

Prasklaidant debesis: WiMAX saugumas

Pranešėjas: Kęstas Gudiničius



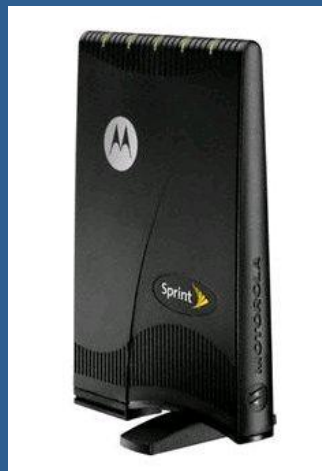
Kas yra WiMAX?

- IEEE 802.16 standartu paremta technologija
- Licencijuotas ryšio bangų spektras (2,3-3,5 GHz)
- Fiksuotas (802.16d) ir judrusis (802.16e) WiMAX
- Didelė sparta (~10Mb/s) bei aprėptis (~10km)
- Perduodamų duomenų šifravimas (DES3, AES)
- Autentifikacijos ir autorizacijos procesai

Kur gauti WiMAX

- AB Lietuvos radijo ir televizijos centras, interneto paslauga “MEZON”
- UAB Balticum TV, belaidis internetas WiMAX

WiMAX jiranga



Terminologija

MS (mobile station) – mobili stotis

SS (subscriber station) - abonento stotelė

BS (base station) - bazinė stotis

AES (Advanced Encryption Standard) - šifravimo algoritmas

EAP (Extensible Authentication Protocol) – autentifikacijos protokolas

AK (Authorization Key) – autorizacijos raktas

WiMAX/IEEE 802.16e ryšio seansas

1. MS ieško BS signalo, išgauna ryšio parametrus
2. MS nustato pradinius ryšio parametrus komunikacijai su BS ir užmezga valdymo kanalą
3. Autentifikacija ir raktų apsikeitimas
4. MS registruojasi tinkle
5. Užmezgamas IP ryšio seansas, gaunamas IP adresas naudojant DHCP

WiMAX/IEEE 802.16e saugumas

- Fizinio lygmens grėsmės
- Kanalo (MAC) lygmens grėsmės
- Taikymo lygmens grėsmės

Fizinio lygmens grėsmės

- Signalų gesinimas (jamming)
- Signalų trikdimas (scrambling)
- Padidintas resursų išnaudojimas (water torture attack)

Kanalo (MAC) lygmenis grėsmės

- Neautentifikuoti pranešimai
- Nešifruota valdymo informacija
- Bendro rakto naudojimas multi- ir broadcast režimuose
- Kenkėjiška bazinė stotis (BS)
- Įrangos klonavimas

Neautentifikuoti pranešimai

- **MOB_TRF-IND** (Traffic Indication Message) – BS nurodo miegančiai MS, kad laikas priimti duomenis, papildomos energijos sunaudojimas
- **MOB_NBR-ADV** (Neighbour Advertising Message) – BS Praneša MS kaimyninių BS charakteristikas, blokuojamas prisijungimas prie patikimesnių BS
- **FPC** (Fast Power Control Message) – BS nurodo MS, sumažinti/padidinti siuntimo galią, sumažinus iki minimumo BS praranda ryšį su MS
- **MSC-REQ** (Multicast Assignment Request Message) – BS pašalina MS iš multicast polling grupės
- **DBPC-REQ** (Downlink Burst Profile Change Request Message) – BS nurodo MS pakeisti pliūpsninį profilį, MS laikinai negali demoduliuoti iš BS gaunamų duomenų
- **PMC-REQ** (Control Mode Change Request) – MS praneša apie galios režimo pakeitimą
- **RNG-REQ** (Ranging Request) – dinamiško laiko suderinimo užklausa

Nešifruota valdymo informacija

- Pasyvus informacijos rinkimas apie BS ir MS
 - ryšio parametrai
 - saugumo nustatymai
 - gamintojo informacija
 - MS ir BS MAC adresai
 - apytikslis MS vietos nustatymas

Bendro rakto naudojimas multi- ir broadcast režimuose

- 802.16e suteikia galimybę perduoti duomenis grupei MS vienu pranešimu
- Bet kuris grupės narys gali netik iššifruoti ir tikrinti broadcast pranešimus, bet ir užšifruoti bei autentifikuoti pranešimus taip, lyg jie atrodytu siųsti iš realios BS

Kenkėjiška bazinė stotis (BS)

- MS autentifikacija naudojant X.509 sertifikatą
- Nėra BS autentifikacijos
- Apibūsės autentifikacijos nebuvimas = kenkėjiška BS
 - Man-in-the-middle ataka

Įrangos klonavimas

- Kiekvienas įrenginys (MS) turi turėti X.509 sertifikatą
- MS sertifikato “subject” dalyje įrašytas MS MAC adresas
- Neturint privataus rakto neįmanoma sugeneruoti naujo sertifikato su kitu MAC adresu
- Klonavimas įmanomas išgaunant patvirtintą X.509 sertifikatą ir klastojant MS MAC adresą.

MEZON SWC-U200 klonavimas?

MEZON SWC-U200 Connection Manager derinimo langas:

- DebugScreen.exe arba Ctrl+Alt+Shift+F1, slaptažodis: **lrtc1234**

MEZON SWC-U200 atnaujinimas

- <http://samsung-update.mezon.lt/>

MEZON SWC-U200 firmware atnaujinimas

- FWUpdate.exe -authkey **dhkdlqmfhakstp** -language Lithuanian -mymodel SWC-U200LRT -loglevel 2 -runby WCM -nvc -debug -silent -leavefw -update W -binpath ./

MEZON SWC-U200 Connection Manager detali derinimo informacija

- MEZONCM.exe **SamsungWiBroNetwork** -log:debug -himlog:debug

- CMC-730 čipsetas

Taikymo lygmens grėsmės

Autorizacijos apėjimas

- Nutraukiama paslauga, pasilieinama įranga
 - Tuneliavimas per DNS
 - Tuneliavimas per HTTP

Atakos prieš vartotojus

- PĮ atnaujinimo proceso sukompromitavimas
- Tvarkyklių spragos
- Maršrutizatorių spragos

Kokie hakerių ateities planai?

- Sukurti atvirą programinę įrangą (firmware)
 - 802.16 saugumo analizė taps prieinama masėms
 - Aktyvios atakos (DoS)
 - Pasyvios atakos (Sniffing)
- Kismet įskiepis
 - Patogumas
- Žaidimai su USRP2
 - Neribotos galimybės

Ačiū už dėmesį!



Nuorodos

http://paper.ijcsns.org/07_book/200711/20071102.pdf

<http://www.ibluemojo.com/contents/IEEE%20802.16%20Security.pdf>

http://wimax-hacking.googlegroups.com/web/wimax_hacking_defcon17.pdf

http://www.motorola.com/staticfiles/Business/Products/Wireless%20Broadband%20Networks/WiMAX/WiMAX%20Access%20Points/WAP%20400/Documents/StaticFile/WiMAX_Security_for_Real_World_Network_Service_Provider_Deployments_Copy.pdf

http://www.airspan.com/pdfs/WP_Mobile_WiMAX_Security.pdf

http://www.eion.com/download/tech_papers/Analysis_on_Mobile_WiMAX_Security.pdf

<http://yota-wimax.ru/yota-firmware/kak-pereproshit-yota-samsung-swc-u200-prinuditelno/>

<http://yota-wimax.ru/yota-firmware/soft-yota-access-v120-i-beta-proshivka-bl22/>

<http://forum.yotatester.ru/showthread.php?t=1366>