Network Working Group
Request for Comments: 3579
Updates: 2869
Category: Informational

B. Aboba
Microsoft
P. Calhoun
Airespace

September 2003

RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP)

Status of this Memo

Copyright Notice

Abstract

This document defines Remote Authentication Dial In User Service (RADIUS) support for the Extensible Authentication Protocol (EAP), an authentication framework which supports multiple authentication mechanisms. In the proposed scheme, the Network Access Server (NAS) forwards EAP packets to and from the RADIUS server, encapsulated within EAP-Message attributes. This has the advantage of allowing the NAS to support any EAP authentication method, without the need for method-specific code, which resides on the RADIUS server. While EAP was originally developed for use with PPP, it is now also in use with IEEE 802.

This document updates RFC 2869.

Table of Contents

1. Introduction

The Remote Authentication Dial In User Service (RADIUS) is an authentication, authorization and accounting protocol used to control network access. RADIUS authentication and authorization is specified in [RFC2865], and RADIUS accounting is specified in [RFC2866]; RADIUS over IPv6 is specified in [RFC3162].

The Extensible Authentication Protocol (EAP), defined in [RFC2284], 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]. It has also been implemented with bridges supporting [IEEE802]. EAP encapsulation on IEEE 802 wired media is described in [IEEE8021X].

RADIUS attributes are comprised of variable length Type-Length-Value 3-tuples. New attribute values can be added without disturbing existing implementations of the protocol. This specification describes RADIUS attributes supporting the Extensible Authentication Protocol (EAP): EAP-Message and Message-Authenticator. These attributes now have extensive field experience. The purpose of this document is to provide clarification and resolve interoperability issues.

As noted in [RFC2865], a Network Access Server (NAS) that does not implement a given service MUST NOT implement the RADIUS attributes for that service. This implies that a NAS that is unable to offer EAP service MUST NOT implement the RADIUS attributes for EAP. A NAS MUST treat a RADIUS Access-Accept requesting an unavailable service as an Access-Reject instead.

1.1. Specification of Requirements

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].

1.2. Terminology

This document frequently uses the following terms:

authenticator
: The end of the link requiring the authentication. Also known as the Network Access Server (NAS) or RADIUS client. Within IEEE 802.1X terminology, the term Authenticator is used.

peer
: The other end of the point-to-point link (PPP), point-to-point LAN segment (IEEE 802.1X) or wireless link, which is being authenticated by the authenticator. In IEEE 802.1X, this end is known as the Supplicant.

authentication server
: An authentication server is an entity that provides an authentication service to an authenticator (NAS). This service verifies from the credentials provided by the peer, the claim of identity made by the peer; it also may provide credentials allowing the peer to verify the identity of the authentication server. Within this document it is assumed that the NAS operates as a pass-through, forwarding EAP packets between the RADIUS server and the EAP peer.

Therefore the RADIUS server operates as an authentication server.

silently discard
: This means the implementation discards the packet without further processing. The implementation SHOULD provide the capability of logging the error, including the contents of the silently discarded packet, and SHOULD record the event in a statistics counter.

displayable message
: This is interpreted to be a human readable string of characters, and MUST NOT affect operation of the protocol. The message encoding MUST follow the UTF-8 transformation format [RFC2279].

Network Access Server (NAS)
: The device providing access to the network. Also known as the Authenticator (IEEE 802.1X or EAP terminology) or RADIUS client.

service
: The NAS provides a service to the user, such as IEEE 802 or PPP.

session
: Each service provided by the NAS to a peer constitutes a session, with the beginning of the session defined as the point where service is first provided and the end of the session defined as the point where service is ended. A peer may have multiple sessions in parallel or series if the NAS supports that, with each session generating a separate start and stop accounting record.

2. RADIUS Support for EAP

The Extensible Authentication Protocol (EAP), described in [RFC2284], provides a standard mechanism for support of additional authentication methods without the NAS to be upgraded to support each new method. Through the use of EAP, support for a number of authentication schemes may be added, including smart cards, Kerberos [RFC1510], Public Key [RFC2716], One Time Passwords [RFC2284], and others.

One of the advantages of the EAP architecture is its flexibility. EAP is used to select a specific authentication mechanism. Rather than requiring the NAS to be updated to support each new authentication method, EAP permits the use of an authentication server implementing authentication methods, with the NAS acting as a pass-through for some or all methods and peers.

A NAS MAY authenticate local peers while at the same time acting as a pass-through for non-local peers and authentication methods it does not implement locally. A NAS implementing this specification is not required to use RADIUS to authenticate every peer. However, once the NAS begins acting as a pass-through for a particular session, it can no longer perform local authentication for that session.

In order to support EAP within RADIUS, two new attributes, EAP-Message and Message-Authenticator, are introduced in this document. This section describes how these new attributes may be used for providing EAP support within RADIUS.

2.1. Protocol Overview

In RADIUS/EAP, RADIUS is used to shuttle RADIUS-encapsulated EAP Packets between the NAS and an authentication server.

The authenticating peer and the NAS begin the EAP conversation by negotiating use of EAP. Once EAP has been negotiated, the NAS SHOULD send an initial EAP-Request message to the authenticating peer. This will typically be an EAP-Request/Identity, although it could be an EAP-Request for an authentication method (Types 4 and greater). A NAS MAY be configured to initiate with a default authentication method. This is useful in cases where the identity is determined by another means (such as Called-Station-Id, Calling-Station-Id and/or Originating-Line-Info); where a single authentication method is required, which includes its own identity exchange; where identity hiding is desired, so that the identity is not requested until after a protected channel has been set up.

The peer replies with an EAP-Response. The NAS MAY determine from the Response that it should proceed with local authentication. Alternatively, the NAS MAY act as a pass-through, encapsulating the EAP-Response within EAP-Message attribute(s) sent to the RADIUS server within a RADIUS Access-Request packet. If the NAS sends an EAP-Request/Identity message as the initial packet, the peer responds with an EAP-Response/Identity. The NAS may determine that the peer is local and proceed with local authentication. If no match is found against the list of local users, the NAS encapsulates the EAP-Response/Identity message within an EAP-Message attribute, enclosed within an Access-Request packet.

On receiving a valid Access-Request packet containing EAP-Message attribute(s), a RADIUS server compliant with this specification and wishing to authenticate with EAP MUST respond with an Access-Challenge packet containing EAP-Message attribute(s). If the RADIUS server does not support EAP or does not wish to authenticate with EAP, it MUST respond with an Access-Reject.

EAP-Message attribute(s) encapsulate a single EAP packet which the NAS decapsulates and passes on to the authenticating peer. The peer then responds with an EAP-Response packet, which the NAS encapsulates within an Access-Request containing EAP-Message attribute(s). EAP is a 'lock step' protocol, so that other than the initial Request, a new Request cannot be sent prior to receiving a valid Response.

The conversation continues until either a RADIUS Access-Reject or Access-Accept packet is received from the RADIUS server. Reception of a RADIUS Access-Reject packet MUST result in the NAS denying access to the authenticating peer. A RADIUS Access-Accept packet successfully ends the authentication phase. The NAS MUST NOT "manufacture" a Success or Failure packet as the result of a timeout. After a suitable number of timeouts have elapsed, the NAS SHOULD instead end the EAP conversation.

Using RADIUS, the NAS can act as a pass-through for an EAP conversation between the peer and authentication server, without needing to implement the EAP method used between them. Where the NAS initiates the conversation by sending an EAP-Request for an authentication method, it may not be required that the NAS fully implement the EAP method reflected in the initial EAP-Request. Depending on the initial method, it may be sufficient for the NAS to be configured with the initial packet to be sent to the peer, and for the NAS to act as a pass-through for subsequent messages. Note that since the NAS only encapsulates the EAP-Response in its initial Access-Request, the initial EAP-Request within the authentication method is not available to the RADIUS server. For the RADIUS server to be able to continue the conversation, either the initial EAP-Request is vestigial, so that the RADIUS server need not be aware of it, or the relevant information from the initial EAP-Request (such as a nonce) is reflected in the initial EAP-Response, so that the RADIUS server can obtain it without having received the initial EAP-Request.

Where the initial EAP-Request sent by the NAS is for an authentication Type (4 or greater), the peer MAY respond with a Nak indicating that it would prefer another authentication method that is not implemented locally. In this case, the NAS SHOULD send Access-Request encapsulating the received EAP-Response/Nak. This provides the RADIUS server with a hint about the authentication method(s) preferred by the peer, although it does not provide information on the Type of the original Request. It also provides the server with the Identifier used in the initial EAP-Request, so that Identifier conflicts can be avoided.

