

Diameter Extensible Authentication Protocol (EAP) Application

Status of This Memo

This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

Copyright Notice

Copyright (C) The Internet Society (2005).

Abstract

The Extensible Authentication Protocol (EAP) provides a standard mechanism for support of various authentication methods. This document defines the Command-Codes and AVPs necessary to carry EAP packets between a Network Access Server (NAS) and a back-end authentication server.

Table of Contents

1.	Introduction	2
1.1.	Conventions Used in This Document	3
2.	Extensible Authentication Protocol Support in Diameter	3
2.1.	Advertising Application Support	3
2.2.	Protocol Overview	4
2.3.	Sessions and NASREQ Interaction	6
2.3.1.	Scenario 1: Direct Connection	7
2.3.2.	Scenario 2: Direct Connection with Redirects	8
2.3.3.	Scenario 3: Direct EAP, Authorization via Agents ..	9
2.3.4.	Scenario 4: Proxy Agents	10
2.4.	Invalid Packets	10
2.5.	Retransmission	11
2.6.	Fragmentation	12
2.7.	Accounting	12
2.8.	Usage Guidelines	13

2.8.1.	User-Name AVP	13
2.8.2.	Conflicting AVPs	13
2.8.3.	Displayable Messages	14
2.8.4.	Role Reversal	14
2.8.5.	Identifier Space	14
3.	Command-Codes	14
3.1.	Diameter-EAP-Request (DER) Command	15
3.2.	Diameter-EAP-Answer (DEA) Command	16
4.	Attribute-Value Pairs	18
4.1.	New AVPs	18
4.1.1.	EAP-Payload AVP	18
4.1.2.	EAP-Reissued-Payload AVP	18
4.1.3.	EAP-Master-Session-Key AVP	19
4.1.4.	EAP-Key-Name AVP	19
4.1.5.	Accounting-EAP-Auth-Method AVP	19
5.	AVP Occurrence Tables	19
5.1.	EAP Command AVP Table	20
5.2.	Accounting AVP Table	21
6.	RADIUS/Diameter Interactions	22
6.1.	RADIUS Request Forwarded as Diameter Request	22
6.2.	Diameter Request Forwarded as RADIUS Request	23
6.3.	Accounting Requests	24
7.	IANA Considerations	24
8.	Security Considerations	24
8.1.	Overview	24
8.2.	AVP Editing	26
8.3.	Negotiation Attacks	27
8.4.	Session Key Distribution	28
8.5.	Privacy Issues	28
8.6.	Note about EAP and Impersonation	29
9.	Acknowledgements	29
10.	References	30
10.1.	Normative References	30
10.2.	Informative References	30

1. Introduction

The Extensible Authentication Protocol (EAP), defined in [EAP], is an authentication framework which supports multiple authentication mechanisms. EAP may be used on dedicated links, switched circuits, and wired as well as wireless links.

To date, EAP has been implemented with hosts and routers that connect via switched circuits or dial-up lines using PPP [RFC1661], IEEE 802 wired switches [IEEE-802.1X], and IEEE 802.11 wireless access points [IEEE-802.11i]. EAP has also been adopted for IPsec remote access in IKEv2 [IKEv2].

This document specifies the Diameter EAP application that carries EAP packets between a Network Access Server (NAS) working as an EAP Authenticator and a back-end authentication server. The Diameter EAP application is based on the Diameter Network Access Server Application [NASREQ] and is intended for environments similar to NASREQ.

In the Diameter EAP application, authentication occurs between the EAP client and its home Diameter server. This end-to-end authentication reduces the possibility for fraudulent authentication, such as replay and man-in-the-middle attacks. End-to-end authentication also provides a possibility for mutual authentication, which is not possible with PAP and CHAP in a roaming PPP environment.

The Diameter EAP application relies heavily on [NASREQ], and in earlier versions was part of the Diameter NASREQ application. It can also be used in conjunction with NASREQ, selecting the application based on the user authentication mechanism (EAP or PAP/CHAP). The Diameter EAP application defines new Command-Codes and Attribute-Value Pairs (AVPs), and can work together with RADIUS EAP support [RFC3579].

1.1. Conventions Used in This Document

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].

2. Extensible Authentication Protocol Support in Diameter

2.1. Advertising Application Support

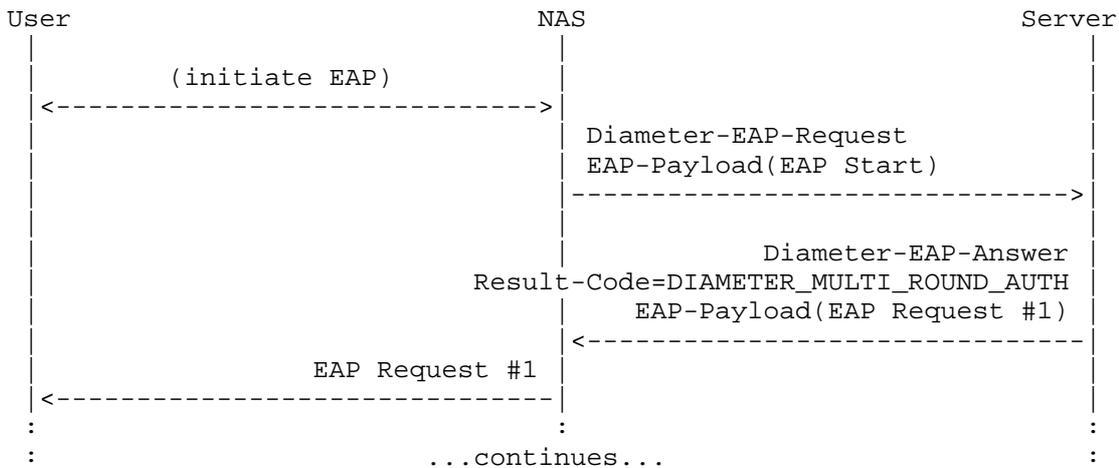
Diameter nodes conforming to this specification MUST advertise support by including the Diameter EAP Application ID value of 5 in the Auth-Application-Id AVP of the Capabilities-Exchange-Request and Capabilities-Exchange-Answer command [BASE].

If the NAS receives a response with the Result-Code set to `DIAMETER_APPLICATION_UNSUPPORTED` [BASE], it indicates that the Diameter server in the home realm does not support EAP. If possible, the access device MAY attempt to negotiate another authentication protocol, such as PAP or CHAP. An access device SHOULD be cautious when determining whether a less secure authentication protocol will be used, since this could result from a downgrade attack (see Section 8.3).

2.2. Protocol Overview

The EAP conversation between the authenticating peer and the access device begins with the initiation of EAP within a link layer, such as PPP [RFC1661] or IEEE 802.11i [IEEE-802.11i]. Once EAP has been initiated, the access device will typically send a Diameter-EAP-Request message with an empty EAP-Payload AVP to the Diameter server, signifying an EAP-Start.

