kommunikál.
- Ha valaki vissza akart volna élni, akkor szüksége lett volna Béla privát kulcsára, hogy megfelelően tudja kódolni az Andrásnak küldendő üzenetet.

13

SSH

- SSH: *Secure SHell*
- Alkalmazási szintű protokoll;
- Célja, hogy
  - távoli gépekre jelentkezzünk be,
  - parancsokat hajtsunk végre távoli gépeken
- Működése RSA kulcson alapul

14

SSH

- A következő támadások ellen véd:
  - IP cím hamisítás (egy távoli gép olyan IP csomagokat küld, mintha azokat egy másik számítógép küldte volna)
  - IP source routing, amikor egy gép azt szimulálja, mintha egy távoli gép csomagjai rajta keresztül továbbítódtak volna
  - DNS hamisítás, ekkor egy name server bejegyzést hamisítanak meg

15

SSH

  - az adatforgalom közbülső gépek által való lehallgatása ellen
  - az IP csomagok közbülső gépek általi megváltoztatása ellen
- Két, különböző és egymással nem kompatibilis változata létezik: SSH1 és SSH2 (Az SSH2 sokkal erősebb védelmet biztosít)

16

SSH

- Funkcionálisan az RSH (*Remote Shell*=távoli futtatás) helyettesítője úgy, hogy
- biztonságos, erős autentikációval ellenőrzött titkosított kapcsolatokat hoz létre
- két „egymásban” nem bízó gép között, amelyeket a nem-biztonságosnak tekintett hálózat köt össze.

17

SSH

- Teljes körű autentikációt tesz lehetővé a felhasználói azonosítóval és jelszóval.
- Ennek során a kommunikáció mindvégig titkosított csatornán folyik.
- A küldött adatok megtekintése lehetséges, de a tartalomhoz a behatoló nem tud hozzáférni a kulcs hiányában.
- Ez lehetővé teszi a kommunikációt nem biztonságos hálózatokban.

18

SSL/SSH

SSH

- Minden ssh-t használó gépnek van egy host-azonosító RSA kulcsa (default 1024 bit).
- A szerver gépen az sshd daemon ezen kívül generál egy szerver RSA kulcsot is (default 768 bit), [SSH2 esetén ilyen nincs!]
- melyet óránként frissít és amit
- soha nem tárol a merevlemezen.

19

SSH

- Amikor egy kliens (SSH) hozzákapcsolódik a szerverhez (SSHD), akkor:
  - először a szerver azonosítása történik meg
  - A szerver elküldi a host- és szerver-kulcsok publikus részét a kliensnek.
  - A kliens összehasonlítja a host-azonosító publikus kulcsot az adatbázisban lévővel és
  - ellenőrzi, hogy az változatlan-e.

20

SSH

- Ezután a kliens generál egy 256 bites véletlenszámot, amit
- a szerver host- és szerver-kulcsával egyaránt titkosít,
- majd ezt visszaküldi a szervernek.
- A szerver az RSA kulcsai ismeretében vissza tudja fejteni a titkosított véletlenszámot,
- amit a továbbiakban a két oldal a forgalom titkosító kulcsául (*session key*) fog használni.

21

SSH

- A következő lépés a kliens azonosítása (rhosts autentikáció).
- Ha a kliens sikeresen azonosította magát, akkor a kapcsolat előkészítéseként különböző szolgáltatásokat kérhet a szervertől.
- Végül a kliens vagy egy shell indítását (slogin, ssh) vagy egy parancs végrehajtását kérheti a szervertől.

22

Források: SSL

- OpenSSL: **http://www.openssl.org/**
- SSL RedHat környezetben: **http://linuxdoc.freeweb.hu/konyv/rh62/**

23

Források: SSH

- Titkosítás, SSH: **http://vili.pmmf.hu/jegyzet/diplom/2000/novak/megoldas.htm**
- Secure Shell: **http://www.hup.hu/wiki/index.php/SSH**
- SSH **http://www.remote.hu/articles.php?id=18&page=3**

24