In order to evaluate whether the alternatives preferred by the authenticating peer are allowed, the RADIUS server will typically respond with an Access-Challenge containing EAP-Message attribute(s) encapsulating an EAP-Request/Identity (Type 1). This allows the RADIUS server to determine the peer identity, so as to be able to retrieve the associated authentication policy. Alternatively, an EAP-Request for an authentication method (Type 4 or greater) could be sent. Since the RADIUS server may not be aware of the Type of the initial EAP-Request, it is possible for the RADIUS server to choose an unacceptable method, and for the peer to respond with another Nak.

In order to permit non-EAP aware RADIUS proxies to forward the Access-Request packet, if the NAS initially sends an EAP-Request/Identity message to the peer, the NAS MUST copy the contents of the Type-Data field of the EAP-Response/Identity received from the peer into the User-Name attribute and MUST include the Type-Data field of the EAP-Response/Identity in the User-Name attribute in every subsequent Access-Request. Since RADIUS proxies are assumed to act as a pass-through, they cannot be expected to parse an EAP-Response/Identity encapsulated within EAP-Message attribute(s). If the NAS initially sends an EAP-Request for an authentication method, and the peer identity cannot be determined from the EAP-Response, then the User-Name attribute SHOULD be determined by another means. As noted in [RFC2865] Section 5.6, it is recommended that Access-Requests use the value of the Calling-Station-Id as the value of the User-Name attribute.

Having the NAS send the initial EAP-Request packet has a number of advantages:

[1] It saves a round trip between the NAS and RADIUS server.

[2] An Access-Request is only sent to the RADIUS server if the authenticating peer sends an EAP-Response, confirming that it supports EAP. In situations where peers may be EAP unaware, initiating a RADIUS Access-Request on a "carrier sense" or "media up" indication may result in many authentication exchanges that cannot complete successfully. For example, on wired networks [IEEE8021X] Supplicants typically do not initiate the 802.1X conversation with an EAPOL-Start. Therefore an IEEE 802.1X-enabled bridge may not be able to determine whether the peer supports EAP until it receives a Response to the initial EAP-Request.

[3] It allows some peers to be authenticated locally.

Although having the NAS send the initial EAP-Request packet has substantial advantages, this technique cannot be universally employed. There are circumstances in which the peer identity is already known (such as when authentication and accounting is handled based on Called-Station-Id, Calling-Station-Id and/or Originating-Line-Info), but where the appropriate EAP method may vary based on that identity.

Rather than sending an initial EAP-Request packet to the authenticating peer, on detecting the presence of the peer, the NAS MAY send an Access-Request packet to the RADIUS server containing an EAP-Message attribute signifying EAP-Start. The RADIUS server will typically respond with an Access-Challenge containing EAP-Message attribute(s) encapsulating an EAP-Request/Identity (Type 1). However, an EAP-Request for an authentication method (Type 4 or greater) can also be sent by the server.

EAP-Start is indicated by sending an EAP-Message attribute with a length of 2 (no data). The Calling-Station-Id SHOULD be included in the User-Name attribute. This may result in a RADIUS Access-Request being sent by the NAS to the RADIUS server without first confirming that the peer supports EAP. Since this technique can result in a large number of uncompleted RADIUS conversations, in situations where EAP unaware peers are common, or where peer support for EAP cannot be determined on initial contact (e.g. [IEEE8021X] Supplicants not initiating the conversation with an EAPOL-Start) it SHOULD NOT be employed by default.

For proxied RADIUS requests, there are two methods of processing. If the domain is determined based on the Calling-Station-Id, Called-Station-Id and/or Originating-Line-Info, the RADIUS server may proxy the initial RADIUS Access-Request/EAP-Start. If the realm is determined based on the peer identity, the local RADIUS server MUST respond with a RADIUS Access-Challenge including an EAP-Message attribute encapsulating an EAP-Request/Identity packet. The response from the authenticating peer SHOULD be proxied to the final authentication server.

If an Access-Request is sent to a RADIUS server which does not support the EAP-Message attribute, then an Access-Reject MUST be sent in response. On receiving an Access-Reject, the NAS MUST deny access to the authenticating peer.

2.2. 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 RADIUS server. On receiving an EAP packet from the peer, the NAS checks the Code (2) and Length fields, and matches the Identifier value against the current Identifier, supplied by the RADIUS server in the most recently validated EAP-Request. On receiving an EAP packet from the RADIUS server (encapsulated within an Access-Challenge), the NAS checks the Code (1) 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 RADIUS server. A RADIUS server receiving EAP-Message attribute(s) it does not understand SHOULD make the determination of whether the error is fatal or non-fatal based on the EAP Type. A RADIUS server determining that a fatal error has occurred MUST send an Access-Reject containing an EAP-Message attribute encapsulating EAP-Failure.

A RADIUS server determining that a non-fatal error has occurred MAY send an Access-Challenge to the NAS including EAP-Message attribute(s) as well as an Error-Cause attribute [RFC3576] with value 202 (decimal), "Invalid EAP Packet (Ignored)". The Access-Challenge SHOULD encapsulate within EAP-Message attribute(s) the most recently sent EAP-Request packet (including the same Identifier value). On receiving such an Access-Challenge, a NAS implementing previous versions of this specification will decapsulate the EAP-Request and send it to the peer, which will retransmit the EAP-Response.

A NAS compliant with this specification, on receiving an Access-Challenge with an Error-Cause attribute of value 202 (decimal) SHOULD discard the EAP-Response packet most recently transmitted to the RADIUS server and check whether additional EAP-Response packets have been received matching the current Identifier value. If so, a new EAP-Response packet, if available, MUST be sent to the RADIUS server within an Access-Request, and the EAP-Message attribute(s) included within the Access-Challenge are silently discarded. If no EAP-Response packet is available, then the EAP-Request encapsulated within the Access-Challenge is sent 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 RADIUS server is advised to permit only a modest number of invalid EAP packets within a single session, prior to terminating the session with an Access-Reject. By default a value of 5 invalid EAP packets is recommended.

2.3. Retransmission

As noted in [RFC2284], 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 timeouts 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 RADIUS server. This can be accomplished by inclusion of Session-Timeout attribute within the Access-Challenge packet.

If Session-Timeout is present in an Access-Challenge packet that also contains an EAP-Message, the value of the Session-Timeout is used to set the EAP retransmission timer for that EAP Request, and that Request alone. Once the EAP-Request has been sent, the NAS sets the retransmission timer, and if it expires without having received an EAP-Response corresponding to the Request, then the EAP-Request is retransmitted.

2.4. Fragmentation

Using the EAP-Message attribute, it is possible for the RADIUS 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 RADIUS server to use MTU discovery to ascertain the link MTU, the Framed-MTU attribute may be included in an Access-Request packet containing an EAP-Message attribute so as to provide the RADIUS server with this information. A RADIUS server having received a Framed-MTU attribute in an Access-Request packet MUST NOT send any subsequent packet in this EAP conversation containing EAP-Message attributes whose values, when concatenated, exceed the length specified by the Framed-MTU value, taking the link type (specified by the NAS-Port-Type attribute) 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), Type (1) and Body Length (2) fields.

2.5. Alternative Uses

Currently the conversation between security servers and the RADIUS server is often proprietary because of lack of standardization. In order to increase standardization and provide interoperability between RADIUS vendors and security vendors, it is recommended that RADIUS- encapsulated EAP be used for this conversation.

This has the advantage of allowing the RADIUS server to support EAP without the need for authentication-specific code within the RADIUS server. Authentication-specific code can then reside on a security server instead.

In the case where RADIUS-encapsulated EAP is used in a conversation between a RADIUS server and a security server, the security server will typically return an Access-Accept message without inclusion of the expected attributes currently returned in an Access-Accept. This means that the RADIUS server MUST add these attributes prior to sending an Access-Accept message to the NAS.

2.6. Usage Guidelines

2.6.1. Identifier Space

In EAP, each session has its own unique Identifier space. RADIUS server implementations MUST be able to distinguish between EAP packets with the same Identifier existing within distinct sessions, originating on the same NAS. For this purpose, sessions can be distinguished based on NAS and session identification attributes. NAS identification attributes include NAS-Identifier, NAS-IPv6-Address and NAS-IPv4-Address. Session identification attributes include User-Name, NAS-Port, NAS-Port-Type, NAS-Port-Id, Called-Station-Id, Calling-Station-Id and Originating-Line-Info.

2.6.2. Role Reversal

Since EAP is a peer-to-peer protocol, an independent and simultaneous authentication may take place in the reverse direction. Both peers may act as authenticators and authenticatees at the same time.

