Wireless LAN a Műegyetemen

Jákó András
jako.andras@eik.bme.hu
BME EISzK

Tartalom

Peremfeltételek

Biztonság

Rádiós problémák

Feltételek az üzemeltetőnél

- skálázhatóság
  - több ezer potenciális felhasználó
    - jelenleg 50+
  - 60+ access point
    - jelenleg 4
- megfizethetőség
  - ha van felhasználó oldali software költség, akkor azt az üzemeltető fizesse
    - de jobb, ha nincs
- felhasználói jelszavak: UNIX hash-elt formában
  - ha szükség van jelszavakra

Feltételek a felhasználónál

- heterogén környezet
  - sokféle operációs rendszeren működnie kell
    - Win2k, WinXP, Linux feltétlenül
    - lehetőleg Win98, WinME, WinMobile, Mac OS X, Net/Open/FreeBSD is
  - sokféle WLAN adapterrel működnie kell
- egyszerűség
  - egyszerűnek kell lennie annyira, hogy az egyetem vendégei is használhassák
    - egy pár napos látogatás idejére is érdemes legyen megtenniük a szükséges lépéseket

Tartalom

Peremfeltételek

Biztonság

Rádiós problémák

Veszélyek

- lehallgatás
  - a vezeték nélküli szakaszon a keretek lehallgatása triviális
  - közvetlenül a felhasználónak árt, közvetetten a hálózat üzemeltetőjének is

Üzemeltető

- nem feladata megvédeni a felhasználót a lehallgatástól
  - de feladata a veszélyről tájékoztatni
- érdeke megvédeni a felhasználót
  - a lehallgatásból később biztonsági incidensek adódhatnak
    - ami számos problémát és feladatot jelent az üzemeltetőnek (is)
  - a felhasználó elégedettsége csökken
    - és valamekkora részben biztosan az üzemeltetőt fogja hibáztatni

Üzemeltető

- lehetőségei a lehallgatás elleni védelemre
  - az adatkapcsolati rétegben
    - WEP (Wired Equivalent Privacy) az IEEE 802.11 szabvány szerint
      - közös kulcs: a potenciális támadók nagy része ellen nem véd
      - hibás az eljárás
    - IEEE 802.11i
      - még nem készült el
    - WPA (Wireless Protected Access): a Wi-Fi Alliance ajánlása
      - még nagyon új (2002. ősz), ezért kevés a működő implementáció
  - a hálózati rétegben
    - remote access IPSec VPN: a „távoli” felhasználó a WLAN felhasználó, a „védett” hálózat az Internet
      - számunkra megfizethető felhasználóbarát multiplatform VPN kliens: határeset
      - két VPN kliens nem tudna egyszerre működni
- jelenleg nem nagyon van számunkra megfelelő lehetőség

Felhasználó

- lehetőségei a lehallgatás elleni védekezésre
  - az elérni kívánt erőforrásoktól függenek
    - hálózati rétegben
      - remote access IPSec VPN (IPSec ESP)
    - megjelenítési rétegben
      - SSL/TLS (+ HTTP, SMTP, POP3, stb.)
    - alkalmazási rétegben
      - ssh, scp, SFTP, S/MIME, PGP, stb.
- általában tehát vannak lehetőségei
  - de rendszerint nem él velük (ha nincs rákényszerítve)

Veszélyek

- lehallgatás
  - a vezeték nélküli szakaszon a keretek lehallgatása triviális
  - közvetlenül a felhasználónak árt, közvetetten a hálózat üzemeltetőjének is
- illetéktelen hozzáférés a hálózathoz
  - fizikailag triviális
  - a szolgáltatás illetéktelen igénybevételét meg kell akadályozni
    - az érvényes szabályzatokba ütközik
    - a hálózat üzemeltetője felelősséggel tartozik azért, ami a hálózatán történik
      - ehhez „utolérhető” felhasználókra van szükség

Autentikációs lehetőségek – 1.

- 802.11 shared key
  - a közös kulcs nem maradhatna titokban
- MAC address alapján
  - kliens oldalon mindig működik, jól skálázható
  - nem annyira biztonságos
- 802.1X EAPoL (Extensible Authentication Protocol over LAN)
  - EAP-TLS
    - nehezen skálázható: nyilvános kulcsú tanúsítvány szükséges minden felhasználónak
  - PEAP
    - része a Windowsnak (2000, XP, Mobile)
    - második fázisban csak MS-CHAP2 implementáció van Windowson
      - ehhez clear-text vagy NT hash jelszóadatbázis kellene
  - EAP-TTLS
    - a tapasztalatok alapján driver/software hibák miatt WinXP-n gyakran nem működik
    - nincs ingyenes Windows Mobile implementáció

Autentikációs lehetőségek – 2.

- PPPoE (pontosabban PPP over WLAN)
  - minden lényeges platformra van ingyenes, működő kliens
  - csak PAP autentikációt tudnánk használni, így viszont lehallgathatók a jelszavak
- remote access IPSec VPN (csak AH)
  - a lehallgatás elleni védekezésnél leírtakkal azonos problémák

Biztonsági intézkedések

- sajnos kizárásos alapon dőlt el a kérdés
- lehallgatás ellen a felhasználó védekezik
  - később talán WPA
  - még később talán 802.11i
- MAC address alapú autentikáció
  - a felhasználó egy meghatározott file-ba leteszi a kártyája MAC címét
    - ezt egy script rendszeresen összegyűjti, és berakja a RADIUS adatbázisába
  - később remélhetőleg valamilyen jelszó alapú EAP autentikáció

Tartalom

Peremfeltételek

Biztonság

Rádiós problémák

Interferencia

- Hol ki szolgáltasson?
  - a közös területeket központilag lenne jó lefedni
  - a tanszéki területek „hátsó részeit” csak a tanszék tudja ellátni
  - térben nehéz meghúzni a határt
  - frekvenciában könnyű a határt meghúzni
    - de kicsi a mozgástér (3 egymást át nem fedő csatorna)
- a szabályzaton jelenleg dolgozunk
  - nehéz lesz betarttatni
    - leszámítva a drasztikus módszereket, amit viszont inkább elkerülnénk

Csatornakészlet

- 14 csatorna az IEEE szabványban
  - a helyi hatóságok szabályozzák, hogy ebből melyik használható
    - Európa nagy részén, így Magyarországon is (ETSI) 1-13
    - Amerikában (FCC) 1-11
- sok kliens nem éri el a 12-13-as csatornán működő hálózatot
  - néha driver probléma (általában megoldható)
  - néha firmware(?) függő (gyakran nem oldható meg)
    - Pl. Intel Centrino
      - MOW (Most Of World) = Amerika
      - ROW (Rest Of World) = Európa, Ázsia, Ausztrália