Fábián Zoltán – Hálózatok elmélet

IP SEC protokoll

Az Internetes kommunikáció védelmének lehetőségei

- Rejtett csatornán nyílt adatokat közlünk
  - Pl. VPN
- Nyílt csatornán rejtett adatokat küldünk
  - Titkosítás
    - A kommunikáció szintjén (Az adatcsomagokat titkosítom)
    - Az üzenetek szintjén (Az üzenetet titkosítom)
  - VPN

Az IP biztonsági követelményei

- Authentikáció (az üzenetet az küldte, aki a message headerben fel van tüntetve + integritásellenőrzés)
- Bizalmasság (A csomópontok közötti kommunikációt nem lehet lehallgatni)
- Kulcs menedzsment (Kulcsok biztonságos cseréje)

Az IPSec koncepció

- Kézenfekvő megoldás a biztonságot
  - a legalsó OSI szinten, azaz a fizikai kapcsolatok szintjén biztosítani.
- Az IP protokollt továbbfejlesztették IPSec protokollá
  - 1994 (The Internet Architecture Board: IAB) report: Security in the Internet Architecture
  - Ennek alapján: IPv6 (amelynek kompatibilisnek kellett lennie a korábbi IPv4-gyel.
- Az IPSec minden kommunikációt az IP szinten képes titkosítani és authentikálni

Az IPSec tulajdonságai

- IPSec tulajdonságai
  - Hozzáférés védelem és bizalmasság
    - Mások nem láthatják az adatforgalmat, nem férhetnek hozzá
  - Integritásvédelem
    - Az adatforgalmat nem lehet megváltoztatni
  - Hitelesítés
    - Bizonyosság, hogy valóban a küld fél küldte az adatokat
    - A kapcsolatban lévő felek ismerik egymást
  - Védelem a visszajátszások ellen
    - Az adatforgalmat nem lehet ugyanazokkal az IP csomagokkal megismételni késbb

IPSec alkalmazásai

- Routereken, tűzfalokon. Minden kommunikációt titkosít és tömörít küldés előtt. A fogadó kibontja a csomagokat.
- A műveletek transzparensek (átlátszóak), mert a szállítási rétegek alatt történik
- A szállítási rétegekre (TCP, UDP) épülő alkalmazásokon nem kell változtatni

Cikkek

- http://technet.microsoft.com/hu-hu/library/cc775944(WS.10).aspx
- http://www.szgti.bmf.hu/~mtoth/download/Adatvedelem es titkositas/IPSec.pdf