802.16e Notes - Mitchell Group

Anupam Datta Changhua He John C. Mitchell Arnab Roy Mukund Sundararajan
Electrical Engineering and Computer Science Departments
Stanford University
Stanford, CA 94305-9045

June 6, 2005

In this document we discuss some issues regarding 802.16e Key Management. We were careful not to repeat issues mentioned in the EAP-WG review. Section 1 identifies the security guarantees that the PKMv2 3-Way SA-TEK Handshake seems to provide and compares it to two similar protocols: ISO three-pass mutual authentication protocol and the 802.11i 4-Way Handshake. It also discusses the state machines described on pages 230-232 of [1] and the possibility of DOS vulnerabilities. Section 2 discusses issues related to the RSA Authentication Protocol. We also identify lack of information in various sections of the draft.

1 3-Way Handshake

The basic purpose of the 3-Way Handshake is the distribution of keying parameters related to all Security Associations (SAs) active between a Mobile Station(MS) and the Base Station(BS). The 3-Way Handshake is executed after the initial Authentication Stage or on Handover. It relies on the shared-secret (Authorization Key) established by the Authentication Stage, which may be implemented as either the PKMv2 RSA Authentication protocol or EAP or a combination of the two. We assume that the Authentication Stage results in mutual authentication of peers and the establishment of a shared secret. The message-arrows description of the 3-Way Protocol is listed in Figure 1. Though it does not appear explicitly in the messages, any TEK keys distributed in the *SAUpdate* are encrypted under the KEK derived from the AK. Also note that all the Message integrity checks are replay protected.

1.1 Security Properties

Under the following *assumptions*:

$$
\begin{array}{lcl}
BS \rightarrow MS & : & BSNonce, AKID, MIC[AK](BSNonce, AKID) \\
MS \rightarrow BS & : & BSNonce, MSNonce, AKID, MSSuite, MIC[AK](MSNonce, BSNonce, AKID, MSSuite) \\
BS \rightarrow MS & : & SAUpdate, BSNonce, MSNonce, AKID, MIC[AK](SAUpdate, MSNonce, BSNonce, AKID)
\end{array}
$$

Figure 1: Arrows and Messages: 802.16e 3-Way Handshake

$$
\begin{array}{lcl}
B \rightarrow A & : & \text{Rb}, Text1 \\
A \rightarrow B & : & \text{Ra}, Text3, \text{f[Kab](Ra,Rb}, B, Text2) \\
B \rightarrow A & : & Text5, \text{f[Kab](Ra,Rb}, Text4)
\end{array}
$$

Figure 2: ISO Three-Pass Mutual Authentication with Cryptographic Check function: f

$$
\begin{array}{lcl}
Authenticator \rightarrow Supplicant & : & \text{ANonce, ``}msg1'' \\
Supplicant \rightarrow Authenticator & : & \text{SNonce, ``}msg2'', \text{MIC[PTK]}(SNonce, \text{``}msg2'') \\
Authenticator \rightarrow Supplicant & : & \text{``}msg4'', \text{MIC[PTK]}(\text{``}msg4'')
\end{array}
$$

Figure 3: Simplified 802.11i 4-Way Handshake

1. The Authentication Stage guarantees that AK is shared between a MS-BS pair. The mutual authentication provided by the 3-Way Handshake relies on this fact.
2. A single principal does not play the roles of both MS and BS simulataneously, or there is an easy reflection attack.

the 3-Way Handshake should provide the following *security guarantees*:

1. Full mutual authentication.
2. Message 2 indicates to the BS that the MS is alive and that the MS possesses the AK.
3. Message 3 indicates to the MS that the BS is alive.
4. MS is guaranteed that SAUpdate is sent by the BS and is fresh (has been sent by the BS after MS generated and sent Message2).
5. Any TEKs distributed in this stage are secret. This is a consequence of encryption of such keys by the AK.

1.2 A three-way Comparison

First, we compare the 3-Way Handshake to the an ISO three pass protocol [3] known to provide mutual authentication. Figure 2 describes the protocol. Note that the 3-Way Handshake 1 is a refinement of the ISO three pass mutual authentication protocol, with two significant differences. Firstly, the first message of the 3-Way Handshake contains a MAC and secondly, identities are missing the MAC of the 3-Way Handshake. The addition of the MAC in the first message does not cause any vulnerabilities as the MAC's cannot be confused for one another. Though the shared key identifies the pair of principals involved, identities need to be included to differentiate the peers - as in message 2 of the ISO protocol. Though this is missing in 802.16e, the assumption that a principal does not play the role of both the MS and the BS allows peer identification. This obviates a reflection attack.

