Network Working Group
Request for Comments: 4017
Category: Informational

D. Stanley
Agere Systems
J. Walker
Intel Corporation
B. Aboba
Microsoft Corporation

March 2005

Extensible Authentication Protocol (EAP) Method Requirements for Wireless LANs

Status of this Memo

Copyright Notice

Abstract

The IEEE 802.11i MAC Security Enhancements Amendment makes use of IEEE 802.1X, which in turn relies on the Extensible Authentication Protocol (EAP). This document defines requirements for EAP methods used in IEEE 802.11 wireless LAN deployments. The material in this document has been approved by IEEE 802.11 and is being presented as an IETF RFC for informational purposes.

Table of Contents

1. Introduction

The IEEE 802.11i MAC Security Enhancements Amendment [IEEE802.11i] makes use of IEEE 802.1X [IEEE802.1X], which in turn relies on the Extensible Authentication Protocol (EAP), defined in [RFC3748].

Today, deployments of IEEE 802.11 wireless LANs are based on EAP and use several EAP methods, including EAP-TLS [RFC2716], EAP-TTLS [TTLS], PEAP [PEAP], and EAP-SIM [EAPSIM]. These methods support authentication credentials that include digital certificates, user-names and passwords, secure tokens, and SIM secrets.

This document defines requirements for EAP methods used in IEEE 802.11 wireless LAN deployments. EAP methods claiming conformance to the IEEE 802.11 EAP method requirements for wireless LANs must complete IETF last call review.

1.1. Requirements Specification

In this document, several words are used to signify the requirements of the specification. The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

An EAP authentication method is not compliant with this specification if it fails to satisfy one or more of the MUST or MUST NOT requirements. An EAP authentication method that satisfies all the MUST, MUST NOT, SHOULD, and SHOULD NOT requirements is said to be "unconditionally compliant"; one that satisfies all the MUST and MUST NOT requirements but not all the SHOULD or SHOULD NOT requirements is said to be "conditionally compliant".

1.2. Terminology

authenticator
The end of the link initiating EAP authentication. The term authenticator is used in [IEEE802.1X], and authenticator has the same meaning in this document.

peer
The end of the link that responds to the authenticator. In [IEEE802.1X], this end is known as the supplicant.

Supplicant
The end of the link that responds to the authenticator in [IEEE802.1X].

backend authentication server
A backend authentication server is an entity that provides an authentication service to an authenticator. When used, this server typically executes EAP methods for the authenticator. This terminology is also used in [IEEE802.1X].

EAP server
The entity that terminates the EAP authentication method with the peer. In the case where no backend authentication server is used, the EAP server is part of the authenticator. In the case where the authenticator operates in pass-through mode, the EAP server is located on the backend authentication server.

Master Session Key (MSK)
Keying material that is derived between the EAP peer and server and exported by the EAP method. The MSK is at least 64 octets in length. In existing implementations, an AAA server acting as an EAP server transports the MSK to the authenticator.

Extended Master Session Key (EMSK)
Additional keying material derived between the EAP client and server that is exported by the EAP method. The EMSK is at least 64 octets in length. The EMSK is not shared with the authenticator or any other third party. The EMSK is reserved for future uses that are not yet defined.

4-Way Handshake
A pairwise Authentication and Key Management Protocol (AKMP) defined in [IEEE802.11i], which confirms mutual possession of a Pairwise Master Key by two parties and distributes a Group Key.

2. Method Requirements

2.1. Credential Types

The IEEE 802.11i MAC Security Enhancements Amendment requires that EAP authentication methods be available. Wireless LAN deployments are expected to use different credential types, including digital certificates, user-names and passwords, existing secure tokens, and mobile network credentials (GSM and UMTS secrets). Other credential types that may be used include public/private key (without necessarily requiring certificates) and asymmetric credential support (such as password on one side, public/private key on the other).

2.2. Mandatory Requirements

EAP authentication methods suitable for use in wireless LAN authentication MUST satisfy the following criteria:

[1] Generation of symmetric keying material. This corresponds to the "Key derivation" security claim defined in [RFC3748], Section 7.2.1.

[2] Key strength. An EAP method suitable for use with IEEE 802.11 MUST be capable of generating keying material with 128-bits of effective key strength, as defined in [RFC3748], Section 7.2.1. As noted in [RFC3748], Section 7.10, an EAP method supporting key derivation MUST export a Master Session Key (MSK) of at least 64 octets, and an Extended Master Session Key (EMSK) of at least 64 octets.

