Network Working Group
INTERNET-DRAFT
Updates: 5247
Category: Standards Track
<draft-dekok-emu-eap-session-id-01.txt>
23 July 2019

DeKok, Alan
FreeRADIUS

EAP Session-Id Derivation
draft-dekok-emu-eap-session-id-01.txt

Abstract

EAP Session-Id derivation has not been defined for EAP-SIM, EAP-AKA, and EAP-AKA' when using the fast re-authentication exchange instead of full authentication. This document updates [RFC5247] to define those derivations for EAP-SIM, and EAP-AKA. Since [AKAP] defines the Session-ID for EAP-AKA', the definition for EAP-AKA' is not included here. [RFC5247] also does not define Session-Id derivation for PEAP. A definition is given here which follows the definition for other TLS-based EAP methods.

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and BCP 79.

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/1id-abstracts.txt.

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

This Internet-Draft will expire on July 22, 2019.

Table of Contents

1. Introduction

EAP [RFC3748] Session-Id derivation has not been defined for EAP-SIM, EAP-AKA, and EAP-AKA' when using the fast re-authentication exchange instead of full authentication. [RFC5247] defines the Session-Id for these EAP methods, but that derivation is only applicable for the full authentication case.

The IEEE is defining FILS authentication [FILS], which needs the EAP Session-Id for in order for the EAP Re-authentication Protocol (ERP) [RFC5296] to work, it would be important to get this resolved with a clearly defined and agreed derivation rules to allow fast re-authentication cases to be used to derive ERP key hierarchy.

Further, [RFC5247] did not define Session-Id for PEAP. We correct that deficiency here.

1.1. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

2. Updates to RFC 5247 Appendix A

This section updates [RFC5247] Appendix A to define Session-Id for fast re-authentication exchange for EAP-AKA and EAP-SIM. It further defines Session-ID derivation for PEAP.

2.1. EAP-AKA

For EAP-AKA, [RFC5247] Appendix A says:

EAP-AKA

> EAP-AKA is defined in [RFC4187]. The EAP-AKA Session-Id is the concatenation of the EAP Type Code (0x17) with the contents of the RAND field from the AT_RAND attribute, followed by the contents of the AUTN field in the AT_AUTN attribute:
>
> Session-Id = 0x17 || RAND || AUTN

It should say:

EAP-AKA

> EAP-AKA is defined in [RFC4187]. When using full authentication, the EAP-AKA Session-Id is the concatenation of the EAP Type Code (0x17) with the contents of the RAND field from the AT_RAND attribute, followed by the contents of the AUTN field in the AT_AUTN attribute:
>
> Session-Id = 0x17 || RAND || AUTN
>
> When using fast re-authentication, the EAP-AKA Session-Id is the concatenation of the EAP Type Code (0x17) with the contents of the NONCE_S field from the AT_NONCE_S attribute, followed by the contents of the MAC field from the AT_MAC attribute from EAP-Request/AKA-Reauthentication:
>
> Session-Id = 0x17 || NONCE_S || MAC

2.2. EAP-SIM

Similarly for EAP-SIM, it says:

EAP-SIM

> EAP-SIM is defined in [RFC4186]. The EAP-SIM Session-Id is the concatenation of the EAP Type Code (0x12) with the contents of the

RAND field from the AT_RAND attribute, followed by the contents of the NONCE_MT field in the AT_NONCE_MT attribute:

Session-Id = 0x12 || RAND || NONCE_MT

The Peer-Id is the contents of the Identity field from the AT_IDENTITY attribute, using only the Actual Identity Length octets from the beginning, however. Note that the contents are used as they are transmitted, regardless of whether the transmitted identity was a permanent, pseudonym, or fast EAP re-authentication identity. The Server-Id is the null string (zero length).

It should say:

EAP-SIM

EAP-SIM is defined in [RFC4186]. The EAP-SIM Session-Id is the concatenation of the EAP Type Code (0x12) with the contents of the RAND field from the AT_RAND attribute, followed by the contents of the NONCE_MT field in the AT_NONCE_MT attribute. RFC 4186 says that EAP server should obtain "n" GSM triplets where "n=2" or "n=3".

For "n=2", the Session-Id is therefore defined as

Session-Id = 0x12 || RAND1 || RAND2 || NONCE_MT

which is 49 octets in length.