We now compare the 3-Way Handshake with the 802.11i 4-Way Handshake [4]. The 4-Way Handshake is a key-refresh protocol while the 3-Way Handshake is a key distribution protocol. The key used in the 4-Way handshake message integrity check is derived using the nonces exchanged in the protocol, this causes

the first message not to have a MAC leading to a DOS vulnerability [5]. This is absent in the 3-Way Handshake as the MAC is based on a shared secret AK established by the previous stage, the nonces do not participate in key derivation. It may be possible without too much additional computational complexity, to allow the AK to be refreshed by the 3-Way Handshake using the nonces exchanged. This may be a more efficient (but less secure ?) way of refreshing the AK. The first message could be MACed using the older AK. The 4-way handshake limits the use of the key obtained from EAP stage (PMK) by deriving a new key. The 3-way handshake does not attempt to do that. Since the 3-Way Handshake does not execute at a significantly higher frequency than the authentication stage, this seems fine.

1.3 State machine and Denial of Service

Since we found DOS vulnerabilities in 802.11i [5], we checked if similar ones recurred here. We assume that the attacker cannot cause the packet of a legitimate principal to be dropped, though the attacker can record, replay and insert messages. All the messages involved have authenticators and a message with a bad authenticator is ignored by the BS and the MS, also all the messages are replay protected. So the attacker cannot modify state at the MS or the BS without possessing the AK. Connections are dropped by a principal when it has retried sending a message a certain number of times without response from the peer. Since an attacker cannot delete messages from the channel, a connection drop would seem to imply that the peer is not alive or the channel is not available for an extended period of time.
Missing Information: The interaction of the SA-TEK state machine with the TEK state machines is missing. The TEK machine on the MS side is missing. The interaction of the SA-TEK state machine with the EAP / RSA Authentication state machines is missing. These interactions are critical to analyze DOS vulnerabilities.

2 PKM-RSA authentication

RSA Authentication Acknowledgement: The PKMv1, PKMv2 RSA Authentication Protocols are listed in Figures 4, 5 resepctively. The final message in Figure 4- PKMv2 RSA Acknowledgement Message (the third message) seems to fix a potential weakness in PKMv1. Without this message, an attacker could replay the first message from an earlier session, and create state on the BS. The BS would then attempt a three-way handshake. After sending the SA-Challenge SAChallengeMaxResends times, it would finally drop the connection. The attacker would require MAC spoofing, which we assume is possible. The MS demonstrates to the BS that it is alive via the RSA Acknowledgement message.
Missing Information: Though the RSA Acknowledgement message is listed in the Section 6.3.2.3.9.14, there is no mention of its usage in Section 7.8.2. The state machines for the PKMv2 RSA Authentication are missing. The addition of new messages would cause the MS state machine to differ from the one listed in the 2004 Draft [2] -Section 7.2.4. The BS side Authorization state machine is missing from all drafts for both PKmv1 and PKMv2. The actions taken by the BS on AK expiration need to be listed.
Hot Lists: There is a ‘hot-list’ mentioned in the 2004 Draft [2] - Section 11.9.10 related to the Permanent Reject message. This is not mentioned in the new drafts. When is an M.S. put onto a BS’s hot-list? Is it possible for an attacker to put a legitimate MS on this list? This would result in DOS.

$MS \rightarrow BS$: $ManufacturerCert, MSRandom, MSCert, SIG[MS](message)$
$BS \rightarrow MS$: $BSRandom, MSRandom, AKSeqNo, AKLifetime, ENC[MS](AK), BSCert, SIG[BS](message)$

Figure 4: PKMv1 RSA Authentication

$MS \rightarrow BS$: $ManufacturerCert, MSRandom, MSCert, SIG[MS](message)$
$BS \rightarrow MS$: $BSRandom, MSRandom, AKSeqNo, AKLifetime, ENC[MS]AK, BSCert, SIG[BS](message)$
$MS \rightarrow BS$: $MSRandom, BSRandom, SIG[MS](message)$

Figure 5: PKMv2 RSA Authentication

References

[1] **P802.16e/D8**
Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems: Amendment for Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands

[2] **P802.16-2004**
Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems

[3] **Information Technology- Security Techniques - Entity Authentication Mechanisms Part 4**
Entity Authentication using Cryptographic Check Functions, 1993.

[4] **IEEE P802.11i/D10.0**
MAC security enhancements, amendment 6 to IEEE local and metropolitan area networks part 11.

[5] **Analysis of 802.11i 4-way Handshake**
Changhua He and John Mitchell.
In proceedings of the Third ACM workshop on Wireless security.