September 12, 2005

Dr. Roger B. Marks
NIST
325 Broadway, MC 818.00
Boulder, CO 80305 USA
Tel: +1 303 497 7837
mailto: marks at nist.gov

With the assistance of Jeff Mandin, 802.16 liaison to IETF, the EAP WG chairs (Jari Arkko and myself) have reviewed IEEE 802.16e D10, in order to determine whether the security issues found in IEEE 802.16eD8 have been addressed. The results of this review are enclosed below. In most cases, the review comments have addressed, but there are a few issues still remaining.

Sincerely yours,

Bernard Aboba
IETF Liaison to IEEE 802

EAP Compatibility Review

In our review of D8, we suggested that the use of the HMAC/CMAC TLV be required for carrying EAP re-authentication messages. This has been addressed in draft D10 sections 7.1.3.2 and 6.3.2.3.9.16 (including table 37f).

3. "Authenticated EAP" mode

In our review of D8, we pointed out that not requiring the BS to demonstrate possession of PMKs from all EAP authentications enables the man-in-the-middle attack described in [BINDING].

This was rectified using cryptographic binding. Reviewer Yoshihiro Ohba provided assistance in the details of the solution which appears in section 7.2.2.2.2 of draft D10 (with some additional details in 6.3.2.3.9.27, 6.3.2.3.9.28, and figure 130n).

4. EAP Method Requirements

IEEE 802.16e D8 did not specify a mandatory-to-implement EAP method, nor did it specify the required security properties of EAP methods to be used with it. This has been fixed in D10 by requiring methods to conform to the mandatory criteria of RFC 4017, as described in Sections 7.1.3.2 and 7.2.2.2.2.

5. Integration with the EAP State Machine

IEEE 802.16e D8 did not describe how to use the variables defined in

RFC 4137 or how to set appropriate values to the variables within the 802.16e state machine. Vagueness in the interaction of EAP with the lower layer statemachine can be a source of serious security vulnerabilities.

This problem has not been fixed in IEEE 802.16eD10.

We recommend that this issue be addressed in a subsequent revision to IEEE 802.16e.

EAP KEY MANAGEMENT REVIEW
---

6. Secure Ciphersuite Negotiation

IEEE 802.16eD8 securely confirmed selection of the "best" ciphersuite within the 3-way handshake, but it did not securely confirm other "security-relevant" capabilities such as the MAC algorithm or replay window size.

This has been addressed in draft D10 section 7.8.1 (step 6), Section 6.3.2.3.9.19 table 37i, Section 6.3.2.3.9.20 table 37j, Section 6.3.2.3.9.22 table 37l, and Section 6.3.2.3.9.23 table 37m.

7. Key Context

IEEE 802.16e D8 did not ensure that the PMK is bound to its context such as the key lifetime and scope. We recommended that this issue be fixed prior to publication.

In particular:

a. IEEE 802.16eD8 did not negotiate the PMK lifetime between the MS and BS, and as a result, these parties could be out of sync with respect to the expected lifetime.

This issue is addressed in D10. PMK Lifetime parameters are described in Section 6.3.2.3.9.18, Table 37h, as well as table 343.

b. IEEE 802.16eD8 did not define the PMK scope.

Since EAP authenticators may have multiple ports, the scope of the PMK may be larger than is indicated by the authenticator lower layer address. As a result, a mechanism needs to be provided for the peer to learn the scope of the PMK that it shares with the authenticator. This was not defined in IEEE 802.16eD8.

The lack of a well defined PMK scope also implies that IEEE 802.16eD8 did not provide complete support for Channel Bindings, described in [RFC3748] Section 7.15.

Lower layer support for Channel Bindings requires that the lower layer provide the same information to the peer as the authenticator provides to the backend authentication server.

While it is the case that 802.11 systems without channel binding support have been widely deployed, these systems leave the EAP peer vulnerable in situations where the service provider is unscrupulous or where the infrastructure is compromised. Frauds of this type have been documented, for example, within the pay phone industry. For more information on Channel Bindings, see:
http://www.watersprings.org/pub/id/draft-arkko-eap-service-identity-auth-03.txt
http://www.watersprings.org/pub/id/draft-ohba-eap-aaakey-binding-01.txt

This issue is not addressed in D10.

c. IEEE 802.16e D8 did not define the PMK SA in sufficient detail. In order to prevent attacks arising from PMK caching, it is necessary for the PMK SA to include all related authorizations (such as those obtained from AAA). An example PMK SA definition is provided in IEEE 802.11i Section 8.4.1.1.1.