However, role reversal is not supported by this specification. A RADIUS server MUST respond to an Access-Request encapsulating an EAP-Request with an Access-Reject. In order to avoid retransmissions

by the peer, the Access-Reject SHOULD include an EAP-Response/Nak packet indicating no preferred method, encapsulated within EAP-Message attribute(s).

2.6.3. Conflicting Messages

The NAS MUST make its access control decision based solely on the RADIUS Packet Type (Access-Accept/Access-Reject). The access control decision MUST NOT be based on the contents of the EAP packet encapsulated in one or more EAP-Message attributes, if present.

Access-Accept packets SHOULD have only one EAP-Message attribute in them, containing EAP Success; similarly, Access-Reject packets SHOULD have only one EAP-Message attribute in them, containing EAP Failure.

Where the encapsulated EAP packet does not match the result implied by the RADIUS Packet Type, the combination is likely to cause confusion, because the NAS and peer will arrive at different conclusions as to the outcome of the authentication.

For example, if the NAS receives an Access-Reject with an encapsulated EAP Success, it will not grant access to the peer. However, on receiving the EAP Success, the peer will be lead to believe that it authenticated successfully.

If the NAS receives an Access-Accept with an encapsulated EAP Failure, it will grant access to the peer. However, on receiving an EAP Failure, the peer will be lead to believe that it failed authentication. If no EAP-Message attribute is included within an Access-Accept or Access-Reject, then the peer may not be informed as to the outcome of the authentication, while the NAS will take action to allow or deny access.

As described in [RFC2284], the EAP Success and Failure packets are not acknowledged, and these packets terminate the EAP conversation. As a result, if these packets are encapsulated within an Access-Challenge, no response will be received, and therefore the NAS will send no further Access-Requests to the RADIUS server for the session. As a result, the RADIUS server will not indicate to the NAS whether to allow or deny access, while the peer will be informed as to the outcome of the authentication.

To avoid these conflicts, the following combinations SHOULD NOT be sent by a RADIUS server:

```
Access-Accept/EAP-Message/EAP Failure
Access-Accept/no EAP-Message attribute
Access-Accept/EAP-Start
Access-Reject/EAP-Message/EAP Success
Access-Reject/no EAP-Message attribute
Access-Reject/EAP-Start
Access-Challenge/EAP-Message/EAP Success
Access-Challenge/EAP-Message/EAP Failure
Access-Challenge/no EAP-Message attribute
Access-Challenge/EAP-Start
```

Since the responsibility for avoiding conflicts lies with the RADIUS server, the NAS MUST NOT "manufacture" EAP packets in order to correct contradictory messages that it receives. This behavior, originally mandated within [IEEE8021X], will be deprecated in the future.

2.6.4. Priority

A RADIUS Access-Accept or Access-Reject packet may contain EAP-Message attribute(s). In order to ensure the correct processing of RADIUS packets, the NAS MUST first process the attributes, including the EAP-Message attribute(s), prior to processing the Accept/Reject indication.

2.6.5. Displayable Messages

The Reply-Message attribute, defined in [RFC2865], Section 5.18, indicates text which may be displayed to the peer. This is similar in concept to EAP Notification, defined in [RFC2284]. When sending a displayable message to a NAS during an EAP conversation, the RADIUS server MUST encapsulate displayable messages within EAP-Message/EAP-Request/Notification attribute(s). Reply-Message attribute(s) MUST NOT be included in any RADIUS message containing an EAP-Message attribute. An EAP-Message/EAP-Request/Notification SHOULD NOT be included within an Access-Accept or Access-Reject packet.

In some existing implementations, a NAS receiving Reply-Message attribute(s) copies the Text field(s) into the Type-Data field of an EAP-Request/Notification packet, fills in the Identifier field, and sends this to the peer. However, several issues arise from this:

[1] Unexpected Responses. On receiving an EAP-Request/Notification, the peer will send an EAP-Response/Notification, and the NAS will pass this on to the RADIUS server, encapsulated within EAP-Message attribute(s). However, the RADIUS server may not be expecting an Access-Request containing an EAP-Message/EAP-Response/Notification attribute.

For example, consider what happens when a Reply-Message is included within an Access-Accept or Access-Reject packet with no EAP-Message attribute(s) present. If the value of the Reply-Message attribute is copied into the Type-Data of an EAP-Request/Notification and sent to the peer, this will result in an Access-Request containing an EAP-Message/EAP-Response/Notification attribute being sent by the NAS to the RADIUS server. Since an Access-Accept or Access-Reject packet terminates the RADIUS conversation, such an Access-Request would not be expected, and could be interpreted as the start of another conversation.

[2] Identifier conflicts. While the EAP-Request/Notification is an EAP packet containing an Identifier field, the Reply-Message attribute does not contain an Identifier field. As a result, a NAS receiving a Reply-Message attribute and wishing to translate this to an EAP-Request/Notification will need to choose an Identifier value. It is possible that the chosen Identifier value will conflict with a value chosen by the RADIUS server for another packet within the EAP conversation, potentially causing confusion between a new packet and a retransmission.

To avoid these problems, a NAS receiving a Reply-Message attribute from the RADIUS server SHOULD silently discard the attribute, rather than attempting to translate it to an EAP Notification Request.

3. Attributes

The NAS-Port or NAS-Port-Id attributes SHOULD be included by the NAS in Access-Request packets, and either NAS-Identifier, NAS-IP-Address or NAS-IPv6-Address attributes MUST be included. In order to permit forwarding of the Access-Reply by EAP-unaware proxies, if a User-Name attribute was included in an Access-Request, the RADIUS server MUST include the User-Name attribute in subsequent Access-Accept packets. Without the User-Name attribute, accounting and billing becomes difficult to manage. The User-Name attribute within the Access-Accept packet need not be the same as the User-Name attribute in the Access-Request.

3.1. EAP-Message

Description

This attribute encapsulates EAP [RFC2284] packets so as to allow the NAS to authenticate peers via EAP without having to understand the EAP method it is passing through.

The NAS places EAP messages received from the authenticating peer into one or more EAP-Message attributes and forwards them to the RADIUS server within an Access-Request message. If multiple EAP-Message attributes are contained within an Access-Request or Access-Challenge packet, they MUST be in order and they MUST be consecutive attributes in the Access-Request or Access-Challenge packet. The RADIUS server can return EAP-Message attributes in Access-Challenge, Access-Accept and Access-Reject packets.

When RADIUS is used to enable EAP authentication, Access-Request, Access-Challenge, Access-Accept, and Access-Reject packets SHOULD contain one or more EAP-Message attributes. Where more than one EAP-Message attribute is included, it is assumed that the attributes are to be concatenated to form a single EAP packet.

Multiple EAP packets MUST NOT be encoded within EAP-Message attributes contained within a single Access-Challenge, Access-Accept, Access-Reject or Access-Request packet.

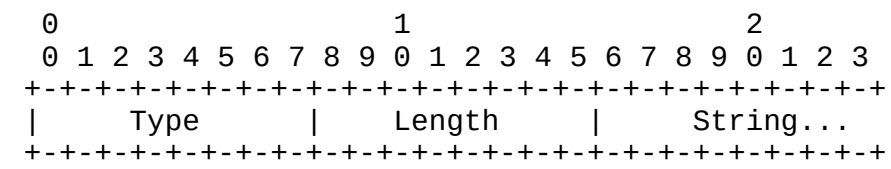
It is expected that EAP will be used to implement a variety of authentication methods, including methods involving strong cryptography. In order to prevent attackers from subverting EAP by attacking RADIUS/EAP, (for example, by modifying EAP Success or EAP Failure packets) it is necessary that RADIUS provide per-packet authentication and integrity protection.

Therefore the Message-Authenticator attribute MUST be used to protect all Access-Request, Access-Challenge, Access-Accept, and Access-Reject packets containing an EAP-Message attribute.

Access-Request packets including EAP-Message attribute(s) without a Message-Authenticator attribute SHOULD be silently discarded by the RADIUS server. A RADIUS server supporting the EAP-Message attribute MUST calculate the correct value of the Message-Authenticator and MUST silently discard the packet if it does not match the value sent. A RADIUS server not supporting the EAP-Message attribute MUST return an Access-Reject if it receives an Access-Request containing an EAP-Message attribute.

Access-Challenge, Access-Accept, or Access-Reject packets including EAP-Message attribute(s) without a Message-Authenticator attribute SHOULD be silently discarded by the NAS. A NAS supporting the EAP-Message attribute MUST calculate the correct value of the Message-Authenticator and MUST silently discard the packet if it does not match the value sent.