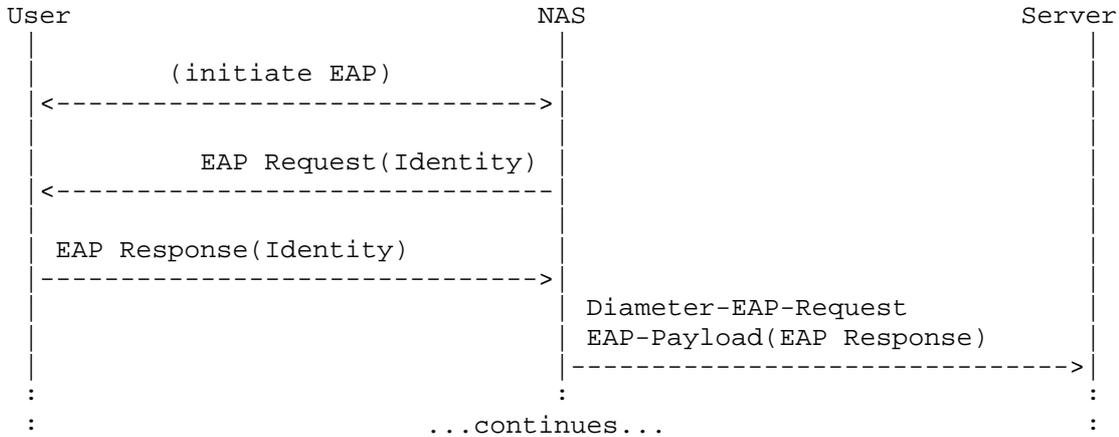
If the Diameter home server is willing to do EAP authentication, it responds with a Diameter-EAP-Answer message containing an EAP-Payload AVP that includes an encapsulated EAP packet. The Result-Code AVP in the message will be set to `DIAMETER_MULTI_ROUND_AUTH`, signifying that a subsequent request is expected. The EAP payload is forwarded by the access device to the EAP client. This is illustrated in the diagram below.



The initial Diameter-EAP-Answer in a multi-round exchange normally includes an EAP-Request/Identity, requesting the EAP client to identify itself. Upon receipt of the EAP client's EAP-Response, the access device will then issue a second Diameter-EAP-Request message, with the client's EAP payload encapsulated within the EAP-Payload AVP.

A preferred approach is for the access device to issue the EAP-Request/Identity message to the EAP client, and forward the EAP-Response/Identity packet, encapsulated within the EAP-Payload AVP, as a Diameter-EAP-Request to the Diameter server (see the diagram below). This alternative reduces the number of Diameter message round trips. When the EAP-Request/Identity message is issued by the access device, it SHOULD interpret the EAP-Response/Identity

packet returned by the authenticating peer, and copy its value to a User-Name AVP in Diameter-EAP-Request. This is useful in roaming environments, since the Destination-Realm is needed for routing purposes. Note that this alternative cannot be universally employed, as there are circumstances in which a user's identity is not needed (such as when authorization occurs based on a calling or called phone number).



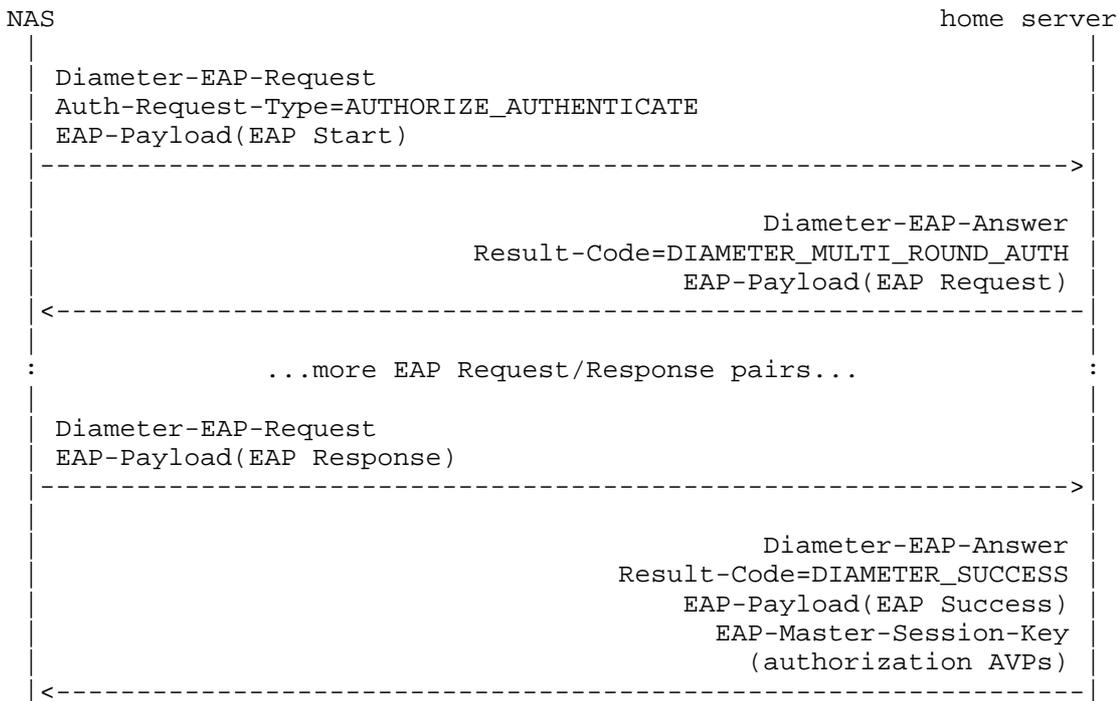
The conversation continues until the Diameter server sends a Diameter-EAP-Answer with a Result-Code AVP indicating success or failure, and an optional EAP-Payload. The Result-Code AVP is used by the access device to determine whether service is to be provided to the EAP client. The access device MUST NOT rely on the contents of the optional EAP-Payload to determine whether service is to be provided.

Basic Diameter security mechanisms (IPsec and TLS) protect Diameter messages hop-by-hop. Since there are currently no end-to-end (NAS-to-home server) security mechanisms defined for Diameter, this section describes possible scenarios on how the messages could be transport protected using these hop-by-hop mechanisms.

This list of scenarios is not intended to be exhaustive, and it is possible to combine them. For instance, the first proxy agent after the NAS could use redirects as in Scenario 2 to bypass any additional proxy agents.

