[802.16e Security Adhoc Proposal]

IEEE 802.16 Presentation Submission Template (Rev. 8.3)

Document Number:

IEEE C802.16e-03/70

Date Submitted:

Thursday, November 13, 2003

Source:

Jose Puthenkulam

Intel Corporation

E-mail: jose.p.puthenkulam@intel.com

Jeff Mandin

Streetwaves

Email: jeff.mandin@streetwaves.com

Venue:

802.16 TGe, Session#28, Albuquerque, NM

Purpose:

This is a proposal to study and address the security issues within 802.16e by forming adhoc group

802.16e Security Adhoc Group Proposal

Jose Puthenkulam, Intel

Jeff Mandin, Streetwaves

Need for 802.16e Security Improvements

1. **802.16e security (PKM) needs mutual authentication, adequate replay protection and a cipher suite stronger than DES-CBC**
2. **802.16e deployment models have additional security related feature and performance (secure fast hand-off) requirements**
3. **Current security solution cannot directly utilize the largest deployed service provider core network AAA infrastructures as very low PKI support exists**
4. **A single mfr. credential based on X.509 certs is too limiting. Multiple user credentials should be supported with flexible protocols like EAP**
5. **A complete scalable security solution that integrates well into existing infrastructures is critical for 802.16e mass market success**

Proposal

- Form a security adhoc in the 16e Task Group
- This Adhoc will do the following:
  - Develop a draft contribution for adding EAP/Security support to 16e
    - First an outline draft covering, Network Model assumptions, and issues of device authentication vs user authentication will be developed
    - This will targeted for the Jan 04 meeting
  - EAP will be added as an optional authentication framework for EAP-TLS and other EAP methods
  - Security requirements for handoff will be addressed
  - Optional AES-CCM cipher suite will also be added
  - Make sure that the solution is fully backwards compatible with the existing solution

Backup

802.16 Authentication Issues

- Privacy Sub-layer (PKM) uses 1-way SS authentication only. No BS authentication is done
  - It is prone to false Base Station attacks (Network Impersonation)
  - It is also prone to Man-in-the-middle attacks
  - It only works when service providers control all the equipment
- SS X.509 certificate uses SS MAC address
  - This could make provisioning hard and not usable easily as user credential as opposed to being a mfr. device credential.
  - Implies a certain business model (CPE modem) and lacks flexibility
  - Ideally such a credential should be used for device authentication only much like the DOCSIS model
- No support for user identity based authentication
  - Service choice and device choice are strongly coupled

802.16 Key Exchange Issues

- 2-key 3DES based key wrap used for TEK exchange
  - Not as strong (82bits) as the TEK keys (128 bits) it carries
- Frequent exchange of TEKs – Not possible to ensure that TEKs don't repeat
- Suffers from replay attacks as there is no liveness in the key exchange protocol
- Suffers from the M-i-t-m attacks

802.16 Data Security Issues

- It provides no data authentication
  - Currently a foot note in the spec
- It uses DES for ciphering
  - It is considered weak by today's ciphering standards
- It provides no per packet integrity protection
- It provides no replay protection for data

802.16e Security Requirements

- Feature Requirements
  - Mutual/Bilateral Authentication
  - Strong per MAC PDU origin authenticity, integrity and privacy protection using AES-CCM
  - Security for hand-offs
- Performance Requirements
  - Fast SA establishment
  - Low latency key exchange