A summary of the EAP-Message attribute format is shown below. The fields are transmitted from left to right.



Type

79 for EAP-Message

Length

>= 3

String

The String field contains an EAP packet, as defined in [RFC2284]. If multiple EAP-Message attributes are present in a packet their values should be concatenated; this allows EAP packets longer than 253 octets to be transported by RADIUS.

3.2. Message-Authenticator

Description

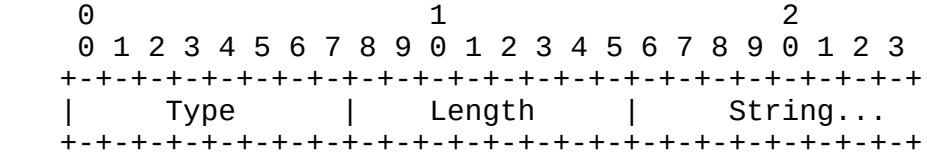
This attribute MAY be used to authenticate and integrity-protect Access-Requests in order to prevent spoofing. It MAY be used in any Access-Request. It MUST be used in any Access-Request, Access-Accept, Access-Reject or Access-Challenge that includes an EAP-Message attribute.

A RADIUS server receiving an Access-Request with a Message-Authenticator attribute present MUST calculate the correct value of the Message-Authenticator and silently discard the packet if it does not match the value sent.

A RADIUS client receiving an Access-Accept, Access-Reject or Access-Challenge with a Message-Authenticator attribute present MUST calculate the correct value of the Message-Authenticator and silently discard the packet if it does not match the value sent.

This attribute is not required in Access-Requests which include the User-Password attribute, but is useful for preventing attacks on other types of authentication. This attribute is intended to thwart attempts by an attacker to setup a "rogue" NAS, and perform online dictionary attacks against the RADIUS server. It does not afford protection against "offline" attacks where the attacker intercepts packets containing (for example) CHAP challenge and response, and performs a dictionary attack against those packets offline.

A summary of the Message-Authenticator attribute format is shown below. The fields are transmitted from left to right.



Type

80 for Message-Authenticator

Length

18

String

When present in an Access-Request packet, Message-Authenticator is an HMAC-MD5 [RFC2104] hash of the entire Access-Request packet, including Type, ID, Length and Authenticator, using the shared secret as the key, as follows.

Message-Authenticator = HMAC-MD5 (Type, Identifier, Length, Request Authenticator, Attributes)

When the message integrity check is calculated the signature string should be considered to be sixteen octets of zero.

For Access-Challenge, Access-Accept, and Access-Reject packets, the Message-Authenticator is calculated as follows, using the Request-Authenticator from the Access-Request this packet is in reply to:

Message-Authenticator = HMAC-MD5 (Type, Identifier, Length, Request Authenticator, Attributes)

When the message integrity check is calculated the signature string should be considered to be sixteen octets of zero. The shared secret is used as the key for the HMAC-MD5 message integrity check. The Message-Authenticator is calculated and inserted in the packet before the Response Authenticator is calculated.

3.3. Table of Attributes

The following table provides a guide to which attributes may be found in packets including EAP-Message attribute(s), and in what quantity. The EAP-Message and Message-Authenticator attributes specified in this document MUST NOT be present in an Accounting-Request. If a table entry is omitted, the values found in [RFC2548], [RFC2865], [RFC2868], [RFC2869] and [RFC3162] should be assumed.

Request	Accept	Reject	Challenge	#	Attribute
0-1	0-1	0	0	1	User-Name
0	0	0	0	2	User-Password [Note 1]
0	0	0	0	3	CHAP-Password [Note 1]
0	0	0	0	18	Reply-Message
0	0	0	0	60	CHAP-Challenge
0	0	0	0	70	ARAP-Password [Note 1]
0	0	0	0	75	Password-Retry
1+	1+	1+	1+	79	EAP-Message [Note 1]
1	1	1	1	80	Message-Authenticator [Note 1]
0-1	0	0	0	94	Originating-Line-Info [Note 3]
0	0	0-1	0-1	101	Error-Cause [Note 2]
Request	Accept	Reject	Challenge	#	Attribute

[Note 1] An Access-Request that contains either a User-Password or CHAP-Password or ARAP-Password or one or more EAP-Message attributes MUST NOT contain more than one type of those four attributes. If it does not contain any of those four attributes, it SHOULD contain a Message-Authenticator. If any packet type contains an EAP-Message attribute it MUST also contain a Message-Authenticator. A RADIUS server receiving an Access-Request not containing any of those four attributes and also not containing a Message-Authenticator attribute SHOULD silently discard it.

[Note 2] The Error-Cause attribute is defined in [RFC3576].

[Note 3] The Originating-Line-Info attribute is defined in [NASREQ].

The following table defines the meaning of the above table entries.

0	This attribute MUST NOT be present.
0+	Zero or more instances of this attribute MAY be present.
0-1	Zero or one instance of this attribute MAY be present.
1	Exactly one instance of this attribute MUST be present.
1+	One or more of these attributes MUST be present.

4. Security Considerations

4.1. Security Requirements

RADIUS/EAP is used in order to provide authentication and authorization for network access. As a result, both the RADIUS and EAP portions of the conversation are potential targets of an attack. Threats are discussed in [RFC2607], [RFC2865], and [RFC3162]. Examples include:

[1] An adversary may attempt to acquire confidential data and identities by snooping RADIUS packets.

[2] An adversary may attempt to modify packets containing RADIUS messages.

[3] An adversary may attempt to inject packets into a RADIUS conversation.

[4] An adversary may launch a dictionary attack against the RADIUS shared secret.

[5] An adversary may launch a known plaintext attack, hoping to recover the key stream corresponding to a Request Authenticator.

[6] An adversary may attempt to replay a RADIUS exchange.

[7] An adversary may attempt to disrupt the EAP negotiation, in order to weaken the authentication, or gain access to peer passwords.

[8] An authenticated NAS may attempt to forge NAS or session identification attributes,

[9] A rogue (unauthenticated) NAS may attempt to impersonate a legitimate NAS.

[10] An attacker may attempt to act as a man-in-the-middle.

To address these threats, it is necessary to support confidentiality, data origin authentication, integrity, and replay protection on a per-packet basis. Bi-directional authentication between the RADIUS client and server also needs to be provided. There is no requirement that the identities of RADIUS clients and servers be kept confidential (e.g., from a passive eavesdropper).

4.2. Security Protocol

To address the security vulnerabilities of RADIUS/EAP, implementations of this specification SHOULD support IPsec [RFC2401] along with IKE [RFC2409] for key management. IPsec ESP [RFC2406] with non-null transform SHOULD be supported, and IPsec ESP with a non-null encryption transform and authentication support SHOULD be used to provide per-packet confidentiality, authentication, integrity and replay protection. IKE SHOULD be used for key management.

Within RADIUS [RFC2865], a shared secret is used for hiding of attributes such as User-Password, as well as in computation of the Response Authenticator. In RADIUS accounting [RFC2866], the shared secret is used in computation of both the Request Authenticator and the Response Authenticator.

Since in RADIUS a shared secret is used to provide confidentiality as well as integrity protection and authentication, only use of IPsec ESP with a non-null transform can provide security services sufficient to substitute for RADIUS application-layer security. Therefore, where IPSEC AH or ESP null is used, it will typically still be necessary to configure a RADIUS shared secret.

Where RADIUS is run over IPsec ESP with a non-null transform, the secret shared between the NAS and the RADIUS server MAY NOT be configured. In this case, a shared secret of zero length MUST be assumed. However, a RADIUS server that cannot know whether incoming traffic is IPsec-protected MUST be configured with a non-null RADIUS shared secret.

When IPsec ESP is used with RADIUS, per-packet authentication, integrity and replay protection MUST be used. 3DES-CBC MUST be supported as an encryption transform and AES-CBC SHOULD be supported. AES-CBC SHOULD be offered as a preferred encryption transform if supported. HMAC-SHA1-96 MUST be supported as an authentication transform. DES-CBC SHOULD NOT be used as the encryption transform.

A typical IPsec policy for an IPsec-capable RADIUS client is "Initiate IPsec, from me to any destination port UDP 1812". This causes an IPsec SA to be set up by the RADIUS client prior to sending RADIUS traffic. If some RADIUS servers contacted by the client do not support IPsec, then a more granular policy will be required: "Initiate IPsec, from me to IPsec-Capable-RADIUS-Server, destination port UDP 1812".