2.3.1. Scenario 1: Direct Connection

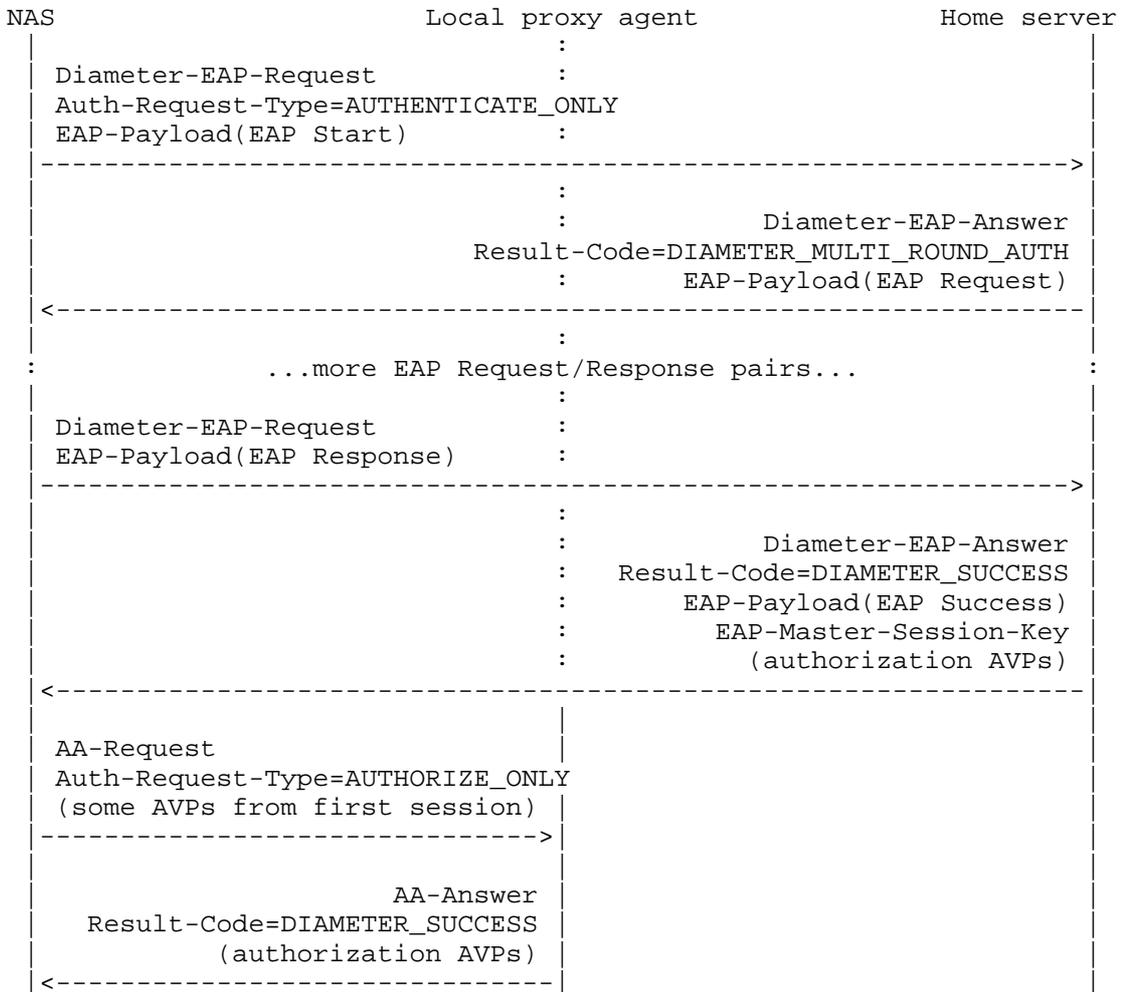
The simplest case is when the NAS contacts the home server directly. All authorization AVPs and EAP keying material are delivered by the home server.



This scenario is the most likely to be used in small networks, or in cases where Diameter agents are not needed to provide routing or additional authorization AVPs.

2.3.3. Scenario 3: Direct EAP, Authorization via Agents

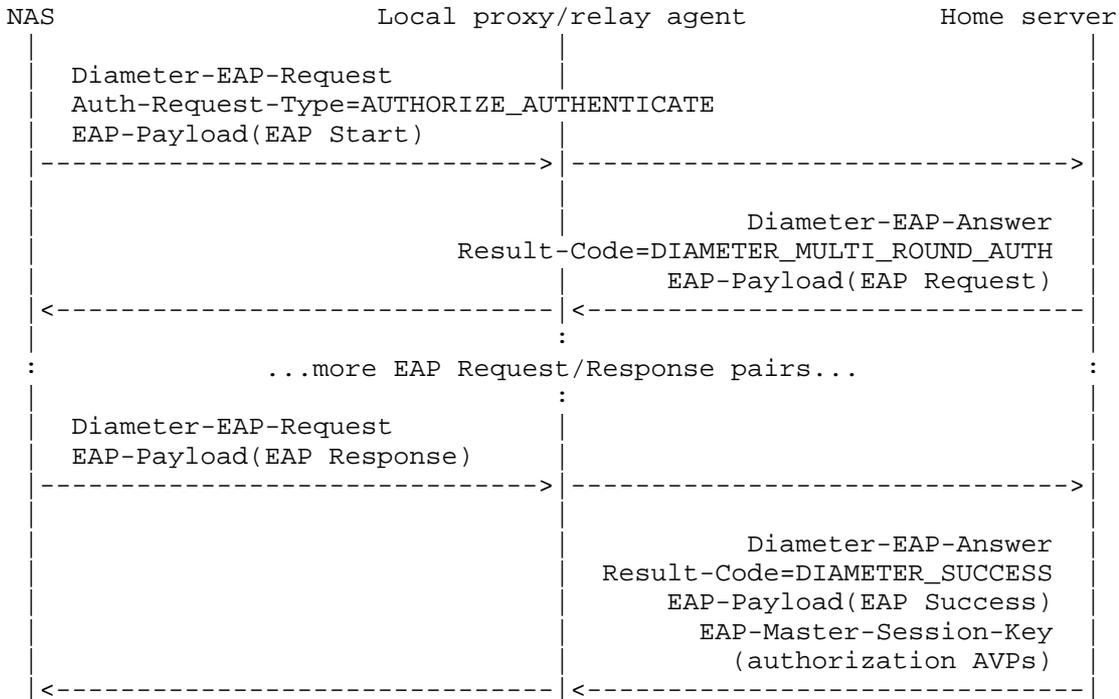
In this scenario the EAP authentication is done directly with the home server (with Auth-Request-Type set to AUTHENTICATE_ONLY), and authorization AVPs are retrieved from local proxy agents. This scenario is intended for environments in which the home server cannot provide all the necessary authorization AVPs to the NAS.



The NASREQ application is used here for authorization because the realm-specific routing table supports routing based on application, not on Diameter commands.

2.3.4. Scenario 4: Proxy Agents

This scenario is the same as Scenario 1, but the NAS contacts the home server through proxies. Note that the proxies can see the EAP session keys, thus it is not suitable for environments where proxies cannot be trusted.



2.4. Invalid Packets

While acting as a pass-through, the NAS MUST validate the EAP header fields (Code, Identifier, Length) prior to forwarding an EAP packet to or from the Diameter server. On receiving an EAP packet from the peer, the NAS checks the Code (Code 2=Response) and Length fields, and matches the Identifier value against the current Identifier, supplied by the Diameter server in the most recently validated EAP Request. On receiving an EAP packet from the Diameter server (encapsulated within a Diameter-EAP-Answer), the NAS checks the Code (Code 1=Request) and Length fields, then updates the current Identifier value. Pending EAP Responses that do not match the current Identifier value are silently discarded by the NAS.

Since EAP method fields (Type, Type-Data) are typically not validated by a NAS operating as a pass-through, despite these checks it is possible for a NAS to forward an invalid EAP packet to or from the Diameter server.

A Diameter server receiving an EAP-Payload AVP that it does not understand SHOULD determine whether the error is fatal or non-fatal based on the EAP Type. A Diameter server determining that a fatal error has occurred MUST send a Diameter-EAP-Answer with a failure Result-Code and an EAP-Payload AVP encapsulating an EAP Failure packet. A Diameter server determining that a non-fatal error has occurred MUST send a Diameter-EAP-Answer with DIAMETER_MULTI_ROUND_AUTH Result-Code, but no EAP-Payload AVP. To simplify RADIUS translation, this message MUST also include an EAP-Reissued-Payload AVP encapsulating the previous EAP Request sent by the server.

When receiving a Diameter-EAP-Answer without an EAP-Payload AVP (and DIAMETER_MULTI_ROUND_AUTH Result-Code), the NAS SHOULD discard the EAP-Response packet most recently transmitted to the Diameter server and check whether additional EAP Response packets that match the current Identifier value have been received. If so, a new EAP Response packet, if available, MUST be sent to the Diameter server within an Diameter-EAP-Request. If no EAP Response packet is available, then the previous EAP Request is resent to the peer, and the retransmission timer is reset.