[3] Mutual authentication support. This corresponds to the "Mutual authentication" security claim defined in [RFC3748], Section 7.2.1.

[4] Shared state equivalence. The shared EAP method state of the EAP peer and server must be equivalent when the EAP method is successfully completed on both sides. This includes the internal state of the authentication protocol but not the state external to the EAP method, such as the negotiation occurring prior to initiation of the EAP method. The exact state attributes that are shared may vary from method to method, but typically include the method version number, the credentials presented and accepted by both parties, the cryptographic keys shared, and the EAP method specific attributes negotiated, such as ciphersuites and limitations of usage on all protocol state. Both parties must be able to distinguish this instance of the protocol from all other instances of the protocol, and they must share the same view regarding which state attributes are public and which are private to the two parties alone. The server must obtain the authenticated peer name, and the peer must obtain the authenticated server name (if the authenticated server name is available).

[5] Resistance to dictionary attacks. This corresponds to the "Dictionary attack resistance" security claim defined in [RFC3748], Section 7.2.1.

[6] Protection against man-in-the-middle attacks. This corresponds to the "Cryptographic binding", "Integrity protection", "Replay protection", and "Session independence" security claims defined in [RFC3748], Section 7.2.1.

[7] Protected ciphersuite negotiation. If the method negotiates the ciphersuite used to protect the EAP conversation, then it MUST support the "Protected ciphersuite negotiation" security claim defined in [RFC3748], Section 7.2.1.

2.3. Recommended Requirements

EAP authentication methods used for wireless LAN authentication SHOULD support the following features:

[8] Fragmentation. This implies support for the "Fragmentation" claim defined in [RFC3748], Section 7.2.1. [RFC3748], Section 3.1 states: "EAP methods can assume a minimum EAP MTU of 1020 octets, in the absence of other information. EAP methods SHOULD include support for fragmentation and reassembly if their payloads can be larger than this minimum EAP MTU."

[9] End-user identity hiding. This corresponds to the "Confidentiality" security claim defined in [RFC3748], Section 7.2.1.

2.4. Optional Features

EAP authentication methods used for wireless LAN authentication MAY support the following features:

[10] Channel binding. This corresponds to the "Channel binding" security claim defined in [RFC3748], Section 7.2.1.

[11] Fast reconnect. This corresponds to the "Fast reconnect" security claim defined in [RFC3748], Section 7.2.1.

2.5. Non-compliant EAP Authentication Methods

EAP-MD5-Challenge (the current mandatory-to-implement EAP authentication method), is defined in [RFC3748], Section 5.4. As defined in [RFC3748], EAP-MD5-Challenge, One-Time Password (Section 5.5), and Generic Token Card (Section 5.6) are non-compliant with the requirements specified in this document. As noted in [RFC3748], these methods do not support any of the mandatory requirements defined in Section 2.2, including key derivation and mutual authentication. In addition, these methods do not support any of the recommended features defined in Section 2.3 or any of the optional features defined in Section 2.4.

3. Security Considerations

Within [IEEE802.11i], EAP is used for both authentication and key exchange between the EAP peer and server. Given that wireless local area networks provide ready access to an attacker within range, EAP usage within [IEEE802.11i] is subject to the threats outlined in [RFC3748], Section 7.1. Security considerations relating to EAP are discussed in [RFC3748], Sections 7; where an authentication server is utilized, the security considerations described in [RFC3579], Section 4, will apply.

The system security properties required to address the threats described in [RFC3748], Section 7.1, are noted in [Housley56]. In the material below, the requirements articulated in [Housley56] are listed, along with the corresponding recommendations.

Algorithm independence
: Requirement: "Wherever cryptographic algorithms are chosen, the algorithms must be negotiable, in order to provide resilience against compromise of a particular cryptographic algorithm."

  This issue is addressed by mandatory requirement [7] in Section 2.2. Algorithm independence is one of the EAP invariants described in [KEYFRAME].

Strong, fresh session keys
: Requirement: "Session keys must be demonstrated to be strong and fresh in all circumstances, while at the same time retaining algorithm independence."

  Key strength is addressed by mandatory requirement [2] in Section 2.2. Recommendations for ensuring the Freshness of keys derived by EAP methods are discussed in [RFC3748], Section 7.10.

Replay protection
: Requirement: "All protocol exchanges must be replay protected."

