Network Working Group
Internet-Draft
Expires: August 11, 2005

P. Eronen
H. Haverinen
Nokia
J. Arkko
Ericsson
J. Salowey
Cisco Systems

February 10, 2005

Evaluation of Cellular Extensible Authentication Protocol (EAP) Methods agaist IEEE 802.11 requirements draft-eronen-eap-sim-aka-80211-00.txt

IESG Note

IESG note goes here.

Abstract

This document evaluates two Extensible Authentication Protocol (EAP) methods, EAP-AKA and EAP-SIM, against the EAP method requirements for Wireless LANs given in [802.11 REQ].

Table of Contents

1. Introduction

The Extensible Authentication Protocol (EAP) allows different authentication protocols to be encapsulated as EAP methods. EAP is specified in [RFC3748]. EAP-AKA ([EAP-AKA]) is an EAP method based on the Authentication and Key Agreement (AKA) mechanisms that are used in 3rd generation mobile network standards Universal Mobile Telecommunications System (UMTS) and cdma2000. EAP-SIM ([EAP-SIM]) is an EAP method based on the GSM Subscriber Identity Modules (SIM). GSM is a 2nd generation mobile network standard.

The IEEE 802.11i MAC Security Enhancements Amendment specifies security enhancements for IEEE 802.11 wireless LANs. The Extensible Authentication Protocol is used in IEEE 802.11i, and [802.11 REQ] specifies the EAP method requirements for IEEE 802.11 wireless LANs.

This document evaluates EAP-SIM and EAP-AKA against the requirements given in [802.11 REQ].

2. Terms

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].

The terms and abbreviations "EAP server", "EAP peer", "Master Session Key (MSK)", "Extended Master Session Key (EMSK)", and the terminology for security claims in this document are to be interpreted as described in [RFC3748].

3. Evaluation

This section goes through the EAP method requirements given in [802.11 REQ] and discusses the support for each feature in EAP-AKA and EAP-SIM.

Many requirements in [802.11 REQ] refer to the security claims defined in [RFC3748]. For EAP-AKA, the support for these claims is stated and justified in Sections 11 and 12 of [EAP-AKA]. For EAP-SIM, the support for the claims is stated and justified in Sections 11 and 12 of [EAP-SIM].

3.1 Mandatory Requirements

[802.11 REQ] lists the features discussed in this section as mandatory requirements, which MUST be supported by EAP methods suitable for use in wireless LAN authentication.

3.1.1 Generation of Symmetric Keying Material

This requirement corresponds to the to the "Key derivation" security claim defined in [RFC3748], Section 7.2.1, which is supported by EAP-AKA and EAP-SIM.

3.1.2 Key Strength

This requirement of [802.11 REQ] requires that the EAP method must be capable of generating keying material with 128 bits of effective key strength. EAP-AKA and EAP-SIM are both capable of this, so they satisfy this requirement. For EAP-AKA, please see section 11.4 of [EAP-AKA], and for EAP-SIM, see Section 11.5 of [EAP-SIM].

3.1.3 Mutual Authentication Support

This requirement corresponds to the to the "mutual authentication" security claim defined in [RFC3748], Section 7.2.1, which is supported by EAP-AKA and EAP-SIM.

3.1.4 Shared State Equivalence

This requirement states that "the shared EAP method state of the EAP peer and server must be equivalent when the EAP method completes successfully on both sides", and also that "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." EAP-AKA and EAP-SIM satisfy this requirement.

The shared state attributes, and whether each attribute is public or private to the EAP peer and server, are summarized below.

When EAP-SIM full authentication completes successfully on both sides, the EAP peer and EAP server share the following state information:

- the fact that the exchange was an EAP-SIM full authentication; public
- the last peer identity communicated in the protocol (and thereby selected for use); public
- the ordered list of server's proposed EAP-SIM version numbers; public
- the EAP-SIM version selected by the peer; public
- peer's NONCE_MT parameter; public
- the number of GSM authentication triplets used in the exchange, 2 or 3; public

- the triplets (RAND, SRES, Kc) used in the exchange; RAND is public, SRES and Kc are private in this protocol
- a new pseudonym username, if sent by the server, and if the peer supports identity privacy. If the peer does not support identity privacy, then the peer ignores this information from the exchange; private until the first full authentication exchange where the peer uses it.
- a re-authentication identity, if sent by the peer and if the peer supports fast re-authentication. If the peer does not support fast re-authentication then the peer ignores this information from the exchange; private until the next re-authentication exchange
- Master Key; private
- Master Session Key; public to parties to which the server sends the key
- Extended Master Session Key; private
- whether protected result indications were used; public

The EAP-SIM full authentication exchange can be distinguished from other instances by 1) RAND challenges, and 2) NONCE_MT parameter.