In order to provide protection against Denial of Service (DoS) attacks, it is advisable for the NAS to allocate a finite buffer for EAP packets received from the peer, and to discard packets according to an appropriate policy once that buffer has been exceeded. Also, the Diameter server is advised to permit only a modest number of invalid EAP packets within a single session, prior to terminating the session with DIAMETER_AUTHENTICATION_REJECTED Result-Code. By default, a value of 5 invalid EAP packets is recommended.

2.5. Retransmission

As noted in [EAP], if an EAP packet is lost in transit between the authenticating peer and the NAS (or vice versa), the NAS will retransmit.

It may be necessary to adjust retransmission strategies and authentication time-outs in certain cases. For example, when a token card is used, additional time may be required to allow the user to find the card and enter the token. Since the NAS will typically not have knowledge of the required parameters, these need to be provided by the Diameter server.

If a Multi-Round-Time-Out AVP [BASE] is present in a Diameter-EAP-Answer message that also contains an EAP-Payload AVP, that value is used to set the EAP retransmission timer for that EAP Request and that Request alone.

2.6. Fragmentation

Using the EAP-Payload AVP, it is possible for the Diameter server to encapsulate an EAP packet that is larger than the MTU on the link between the NAS and the peer. Since it is not possible for the Diameter server to use MTU discovery to ascertain the link MTU, a Framed-MTU AVP may be included in a Diameter-EAP-Request message in order to provide the Diameter server with this information.

A Diameter server having received a Framed-MTU AVP in a Diameter-EAP-Request message MUST NOT send any subsequent packet in this EAP conversation containing EAP-Payload AVP whose length exceeds that specified by the Framed-MTU value, taking the link type (specified by the NAS-Port-Type AVP) into account. For example, as noted in [RFC3580] Section 3.10, for a NAS-Port-Type value of IEEE 802.11, the RADIUS server may send an EAP packet as large as Framed-MTU minus four (4) octets, taking into account the additional overhead for the IEEE 802.1X Version (1 octet), Type (1 octet) and Body Length (2 octets) fields.

2.7. Accounting

When a user is authenticated using EAP, the NAS MAY include an Accounting-Auth-Method AVP [NASREQ] with value 5 (EAP) in Accounting-Request messages. This document specifies one additional AVP for accounting messages. One or more Accounting-EAP-Auth-Method AVPs (see Section 4.1.5) MAY be included in Accounting-Request messages to indicate the EAP method(s) used to authenticate the user.

If the NAS has authenticated the user with a locally implemented EAP method, it knows the method used and SHOULD include it in an Accounting-EAP-Auth-Method AVP.

If the authentication was done using Diameter-EAP-Request/Answer messages, the Diameter server SHOULD include one or more Accounting-EAP-Auth-Method AVPs in Diameter-EAP-Answer packets with a successful result code. In this case, the NAS SHOULD include these AVPs in Accounting-Request messages.

2.8. Usage Guidelines

2.8.1. User-Name AVP

Unless the access device interprets the EAP-Response/Identity packet returned by the authenticating peer, it will not have access to the user's identity. Furthermore, some EAP methods support identity protection where the user's real identity is not included in EAP-Response/Identity. Therefore, the Diameter Server SHOULD return the user's identity by inserting a User-Name AVP to Diameter-EAP-Answer messages that have a Result-Code of DIAMETER_SUCCESS. A separate billing identifier or pseudonym MAY be used for privacy reasons (see Section 8.5). If the user's identity is not available to the NAS, the Session-Id AVP MAY be used for accounting and billing; however operationally this could be very difficult to manage.

2.8.2. Conflicting AVPs

A Diameter-EAP-Answer message containing an EAP-Payload of type EAP-Success or EAP-Failure MUST NOT have the Result-Code AVP set to DIAMETER_MULTI_ROUND_AUTH.

Some lower layers assume that the authorization decision is made by the EAP server, and thus the peer considers EAP Success as an indication that access was granted. In this case, the Result-Code SHOULD match the contained EAP packet: a successful Result-Code for EAP-Success, and a failure Result-Code for EAP-Failure. If the encapsulated EAP packet does not match the result implied by the Result-Code AVP, the combination is likely to cause confusion, because the NAS and peer will conclude the outcome of the authentication differently. For example, if the NAS receives a failure Result-Code with an encapsulated EAP Success, it will not grant access to the peer. However, on receiving the EAP Success, the peer will be led to believe that access was granted.

This situation can be difficult to avoid when Diameter proxy agents make authorization decisions (that is, proxies can change the Result-Code AVP sent by the home server). Because it is the responsibility of the Diameter server to avoid conflicts, the NAS MUST NOT "manufacture" EAP result packets in order to correct the contradictory messages that it receives. This behavior, originally mandated within [IEEE-802.1X], is now deprecated.

2.8.3. Displayable Messages

The Reply-Message AVP [NASREQ] MUST NOT be included in any Diameter message containing an EAP-Payload AVP.

2.8.4. Role Reversal

Some environments in which EAP is used, such as PPP, support peer-to-peer operation. Both parties act as authenticators and authenticates at the same time, in two simultaneous and independent EAP conversations.

This specification is intended for communication between EAP (passthrough) authenticator and backend authentication server. A Diameter client MUST NOT send a Diameter-EAP-Request encapsulating an EAP Request packet, and a Diameter server receiving such a packet MUST respond with a failure Result-Code.

2.8.5. Identifier Space

In EAP, each session has its own unique Identifier space. Diameter server implementations MUST be able to distinguish between EAP packets with the same Identifier existing within distinct EAP sessions and originating on the same NAS. This is done by using the Session-Id AVP.

If a Diameter NAS is in the middle of a multi-round authentication exchange, and it detects that the EAP session between the client and the NAS has been terminated, it MUST select a new Diameter Session-Id for any subsequent EAP sessions. This is necessary in order to distinguish a restarted EAP authentication process from the continuation of an ongoing process (by the same user on the same NAS and port).

In RADIUS, the same functionality can be achieved through the inclusion or omission of the State attribute. Translation rules in [NASREQ] ensure that an Access-Request without the State attribute maps to a new Diameter Session-Id AVP value. Furthermore, a translation agent will always include a State attribute in Access-Challenge messages, making sure that the State attribute is available for a RADIUS NAS.

3. Command-Codes

This section defines new Command-Code values that MUST be supported by all Diameter implementations conforming to this specification. The following commands are defined in this section:

Command-Name	Abbrev.	Code	Reference
Diameter-EAP-Request	DER	268	3.1
Diameter-EAP-Answer	DEA	268	3.2

When the NASREQ AA-Request (AAR) or AA-Answer (AAA) commands are used for AUTHORIZE_ONLY messages in conjunction with EAP (see Section 2.3.3), an Application Identifier value of 1 (NASREQ) is used, and the commands follow the rules and ABNF defined in [NASREQ].

When the Re-Auth-Request (RAR), Re-Auth-Answer (RAA), Session-Termination-Request (STR), Session-Termination-Answer (STA), Abort-Session-Request (ASR), Abort-Session-Answer (ASA), Accounting-Request (ACR), and Accounting-Answer (ACA) commands are used together with the Diameter EAP application, they follow the rules in [NASREQ] and [BASE]. The accounting commands use Application Identifier value of 3 (Diameter Base Accounting); the others use 0 (Diameter Common Messages).