For an IPsec-capable RADIUS server, a typical IPsec policy is "Accept IPsec, from any to me, destination port 1812". This causes the RADIUS server to accept (but not require) use of IPsec. It may not be appropriate to require IPsec for all RADIUS clients connecting to an IPsec-enabled RADIUS server, since some RADIUS clients may not support IPsec.

Where IPsec is used for security, and no RADIUS shared secret is configured, it is important that the RADIUS client and server perform an authorization check. Before enabling a host to act as a RADIUS client, the RADIUS server SHOULD check whether the host is authorized to provide network access. Similarly, before enabling a host to act as a RADIUS server, the RADIUS client SHOULD check whether the host is authorized for that role.

RADIUS servers can be configured with the IP addresses (for IKE Aggressive Mode with pre-shared keys) or FQDNs (for certificate authentication) of RADIUS clients. Alternatively, if a separate Certification Authority (CA) exists for RADIUS clients, then the RADIUS server can configure this CA as a trust anchor [RFC3280] for use with IPsec.

Similarly, RADIUS clients can be configured with the IP addresses (for IKE Aggressive Mode with pre-shared keys) or FQDNs (for certificate authentication) of RADIUS servers. Alternatively, if a separate CA exists for RADIUS servers, then the RADIUS client can configure this CA as a trust anchor for use with IPsec.

Since unlike SSL/TLS, IKE does not permit certificate policies to be set on a per-port basis, certificate policies need to apply to all uses of IPsec on RADIUS clients and servers. In IPsec deployments supporting only certificate authentication, a management station initiating an IPsec-protected telnet session to the RADIUS server would need to obtain a certificate chaining to the RADIUS client CA. Issuing such a certificate might not be appropriate if the management station was not authorized as a RADIUS client.

Where RADIUS clients may obtain their IP address dynamically (such as an Access Point supporting DHCP), IKE Main Mode with pre-shared keys [RFC2409] SHOULD NOT be used, since this requires use of a group

pre-shared key; instead, Aggressive Mode SHOULD be used. IKEv2, a work in progress, may address this issue in the future. Where RADIUS client addresses are statically assigned, either Aggressive Mode or Main Mode MAY be used. With certificate authentication, Main Mode SHOULD be used.

Care needs to be taken with IKE Phase 1 Identity Payload selection in order to enable mapping of identities to pre-shared keys even with Aggressive Mode. Where the ID_IPV4_ADDR or ID_IPV6_ADDR Identity Payloads are used and addresses are dynamically assigned, mapping of identities to keys is not possible, so that group pre-shared keys are still a practical necessity. As a result, the ID_FQDN identity payload SHOULD be employed in situations where Aggressive mode is utilized along with pre-shared keys and IP addresses are dynamically assigned. This approach also has other advantages, since it allows the RADIUS server and client to configure themselves based on the fully qualified domain name of their peers.

Note that with IPsec, security services are negotiated at the granularity of an IPsec SA, so that RADIUS exchanges requiring a set of security services different from those negotiated with existing IPsec SAs will need to negotiate a new IPsec SA. Separate IPsec SAs are also advisable where quality of service considerations dictate different handling RADIUS conversations. Attempting to apply different quality of service to connections handled by the same IPsec SA can result in reordering, and falling outside the replay window. For a discussion of the issues, see [RFC2983].

4.3. Security Issues

This section provides more detail on the vulnerabilities identified in Section 4.1., and how they may be mitigated. Vulnerabilities include:

Privacy issues
Spoofing and hijacking
Dictionary attacks
Known plaintext attacks
Replay attacks
Negotiation attacks
Impersonation
Man in the middle attacks
Separation of authenticator and authentication server
Multiple databases

4.3.1. Privacy Issues

Since RADIUS messages may contain the User-Name attribute as well as NAS-IP-Address or NAS-Identifier attributes, an attacker snooping on RADIUS traffic may be able to determine the geographic location of peers in real time. In wireless networks, it is often assumed that RADIUS traffic is physically secure, since it typically travels over the wired network and that this limits the release of location information.

However, it is possible for an authenticated attacker to spoof ARP packets [RFC826] so as to cause diversion of RADIUS traffic onto the wireless network. In this way an attacker may obtain RADIUS packets from which it can glean peer location information, or which it can subject to a known plaintext or offline dictionary attack. To address these vulnerabilities, implementations of this specification SHOULD use IPsec ESP with non-null transform and per-packet encryption, authentication, integrity and replay protection to protect both RADIUS authentication [RFC2865] and accounting [RFC2866] traffic, as described in Section 4.2.

4.3.2. Spoofing and Hijacking

Access-Request packets with a User-Password attribute establish the identity of both the user and the NAS sending the Access-Request, because of the way the shared secret between the NAS and RADIUS server is used. Access-Request packets with CHAP-Password or EAP-Message attributes do not have a User-Password attribute. As a result, the Message-Authenticator attribute SHOULD be used in Access-Request packets that do not have a User-Password attribute, in order to establish the identity of the NAS sending the request.

An attacker may attempt to inject packets into the conversation between the NAS and the RADIUS server, or between the RADIUS server and the security server. RADIUS [RFC2865] does not support encryption other than attribute hiding. As described in [RFC2865], only Access-Reply and Access-Challenge packets are integrity protected. Moreover, the per-packet authentication and integrity protection mechanism described in [RFC2865] has known weaknesses [MD5Attack], making it a tempting target for attackers looking to subvert RADIUS/EAP.

To provide stronger security, the Message-Authenticator attribute MUST be used in all RADIUS packets containing an EAP-Message attribute. Implementations of this specification SHOULD use IPsec ESP with non-null transform and per-packet encryption, authentication, integrity and replay protection, as described in Section 4.2.

4.3.3. Dictionary Attacks

The RADIUS shared secret is vulnerable to offline dictionary attack, based on capture of the Response Authenticator or Message-Authenticator attribute. In order to decrease the level of vulnerability, [RFC2865] recommends:

> The secret (password shared between the client and the RADIUS server) SHOULD be at least as large and unguessable as a well-chosen password. It is preferred that the secret be at least 16 octets.

The risk of an offline dictionary attack can be further reduced by employing IPsec ESP with non-null transform in order to encrypt the RADIUS conversation, as described in Section 4.2.

4.3.4. Known Plaintext Attacks

Since EAP [RFC2284] does not support PAP, the RADIUS User-Password attribute is not used to carry hidden user passwords within RADIUS/EAP conversations. The User-Password hiding mechanism, defined in [RFC2865] utilizes MD5, defined in [RFC1321], in order to generate a key stream based on the RADIUS shared secret and the Request Authenticator. Where PAP is in use, it is possible to collect key streams corresponding to a given Request Authenticator value, by capturing RADIUS conversations corresponding to a PAP authentication attempt, using a known password. Since the User-Password is known, the key stream corresponding to a given Request Authenticator can be determined and stored.

Since the key stream may have been determined previously from a known plaintext attack, if the Request Authenticator repeats, attributes encrypted using the RADIUS attribute hiding mechanism should be considered compromised. In addition to the User-Password attribute, which is not used with EAP, this includes attributes such as Tunnel-Password [RFC2868, section 3.5] and MS-MPPE-Send-Key and MS-MPPE-Recv-Key attributes [RFC2548, section 2.4], which include a Salt field as part of the hiding algorithm.

To avoid this, [RFC2865], Section 3 advises:

> Since it is expected that the same secret MAY be used to authenticate with servers in disparate geographic regions, the Request Authenticator field SHOULD exhibit global and temporal uniqueness.

Where the Request Authenticator repeats, the Salt field defined in [RFC2548], Section 2.4 does not provide protection against compromise. This is because MD5 [RFC1321], rather than HMAC-MD5 [RFC2104], is used to generate the key stream, which is calculated from the 128-bit RADIUS shared secret (S), the 128-bit Request Authenticator (R), and the Salt field (A), using the formula b(1) = MD5(S + R + A). Since the Salt field is placed at the end, if the Request Authenticator were to repeat on a network where PAP is in use, then the salted keystream could be calculated from the User-Password keystream by continuing the MD5 calculation based on the Salt field (A), which is sent in the clear.

Even though EAP does not support PAP authentication, a security vulnerability can still exist where the same RADIUS shared secret is used for hiding User-Password as well as other attributes. This can occur, for example, if the same RADIUS proxy handles authentication requests for both EAP and PAP.

The threat can be mitigated by protecting RADIUS with IPsec ESP with non-null transform, as described in Section 4.2. Where RADIUS shared secrets are configured, the RADIUS shared secret used by a NAS supporting EAP MUST NOT be reused by a NAS utilizing the User-Password attribute, since improper shared secret hygiene could lead to compromise of hidden attributes.

