11. tétel: Milyen forgalom védelmét látja el az SSL (Secure Socket Layer) protokoll és miben befolyásolhatja ez a tervezést? Mutassa be az SSL protokoll felépítését és működését!)

1. Bevezetés:

- internetbiztonság (miért van rá szükség, mit várunk el?)

- TLS elődje

2. Szállítási réteg és alkalmazási réteg közt operáló védelem (layer 4-7)

- nyílt hálózatokban, kapcsolatorientált kommunikációban nyújt védelmet

- védelmet nyújt az elküdött érzékeny adatokhoz 2 rendszer közt

- 1-1 kommunikációs csatornát (http forgalmat) titkosít

- kliens és szerver oldalon is szükség van támogatásra

- SSL réteg átlátszó

- bármilyen alkalmazáshoz használható

3. Tervezés befolyásolás:

(forrás: https://fallbackstatus.com/planning-deploying-and-maintaining-ssl-certificates-to-protect-against-information-loss-and-build-customer-trust/#planning-for-the-use-of-ssl-certificates)

- figyelembe kell venni mi szükséges a működéséhez

- 2 fő megfontolás:

a) melyik alkalmazások és szerverek számár előny az SSL használata

- milyen adatot fognak küldeni/fogadni? (pl bizalmas, publikus)

- milyen alkalmazások fognak futni a szervereken?

- melyekhez férnek hozzá a felhasználók?

- hány eszközön fog "átutazni" az adat? (pl többrétegű alkalmazás-> online fizetés)

b) az egyes használati esetekre milyen típusú SSL certificate megfelelő? pl:

- self-signed (fejlesztéshez és teszteléshez előnyös)

- single server certificate

- domain wildcard certificate

- EV cert. (extended validation)

4. Működés:

- nyilvános kulcsú technológiát használ

1) minden session-höz rövid életű, véletlen, egyedi kulccsal titkosít

2) ezt a szerver titkos kulcsával küldi el a klienshez

3) szervert tanusítvány igazolja

4) szerver és kliens közti adatforgalom titkosítása szimmetrikus algoritmussal (típus: megegyezés alapján)

4.2 Record protokoll működése:

1. fragmentálja (ha szükséges),

2. a fragmenseket tömöríti,

3. a tömörített fragmenseket fejléccel látja el,

4. a fejléccel ellátott, tömörített fragmensre üzenethitelesítő kódot (MAC) számol, és azt a fragmenshez csatolja

5. az üzenethitelesítő kóddal ellátott fragmenst rejtjelezi

5. Felépítés (alprotokollok):

1) Record protokoll; feladata: titkosítás, integritásvédelem, üzenet-visszajátszás elleni védelem

2) Handshake protokoll; feladata: kripto-algoritmus egyeztetés, kulcscsere, hitelesítés

3) Change-Cipher-Spec protokoll; feladata: kulcscsere végének jelzése

4) Alert protokoll; feladata: figyelmeztető- és hibaüzenetek továbbítása