Internet Engineering Task Force (IETF)
Request for Comments: 8940
Updates: 5247
Category: Standards Track
ISSN: 2070-1721

A. DeKok
FreeRADIUS

October 2020

Extensible Authentication Protocol (EAP) Session-Id Derivation for EAP Subscriber Identity Module (EAP-SIM), EAP Authentication and Key Agreement (EAP-AKA), and Protected EAP (PEAP)

Abstract

RFC 5247 is updated to define and clarify EAP Session-Id derivation for multiple Extensible Authentication Protocol (EAP) methods. The derivation of Session-Id was not given for EAP Subscriber Identity Module (EAP-SIM) or EAP Authentication and Key Agreement (EAP-AKA) when using the fast reconnect exchange instead of full authentication. The derivation of Session-Id for full authentication is clarified for both EAP-SIM and EAP-AKA. The derivation of Session-Id for Protected EAP (PEAP) is also given. The definition for PEAP follows the definition for other TLS-based EAP methods.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc8940.

Table of Contents

1. Introduction

2.1. EAP-AKA
2.2. EAP-SIM
2.3. Rationale for EAP-AKA and EAP-SIM Updates
3. Session-Id for PEAP
4. Security Considerations
5. IANA Considerations
6. References
6.1. Normative References
6.2. Informative References
Acknowledgments
Author's Address

1. Introduction

EAP [RFC3748] Session-Id derivation has not been defined for EAP-SIM and EAP-AKA when using the fast reconnect 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 Session-Id derivation was not defined for EAP-AKA', but [AKAP] now defines it, along with other updates. As such, the definition for EAP-AKA' is not included here.

Further, the derivation of Session-Id for full authentication is clarified, as the text in [RFC5247] is ambiguous.

The IEEE has defined Fast Initial Link Setup (FILS) authentication [FILS], which needs the EAP Session-Id in order for the EAP Re-authentication Protocol (ERP) [RFC6696] to work. It is therefore important to address the existing deficiencies in the definition of EAP Session-Id.

Finally, [RFC5247] did not define Session-Id for PEAP [MS-PEAP] [PEAP]. We correct these deficiencies here by updating [RFC5247] with the Session-Id derivation during fast-reconnect exchange for EAP-SIM and EAP-AKA; clarifying the Session-Id derivation during full authentication for EAP-SIM and EAP-AKA; and defining the Session-Id derivation for PEAP, which is the same for both full authentication and fast reconnect.

2. Updates to RFC 5247, Appendix A

This section updates [RFC5247], Appendix A to define Session-Id for fast reconnect exchange for EAP-AKA and EAP-SIM.

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 reconnect, 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, [RFC5247], Appendix A 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

It should say:

> EAP-SIM
>
> EAP-SIM is defined in [RFC4186]. When using full authentication, 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 the 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.
>
> RAND1, RAND2, and RAND3 correspond to the RAND value from the first, second, and third GSM triplet, respectively.

When using fast reconnect, 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/SIM/Reauthentication:

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

which is 33 octets in length.

2.3. Rationale for EAP-AKA and EAP-SIM Updates

Appendix A of [RFC5247] was supposed to define exported parameters for existing EAP methods. 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 reconnect case is used since the used parameters (RAND, AUTN, NONCE_MT) are not used in the fast reconnect case. Based on [RFC4187], Section 5.2 and similar text in [RFC4186], Section 5.2, NONCE_S corresponds to RAND and MAC in EAP-Request/AKA-Reauthentication, and EAP-Request/SIM/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.

This derivation is done via a random value created by the server, along with a secret key and the peer's identity. We believe that this derivation is secure, though no formal analysis has been done.

3. Session-Id for PEAP

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

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

This definition is that same for both full authentication and for fast reconnect.

This definition is already in widespread use in all known 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 in [TLS-EAP-TYPES].

4. 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 reconnect with EAP-SIM and EAP-AKA.

The Session-Id definitions given here are unique per session, unforgeable, and unguessable by an outside party, as per the requirements of [RFC5247], Section 10.