This issue is only partially addressed in D10.

While the text in Section 7.2.2.4.3 indicates that the PMK context includes "all parameters", table 132c omits most of the parameters defined in the EAP Key Management framework or IEEE 802.11i Section 8.4.1.1.1. For example, a PMK SA definition includes the PMK name (e.g. PMKID for IEEE 802.11i), scope of the PMK (e.g. Peer and Authenticator identifiers), Key Lifetime, Authorization parameters, handshake algorithms, etc.

Our recommendation is that table 132c be revised to include a more complete definition of the PMK SA.

8. Key installation and deletion

As part of the PMK cache definition, IEEE 802.16eD8 did not explicitly describe when PMKs are installed and deleted.

This is clarified in draft D10 section 7.2.2.2.11 (additional details in 6.3.2.3.9.20 and 7.8.1)

9. Key Selection and Naming

In Section 7.2.2.2.3 of IEEE 802.16eD8, the AK was directly derived from the PMK (for pure EAP authentication). As a result, the AK and PMK lifetimes were the same. However, IEEE 802.16e D8 did not insist that discard of the AK context result in discard of the PMK context.

This has been addressed in D10. AKId and related parameters are defined

in draft D10 table 132a (AKId is additionally used in table 37h, 37i, 37j).

10. AAA Integration

IEEE 802.16eD8 had no equivalent of RFC 3580 -- a description of AAA attributes to be used with it. In our review, we pointed out that this is likely to result in interoperability problems with backend authentication servers. Our recommendation was that the needed attributes be defined in a RADEXT WG document.

This issue still has not been addressed in D10. However, we understand that this is considered outside the scope of IEEE 802.16e, and may be addressed elsewhere, such as in 802.16g or in other standards organizations.

AAA Key Management Criteria Review

During discussion of IEEE 802.16eD8, it appeared that some participants believed that the specification permitted parties other than the EAP peer or authenticator to access keying material. The lack of a defined PMK scope contributed to this confusion. We recommended that this issue be clarified.

This issue has not been addressed in D10.

In IEEE 802.16eD8, the 3-way handshake was not replay protected in one of the HMAC variants.

This has been addressed in D10. Replay protection was added to short HMAC tuple, as described in Section 11.1.2.3, table 348d.

Via the 802.16e 3-way handshake the BS and MS both demonstrate possession of the PMK (via the AK). However, since 802.16eD8 did not define the PMK key context, it did not ensure the synchronization of the key context between the BS and MS.

This issue has not been addressed in D10.

Since the independence of TEKs from each other depends on the quality of the MS random number generator, we recommended that text be added be emphasizing the importance of a high quality random number generator.

This issue has not been addressed in D10.

NITS

The editorial issues pointed out in the review of IEEE 802.16eD8 have been addressed in D10. For example, the term "AAA-Key" was replaced with "MSK" as suggested and the suggested changes to Section 7.1.3.2 were adopted.

IPv6 Address Assignment issues

IEEE 802.16e D8 Section 6.3.9.10 has made some incorrect assumptions about how IPv6 address assignment works and we recommended that this section should be revised or deprecated.

IEEE 802.16e D8 Section 6.3.9.10 states:

"For an MS, if mobile IP is being used, the MS may secure it's address on the secondary management connection using Mobile IP."

Since Mobile IP does not provide for CoA assignment, we assume that this is referring to dynamic HoA assignment. Please clarify.

"For MS using IPv6 the MS shall either invoke DHCPv6 [IETF RFC 3315] or IPv6 Stateless Address Autoconfiguration [IETF RFC 2462] based on the value of a TLV tuple in REG_RSP."

In IPv6, this determination is made based on contents of the Router Advertisement, not within the lower layer. Doing the assignment in the lower layer may result in issues with DNAv6 and SEND.

These problems have not been fixed in IEEE 802.16eD10.

New NITS

The following text from 7.2.2.2.2 is confusing (and ungrammatical):

"The product of the EAP exchange which is transferred to 802.16 layer is the MSK. This key is derived (or may be equivalent to the 512-bits Master Session Key (MSK)."

Suggest changing this to:

"The product of the EAP exchange which is transferred to the 802.16 layer is the Master Session Key (MSK), which as described in RFC 3748 is a minimum of 512-bits in length."

Section 6.3.2.3.9.15

The words "for EAP methods deriving keys" appears redundant, since the mandatory criteria of RFC 4017 include key derivation. Therefore all EAP methods used with IEEE 802.16e should support key derivation. We recommend that this be deleted.