3.1. Diameter-EAP-Request (DER) Command

The Diameter-EAP-Request (DER) command, indicated by the Command-Code field set to 268 and the 'R' bit set in the Command Flags field, is sent by a Diameter client to a Diameter server, and conveys an EAP-Response from the EAP client. The Diameter-EAP-Request MUST contain one EAP-Payload AVP containing the actual EAP payload. An EAP-Payload AVP with no data MAY be sent to the Diameter server to initiate an EAP authentication session.

The DER message MAY be the result of a multi-round authentication exchange that occurs when the DEA is received with the Result-Code AVP set to DIAMETER_MULTI_ROUND_AUTH [BASE]. A subsequent DER message MUST include any State AVPs [NASREQ] that were present in the DEA. For re-authentication, it is recommended that the Identity request be skipped in order to reduce the number of authentication round trips. This is only possible when the user's identity is already known by the home Diameter server.

Message format

```
<Diameter-EAP-Request> ::= < Diameter Header: 268, REQ, PXY >
                             < Session-Id >
                             { Auth-Application-Id }
                             { Origin-Host }
                             { Origin-Realm }
                             { Destination-Realm }
                             { Auth-Request-Type }
                             [ Destination-Host ]
```

```

    [ NAS-Identifier ]
    [ NAS-IP-Address ]
    [ NAS-IPv6-Address ]
    [ NAS-Port ]
    [ NAS-Port-Id ]
    [ NAS-Port-Type ]
    [ Origin-State-Id ]
    [ Port-Limit ]
    [ User-Name ]
    { EAP-Payload }
    [ EAP-Key-Name ]
    [ Service-Type ]
    [ State ]
    [ Authorization-Lifetime ]
    [ Auth-Grace-Period ]
    [ Auth-Session-State ]
    [ Callback-Number ]
    [ Called-Station-Id ]
    [ Calling-Station-Id ]
    [ Originating-Line-Info ]
    [ Connect-Info ]
*   [ Framed-Compression ]
    [ Framed-Interface-Id ]
    [ Framed-IP-Address ]
*   [ Framed-IPv6-Prefix ]
    [ Framed-IP-Netmask ]
    [ Framed-MTU ]
    [ Framed-Protocol ]
*   [ Tunneling ]
*   [ Proxy-Info ]
*   [ Route-Record ]
*   [ AVP ]

```

3.2. Diameter-EAP-Answer (DEA) Command

The Diameter-EAP-Answer (DEA) message, indicated by the Command-Code field set to 268 and the 'R' bit cleared in the Command Flags field, is sent by the Diameter server to the client for one of the following reasons:

1. The message is part of a multi-round authentication exchange, and the server is expecting a subsequent Diameter-EAP-Request. This is indicated by setting the Result-Code to `DIAMETER_MULTI_ROUND_AUTH`, and MAY include zero or more State AVPs.

2. The EAP client has been successfully authenticated and authorized, in which case the message MUST include the Result-Code AVP indicating success, and SHOULD include an EAP-Payload of type EAP-Success. This event MUST cause the access device to provide service to the EAP client.
3. The EAP client has not been successfully authenticated and/or authorized, and the Result-Code AVP is set to indicate failure. This message SHOULD include an EAP-Payload, but this AVP is not used to determine whether service is to be provided.

If the message from the Diameter client included a request for authorization, a successful response MUST include the authorization AVPs that are relevant to the service being provided.

Message format

```
<Diameter-EAP-Answer> ::= < Diameter Header: 268, PXY >
    < Session-Id >
    { Auth-Application-Id }
    { Auth-Request-Type }
    { Result-Code }
    { Origin-Host }
    { Origin-Realm }
    [ User-Name ]
    [ EAP-Payload ]
    [ EAP-Reissued-Payload ]
    [ EAP-Master-Session-Key ]
    [ EAP-Key-Name ]
    [ Multi-Round-Time-Out ]
    [ Accounting-EAP-Auth-Method ]
    [ Service-Type ]
    * [ Class ]
    * [ Configuration-Token ]
    [ Acct-Interim-Interval ]
    [ Error-Message ]
    [ Error-Reporting-Host ]
    * [ Failed-AVP ]
    [ Idle-Timeout ]
    [ Authorization-Lifetime ]
    [ Auth-Grace-Period ]
    [ Auth-Session-State ]
    [ Re-Auth-Request-Type ]
    [ Session-Timeout ]
    [ State ]
    * [ Reply-Message ]
    [ Origin-State-Id ]
    * [ Filter-Id ]
```

```

    [ Port-Limit ]
    [ Callback-Id ]
    [ Callback-Number ]
    [ Framed-Appletalk-Link ]
  * [ Framed-Appletalk-Network ]
    [ Framed-Appletalk-Zone ]
  * [ Framed-Compression ]
    [ Framed-Interface-Id ]
    [ Framed-IP-Address ]
  * [ Framed-IPv6-Prefix ]
    [ Framed-IPv6-Pool ]
  * [ Framed-IPv6-Route ]
    [ Framed-IP-Netmask ]
  * [ Framed-Route ]
    [ Framed-Pool ]
    [ Framed-IPX-Network ]
    [ Framed-MTU ]
    [ Framed-Protocol ]
    [ Framed-Routing ]
  * [ NAS-Filter-Rule ]
  * [ QoS-Filter-Rule ]
  * [ Tunneling ]
  * [ Redirect-Host ]
    [ Redirect-Host-Usage ]
    [ Redirect-Max-Cache-Time ]
  * [ Proxy-Info ]
  * [ AVP ]

```

4. Attribute-Value Pairs

This section both defines new AVPs, unique to the EAP Diameter application and describes the usage of AVPs defined elsewhere (if that usage in the EAP application is noteworthy).

4.1. New AVPs

4.1.1. EAP-Payload AVP

The EAP-Payload AVP (AVP Code 462) is of type OctetString and is used to encapsulate the actual EAP packet that is being exchanged between the EAP client and the home Diameter server.

4.1.2. EAP-Reissued-Payload AVP

The EAP-Reissued-Payload AVP (AVP Code 463) is of type OctetString. The use of this AVP is described in Section 2.4.

4.1.3. EAP-Master-Session-Key AVP

The EAP-Master-Session-Key AVP (AVP Code 464) is of type OctetString. It contains keying material for protecting the communications between the user and the NAS. Exactly how this keying material is used depends on the link layer in question, and is beyond the scope of this document.

4.1.4. EAP-Key-Name AVP

The EAP-Key-Name AVP (Radius Attribute Type 102) is of type OctetString. It contains an opaque key identifier (name) generated by the EAP method. Exactly how this name is used depends on the link layer in question, and is beyond the scope of this document (see [EAPKey] for more discussion).

Note that not all link layers use this name, and currently most EAP methods do not generate it. Since the NAS operates in pass-through mode, it cannot know the Key-Name before receiving it from the AAA server. As a result, a Key-Name AVP sent in a Diameter-EAP-Request MUST NOT contain any data. A home Diameter server receiving a Diameter-EAP-Request with a Key-Name AVP with non-empty data MUST silently discard the AVP. In addition, the home Diameter server SHOULD include this AVP in Diameter-EAP-Response only if an empty EAP-Key-Name AVP was present in Diameter-EAP-Request.

4.1.5. Accounting-EAP-Auth-Method AVP

The Accounting-EAP-Auth-Method AVP (AVP Code 465) is of type Unsigned64. In case of expanded types [EAP, Section 5.7], this AVP contains the value $((\text{Vendor-Id} * 2^{32}) + \text{Vendor-Type})$.

