Overview of IEEE 802.16 Security

David Johnston & Jesse Walker
Presented By: Anil Bazaz
Intro to IEEE 802.16

- Standard for Wireless Metropolitan Area Networks (WMANs)
- Flavors: IEEE 802.16-2001, 802.16a, 802.16c, 802.16d, 802.16e
- Security Based DOCSIS
Intro to IEEE 802.16

HOW IT WORKS

802.16
IEEE 802.16 standards define how wireless traffic will move between subscribers and core networks.

1. A subscriber sends wireless traffic at speeds ranging from 2M to 155M bit/sec from a fixed antenna on a building.

2. The base station receives transmissions from multiple sites and sends traffic over wireless or wired links to a switching center using 802.16 protocol.

3. The switching center sends traffic to an ISP or the public switched telephone network.


CS6204, Spring 2005
Threats to Wireless Medium

♦ Anyone can intercept messages
♦ Anyone can write to wireless channel
♦ Anyone can resend valid, already send frames
Authorization in 802.16

- Authorization SA:
  1. X.509 certificate of SS
  2. AK
  3. AK identifier
  4. AK lifetime
  5. Downlink HMAC key
  6. KEK
  7. Uplink HMAC Key
  8. List of Authorized Data SA’s
Authorization Protocol

- SS $\rightarrow$ BS: Cert(Manufacturer)
- SS $\rightarrow$ BS: Cert(SS)
- BS $\rightarrow$ SS: RSA-Encrypt(PubKey(SS),AK) | Lifetime | SeqNo | SAID List
Authorization Security

- No explicit def. for authorization SA
- No distinction between two SAs
- No BS certificate
- No requirements for AK generation
- BS contributes all bits in an AK
- Assumption that certificates are unique
Privacy and Key Management (PKM)

- Data SA
  1. SAID
  2. DES-CBC Mode
  3. Two TEKs
  4. Two TEK Ids
  5. TEK Lifetime
  6. TEK IV
  7. Data SA Type
PKM Protocol

- BS → SS: SeqNo | SAID | HMAC(1)
- SS → BS: SeqNo | SAID | HMAC(2)
- BS → SS: SeqNo | SAID | OldTEK | NewTEK | HMAC(3)
PKM Security

- No distinction between Data SA’s
- TEK Identifier: 2 Bits
  - A single AK can consume 3360 TEKs
  - Need 12 Bits to identify TEKs
- TEK Expiry Default: Half a day
  - Used for DES CBC mode - 64bit Data Blocks
  - Cipher looses security after $2^{n/2}$ blocks
  - Avg. Throughput: 6.36Mbps/0.5day or 455Kbps/7days
- Fails to specify requirements for TEKs
Corrections & Suggestions

♦ Use AES with cipher block chaining MAC

♦ EAP

♦ Authorization SA as a first class concept
Corrections & Suggestions (Cont.)

♦ Authorization Changes:
  – SS → BS: Cert (Manufacturer(SS))
  – SS → BS: SS Random | Cert(SS) | Capabilities | SAID
  – BS → SS: SS-Random | RSA-Encrypt(PubKey(SS), pre-AK) | Lifetime | SeqNo | SAIDList | Cert(BS) | Sig (BS)

♦ New AK: HMAC-SHA-1(BS & SS Random data and Mac Addresses; Bit Length)
Corrections & Suggestions (Cont.)

♦ PKM Changes

- **BS → SS**: SS-Random | BS-Random | SeqNo12 | SAID | HMAC(1)
- **SS → BS**: SS-Random | BS-Random | SeqNo12 | SAID | HMAC(2)
- **BS → SS**: SS-Random | BS-Random | SeqNo12 | SAID | OldTEK | NewTEK | HMAC(3)
Conclusion

♦ Paper Identifies Security Issues
♦ Suggests simple corrections
♦ Security Issues are being dealt with by IEEE 802.16d and IEEE 802.16e working groups