IEEE 802.16e Security Review

IEEE 802.16 Presentation Submission Template (Rev. 8.3)

Document Number:

[IEEE S802.16e-05/373, for example. The document number will match that of the base contribution, with “S” replacing “C”.]

Date Submitted:

[2005-07-18]

Source:

[Bernard Aboba]	Voice:	[425-706-6605]
[Microsoft]	Fax:	[425-936-7936]
[One Microsoft Way]	E-mail:	[bernarda@microsoft.com]
[Redmond, WA]		

Venue:

[IEEE 802 Plenary, San Francisco, CA]

Base Document:

[If this presentation accompanies an 802.16 document, cite the document number (e.g., IEEE C802.16x-02/NNr0) and URL <http://ieee802.org/16/… C80216x-02_NNr0.pdf>.]

Purpose:

[Summary of the IEEE 802.16eD8 Security Review]

Notice:

This document has been prepared to assist IEEE 802.16. It is offered as a basis for discussion and is not binding on the contributing individual(s) or organization(s). The material in this document is subject to change in form and content after further study. The contributor(s) reserve(s) the right to add, amend or withdraw material contained herein.

IEEE 802.16e Security Review

Jeff Mandin, Streetwaves Networks

Yoshihiro Ohba, Toshiba

Bernard Aboba, Microsoft

IEEE 802.16e

Monday, July 18, 2005

http://www.drizzle.com/~aboba/EAP/review.txt

IEEE 802.16e Security Review

- May 5, 2005: Liaison request sent by Roger Marks, Chair of IEEE 802.16 to IETF EAP and MSEC WGs
- Participants
  - Jeff Mandin, IEEE 802.16 liaison to IETF
  - Jari Arkko, Co-Chair, EAP WG
  - Yoshihiro Ohba
  - Gabriel Montenegro
  - Bernard Aboba, IETF liaison to IEEE 802
  - Team from Stanford University
    - Prof. John C. Mitchell
    - Anupam Datta
    - Changhua He
    - Arnab Roy
    - Mukund Sundararajan
- June 6, 2005: Review made public
  - http://www.drizzle.com/~aboba/EAP/review.txt
  - http://www.drizzle.com/~aboba/EAP/802.16eNotes.pdf

Review Format

- Focus: “EAP only” mode
- Components
  - EAP compatibility review: RFC 3748, Section 3.1
  - AAA Key Management requirements review:
    - RFC 4017
    - http://www.ietf.org/internet-drafts/draft-housley-aaa-key-mgmt-00.txt
  - EAP Key Management Framework review
    - http://www.ietf.org/internet-drafts/draft-ietf-eap-keying-07.txt
  - Formal security analysis
    - http://www.drizzle.com/~aboba/EAP/802.16eNotes.pdf

Issues

- Critical
  - Lack of EAP method requirements
  - Man-in-the-middle vulnerability in “Authenticated EAP” mode
- Important
  - Integration with the EAP state machine
  - AAA integration
  - Use of HMAC/CMAC TLV to protect EAP re-authentication
  - Secure confirmation of “security relevant” parameters
  - Key Context
  - Key Installation and Deletion
  - IPv6 compatibility

EAP Method Requirements

- IEEE 802.16e D8 did not specify a mandatory-to-implement EAP method
  - Enables use of MD5-Challenge which does not generate keys and is vulnerable to offline dictionary attack.
- Suggestion
  - At a minimum, IEEE 802.16e should specify the security requirements of methods to be used with it. RFC 4017 is an example of this.

MiTM Vulnerability

- Compound authentication mechanisms are vulnerable to man-in-the-middle attacks unless *cryptographic binding* is used to prove participation in each authentication.
  - http://www.saunalahti.fi/~asokan/research/tunnel.pdf
  - http://www.ietf.org/proceedings/02nov/slides/eap-4/eap-4.ppt
- IEEE 802.16e D8 does *not* violate RFC 3748 Section 2.1 (prohibition on sequences of EAP methods)
  - In RFC 3748, a sequence is a series of EAP authentication mechanisms without intervening EAP Success/Failure

Integration with EAP State Machine

- The EAP state machine defines interface variables that are exchanged between lower-layer and EAP-layer (peer and authenticator). IEEE 802.16e D8 does not describe how these variables interact with the 802.16e state machine.
  - http://www.ietf.org/internet-drafts/draft-ietf-eap-statemachine-06.pdf
- What is the problem?
  - Lack of integration between IEEE 802.1X and EAP state machines resulted in vulnerabilities in IEEE 802.1X-2001
    - For details, see:http://www.cs.umd.edu/~waa/1x.pdf
  - Vulnerabilities fixed in IEEE 802.1X-2004 by integrating IEEE 802.1X and EAP state machines

AAA Integration

- IEEE 802.16e has no equivalent of RFC 3580, “IEEE 802.1X RADIUS Usage Guidelines”
- Are existing AAA attributes sufficient, or are additional attributes needed?
- Suggestion
  - IETF RADEXT WG developing additional attributes for WLAN, IEEE 802
  - IEEE 802.16e can send a liaison request to IETF RADEXT WG describing additional attributes, if needed

Protection of EAP Re-Authentication

- Vulnerabilities
  - Initial EAP messages (Request/Response-Identity) sent in the clear
  - Common EAP methods treat a MIC failure as a fatal error (e.g. all methods based on TLS)
  - Result: potential for DoS attacks
- Suggestion
  - Require HMAC/CMAC TLV for carrying EAP re-authentication messages

Secure Confirmation

- IEEE 802.16e D8 securely confirms the selection of the “best” ciphersuite
- IEEE 802.16e D8 does not securely confirm other parameters such as the MAC algorithm or replay window size
- What can go wrong?
  - MAC algorithm can be compromised, leading to a downgrade attack
  - Replay window size can be manipulated by an attacker leading to a DoS

Key Context

- Definition
  - Key context determines who is authorized to use the key, for what purpose and for how long. Without context binding, key misuse cannot be prevented or even detected.
- From draft-housley-aaa-key-mgmt:
  - "Keying material MUST be bound to the appropriate context… including the scope of key usage and the key lifetime…the protocol MUST ensure that all parties... have the same context for the keying material. This requires that the parties are properly identified and authenticated, so that the key scope can be determined."

Key Context Issues

- No PMK lifetime negotiation between the MS and BS.
  - Long default lifetimes do not solve the problem since the BS may reclaim resources.
- Undefined PMK scope and cache structure.
  - The peer and authenticator may not be identified by their MAC addresses.
  - Cache entries may include more than just keying material (e.g. authorizations).
- Lack of support for Channel Bindings
  - RFC 3748, Section 7.15

Key Installation, Deletion and Naming

- 3-way handshake is not replay protected in one of the HMAC variants
- BS can hold more than one PMK for a given MS
  - Example: EAP re-authentication.
  - Does installation of a new PMK automatically destroy a previous PMK?
- When is PMK context destroyed?
  - On failure of the 3-way handshake?
  - On failure of EAP authentication?
- AK directly derived from the PMK
  - Yet discard of the AK context may not result in discard of the PMK context.
- D7 reference to the Session-ID removed in D8

IPv6

- IEEE 802.16e D8 Section 6.3.9.10
  - IPv6 Stateless Address AutoConfiguration handled via REG_RSP TLV rather than Router Advertisement
  - Mobile IPv6 reference should be updated to RFC 3775
  - Confusion between CoA and dynamic HoA assignment

Feedback?