Existing Security Specifications for Long Range Wireless Networks

Background

- JTC1/SC6 Document 6N14745 (2011-05-20) introduces into SC6 the notion of a “Long Range Wireless Network” (LRWN) and presents views regarding “activities on the MAC Security Specifications” for such networks
- Doc. 6N14745 does not define “Long Range Wireless Networks”

What is an existing LRWN?

- Document 6N14745 refers to specific security technology of "Long Range Wireless Networks" using the following terms:
  - *PKMv1*
  - *PKMv2*
  - *IEEE 802.16e*
- PKMv1 and PKMv2 are specifications in IEEE Std 802.16
- So, it appears that Doc. 6N14745 is considering IEEE Std 802.16 as its example of an LRWN

Some existing networks based on IEEE 802.16

- *The WiMAX Forum*: Mobile WiMAX Release 1 specifications
- *International Telecommunication Union* (ITU) Recommendations, including:
  - Recommendation ITU-R F.1763
  - Recommendation ITU-R M.1801
  - Recommendation ITU-R M.1457 (**IMT-2000**)
  - Future recommendation on **IMT-Advanced**
    - Development since 2007; draft completed in 2011

Example: WiMAX Forum network based on IEEE 802.16

- WiMAX Forum's Mobile WiMAX Release 1 specifications specify a network based on IEEE 802.16
  - Including network and security specifications
- Widely deployed in many countries

ITU-standardized IMT-2000 networks based on IEEE 802.16

- ITU Recommendation ITU-R M.1457
  - Detailed specifications of the terrestrial radio interfaces of International Mobile Telecommunications-2000 (*IMT-2000*)
- Specifies a radio interface *IMT-2000 OFDMA TDD WMAN* (abbreviated here as *IMT-2000 OFDMA*) based on:
  - IEEE Standard 802.16
  - Mobile WiMAX Release 1
- Also specifies five other radio interfaces
  - Most could be considered LRWNs

IMT-2000 OFDMA: Typical, Existing 802.16-based LRWN

- For an example of a typical, existing LRWN based on IEEE 802.16, consider *IMT-2000 OFDMA*, because it is:
  - Based on subset of IEEE Std 802.16
  - Based on Mobile WiMAX Release 1
  - Widely deployed
  - Internationally standardized
  - Specified under the popular IMT-2000 standard

Existing Security Specifications of *IMT-2000 OFDMA*

- Based on subset of IEEE Std 802.16 security
  - PKMv2, per IEEE Std 802.16
    - note: PKMv1 is not specified
  - EAP-based authorization
  - CCM mode
    - counter mode encryption
    - cipher block chaining message authentication code
  - 128-bit AES encryption
  - AES Key Wrap with 128-bit key

IMT-Advanced

- New radio network “beyond IMT-2000”
- Began development in 2007
- Massive international participation
- Draft New Recommendation on “Detailed specifications of the terrestrial radio interfaces of IMT-Advanced” completed April 2011
  - Contains two radio interfaces
    - Both can be considered Long Range Wireless Networks
  - Final approval in 2012

IEEE 802.16 in IMT-Advanced

- Draft Recommendation includes *WirelessMAN-Advanced* air interface based on IEEE 802.16m-2011
  - No change to security system of IEEE 802.16
  - Per the Draft Recommendation, *WirelessMAN-Advanced* specifications are based on "detailed information developed by the ITU and 'IEEE' (the GCS Proponent) and IEEE, ARIB, TTA, and WiMAX Forum (the Transposing Organizations)
    - ARIB: Association of Radio Industries and Businesses (Japan)
    - TTA: Telecommunications Technology Association of Korea

Document 6N14745's Views on Security issues in LRWN

- Document 6N14745 provides views on "Typical Flaws in PKMv2":
  - *It remains the possibility of fake BS attack on introducing of EAP authentication.*
    - *It needs the reliable third party.*
    - *The security channel should be pre-established between the reliable third party and the SS because the AK sent to BS is created by the reliable third party and the SS.*
    - *The direct mutual authentication between the reliable third party and the SS is realized by EAP mechanism, rather then the direct mutual authentication between the BS and the SS, remaining the possibility of fake BS attack.*
  - *Low quality of authentication key in authentication process based on RSA.*
    - *The pre-authorization key PAK is only created by the BS. The generation approach of the PAK is not defined in IEEE 802.16e.*
    - *There will be a very serious security vulnerability if the generation of the key is not random.*

Document 6N14745's Views on Security issues in LRWN: Comment 1

- 6N14745 view:
  - *It remains the possibility of fake BS attack on introducing of EAP authentication.*
- Response:
  - This assertion, if true, would indicate a fault not in PKMv2 but in EAP.
  - Due to the nature of EAP, the assertion is incorrect. EAP explicitly requires a reliable third party and a secure network channel between the BS and Authenticator.
  - Since a malicious BS lacks a secure network channel to the Authenticator with trusted third-party credentials, it cannot conduct the required bi-directional EAP authentication transaction and cannot obtain authentic security key material. An EAP authentication attempt through a malicious BS would fail.
  - There is no known security vulnerability to this standardized EAP communication mechanism.

Document 6N14745's Views on Security issues in LRWN: Comment 2

- 6N14745 view:
  - *Low quality of authentication key in authentication process based on RSA.*
- Response:
  - *IMT-2000 OFDMA* specifies the use of EAP-based authorization, not RSA-based authorization.
  - Secure RSA-based authorization can also be readily implemented in accordance with IEEE Std 802.16.

Summary

- A subset of IEEE Std 802.16 has been adopted internationally as *IMT-2000 OFDMA* and *Mobile WiMAX*.
- ITU has developed IMT-Advanced, including *WirelessMAN-Advanced* based on IEEE 802.16, in conjunction with international and national SDOs
  - ISO, IEC, and JTC1 are not involved.
- The security systems in these standards are sound.
- Security concerns have not arisen within ITU during the internationalization of IEEE 802.16.
- Document 6N14745 raises no valid security concerns with these standards.

Venue to discuss Enhancements

- The IEEE 802.16 WG and the WiMAX Forum develop and maintain the "Global Core Specifications" underlying *IMT-2000 OFDMA*
- The IEEE 802.16 WG develops and maintains the "Global Core Specifications" underlying *WirelessMAN-Advanced*
- The IEEE 802.16 WG welcomes participation and contributions by all parties, including SC6 participants.
- The IEEE 802.16 WG meets every two months, throughout the world:
  - http://ieee802.org/16
  - http://ieee802.org/16/calendar.html
- The IEEE 802.16 WG strongly encourages any parties with awareness of any security concerns to bring them immediately and directly to the WG for review.
- Updates to IEEE standards follow IEEE development procedures.
- ITU is the relevant internationalizing body
- EAP is specified by IETF.

Recommended SC6 Actions

- Any SC6 concerns regarding internationally-adopted Long Range Wireless Networks should certainly be addressed by liaison statement to all the responsible bodies developing IMT-2000 and IMT-Advanced, including:
  - ITU-R Working Party 5D
  - IEEE 802.16 Working Group
  - 3rd Generation Partnership Project (3GPP)
  - Association of Radio Industries and Businesses (ARIB, Japan)
  - ATIS (USA)
  - China Communications Standards Association (CCSA)
  - European Telecommunications Standards Institute (ETSI)
  - Telecommunications Technology Association of Korea (TTA)
  - Telecommunication Technology Committee (TTC, Japan)
  - WiMAX Forum
- Any SC6 comments regarding new discoveries of flaws in EAP or RSA should be brought to the immediate attention of the IETF Security Directorate and to the above bodies.