When EAP-AKA full authentication completes successfully on both sides, the EAP peer and EAP server share the following state information:

- the fact that the exchange was an EAP-AKA full authentication
- the last peer identity communicated in the protocol (and thereby selected for use); public
- the 3G AKA authentication vector used in the exchange (RAND, AUTN, RES, CK, IK); RAND, AUTN, RES are public, CK and IK are private
- a new pseudonym username, if sent by the server, and if the peer supports identity privacy. If the peer does not support identity privacy, then the peer ignores this information from the exchange; private until the first full authentication exchange where the peer uses it.
- a re-authentication identity, if sent by the peer and if the peer supports fast re-authentication. If the peer does not support fast re-authentication then the peer ignores this information from the exchange; private until the next re-authentication exchange
- Master Key; private
- Master Session Key; public to parties to which the server sends the key
- Extended Master Session Key; private
- whether protected result indications were used; public

The EAP-AKA full authentication exchange can be distinguished from other instances by 1) RAND, and 2) AUTN (or actually the 3G AKA sequence number that is contained within the AUTN).

When an EAP-AKA or EAP-SIM fast re-authentication exchange completes successfully on both sides, the EAP peer and the EAP server share the following state information:

- the EAP method used (EAP-AKA or EAP-SIM), which is the same method as in full authentication; public
- the fact that the exchange was a fast re-authentication; public
- the preceding instance of full authentication, and the Master Key derived upon the full authentication exchange; private
- the re-authentication identity used; public
- server's NONCE_S; private
- the value of the counter; private (observers may be able to guess the value of the counter by counting the number of re-authentication exchanges)
- a new re-authentication identity, if sent by the server. The peer may ignore this information if the peer does not want to run fast re-authentication again; private until the next re-authentication exchange
- Master Session Key; public to parties to which the server sends the key
- Extended Master Session Key; private
- whether protected result indications were used; public

The fast re-authentication exchange can be distinguished from other instances by 1) the full authentication exchange instance 2) the value of the counter.

3.1.5 Resistance to Dictionary Attacks

This requirement corresponds to the to the "dictionary attack resistance" security claim defined in [RFC3748], Section 7.2.1. This claim is only applicable to password or passphrase based protocols, so it is not applicable to EAP-AKA or EAP-SIM that are based on strong 128-bit shared keys.

3.1.6 Protection against Man-in-the-Middle Attacks

According to [802.11 REQ], this requirement corresponds to the "Cryptographic binding", "Integrity protection", "Replay protection", and "Session independence" security claims defined in [RFC3748], Section 7.2.1.

The "Cryptographic binding" security claim is only applicable to tunnel methods which are capable of encapsulating another EAP method within a protected tunnel. Since EAP-AKA and EAP-SIM are not tunnel methods, this claim is not applicable to EAP-AKA or EAP-SIM. A tunnel method that supports cryptographic binding can encapsulate and bind to EAP-AKA or EAP-SIM, because EAP-AKA and EAP-SIM support key

derivation, which is needed in order for the binding to work.

EAP-AKA and EAP-SIM satisfy the security claims "Integrity protection", "Replay protection" and "Session independence".

3.1.7 Protected Ciphersuite Negotiation

[802.11 REQ] requires that "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." Since EAP-AKA and EAP-SIM do not negotiate the ciphersuite, this requirement is not applicable to EAP-AKA and EAP-SIM.

EAP-SIM supports protected EAP method version negotiation, so if a new EAP-SIM version later introduces a different ciphersuite, then the protected EAP method version negotiation will protect the (implied) ciphersuite negotiation.

EAP-AKA does not support EAP method version negotiation. However, if new extensions, such as EAP method version negotiation extensions or ciphersuite negotiation extensions, are later introduced to the very first messages of EAP-AKA that do not contain a message authentication code, then EAP-AKA requires that these messages MUST be protected with the AT_CHECKCODE attribute.

3.2 Recommended Requirements

In [802.11 REQ], the features discussed in this section are mentioned as recommended requirements, which SHOULD be supported by EAP method suitable for use in wireless LAN authentication.

3.2.1 Fragmentation

Fragmentation is not supported by EAP-AKA and EAP-SIM. For more discussion, please see Section 4.