The definitions used here have been widely deployed for years in all major EAP implementations. However, we acknowledge that very little security analysis has been done for these definitions. As a result, any security issues would result in serious issues for the Internet as a whole.

These updates do not modify the security considerations outlined in [RFC5247].

5. IANA Considerations

This document has no IANA actions.

6. References

6.1. Normative References

[FILS] IEEE, "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", DOI 10.1109/IEEESTD.2016.7792308, IEEE Std 802.11ai-2016, December 2016, <https://doi.org/10.1109/IEEESTD.2016.7792308>.

[RFC3748] Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., and H. Levkowetz, Ed., "Extensible Authentication Protocol (EAP)", RFC 3748, DOI 10.17487/RFC3748, June 2004, <https://www.rfc-editor.org/info/rfc3748>.

[RFC5216] Simon, D., Aboba, B., and R. Hurst, "The EAP-TLS Authentication Protocol", RFC 5216, DOI 10.17487/RFC5216, March 2008, <https://www.rfc-editor.org/info/rfc5216>.

[RFC5247] Aboba, B., Simon, D., and P. Eronen, "Extensible Authentication Protocol (EAP) Key Management Framework", RFC 5247, DOI 10.17487/RFC5247, August 2008, <https://www.rfc-editor.org/info/rfc5247>.

6.2. Informative References

[AKAP] Arkko, J., Lehtovirta, V., Torvinen, V., and P. Eronen, "Improved Extensible Authentication Protocol Method for 3GPP Mobile Network Authentication and Key Agreement (EAP-AKA')", Work in Progress, Internet-Draft, draft-ietf-emu-rfc5448bis-07, 9 March 2020, <https://tools.ietf.org/html/draft-ietf-emu-rfc5448bis-07>.

[Err5011] RFC Errata, Erratum ID 5011, RFC 5247, <https://www.rfc-editor.org/errata/eid5011>.

[MS-PEAP] Microsoft, "[MS-PEAP]: Protected Extensible Authentication Protocol (PEAP)", <https://docs.microsoft.com/en-

us/openspecs/windows_protocols/ms-peap/5308642b-90c9-4cc4-beec-fb367325c0f9>.

[PEAP] Palekar, A., Josefsson, S., Simon, D., and G. Zorn, "Protected EAP Protocol (PEAP) Version 2", Work in Progress, Internet-Draft, draft-josefsson-pppext-eap-tls-eap-10, 21 October 2004, <https://tools.ietf.org/html/draft-josefsson-pppext-eap-tls-eap-10>.

[RFC4186] Haverinen, H., Ed. and J. Salowey, Ed., "Extensible Authentication Protocol Method for Global System for Mobile Communications (GSM) Subscriber Identity Modules (EAP-SIM)", RFC 4186, DOI 10.17487/RFC4186, January 2006, <https://www.rfc-editor.org/info/rfc4186>.

[RFC4187] Arkko, J. and H. Haverinen, "Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)", RFC 4187, DOI 10.17487/RFC4187, January 2006, <https://www.rfc-editor.org/info/rfc4187>.

[RFC6696] Cao, Z., He, B., Shi, Y., Wu, Q., Ed., and G. Zorn, Ed., "EAP Extensions for the EAP Re-authentication Protocol (ERP)", RFC 6696, DOI 10.17487/RFC6696, July 2012, <https://www.rfc-editor.org/info/rfc6696>.

[TLS-EAP-TYPES] DeKok, A., "TLS-based EAP types and TLS 1.3", Work in Progress, Internet-Draft, draft-ietf-emu-tls-eap-types-01, 29 July 2020, <https://tools.ietf.org/html/draft-ietf-emu-tls-eap-types-01>.

Acknowledgments

The issue corrected in this specification was first reported by Jouni Malinen in a technical erratum for RFC 5247 [Err5011].

The text in this document follows Jouni's suggestions.

Author's Address

Alan DeKok
The FreeRADIUS Server Project

Email: aland@freeradius.org