The use of this AVP is described in Section 2.7.

5. AVP Occurrence Tables

The following tables use these symbols:

- 0 The AVP MUST NOT be present in the message
- 0+ Zero or more instances of the AVP MAY be present in the message
- 0-1 Zero or one instance of the AVP MAY be present in the message
- 1 One instance of the AVP MUST be present in the message

Note that AVPs that can only be present within a Grouped AVP are not represented in these tables.

5.1. EAP Command AVP Table

The following table lists the AVPs that may be present in the DER and DEA Commands, as defined in this document; the AVPs listed are defined both here and in [NASREQ].

Attribute Name	Command-Code	
	DER	DEA
Accounting-EAP-Auth-Method	0	0+
Acct-Interim-Interval [BASE]	0	0-1
Auth-Application-Id [BASE]	1	1
Auth-Grace-Period [BASE]	0-1	0-1
Auth-Request-Type [BASE]	1	1
Auth-Session-State [BASE]	0-1	0-1
Authorization-Lifetime [BASE]	0-1	0-1
Callback-Id [NASREQ]	0	0-1
Callback-Number [NASREQ]	0-1	0-1
Called-Station-Id [NASREQ]	0-1	0
Calling-Station-Id [NASREQ]	0-1	0
Class [BASE]	0	0+
Configuration-Token [NASREQ]	0	0+
Connect-Info [NASREQ]	0-1	0
Destination-Host [BASE]	0-1	0
Destination-Realm [BASE]	1	0
EAP-Master-Session-Key	0	0-1
EAP-Key-Name	0-1	0-1
EAP-Payload	1	0-1
EAP-Reissued-Payload	0	0-1
Error-Message [BASE]	0	0-1
Error-Reporting-Host [BASE]	0	0-1
Failed-AVP [BASE]	0	0+
Filter-Id [NASREQ]	0	0+
Framed-Appletalk-Link [NASREQ]	0	0-1
Framed-Appletalk-Network [NASREQ]	0	0+
Framed-Appletalk-Zone [NASREQ]	0	0-1
Framed-Compression [NASREQ]	0+	0+
Framed-Interface-Id [NASREQ]	0-1	0-1
Framed-IP-Address [NASREQ]	0-1	0-1
Framed-IP-Netmask [NASREQ]	0-1	0-1
Framed-IPv6-Prefix [NASREQ]	0+	0+
Framed-IPv6-Pool [NASREQ]	0	0-1
Framed-IPv6-Route [NASREQ]	0	0+
Framed-IPX-Network [NASREQ]	0	0-1
Framed-MTU [NASREQ]	0-1	0-1
Framed-Pool [NASREQ]	0	0-1

Framed-Protocol [NASREQ]	0-1	0-1
Framed-Route [NASREQ]	0	0+
Framed-Routing [NASREQ]	0	0-1
Idle-Timeout [NASREQ]	0	0-1
Multi-Round-Time-Out [BASE]	0	0-1
NAS-Filter-Rule [NASREQ]	0	0+
NAS-Identifier [NASREQ]	0-1	0
NAS-IP-Address [NASREQ]	0-1	0
NAS-IPv6-Address [NASREQ]	0-1	0
NAS-Port [NASREQ]	0-1	0
NAS-Port-Id [NASREQ]	0-1	0
NAS-Port-Type [NASREQ]	0-1	0
Originating-Line-Info [NASREQ]	0-1	0
Origin-Host [BASE]	1	1
Origin-Realm [BASE]	1	1
Origin-State-Id [BASE]	0-1	0-1
Port-Limit [NASREQ]	0-1	0-1
Proxy-Info [BASE]	0+	0+
QoS-Filter-Rule [NASREQ]	0	0+
Re-Auth-Request-Type [BASE]	0	0-1
Redirect-Host [BASE]	0	0+
Redirect-Host-Usage [BASE]	0	0-1
Redirect-Max-Cache-Time [BASE]	0	0-1
Reply-Message [NASREQ]	0	0+
Result-Code [BASE]	0	1
Route-Record [BASE]	0+	0+
Service-Type [NASREQ]	0-1	0-1
Session-Id [BASE]	1	1
Session-Timeout [BASE]	0	0-1
State [NASREQ]	0-1	0-1
Tunneling [NASREQ]	0+	0+
User-Name [BASE]	0-1	0-1

5.2. Accounting AVP Table

The table in this section is used to represent which AVPs defined in this document are to be present in the Accounting messages, as defined in [BASE].

Attribute Name	Command Code	
	ACR	ACA
Accounting-EAP-Auth-Method	0+	0

6. RADIUS/Diameter Interactions

Section 9 of [NASREQ] describes basic guidelines for translation agents that translate between RADIUS and Diameter protocols. These guidelines SHOULD be followed for Diameter EAP application as well, with some additional guidelines given in this section. Note that this document does not restrict implementations from creating additional methods, as long as the translation function does not violate the RADIUS or the Diameter protocols.

6.1. RADIUS Request Forwarded as Diameter Request

RADIUS Access-Request to Diameter-EAP-Request:

- o RADIUS EAP-Message attribute(s) are translated to a Diameter EAP-Payload AVP. If multiple RADIUS EAP-Message attributes are present, they are concatenated and translated to a single Diameter EAP-Payload AVP.
- o An empty RADIUS EAP-Message attribute (with length 2) signifies EAP-Start, and it is translated to an empty EAP-Payload AVP.

Diameter-EAP-Answer to RADIUS Access-Accept/Reject/Challenge:

- o Diameter EAP-Payload AVP is translated to RADIUS EAP-Message attribute(s). If necessary, the value is split into multiple RADIUS EAP-Message attributes.
- o Diameter EAP-Reissued-Payload AVP is translated to a message that contains RADIUS EAP-Message attribute(s), and a RADIUS Error-Cause attribute [RFC3576] with value 202 (decimal), "Invalid EAP Packet (Ignored)" [RFC3579].
- o As described in [NASREQ], if the Result-Code AVP set to `DIAMETER_MULTI_ROUND_AUTH` and the Multi-Round-Time-Out AVP is present, it is translated to the RADIUS Session-Timeout attribute.
- o Diameter EAP-Master-Session-Key AVP can be translated to the vendor-specific RADIUS MS-MPPE-Recv-Key and MS-MPPE-Send-Key attributes [RFC2548]. The first up to 32 octets of the key is stored into MS-MPPE-Recv-Key, and the next up to 32 octets (if present) are stored into MS-MPPE-Send-Key. The encryption of this attribute is described in [RFC2548].
- o Diameter Accounting-EAP-Auth-Method AVPs, if present, are discarded.

6.2. Diameter Request Forwarded as RADIUS Request

Diameter-EAP-Request to RADIUS Access-Request:

- o The Diameter EAP-Payload AVP is translated to RADIUS EAP-Message attribute(s).
- o An empty Diameter EAP-Payload AVP signifies EAP-Start, and is translated to an empty RADIUS EAP-Message attribute.
- o The type (or expanded type) field from the EAP-Payload AVP can be saved either in a local state table, or encoded in a RADIUS Proxy-State attribute. This information is needed to construct an Accounting-EAP-Auth-Method AVP for the answer message (see below).