  This is addressed by mandatory requirement [6] in Section 2.2.

Authentication
: Requirements: "All parties need to be authenticated. The confidentiality of the authenticator must be maintained. No plaintext passwords are allowed."

Mutual authentication is required as part of mandatory requirement [3] in Section 2.2. Identity protection is a recommended capability, described in requirement [9] in Section 2.3. EAP does not support plaintext passwords, as noted in [RFC3748], Section 7.14.

Authorization
Requirement: "EAP peer and authenticator authorization must be performed."

Authorization issues are discussed in [RFC3748], Sections 1.2 and 7.16. Authentication, Authorization, and Accounting (AAA) protocols such as RADIUS [RFC2865][RFC3579] may be used to enable authorization of EAP peers by a central authority. AAA authorization issues are discussed in [RFC3579], Sections 2.6.3 and 4.3.7.

Session keys
Requirement: "Confidentiality of session keys must be maintained."

Issues relating to Key Derivation are described in [RFC3748], Section 7.10, as well as in [KEYFRAME].

Ciphersuite negotiation
Requirement: "The selection of the "best" ciphersuite must be securely confirmed."

This is addressed in mandatory requirement [7] in Section 2.2.

Unique naming
Requirement: "Session keys must be uniquely named."

Key naming issues are addressed in [KEYFRAME].

Domino effect
Requirement: "Compromise of a single authenticator cannot compromise any other part of the system, including session keys and long-term secrets."

This issue is addressed by mandatory requirement [6] in Section 2.2.

Key binding
Requirement: "The key must be bound to the appropriate context."

This issue is addressed in optional requirement [10] in Section 2.4. Channel binding is also discussed in Section 7.15 of [RFC3748] and Section 4.3.7 of [RFC3579].

4. References

4.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2865] Rigney, C., Willens, S., Rubens, A., and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)", RFC 2865, June 2000.

[RFC3579] Aboba, B. and P. Calhoun, "RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP)", RFC 3579, September 2003.

[RFC3748] Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., and H. Levkowetz, "Extensible Authentication Protocol (EAP)", RFC 3748, June 2004.

[802.11] Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, IEEE Std. 802.11-2003, 2003.

[IEEE802.1X] IEEE Standards for Local and Metropolitan Area Networks: Port based Network Access Control, IEEE Std 802.1X-2004, December 2004.

[IEEE802.11i] Institute of Electrical and Electronics Engineers, "Supplement to Standard for Telecommunications and Information Exchange Between Systems - LAN/MAN Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Specification for Enhanced Security", IEEE 802.11i, July 2004.

4.2. Informative References

[Housley56] Housley, R., "Key Management in AAA", Presentation to the AAA WG at IETF 56, http://www.ietf.org/proceedings/03mar/slides/aaa-5/index.html, March 2003.

[RFC2716] Aboba, B. and D. Simon, "PPP EAP TLS Authentication Protocol", RFC 2716, October 1999.

[PEAP] Palekar, A., et al., "Protected EAP Protocol (PEAP)", Work in Progress, July 2004.

[TTLS] Funk, P. and S. Blake-Wilson, "EAP Tunneled TLS Authentication Protocol (EAP-TTLS)", Work in Progress, August 2004.

[EAPSIM] Haverinen, H. and J. Salowey, "EAP SIM Authentication", Work in Progress, April 2004.

[KEYFRAME] Aboba, B., et al., "EAP Key Management Framework", Work in Progress, July 2004.

Acknowledgements

The authors would like to acknowledge contributions to this document from members of the IEEE 802.11i Task Group, including Russ Housley of Vigil Security, David Nelson of Enterasys Networks and Clint Chaplin of Symbol Technologies, as well as members of the EAP WG including Joe Salowey of Cisco Systems, Pasi Eronen of Nokia, Jari Arkko of Ericsson, and Florent Bersani of France Telecom.

Authors' Addresses

Dorothy Stanley
Agere Systems
2000 North Naperville Rd.
Naperville, IL 60566

Phone: +1 630 979 1572
EMail: dstanley@agere.com

Jesse R. Walker
Intel Corporation
2111 N.E. 25th Avenue
Hillsboro, OR 97214

EMail: jesse.walker@intel.com

Bernard Aboba
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052

Phone: +1 425 818 4011
Fax: +1 425 936 7329
EMail: bernarda@microsoft.com

Full Copyright Statement

Intellectual Property

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.