4.3.5. Replay Attacks

The RADIUS protocol provides only limited support for replay protection. RADIUS Access-Requests include liveness via the 128-bit Request Authenticator. However, the Request Authenticator is not a replay counter. Since RADIUS servers may not maintain a cache of previous Request Authenticators, the Request Authenticator does not provide replay protection.

RADIUS accounting [RFC2866] does not support replay protection at the protocol level. Due to the need to support failover between RADIUS accounting servers, protocol-based replay protection is not sufficient to prevent duplicate accounting records. However, once accepted by the accounting server, duplicate accounting records can be detected by use of the the Acct-Session-Id [RFC2866, section 5.5] and Event-Timestamp [RFC2869, section 5.3] attributes.

Unlike RADIUS authentication, RADIUS accounting does not use the Request Authenticator as a nonce. Instead, the Request Authenticator contains an MD5 hash calculated over the Code, Identifier, Length, and request attributes of the Accounting Request packet, plus the shared secret. The Response Authenticator also contains an MD5 hash calculated over the Code, Identifier and Length, the Request

Authenticator field from the Accounting-Request packet being replied to, the response attributes and the shared secret.

Since the Accounting Response Authenticator depends in part on the Accounting Request Authenticator, it is not possible to replay an Accounting-Response unless the Request Authenticator repeats. While it is possible to utilize EAP methods such as EAP TLS [RFC2716] which include liveness checks on both sides, not all EAP messages will include liveness so that this provides incomplete protection.

Strong replay protection for RADIUS authentication and accounting can be provided by enabling IPsec replay protection with RADIUS, as described in Section 4.2.

4.3.6. Negotiation Attacks

In a negotiation attack a rogue NAS, tunnel server, RADIUS proxy or RADIUS server attempts to cause the authenticating peer to choose a less secure authentication method. For example, a session that would normally be authenticated with EAP would instead be authenticated via CHAP or PAP; alternatively, a connection that would normally be authenticated via a more secure EAP method such as EAP-TLS [RFC2716] might be made to occur via a less secure EAP method, such as MD5-Challenge. The threat posed by rogue devices, once thought to be remote, has gained currency given compromises of telephone company switching systems, such as those described in [Masters].

Protection against negotiation attacks requires the elimination of downward negotiations. The RADIUS exchange may be further protected by use of IPsec, as described in Section 4.2. Alternatively, where IPsec is not used, the vulnerability can be mitigated via implementation of per-connection policy on the part of the authenticating peer, and per-peer policy on the part of the RADIUS server. For the authenticating peer, authentication policy should be set on a per-connection basis. Per-connection policy allows an authenticating peer to negotiate a strong EAP method when connecting to one service, while negotiating a weaker EAP method for another service.

With per-connection policy, an authenticating peer will only attempt to negotiate EAP for a session in which EAP support is expected. As a result, there is a presumption that an authenticating peer selecting EAP requires that level of security. If it cannot be provided, it is likely that there is some kind of misconfiguration, or even that the authenticating peer is contacting the wrong server. Should the NAS not be able to negotiate EAP, or should the EAP-Request sent by the NAS be of a different EAP type than what is expected, the authenticating peer MUST disconnect. An authenticating

peer expecting EAP to be negotiated for a session MUST NOT negotiate a weaker method, such as CHAP or PAP. In wireless networks, the service advertisement itself may be spoof-able, so that an attacker could fool the peer into negotiating an authentication method suitable for a less secure network.

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 it is possible for one reseller to implement EAP while another does not. Alternatively, some peer might be authenticated locally by the NAS while other peers are authenticated via RADIUS. 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.

If CHAP is negotiated, the NAS will pass the User-Name and CHAP-Password attributes to the RADIUS server in an Access-Request packet. If the peer is not required to use EAP, then the RADIUS server will respond with an Access-Accept or Access-Reject packet as appropriate. However, if CHAP has been negotiated but EAP is required, the RADIUS server MUST respond with an Access-Reject, rather than an Access-Challenge/EAP-Message/EAP-Request packet. The authenticating peer MUST refuse to renegotiate authentication, even if the renegotiation is from CHAP to EAP.

If EAP is negotiated but is not supported by the RADIUS proxy or server, then the server or proxy MUST respond with an Access-Reject. In these cases, a PPP NAS MUST send an LCP-Terminate and disconnect the peer. This is the correct behavior since the authenticating peer is expecting EAP to be negotiated, and that expectation cannot be fulfilled. An EAP-capable authenticating peer MUST refuse to renegotiate the authentication protocol if EAP had initially been negotiated. Note that problems with a non-EAP capable RADIUS proxy could prove difficult to diagnose, since a peer connecting from one location (with an EAP-capable proxy) might be able to successfully authenticate via EAP, while the same peer connecting at another location (and encountering an EAP-incapable proxy) might be consistently disconnected.

4.3.7. Impersonation

[RFC2865] Section 3 states:

> A RADIUS server MUST use the source IP address of the RADIUS UDP packet to decide which shared secret to use, so that RADIUS requests can be proxied.

When RADIUS requests are forwarded by a proxy, the NAS-IP-Address or NAS-IPv6-Address attributes may not match the source address. Since the NAS-Identifier attribute need not contain an FQDN, this attribute also may not correspond to the source address, even indirectly, with or without a proxy present.

As a result, the authenticity check performed by a RADIUS server or proxy does not verify the correctness of NAS identification attributes. This makes it possible for a rogue NAS to forge NAS-IP-Address, NAS-IPv6-Address or NAS-Identifier attributes within a RADIUS Access-Request in order to impersonate another NAS. It is also possible for a rogue NAS to forge session identification attributes such as Called-Station-Id, Calling-Station-Id, and Originating-Line-Info.

This could fool the RADIUS server into subsequently sending Disconnect or CoA-Request messages [RFC3576] containing forged session identification attributes to a NAS targeted by an attacker.

To address these vulnerabilities RADIUS proxies SHOULD check whether NAS identification attributes (NAS-IP-Address, NAS-IPv6-Address, NAS-Identifier) match the source address of packets originating from the NAS. Where a match is not found, an Access-Reject SHOULD be sent, and an error SHOULD be logged.

However, such a check may not always be possible. Since the NAS-Identifier attribute need not correspond to an FQDN, it may not be resolvable to an IP address to be matched against the source address. Also, where a NAT exists between the RADIUS client and proxy, checking the NAS-IP-Address or NAS-IPv6-Address attributes may not be feasible.

To allow verification of NAS and session identification parameters, EAP methods can support the secure exchange of these parameters between the EAP peer and EAP server. NAS identification attributes include NAS-IP-Address, NAS-IPv6-Address and Called-Station-Id; session identification attributes include User-Name and Calling-Station-Id. The secure exchange of these parameters between the EAP peer and server enables the RADIUS server to check whether the attributes provided by the NAS match those provided by the peer; similarly, the peer can check the parameters provided by the NAS against those provided by the EAP server. This enables detection of a rogue NAS.

4.3.8. Man in the Middle Attacks

RADIUS only provides security on a hop-by-hop basis, even where IPsec is used. As a result, an attacker gaining control of a RADIUS proxy could attempt to modify EAP packets in transit. To protect against this, EAP methods SHOULD incorporate their own per-packet integrity protection and authentication mechanisms.

4.3.9. Separation of Authenticator and Authentication Server

As noted in [RFC2716], it is possible for the EAP peer and authenticator to mutually authenticate, and derive a Master Session Key (MSK) for a ciphersuite used to protect subsequent data traffic. This does not present an issue on the peer, since the peer and EAP client reside on the same machine; all that is required is for the EAP client module to derive and pass a Transient Session Key (TSK) to the ciphersuite module.

The situation is more complex when EAP is used with RADIUS, since the authenticator and authentication server may not reside on the same host.

In the case where the authenticator and authentication server reside on different machines, there are several implications for security. First, mutual authentication will occur between the peer and the authentication server, not between the peer and the authenticator. This means that it is not possible for the peer to validate the identity of the NAS or tunnel server that it is speaking to, using EAP alone.

As described in Section 4.2, when RADIUS/EAP is used to encapsulate EAP packets, IPsec SHOULD be used to provide per-packet authentication, integrity, replay protection and confidentiality. The Message-Authenticator attribute is also required in RADIUS Access-Requests containing an EAP-Message attribute sent from the NAS or tunnel server to the RADIUS server. Since the Message-Authenticator attribute involves an HMAC-MD5 message integrity check, it is possible for the RADIUS server to verify the integrity of the Access-Request as well as the NAS or tunnel server’s identity, even where IPsec is not used. Similarly, Access-Challenge packets containing an EAP-Message attribute sent from the RADIUS server to the NAS are also authenticated and integrity protected using an HMAC-MD5 message integrity check, enabling the NAS or tunnel server to determine the integrity of the packet and verify the identity of the RADIUS server, even where IPsec is not used. Moreover, EAP packets sent using methods that contain their own integrity protection cannot be successfully modified by a rogue NAS or tunnel server.