RADIUS Access-Accept/Reject/Challenge to Diameter-EAP-Answer:

- o If the RADIUS Access-Challenge message does not contain an Error-Cause attribute [RFC3576] with value 202 (decimal), "Invalid EAP Packet (Ignored)" [RFC3579], any RADIUS EAP-Message attributes are translated to a Diameter EAP-Payload AVP, concatenating them if multiple attributes are present.
- o If the Error-Cause attribute with value 202 is present, any RADIUS EAP-Message attributes are translated to a Diameter EAP-Reissued-Payload AVP, concatenating them if multiple attributes are present.
- o As described in [NASREQ], if the Session-Timeout attribute is present in a RADIUS Access-Challenge message, it is translated to the Diameter Multi-Round-Time-Out AVP.
- o If the vendor-specific RADIUS MS-MPPE-Recv-Key and/or MS-MPPE-Send-Key attributes [RFC2548] are present, they can be translated to a Diameter EAP-Master-Session-Key AVP. The attributes have to be decrypted before conversion, and the Salt, Key-Length and Padding sub-fields are discarded. The Key sub-fields are concatenated (MS-MPPE-Recv-Key first, MS-MPPE-Send-Key next), and the concatenated value is stored into a Diameter EAP-Master-Session-Key AVP.
- o If the Diameter-EAP-Answer will have a successful result code, the saved state (see above) can be used to construct an Accounting-EAP-Auth-Method AVP.

6.3. Accounting Requests

In Accounting-Requests, the vendor-specific RADIUS MS-Acct-EAP-Type attribute [RFC2548] can be translated to a Diameter Accounting-EAP-Auth-Method AVP, and vice versa.

When translating from Diameter to RADIUS, note that the MS-Acct-EAP-Type attribute does not support expanded EAP types. Type values greater than 255 should be translated to type 254.

7. IANA Considerations

This document does not create any new namespaces to be maintained by IANA, but it requires new values in namespaces that have been defined in the Diameter Base protocol and RADIUS specifications.

- o This document defines one new Diameter command (in Section 3) whose Command Code is allocated from the Command Code namespace defined in [BASE]. The Command Code for DER / DEA is 268.
- o This document defines four new AVPs whose AVP Codes are allocated from the AVP Code namespace defined in [BASE] as follows:
 - 462 for EAP-Payload (defined in Section 4.1.1),
 - 463 for EAP-Reissued-Payload (defined in Section 4.1.2),
 - 464 for EAP-Master-Session-Key (defined in Section 4.1.3), and
 - 465 for Accounting-EAP-Auth-Method (defined in Section 4.1.5).
- o This document defines one new AVP (attribute) whose AVP Code (Attribute Type) is to be allocated from the Attribute Type namespace defined in [RFC2865] and [RFC3575]. The Radius Attribute Type for EAP-Key-Name (defined in Section 4.1.4) is 102.
- o This document defines one new Diameter application (in Section 2.1) whose Application ID is to be allocated from the Application Identifier namespace defined in [BASE]. The Application ID for Diameter EAP is 5.

8. Security Considerations

8.1. Overview

Diameter peer-to-peer connections can be protected with IPsec or TLS. These mechanisms are believed to provide sufficient protection under the normal Internet threat model, that is, assuming the authorized nodes engaging in the protocol have not been compromised, but the attacker has complete control over the communication channels between them. This includes eavesdropping, message modification, insertion,

man-in-the-middle and replay attacks. The details and related security considerations are discussed in [BASE].

In addition to authentication provided by IPsec or TLS, authorization is also required. Here, authorization means determining if a Diameter message received from an authenticated Diameter peer should be accepted (and not authorization of users requesting network access from a NAS). In other words, when a Diameter server receives a Diameter-EAP-Request, it has to decide if the client is authorized to act as a NAS for the specific user, service type, and so on. Correspondingly, when a NAS contacts a server to send a Diameter-EAP-Request, it has to determine whether the server is authorized to act as home server for the realm in question.

Authorization can involve local Access Control Lists (ACLs), information contained in certificates, or some other means. See [BASE] for more discussion and related security considerations. Note that authorization issues are particularly relevant when Diameter redirects are used. While redirection reduces the number of nodes which have access to the contents of Diameter messages, a compromised Diameter agent may not supply the right home server's address. If the Diameter client is unable to tell whether this particular server is authorized to act as the home server for this particular user, the security of the communications rests on the redirect agent.

The hop-by-hop security mechanisms (IPsec and TLS) combined with proper authorization provide good protection against "outside" attackers, except for denial-of-service attacks. The remaining part of this section deals with attacks by nodes that have been properly authorized (to function as a NAS, Diameter agent, or Diameter server), but abuse their authorization or have been compromised. In general, it is not possible to completely protect against attacks by compromised nodes, but this section offers advice on limiting the extent of the damage.

Attacks involving eavesdropping or modification of EAP messages are beyond the scope of these document. See [EAP] for discussion of these security considerations (including method negotiation, dictionary attacks, and privacy issues). While these attacks can be carried out by an attacker between the client and the NAS, compromised NASes and Diameter agents are naturally also in a good position to modify and eavesdrop on the EAP messages.

Similarly, attacks involving the link layer protocol used between the client and the NAS, such as PPP or IEEE 802.11, are beyond the scope of this document.

8.2. AVP Editing

Diameter agents can modify, insert, and delete AVPs. Diameter agents are usually meant to modify AVPs, and the protocol cannot distinguish well-intentioned and malicious modifications (see [RFC2607] for more discussion). Similarly, a compromised NAS or server can naturally include a different set of AVPs than expected.

Therefore, the question is what an attacker who compromises an authorized NAS, agent, or server can do using Diameter EAP messages. Some of the consequences are rather obvious. For instance, a Diameter agent can give access to unauthorized users by changing the Result-Code to DIAMETER_SUCCESS. Other consequences are less obvious and are discussed below and authentication method negotiation attacks are discussed in the next section.

By including suitable AVPs in an AA-Answer/Diameter-EAP-Answer messages, an attacker may be able (depending on implementation and configuration details) to:

- o Give unauthorized users access, or deny access to authorized users (Result-Code).
- o Give an attacker a login session to a host otherwise protected by firewalls, or redirect an authorized user's login session to a host controlled by the attacker (Login-Host).
- o Route an authorized user's traffic through a host controlled by the attacker (various tunneling AVPs).
- o Redirect an authorized user's DNS requests to a malicious DNS server (various vendor-specific AVPs).
- o Modify routing tables at the NAS and thus redirect packets destined for someone else (Framed-Route, Framed-Routing).
- o Remove packet filters and other restrictions for user (Filter, Callback, various vendor-specific AVPs).
- o Cause the NAS to call some number, possibly an expensive toll number controlled by the attacker (callback AVPs).
- o Execute Command Line Interface (CLI) commands on the NAS (various vendor-specific attributes).

By modifying an AA-Request/Diameter-EAP-Request, an attacker may be able to:

- o Change NAS-Identifier/NAS-Port/Origin-Host (or another attribute) so that a valid user appears to be accessing the network from a different NAS than in reality.
- o Modify Calling-Station-ID (either to hide the true value, gain access, or frame someone else).
- o Modify password change messages (some vendor-specific attributes).
- o Modify usage information in accounting messages.
- o Modify contents of Class and State AVPs.

Some of these attacks can be prevented if the NAS or server is configured to not accept some particular AVPs, or accepts them only from some nodes.

8.3. Negotiation Attacks

This section deals with attacks where the NAS, any Diameter agents, or Diameter server attempt to cause the authenticating user to choose some authentication method other than EAP, such as PAP or CHAP (negotiation attacks within EAP are discussed in [EAP], Section 7.8).