3.2.2 End-User Identity Hiding

According to [802.11 REQ], this requirement corresponds to the "Confidentiality" security claim defined in [RFC3748], Section 7.2.1. In [RFC3748], Confidentiality "refers to encryption of EAP messages, including EAP Requests and Responses, and success and failure result indications. A method making this claim MUST support identity protection." [RFC3748] does not clearly define "Identity protection", but in Section 7.3 identity protection is discussed as follows: "It is possible for the identity in the identity response to be different from the identity authenticated by the EAP method. This

may be intentional in the case of identity privacy."

EAP-AKA and EAP-SIM support the security claim "Confidentiality", except for method specific success and failure indications. EAP-AKA and EAP-SIM support identity privacy against passive attacks via temporary identities that are used instead of the permanent identity. Protection against active attacks may also be implemented if the peer and the server can maintain the temporary identities reliably and the client follows a policy where the cleartext identity is not given out after an initial successful authentication.

3.3 Optional Features

The features discussed in this section are listed in [802.11 REQ] as optional features, which MAY be supported by EAP methods.

3.3.1 Channel Binding

EAP-AKA and EAP-SIM do not include the optional channel binding feature. However, ongoing work such as [Service Identity] may provide such support as an extension to popular EAP methods such as EAP-TLS, EAP-SIM, or EAP-AKA.

3.3.2 Fast Reconnect

This requirement corresponds to the to the "fast reconnect" security claim defined in [RFC3748], Section 7.2.1, which is supported by EAP-AKA and EAP-SIM. Fast reconnect is called fast re-authentication in the EAP-AKA and EAP-SIM specifications. Both methods satisfy this requirement.

4. Conclusions

The support in EAP-AKA and EAP-SIM for each requirement and optional feature listed in [802.11 REQ] is discussed in the previous section of this document. In summary, both EAP methods satisfy all the applicable mandatory (MUST and MUST NOT) requirements.

The methods do not satisfy the recommended (SHOULD) requirement about EAP message fragmentation. In EAP-AKA and EAP-SIM, protocol messages include variable-length fields that can be used to transmit Network Access Identifiers, and the protocols can be extended with new attributes, so in theory it is possible that the message size could exceed the EAP Maximum Transfer Unit (MTU) of 1020 octets. However, in practice the EAP packets transmitted in these protocols, in particular when the identity formats specified by 3GPP are used, are considerably smaller than the EAP MTU so the lack of fragmentation is not a problem.

The methods satisfy the second recommended (SHOULD) requirement, "end-user identity hiding", against all passive attacks and in some cases against active attacks. The methods support the optional feature "fast reconnect". These versions of the methods do not support the optional feature "channel binding".

5. IANA Considerations

This document does not require any new IANA registries or parameter allocation by IANA.

6. Security Considerations

Security issues are discussed throughout this document.

7. Acknowledgements

The authors would like to thank Bernard Aboba and Yoshihiro Ohba for the most valuable discussions on these protocols.

8. References

8.1 Normative References

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

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

[802.11 REQ] Stanley, D., Walker, J. and B. Aboba, "EAP Method Requirements for Wireless LANs", draft-walker-ieee802-req-04 (work in progress), August 2004.

[EAP-AKA] Arkko, J. and H. Haverinen, "EAP-AKA Authentication", draft-arkko-pppext-eap-aka-15 (work in progress), December 2004.

[EAP-SIM] Haverinen, H. and J. Salowey, "Extensible Authentication Protocol Method for GSM Subscriber Identity Modules (EAP-SIM)", draft-arkko-pppext-eap-sim-16 (work in progress), December 2004.

8.2 Informative References

[Service Identity]
Arkko, J. and P. Eronen, "Authenticated Service Information for the Extensible Authentication Protocol (EAP)", draft-arkko-service-identity-auth-01 (work in progress), October 2004.

Authors' Addresses

Pasi Eronen
Nokia Research Center
P.O. Box 407
FIN-00045 Nokia Group
Finland

EMail: pasi.eronen@nokia.com

Henry Haverinen
Nokia Enterprise Solutions
P.O. Box 12
FIN-40101 Jyvaskyla
Finland

EMail: henry.haverinen@nokia.com

Jari Arkko
Ericsson
FIN-02420 Jorvas
Finland

Phone: +358 40 5079256
EMail: jari.Arkko@ericsson.com

Joseph Salowey
Cisco Systems
2901 Third Avenue
Seattle, WA 98121
USA

Phone: +1 206 256 3380
EMail: jsalowey@cisco.com

Intellectual Property Statement

Disclaimer of Validity

Copyright Statement

Acknowledgment

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