For "n=3", the Session-Id is therefore defined as

Session-Id = 0x12 || RAND1 || RAND2 || RAND3 || NONCE_MT

which is 65 octets in length.

The Peer-Id is the contents of the Identity field from the AT_IDENTITY attribute, using only the Actual Identity Length octets from the beginning, however. Note that the contents are used as they are transmitted, regardless of whether the transmitted identity was a permanent, pseudonym, or fast EAP re-authentication identity. The Server-Id is the null string (zero length).

When using fast re-authentication, the EAP-SIM Session-Id is the concatenation of the EAP Type Code (0x12) with the contents of the NONCE_S field from the AT_NONCE_S attribute, followed by the

contents of the MAC field from the AT_MAC attribute from EAP-Request/AKA-Reauthentication:

Session-Id = 0x12 || NONCE_S || MAC

which is 33 octets in length.

2.3. Rationale

[RFC5247] was supposed to define exported parameters for existing EAP methods in Appendix A. The way Session-Id was defined for EAP-AKA and EAP-SIM works only for the full authentication case, i.e., it cannot be used when the optional fast re-authentication case is used since the used parameters (RAND, AUTN, NONCE_MT) are not used in the fast re-authentication case. Based on [RFC4187] Section 5.2, and similar text in [RFC4186], NONCE_S corresponds to RAND and MAC in EAP-Request/AKA-Reauthentication corresponds to AUTN. That would seem to imply that the Session-Id could be defined using NONCE_S and MAC instead of RAND and AUTN/NONCE_MT.

2.4. Session-Id for PEAP

[RFC5247] did not define Session-Id definition for Microsoft's Protected EAP (PEAP). Similar to the definition in [RFC5216] Section 2.3, we define it as:

Session-Id = 0x19 || client.random || server.random

This definition is already in wide-spread use in multiple PEAP implementations.

Note that this definition for Session-Id only applies when TLS 1.2 or earlier is used. A different derivation is defined for TLS 1.3.

3. Security Considerations

This specification defines EAP Session-Ids for ERP with EAP-SIM and EAP-AKA. It therefore enables ERP key hierarchy establishment using fast re-authentication with EAP-SIM and EAP-AKA.

There are no known security issues from using the NONCE_S and MAC as defined above.

This specification also defines the EAP Session-Id for PEAP. That deriviation has no known security issues.

4. IANA Considerations

There are no actions for IANA. RFC EDITOR: This section may be removed before publication.

5. References

5.1. Normative References

[RFC2119]
Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", RFC 2119, March, 1997, <http://www.rfc-editor.org/info/rfc2119>.

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

[RFC5216]
Simon, D., Aboba, B., and R. Hurst, "The EAP-TLS Authentication Protocol", RFC 5216, March 2008

[RFC5247]
Aboba, B., Simon, D., and P. Eronen, "Extensible Authentication Protocol (EAP) Key Management Framework", RFC 5247, August 2008,

[RFC5296]
Narayanan, V. and L. Dondeti, "EAP Extensions for EAP Re-authentication Protocol (ERP)", RFC 5296, August 2008.

[RFC8174]
Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", RFC 8174, May 2017, <http://www.rfc-editor.org/info/rfc8174>.

[FILS]
"IEEE Standard for 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 - Amendment 1: Fast Initial Link Setup", IEEE Std 802.11ai-2016, 2016.

5.2. Informative References

[RFC4186]
Haverinen, H. (Ed), Salowey, J., "Extensible Authentication

Protocol Method for Global System for Mobile Communications (GSM) Subscriber Identity Modules (EAP-SIM)", RFC 4186, January 2006.

[RFC4187]
Arkko, J., Haverinen, H., "Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)", RFC 4187, January 2006.

[AKAP]
Arkko, J., et al, "Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA')", draft-arkko-eap-rfc5448bis-04.txt, January 2019.

Acknowledgments

The issue corrected in this specification was first reported by Jouni Malinen in a technical errata at https://www.rfc-editor.org/errata_search.php/doc/html/rfc5247

The text in this document follows his suggestions.

Authors' Addresses

Alan DeKok
The FreeRADIUS Server Project

Email: aland@freeradius.org