

Network Working Group
INTERNET-DRAFT
Category: Best Current Practice
<[draft-walker-ieee802-req-01.txt](#)>
[11](#) May 2004

Dorothy Stanley
Agere
Jesse Walker
Intel Corporation
Bernard Aboba
Microsoft Corporation

EAP Method Requirements for Wireless LANs

This document is an Internet-Draft and is in full conformance with all provisions of [Section 10 of RFC 2026](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/lid-abstracts.txt>

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

Copyright Notice

Copyright (C) The Internet Society (2004). All Rights Reserved.

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 it is being presented as an IETF RFC for informational purposes.

INTERNET-DRAFT

EAP Method Reqs. for WLAN

11 May 2004

1. Introduction

The IEEE 802.11i MAC Security Enhancements Amendment [[IEEE802.11i](#)] makes use of IEEE 802.1X [[IEEE8021X-REV](#)] which in turn relies on the Extensible Authentication Protocol (EAP), defined in [[RFC3748](#)].

Deployments of IEEE 802.11 wireless LANs today are based on EAP, and use several EAP methods, including EAP-TLS [[RFC2716](#)], EAP-TTLS [[TTLS](#)], PEAP [[PEAP](#)] and EAP-SIM [[SIM](#)]. 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 wireless LAN requirements for EAP methods 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 [IEEE-802.1X], and authenticator has the same meaning in this document.

peer The end of the link that responds to the authenticator. In [IEEE-802.1X], this end is known as the Supplicant.

Supplicant

The end of the link that responds to the authenticator in [IEEE-802.1X].

Stanley, et al.

Best Current Practice

[Page 2]

INTERNET-DRAFT

EAP Method Reqs. for WLAN

11 May 2004

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 [IEEE-802.1X].

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 a 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 defined yet.

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 are available. Wireless LAN deployments are expected to use different credentials 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] Synchronization of state. This requirement applies when the EAP method completes successfully. The exact state attributes that are shared may vary from method to method but typically include the protocol both executed, what credentials were presented and accepted by both parties, what cryptographic keys are shared and what EAP method specific attributes were negotiated, such as cipher suites 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 of which state attributes are public and which are

private to the two parties alone.

- [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. [\[RFC3748\]](#) [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." This implies support for the "Fragmentation" claim defined in [\[RFC3748\]](#), [Section 7.2.1](#).
- [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](#). EAP-MD5-Challenge, One-Time Password ([Section 5.5](#)) and Generic Token Card ([Section 5.6](#)), as defined in [\[RFC3748\]](#) 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, or 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 [\[Housley56\]](#):

Algorithm independence

Wherever cryptographic algorithms are chosen, the algorithms must be negotiable, in order to provide resilience against compromise of a particular cryptographic algorithm. This 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

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

All protocol exchanges must be replay protected. This is addressed by mandatory requirement [6] in [Section 2.2](#).

Authentication

All parties need to be authenticated. Mutual authentication is required as part of mandatory requirement [3] in [Section 2.2](#). The confidentiality of the authenticator must be maintained. Identity protection is a recommended capability, described in requirement [9] in [Section 2.3](#). No plaintext passwords are allowed. EAP does not support plaintext passwords, as noted in [\[RFC3748\]](#) [Section 7.14](#).

Authorization

EAP peer and authenticator authorization must be performed. Issues relating to authorization are discussed in [\[RFC3748\]](#) [Section 7.15](#), and [\[RFC3579\]](#) [Section 4.3.7](#).

Session keys

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

The selection of the "best" ciphersuite must be securely confirmed. This is addressed in mandatory requirement [7] in [Section 2.2](#).

Unique naming

Session keys must be uniquely named. Key naming issues are addressed in [\[KEYFRAME\]](#).

Domino effect

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

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 \[RFC3748\]](#).

[4.](#) References

[4.1.](#) Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [RFC 2119](#), March, 1997.
- [RFC3748] Blunk, L. , et al., "Extensible Authentication Protocol (EAP)", [RFC 3748](#), May 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. 802.11-1999, 1999.
- [IEEE8021X-REV] IEEE Standards for Local and Metropolitan Area Networks: Port based Network Access Control, IEEE Std 802.1X-REV, Draft 9, March 2004.
- [IEEE802.11i] Institute of Electrical and Electronics Engineers, "Unapproved Draft 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 Draft 802.11i (work in progress), 2003.

[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.

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

[PEAP] Palekar, A., et al., "Protected EAP Protocol (PEAP)", [draft-josefsson-pppext-eap-tls-eap-08.txt](#), Internet draft (work in progress), May 2004.

[TTLS] Funk, P. and S. Blake-Wilson, "EAP Tunneled TLS Authentication Protocol (EAP-TTLS)", [draft-ietf-pppext-eap-ttls-03.txt](#), August 2003.

[EAPSIM] Haverinen, H. and J. Salowey, "EAP SIM Authentication", [draft-haverinen-pppext-eap-sim-12.txt](#), Internet draft (work in progress), October 2003.

[IEEE802] IEEE Standards for Local and Metropolitan Area Networks: Overview and Architecture, ANSI/IEEE Std 802, 1990.

[KEYFRAME]

Aboba, B., "EAP Key Management Framework", [draft-ietf-eap-keying-02](#) (work in progress), May 2004.

Acknowledgments

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

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

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

EMail: bernarda@microsoft.com
Phone: +1 425 706 6605
Fax: +1 425 936 7329

Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on the IETF's procedures with respect to rights in standards-track and standards-related documentation can be found in [BCP-11](#). Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementors or users of this specification can be obtained from the IETF Secretariat.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights which may cover technology that may be required to practice this standard. Please address the information to the IETF Executive Director.

Full Copyright Statement

Copyright (C) The Internet Society (2004). All Rights Reserved.

This document and translations of it may be copied and furnished to

others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English. The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns. This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Open issues

Open issues relating to this specification are tracked on the following web site:

<http://www.drizzle.com/~aboba/EAP/eapissues.html>

Expiration Date

This memo is filed as <[draft-walker-ieee802-req-01.txt](#)>, and expires November 22, 2004.