The second issue that arises where the authenticator and authentication server reside on separate hosts is that the EAP Master Session Key (MSK) negotiated between the peer and authentication server will need to be transmitted to the authenticator. Therefore a mechanism needs to be provided to transmit the MSK from the authentication server to the NAS or tunnel server that needs it. The specification of the key transport and wrapping mechanism is outside the scope of this document. However, it is expected that the wrapping mechanism will provide confidentiality, integrity and replay protection, and data origin authentication.

4.3.10. Multiple Databases

In many cases a security server will be deployed along with a RADIUS server in order to provide EAP services. Unless the security server also functions as a RADIUS server, two separate user databases will exist, each containing information about the security requirements for the user. This represents a weakness, since security may be compromised by a successful attack on either of the servers, or their databases. With multiple user databases, adding a new user may require multiple operations, increasing the chances for error. The problems are further magnified in the case where user information is also being kept in an LDAP server. In this case, three stores of user information may exist.

In order to address these threats, consolidation of databases is recommended. This can be achieved by having both the RADIUS server and security server store information in the same database; by having the security server provide a full RADIUS implementation; or by consolidating both the security server and the RADIUS server onto the same machine.

5. IANA Considerations

This specification does not create any new registries, or define any new RADIUS attributes or values.

6. References

6.1. Normative References

[RFC1321] Rivest, R., "The MD5 Message-Digest Algorithm", RFC 1321, April 1992.

[RFC2104] Krawczyk, H., Bellare, M. and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication", RFC 2104, February 1997.

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

[RFC2279] Yergeau, F., "UTF-8, a transformation format of ISO 10646", RFC 2279, January 1998.

[RFC2284] Blunk, L. and J. Vollbrecht, "PPP Extensible Authentication Protocol (EAP)", RFC 2284, March 1998.

[RFC2401] Atkinson, R. and S. Kent, "Security Architecture for the Internet Protocol", RFC 2401, November 1998.

[RFC2406] Kent, S. and R. Atkinson, "IP Encapsulating Security Payload (ESP)", RFC 2406, November 1998.

[RFC2409] Harkins, D. and D. Carrel, "The Internet Key Exchange (IKE)", RFC 2409, November 1998.

[RFC2486] Aboba, B. and M. Beadles, "The Network Access Identifier", RFC 2486, January 1999.

[RFC2865] Rigney, C., Willens, S., Rubens, A. and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)", RFC 2865, June 2000.

[RFC2988] Paxson, V. and M. Allman, "Computing TCP's Retransmission Timer", RFC 2988, November 2000.

[RFC3162] Aboba, B., Zorn, G. and D. Mitton, "RADIUS and IP6", RFC 3162, August 2001.

[RFC3280] Housley, R., Polk, W., Ford, W. and D. Solo, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 3280, April 2002.

[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.

6.2. Informative References

[RFC826] Plummer, D., "An Ethernet Address Resolution Protocol", STD 37, RFC 826, November 1982.

[RFC1510] Kohl, J. and C. Neuman, "The Kerberos Network Authentication Service (V5)", RFC 1510, September 1993.

[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.

[RFC2716] Aboba, B. and D. Simon,"PPP EAP TLS Authentication Protocol", RFC 2716, October 1999.

[RFC2866] Rigney, C., "RADIUS Accounting", RFC 2866, June 2000.

[RFC2867] Zorn, G., Aboba, B. and D. Mitton, "RADIUS Accounting Modifications for Tunnel Protocol Support", RFC 2867, June 2000.

[RFC2868] Zorn, G., Leifer, D., Rubens, A., Shriver, J., Holdrege, M. and I. Goyret, "RADIUS Attributes for Tunnel Protocol Support", RFC 2868, June 2000.

[RFC2869] Rigney, C., Willats, W. and P. Calhoun, "RADIUS Extensions", RFC 2869, June 2000.

[RFC2983] Black, D. "Differentiated Services and Tunnels", RFC 2983, October 2000.

[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.

[IEEE802] IEEE Standards for Local and Metropolitan Area Networks: Overview and Architecture, ANSI/IEEE Std 802, 1990.

[IEEE8021X] IEEE Standards for Local and Metropolitan Area Networks: Port based Network Access Control, IEEE Std 802.1X-2001, June 2001.

[MD5Attack] Dobbertin, H., "The Status of MD5 After a Recent Attack", CryptoBytes Vol.2 No.2, Summer 1996.

[Masters] Slatalla, M. and J. Quittner, "Masters of Deception." HarperCollins, New York, 1995.

[NASREQ] Calhoun, P., et al., "Diameter Network Access Server Application", Work in Progress.

Appendix A - Examples

The examples below illustrate conversations between an authenticating peer, NAS, and RADIUS server. The OTP and EAP-TLS protocols are used only for illustrative purposes; other authentication protocols could also have been used, although they might show somewhat different behavior.

Where the NAS sends an EAP-Request/Identity as the initial packet, the exchange appears as follows:

```
Authenticating peer     NAS                    RADIUS server
-------------------     ---                    -------------
                        <- EAP-Request/
                        Identity
EAP-Response/
Identity (MyID) ->
                        RADIUS Access-Request/
                        EAP-Message/EAP-Response/
                        (MyID) ->
                                               <- RADIUS
                                               Access-Challenge/
                                               EAP-Message/EAP-Request
                                               OTP/OTP Challenge
                        <- EAP-Request/
                        OTP/OTP Challenge
EAP-Response/
OTP, OTPpw ->
                        RADIUS Access-Request/
                        EAP-Message/EAP-Response/
                        OTP, OTPpw ->
                                                <- RADIUS
                                                Access-Accept/
                                                EAP-Message/EAP-Success
                                                (other attributes)
                        <- EAP-Success
```

In the case where the NAS initiates with an EAP-Request for EAP TLS [RFC2716], and the identity is determined based on the contents of the client certificate, the exchange will appear as follows:

```
EAP-Response/
EAP-Type=EAP-TLS ->
                        RADIUS Access-Request/
                        EAP-Message/EAP-Response/
                        EAP-Type=EAP-TLS->
                                              <-RADIUS Access-Accept/
                                              EAP-Message/EAP-Success
                                              (other attributes)
                        <- EAP-Success
```

In the case where the NAS first sends an EAP-Start packet to the RADIUS server, the conversation would appear as follows:

```
Authenticating peer     NAS                    RADIUS server
-------------------     ---                    -------------
                        RADIUS Access-Request/
                        EAP-Message/Start ->
                                               <- RADIUS
                                               Access-Challenge/
                                               EAP-Message/EAP-Request/
                                               Identity
                        <- EAP-Request/
                        Identity
EAP-Response/
Identity (MyID) ->
                        RADIUS Access-Request/
                        EAP-Message/EAP-Response/
                        Identity (MyID) ->
                                               <- RADIUS
                                               Access-Challenge/
                                               EAP-Message/EAP-Request/
                                               OTP/OTP Challenge
                        <- EAP-Request/
                        OTP/OTP Challenge
EAP-Response/
OTP, OTPpw ->
                        RADIUS Access-Request/
                        EAP-Message/EAP-Response/
                        OTP, OTPpw ->
                                               <- RADIUS
                                               Access-Accept/
                                               EAP-Message/EAP-Success
                                               (other attributes)
                        <- EAP-Success
```

In the case where the NAS initiates with an EAP-Request for EAP TLS [RFC2716], but the peer responds with a Nak, indicating that it would prefer another method not implemented locally on the NAS, the exchange will appear as follows:

```
Authenticating peer     NAS                     RADIUS server
-------------------     ---                     -------------
                        <- EAP-Request/
                        EAP-Type=EAP-TLS
                        (TLS Start, S bit set)
EAP-Response/
EAP-Type=Nak
(Alternative(s))->
                        RADIUS Access-Request/
                        EAP-Message/EAP-Response/
                        Nak ->
                                                <- RADIUS
                                                Access-Challenge/
                                                EAP-Message/EAP-Request/
                                                Identity
                        <- EAP-Request/
                        Identity
EAP-Response/
Identity (MyID) ->
                        RADIUS Access-Request/
                        EAP-Message/EAP-Response/
                        (MyID) ->
                                                <- RADIUS
                                                Access-Challenge/
                                                EAP-Message/EAP-Request
                                                OTP/OTP Challenge
                        <- EAP-Request/
                        OTP/OTP Challenge
EAP-Response/
OTP, OTPpw ->
                        RADIUS Access-Request/
                        EAP-Message/EAP-Response/
                        OTP, OTPpw ->
                                                 <- RADIUS
                                                 Access-Accept/
                                                 EAP-Message/EAP-Success
                                                 (other attributes)
                        <- EAP-Success
```