The vulnerability can be mitigated via implementation of a per-connection policy by the authenticating peer, and a per-user policy by the Diameter server. For the authenticating peer, the authentication policy should be set on a per-connection basis.

With a per-connection policy, an authenticating peer will only attempt to negotiate EAP for a session in which EAP support is expected. As a result, it is presumed that an authenticating peer selecting EAP requires that level of security. If it cannot be provided, there is likely a misconfiguration, or the authenticating peer may be contacting the wrong server. In this case, the authenticating peer simply disconnects.

Similarly, with a per-user policy, the home server will not accept authentication methods other than EAP for users for which EAP support is expected.

For a NAS, it may not be possible to determine whether a peer is required to authenticate with EAP until the peer's identity is known. For example, for shared-uses NASes one reseller may implement EAP while another does not. Alternatively, some peer might be

authenticated locally by the NAS while other peers are authenticated via Diameter. In such cases, if any peers of the NAS MUST do EAP, then the NAS MUST attempt to negotiate EAP for every session. This avoids forcing a peer to support more than one authentication type, which could weaken security.

8.4. Session Key Distribution

Since there are currently no end-to-end (NAS-to-home server) security mechanisms specified for Diameter, any agents that process Diameter-EAP-Answer messages can see the contents of the EAP-Master-Session-Key AVP. For this reason, this specification strongly recommends avoiding Diameter agents when they cannot be trusted to keep the keys secret.

In environments where agents are present, several factors should be considered when deciding whether the agents that are authorized (and considered "trustworthy enough") to grant access to users and specify various authorization and tunneling AVPs are also "trustworthy enough" to handle the session keys. These factors include (but are not limited to) the type of access provided (e.g., public Internet or corporate internet), security level of the agents, and the possibilities for attacking user's traffic after it has been decrypted by the NAS.

Note that the keys communicated in Diameter messages are usually short-term session keys (or short-term master keys that are used to derive session keys). To actually cause any damage, those session keys must end up with some malicious party that must be able to eavesdrop, modify, or insert traffic between the user and the NAS during the lifetime of those keys (for example, in 802.11i the attacker must also eavesdrop the "four-way handshake").

8.5. Privacy Issues

Diameter messages can contain AVPs that can be used to identify the user (e.g., User-Name) and approximate location of the user (e.g., Origin-Host for WLAN access points, Calling-Station-Id for fixed phone lines). Thus, any Diameter nodes that process the messages may be able to determine the geographic location of users.

Note that in many cases, the user identity is also sent in clear inside EAP-Payload AVPs, and it may be possible to eavesdrop this between the user and the NAS.

This can be mitigated somewhat by using EAP methods that provide identity protection (see [EAP], Section 7.3), and using Session-Id or pseudonyms for accounting.

8.6. Note about EAP and Impersonation

If the EAP method used does not provide mutual authentication, obviously anyone can impersonate the network to the user. Even when EAP mutual authentication is used, it occurs between the user and the Diameter home server. See [EAPKey] for an extensive discussion about the details and their implications.

One issue is worth pointing out here. As described in [EAPKey], the current EAP architecture does not allow the home server to restrict what service parameters or identities (such as SSID or BSSID in 802.11 wireless LANs) are advertised by the NAS to the client. That is, a compromised NAS can change its BSSID or SSID, and thus appear to offer a different service than intended. Even if these parameters are included in Diameter-EAP-Answer messages, the NAS can tell different values to the client.

Therefore, the NAS's possession of the session keys proves that the user is talking to an authorized NAS, but a compromised NAS can lie about its exact identity. See [EAPKey] for discussion on how individual EAP methods can provide authentication of NAS service parameters and identities.

Note that the usefulness of this authentication may be rather limited in many environments. For instance, in wireless LANs the user does not usually securely know the identity (such as BSSID) of the "right" access point; it is simply picked from a beacon message that has the correct SSID and good signal strength (something that is easy to spoof). Thus, simply authenticating the identity may not allow the user to distinguish the "right" access point from all others.

9. Acknowledgements

This Diameter application relies heavily on earlier work on Diameter NASREQ application [NASREQ] and RADIUS EAP support [RFC3579]. Much of the material in this specification has been copied from these documents.

The authors would also like to acknowledge the following people for their contributions to this document: Bernard Aboba, Jari Arkko, Julien Bournelle, Pat Calhoun, Henry Haverinen, John Loughney, Yoshihiro Ohba, and Joseph Salowey.

10. References

10.1. Normative References

- [BASE] Calhoun, P., Loughney, J., Guttman, E., Zorn, G., and J. Arkko, "Diameter Base Protocol", RFC 3588, September 2003.
- [EAP] Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., and H. Levkowitz, "Extensible Authentication Protocol (EAP)", RFC 3748, June 2004.
- [NASREQ] Calhoun, P., Zorn, G., Spence, D., and D. Mitton, "Diameter Network Access Server Application", RFC 4005, August 2005.
- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

10.2. Informative References

- [EAPKey] Aboba, B., Simon, D., Arkko, J., Eronen, P., and H. Levkowitz, "Extensible Authentication Protocol (EAP) Key Management Framework", Work in Progress, July 2004.
- [IEEE-802.1X] Institute of Electrical and Electronics Engineers, "Local and Metropolitan Area Networks: Port-Based Network Access Control", IEEE Standard 802.1X, September 2001.
- [IEEE-802.11i] Institute of Electrical and Electronics Engineers, "IEEE Standard for Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements - Part 11: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Amendment 6: Medium Access Control (MAC) Security Enhancements", IEEE Standard 802.11i-2004, July 2004.
- [IKEv2] Kaufman, C., Ed., "Internet Key Exchange (IKEv2) Protocol", Work in Progress, June 2004.
- [RFC1661] Simpson, W., "The Point-to-Point Protocol (PPP)", STD 51, RFC 1661, July 1994.

- [RFC2548] Zorn, G., "Microsoft Vendor-specific RADIUS Attributes", RFC 2548, March 1999.
- [RFC2607] Aboba, B. and J. Vollbrecht, "Proxy Chaining and Policy Implementation in Roaming", RFC 2607, June 1999.
- [RFC2865] Rigney, C., Willens, S., Rubens, A., and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)", RFC 2865, June 2000.
- [RFC3575] Aboba, B., "IANA Considerations for RADIUS (Remote Authentication Dial In User Service)", RFC 3575, July 2003.
- [RFC3576] Chiba, M., Dommety, G., Eklund, M., Mitton, D., and B. Aboba, "Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)", RFC 3576, July 2003.
- [RFC3579] Aboba, B. and P. Calhoun, "RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP)", RFC 3579, September 2003.
- [RFC3580] Congdon, P., Aboba, B., Smith, A., Zorn, G., and J. Roese, "IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines", RFC 3580, September 2003.

Authors' Addresses

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

EMail: pasi.eronen@nokia.com

Tom Hiller
Lucent Technologies
1960 Lucent Lane
Naperville, IL 60566
USA

Phone: +1 630 979 7673
EMail: tomhiller@lucent.com

Glen Zorn
Cisco Systems
500 108th Avenue N.E., Suite 500
Bellevue, WA 98004
USA

Phone: +1 425 344 8113
EMail: gwz@cisco.com

Full Copyright Statement

Copyright (C) The Internet Society (2005).

This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM 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.

Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights 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; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat 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 implementers or users of this specification can be obtained from the IETF on-line IPR repository at <http://www.ietf.org/ipr>.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Acknowledgement

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

