EAP Method Support for Transporting AAA Payloads
draft-clancy-emu-aaapay-00

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with Section 6 of 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 August 21, 2008.

Copyright Notice

Copyright (C) The IETF Trust (2008).

Abstract

This document defines bindings for existing EAP methods to transport Diameter AVPs, called "AAA payloads". The primary application is to support EAP channel bindings, but this could be used for other applications as well.
1. Introduction ............................................. 3
2. Terminology .............................................. 3
3. Overview and Requirements .............................. 3
4. AAA Payload Format ....................................... 4
5. Bindings for Existing EAP Methods ..................... 5
   5.1. Generalized Pre-Shared Key (GPSK) .................... 5
   5.2. Pre-Shared Key (PSK) .................................. 5
   5.3. Password Authenticated Exchange (PAX) ............... 5
   5.4. Tunneled Transport Layer Security (TTLS) ............ 5
   5.5. Flexible Authentication via Secure Tunneling (FAST) . 5
6. Security Considerations ................................... 5
7. IANA Considerations ....................................... 6
8. References .................................................. 6
   8.1. Normative References .................................. 6
   8.2. Informative References ............................... 7

Author’s Address ............................................ 8
Intellectual Property and Copyright Statements ............ 9
1. Introduction

This document defines a payload which can be securely transported by an Extensible Authentication Method (EAP) method [RFC3748] that carries arbitrary Diameter Attribute-Value Pairs (AVPs) [RFC3588]. While it may seem strange for EAP to encapsulate Authorization, Authentication, and Accounting (AAA) messages, since AAA typically encapsulates EAP, the security properties are different. In particular, AAA data transported by EAP between the client and server will be protected by an end-to-end security relationship. This provides a secure channel for doing things like channel bindings [RFC5056].

2. Terminology

In this document, several words are used to signify the requirements of the specification. These words are often capitalized. 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].

3. Overview and Requirements

Many EAP [RFC3748] methods have extensible properties that allow you to embed arbitrary data within a secure channel. This channel is secured using keys derived during the EAP authentication. These channels vary in the properties that they provide, typically either providing integrity protection or both confidentiality and integrity protection.

In this document we define a payload format for encapsulating Diameter AVPs [RFC3588], and via backwards compatibility [RFC4005], RADIUS TLVs [RFC2865]. We provide bindings for a variety of existing EAP methods that would allow them to transport this data. One specific application of this is to support EAP channel bindings [RFC5056][I-D.clancy-emu-chbind].

The main goal is to provide the peer and server to exchange AAA messages protected by an end-to-end security association. As such, any EAP method transporting the AAA payloads defined in this document MUST support integrity protection. To accomplish this, a method supporting AAA payloads MUST perform mutual authentication and derive session keys (i.e. MSK, etc), and during this derivation process MUST derive a unique, cryptographically independent, fresh key for protecting AAA payloads. Protocols SHOULD also support confidentiality in addition to integrity protection. Confidentiality
is important for identity protection, as a variety of identities can be passed over this channel.

4. AAA Payload Format

This section describes the formatting for the AAA Payloads. Each payload consists of the following fields:

- Version, 2 octets
- length(Session-ID), 2 octets
- Session-ID [I-D.ietf-eap-keying], arbitrary length
- One or more Diameter AVPs [RFC3588], arbitrary length

The version field is 2 octets. This document defines version 0x0001.

The Session-ID field is arbitrary length and is proceeded by its 2-octet length specified in network-byte order.

Following the Session-ID is an arbitrary number of Diameter AVPs. AVPs already contain a length field internally, so they can be parsed without additional information.

The payload can be graphically depicted as:

--- bit offset -->
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|          Version=0x01         |       length(Session-ID)      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
...                         Session-ID                        ...
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
...                       Diameter AVP 1                      ...
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
...                       Diameter AVP N                      ...
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

Figure 1
5. Bindings for Existing EAP Methods

This section describes how binding tokens can be included in all current EAP methods that support secure transport of arbitrary data. Future EAP methods SHOULD describe how they can implement binding tokens.

5.1. Generalized Pre-Shared Key (GPSK)


- 0x0000002 (IANA-TBD): AAA Payload

5.2. Pre-Shared Key (PSK)

EAP-PSK [RFC4764] defines a protected channel. Use by PSK simply requires instantiation of a new EXT_Type value:

- 0x01 (IANA-TBD): AAA Payload

5.3. Passord Authenticated Exchange (PAX)

EAP-PAX [RFC4746] defines an authenticated data exchange (ADE). Use by PAX simply requires instantiation of a new ADE type:

- 0x04 (IANA-TBD): AAA Payload

5.4. Tunneled Transport Layer Security (TTLS)

EAP-TTLS [I-D.funk-eap-ttls-v0] uses Diameter Attribute-Value-Pairs (AVPs) for its messaging. As such it natively supports transporting AAA payloads. No protocol changes are necessary.

5.5. Flexible Authentication via Secure Tunneling (FAST)

EAP-FAST [RFC4851] uses Type-Length-Values (TLVs) for its messaging. To embed binding tokens, a new TLV must be defined:

- 0x15 (IANA-TBD): AAA Payload

6. Security Considerations

Section 3 documented a variety of requirements for EAP methods to transport these AAA payloads. They MUST support identity protection of arbitrary payloads, and SHOULD support confidentiality. Each
method’s security considerations section would detail how they achieve those requirements.

The payload includes the EAP Session-ID field. This is to prevent replay attacks. In particular, depending on how an EAP method implements their secured channel, it may or may not be cryptographically bound to the rest of the session. By explicitly including the EAP Session-ID, we prevent replay attacks. Implementations MUST verify the consistency of the Session-ID received in the AAA payloads.

Certainly there are a whole host of issues surrounding the security of what may be contained within the AAA payload format. If the information being transported requires confidentiality, then the method SHOULD support that. Otherwise sensitive data could be disclosed.

7. IANA Considerations

We require registry from a variety of IANA repositories.

From "EAP-GPSK PData/Specifier":

- 0x00000002 (IANA-TBD): AAA Payload

From "EAP EXT_Type Numbers":

- 0x01 (IANA-TBD): AAA Payload

From "EAP-PAX ADE Type Namespace":

- 0x04 (IANA-TBD): AAA Payload

From "EAP-FAST TLV Types":

- 0x15 (IANA-TBD): AAA Payload

8. References

8.1. Normative References


8.2. Informative References

[I-D.ietf-eap-keying]

[I-D.ietf-emu-eap-gpsk]

[I-D.funk-eap-ttls-v0]

[I-D.clancy-emu-chbind]


Author’s Address

T. Charles Clancy
DoD Laboratory for Telecommunications Sciences
8080 Greenmead Drive
College Park, MD 20740
USA

Email: clancy@ltsnet.net