In the case where the authenticating peer attempts to authenticate the NAS, the conversation would appear as follows:

```
Authenticating peer     NAS                    RADIUS Server
-------------------     ---                    -------------
EAP-Request/
Challenge, MD5 ->
                        RADIUS Access-Request/
                        EAP-Message/EAP-Request/
                        Challenge, MD5 ->
                                                <- RADIUS
                                                Access-Reject/
                                                EAP-Message/
                                                EAP-Response/
                                                Nak (no alternative)

                        <- EAP-Response/Nak
                         (no alternative)
EAP-Failure ->
```

In the case where an invalid EAP Response is inserted by an attacker, the conversation would appear as follows:

```
Authenticating peer     NAS                     RADIUS server
-------------------     ---                     -------------
                        <- EAP-Request/
                        EAP-Type=Foo
EAP-Response/
EAP-Type=Foo ->
                        RADIUS Access-Request/
                        EAP-Message/EAP-Response/
                        EAP-Type=Foo ->
                                                <- RADIUS
                                                Access-Challenge/
                                                EAP-Message/EAP-Request/
                                                EAP-Type=Foo
                        <- EAP-Request/
                        EAP-Type=Foo
Attacker spoof:
EAP-Response/
EAP-Type=Bar ->

Good guy:
EAP-Response/
EAP-Type=Foo ->
                        RADIUS Access-Request/
                        EAP-Message/EAP-Response/
                        EAP-Type=Bar ->

                                                <- RADIUS
                                                Access-Challenge/
                                                EAP-Message/EAP-Request/
                                                EAP-Type=Foo,
                                                Error-Cause="Invalid EAP
                                                 Packet (Ignored)"
                        RADIUS Access-Request/
                        EAP-Message/EAP-Response/
                        EAP-Type=Foo ->
                                                <- Access-Accept/
                                                EAP-Message/Success
                        <- EAP Success
```

In the case where the client fails EAP authentication, and an error message is sent prior to disconnection, the conversation would appear as follows:

```
Authenticating peer     NAS                     RADIUS server
-------------------     ---                     -------------
                        RADIUS Access-Request/
                        EAP-Message/Start ->
                                                <- RADIUS
                                                Access-Challenge/
                                                EAP-Message/EAP-Response/
                                                Identity
                        <- EAP-Request/
                        Identity
EAP-Response/
Identity (MyID) ->
                        RADIUS Access-Request/
                        EAP-Message/EAP-Response/
                        (MyID) ->
                                                <- RADIUS
                                                Access-Challenge/
                                                EAP-Message/EAP-Request
                                                OTP/OTP Challenge
                        <- EAP-Request/
                        OTP/OTP Challenge
EAP-Response/
OTP, OTPpw ->
                        RADIUS Access-Request/
                        EAP-Message/EAP-Response/
                        OTP, OTPpw ->
                                                <- RADIUS
                                                Access-Challenge/
                                                EAP-Message/EAP-Request/
                                                Notification
                        <- EAP-Request/
                           Notification

EAP-Response/
Notification ->
                        RADIUS Access-Request/
                        EAP-Message/EAP-Response/
                        Notification ->
                                                <- RADIUS
                                                Access-Reject/
                                                EAP-Message/EAP-Failure
                        <- EAP-Failure
                        (client disconnected)
```

In the case that the RADIUS server or proxy does not support EAP-Message, but no error message is sent, the conversation would appear as follows:

```
Authenticating peer     NAS                        RADIUS server
-------------------     ---                        -------------
                        RADIUS Access-Request/
                        EAP-Message/Start ->
                                                   <- RADIUS
                                                   Access-Reject
                        (User Disconnected)
```

In the case where the local RADIUS server does support EAP-Message, but the remote RADIUS server does not, the conversation would appear as follows:

```
Authenticating peer     NAS                        RADIUS server
-------------------     ---                        -------------
                        RADIUS Access-Request/
                        EAP-Message/Start ->
                                                   <- RADIUS
                                                   Access-Challenge/
                                                   EAP-Message/
                                                   EAP-Response/
                                                   Identity
                        <- EAP-Request/
                        Identity

EAP-Response/
Identity
(MyID) ->
                        RADIUS Access-Request/
                        EAP-Message/EAP-Response/
                        (MyID) ->
                                                   <- RADIUS
                                                   Access-Reject
                                                   (proxied from remote
                                                    RADIUS server)
                        (User Disconnected)
```

In the case where PPP is the link and the authenticating peer does not support EAP, but where EAP is required for that user, the conversation would appear as follows:

```
Authenticating peer     NAS                        RADIUS server
-------------------     ---                        -------------
                        <- PPP LCP Request-EAP
                        auth
PPP LCP NAK-EAP
auth ->
                        <- PPP LCP Request-CHAP
                        auth
PPP LCP ACK-CHAP
auth ->
                        <- PPP CHAP Challenge
PPP CHAP Response ->
                        RADIUS Access-Request/
                        User-Name,
                        CHAP-Password ->
                                                   <- RADIUS
                                                   Access-Reject
                        <-  PPP LCP Terminate
                        (User Disconnected)
```

In the case where PPP is the link, the NAS does not support EAP, but where EAP is required for that user, the conversation would appear as follows:

```
Authenticating peer     NAS                        RADIUS server
-------------------     ---                        -------------
                        <- PPP LCP Request-CHAP
                        auth

PP LCP ACK-CHAP
auth ->
                        <- PPP CHAP Challenge
PPP CHAP Response ->
                        RADIUS Access-Request/
                        User-Name,
                        CHAP-Password ->

                                                 <- RADIUS
                                                 Access-Reject
                        <-  PPP LCP Terminate
                        (User Disconnected)
```

Appendix B - Change Log

The following changes have been made from RFC 2869:

A NAS may simultaneously support both local authentication and pass-through; once the NAS enters pass-through mode within a session, it cannot revert back to local authentication. Also EAP is explicitly described as a 'lock step' protocol. (Section 2).

The NAS may initiate with an EAP-Request for an authentication Type. If the Request is NAK'd, the NAS should send an initial Access-Request with an EAP-Message attribute containing an EAP-Response/Nak.

The RADIUS server may treat an invalid EAP Response as a non-fatal error (Section 2.2)

For use with RADIUS/EAP, the Password-Retry (Section 2.3) and Reply-Message (2.6.5) attributes are deprecated.

Each EAP session has a unique Identifier space (Section 2.6.1).

Role reversal is not supported (Section 2.6.2).

Message combinations (e.g. Access-Accept/EAP-Failure) that conflict are discouraged (Section 2.6.3).

Only a single EAP packet may be encapsulated within a RADIUS message (Section 3.1).

An Access-Request lacking explicit authentication as well as a Message- Authenticator attribute SHOULD be silently discarded (Section 3.3).

The Originating-Line-Info attribute is supported (Section 3.3).

IPsec ESP with non-null transform SHOULD be used and the usage model is described in detail (Section 4.2).

Additional discussion of security vulnerabilities (Section 4.1) and potential fixes (Section 4.3).

Separated normative (Section 6.1) and informative (Section 6.2) references.

Added additional examples (Appendix A): a NAS initiating with an EAP-Request for an authentication Type; attempted role reversal.

Intellectual Property Statement

Acknowledgments

Thanks to Dave Dawson and Karl Fox of Ascend, Glen Zorn of Cisco Systems, Jari Arkko of Ericsson and Ashwin Palekar, Tim Moore and Narendra Gidwani of Microsoft for useful discussions of this problem space. The authors would also like to acknowledge Tony Jeffree, Chair of IEEE 802.1 for his assistance in resolving RADIUS/EAP issues in IEEE 802.1X-2001.

Authors' Addresses

Bernard Aboba
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052

Phone: +1 425 706 6605
Fax: +1 425 936 7329
EMail: bernarda@microsoft.com

Pat R. Calhoun
Airespace
110 Nortech Parkway
San Jose, California, 95134
USA

Phone: +1 408 635 2023
Fax: +1 408 635 2020
EMail: pcalhoun@airespace.com

Full Copyright Statement

Acknowledgement

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