RADIUS Working Group
INTERNET-DRAFT
Updates: RFC 2138
Category: Standards Track
<draft-ietf-radius-eap-05.txt>
8 May 1998

Pat Calhoun
Sun Microsystems
Allan C. Rubens
Merit Network, Inc.
Bernard Aboba
Microsoft

Extensible Authentication Protocol Support in RADIUS

1. Status of this Memo

2. Abstract

The Extensible Authentication Protocol (EAP) is a PPP extension that provides support for additional authentication methods within PPP. This document describes how the EAP-Message and Signature attributes may be used for providing EAP support within RADIUS.

3. Changes from -04 draft

Updated section on retransmission
Added section on fragmentation
Added EAP-Timeout attribute
Updated references.

4. Introduction

The Extensible Authentication Protocol (EAP), described in [1], provides a standard mechanism for support of additional authentication methods within PPP. Through the use of EAP, support for a number of

authentication schemes may be added, including smart cards, Kerberos, Public Key, One Time Passwords, and others. In order to provide for support of EAP within RADIUS, two new attributes, EAP-Message and Signature, were introduced as RADIUS extensions in [4]. This document describes how these new attributes may be used for providing EAP support within RADIUS.

In the proposed scheme, the RADIUS server is used to shuttle RADIUS-encapsulated EAP Packets between the NAS and a backend security server. While the conversation between the RADIUS server and the backend security server will typically occur using a proprietary protocol developed by the backend security server vendor, it is also possible to use RADIUS-encapsulated EAP via the EAP-Message attribute. This has the advantage of allowing the RADIUS server to support EAP without the need for authentication-specific code, which can instead reside on a backend security server.

4.1. Requirements language

This specification uses the same words as [6] for defining the significance of each particular requirement. These words are:

MUST This word, or the adjectives "REQUIRED" or "SHALL", means that the definition is an absolute requirement of the specification.

MUST NOT This phrase, or the phrase "SHALL NOT", means that the definition is an absolute prohibition of the specification.

SHOULD This word, or the adjective "RECOMMENDED", means that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.

SHOULD NOT
This phrase means that there may exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.

MAY This word, or the adjective "", means that an item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because the vendor feels that it enhances the product while another vendor may omit the same item. An implementation which does not

include a particular option MUST be prepared to interoperate with another implementation which does include the option, though perhaps with reduced functionality. In the same vein an implementation which does include a particular option MUST be prepared to interoperate with another implementation

which does not include the option.(except, of course, for the feature the option provides)

An implementation is not compliant if it fails to satisfy one or more of the must or must not requirements for the protocols it implements. An implementation that satisfies all the must, must not, should and should not requirements for its protocols is said to be "unconditionally compliant"; one that satisfies all the must and must not requirements but not all the should or should not requirements for its protocols is said to be "conditionally compliant."

5. Protocol overview

The EAP conversation between the authenticating peer (dial-in user) and the NAS begins with the negotiation of EAP within LCP. Once EAP has been negotiated, the NAS MUST send an EAP-Request/Identity message to the authenticating peer, unless identity is determined via some other means such as Called-Station-Id or Calling-Station-Id. The peer will then respond with an EAP-Response/Identity which the the NAS will then forward to the RADIUS server in the EAP-Message attribute of a RADIUS Access-Request packet. The RADIUS Server will typically use the EAP-Response/Identity to determine which EAP type is to be applied to the user.

In order to permit non-EAP aware RADIUS proxies to forward the Access-Request packet, if the NAS sends the EAP-Request/Identity, the NAS MUST copy the contents of the EAP-Response/Identity into the User-Name attribute and MUST include the EAP-Response/Identity in the User-Name attribute in every subsequent Access-Request. NAS-Port SHOULD be included in the attributes issued by the NAS in the Access-Request packet, and either NAS-Identifier or NAS-IP-Address 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-Challenge and Access-Accept packets. Without the User-Name attribute, accounting and billing becomes very difficult to manage.

If identity is determined via another means such as Called-Station-Id or Calling-Station-Id, the NAS MUST include these identifying attributes in every Access-Request, and the RADIUS Server MUST include them in every Access-Challenge and Access-Accept.

While this approach will save a round-trip, it cannot be universally employed. There are circumstances in which the user's identity may not be needed (such as when authentication and accounting is handled based on Called-Station-Id or Calling-Station-Id), and therefore an EAP-Request/Identity packet may not necessarily be issued by the NAS

to the authenticating peer. In cases where an EAP-Request/Identity packet will not be sent, the NAS will send to the RADIUS server a RADIUS Access-Request packet containing an EAP-Message attribute signifying EAP-Start. EAP-Start is indicated by sending an EAP-Message attribute with a length of 2 (no data). However, it should be noted that since no User-Name attribute is included in the Access-Request,

this approach is not compatible with RADIUS as specified in [2], nor can it easily be applied in situations where proxies are deployed, such as roaming or shared use networks.

If the RADIUS server supports EAP, it MUST respond with an Access-Challenge packet containing an EAP-Message attribute. If the RADIUS server does not support EAP, it MUST respond with an Access-Reject. The EAP-Message attribute includes an encapsulated EAP packet which is then passed on to the authenticating peer. In the case where the NAS does not initially send an EAP-Request/Identity message to the peer, the Access-Challenge typically will contain an EAP-Message attribute encapsulating an EAP-Request/Identity message, requesting the dial-in user to identify themself. The NAS will then respond with a RADIUS Access-Request packet containing an EAP-Message attribute encapsulating an EAP-Response. The conversation continues until either a RADIUS Access-Reject or Access-Accept packet is received.

Reception of a RADIUS Access-Reject packet, with or without an EAP-Message attribute encapsulating EAP-Failure, MUST result in the NAS issuing an LCP Terminate Request to the authenticating peer. A RADIUS Access-Accept packet with an EAP-Message attribute encapsulating EAP-Success successfully ends the authentication phase. The RADIUS Access-Accept/EAP-Message/EAP-Success packet MUST contain all of the expected attributes which are currently returned in an Access-Accept packet.

The above scenario creates a situation in which the NAS never needs to manipulate an EAP packet. An alternative may be used in situations where an EAP-Request/Identity message will always be sent by the NAS to the authenticating peer.

For proxied RADIUS requests there are two methods of processing. If the domain is determined based on the Called-Station-Id, the RADIUS Server may proxy the initial RADIUS Access-Request/EAP-Start. If the domain is determined based on the user's identity, the local RADIUS Server MUST respond with a RADIUS Access-Challenge/EAP-Identity packet. The response from the authenticating peer MUST be proxied to the final authentication server.

For proxied RADIUS requests, the NAS may receive an Access-Reject packet in response to its Access-Request/EAP-Identity packet. This would occur if the message was proxied to a RADIUS Server which does not support the EAP-Message extension. On receiving an Access-Reject, the NAS MUST send an LCP Terminate Request to the authenticating peer, and disconnect.

5.1. Retransmission

As noted in [1], the EAP authenticator (NAS) is responsible for

retransmission of packets between the authenticating peer and the NAS. Thus if an EAP packet is lost in transit between the authenticating peer and the NAS (or vice versa), the NAS will retransmit. As in RADIUS [2], the RADIUS client is responsible for retransmission of packets between the RADIUS client and the RADIUS server.

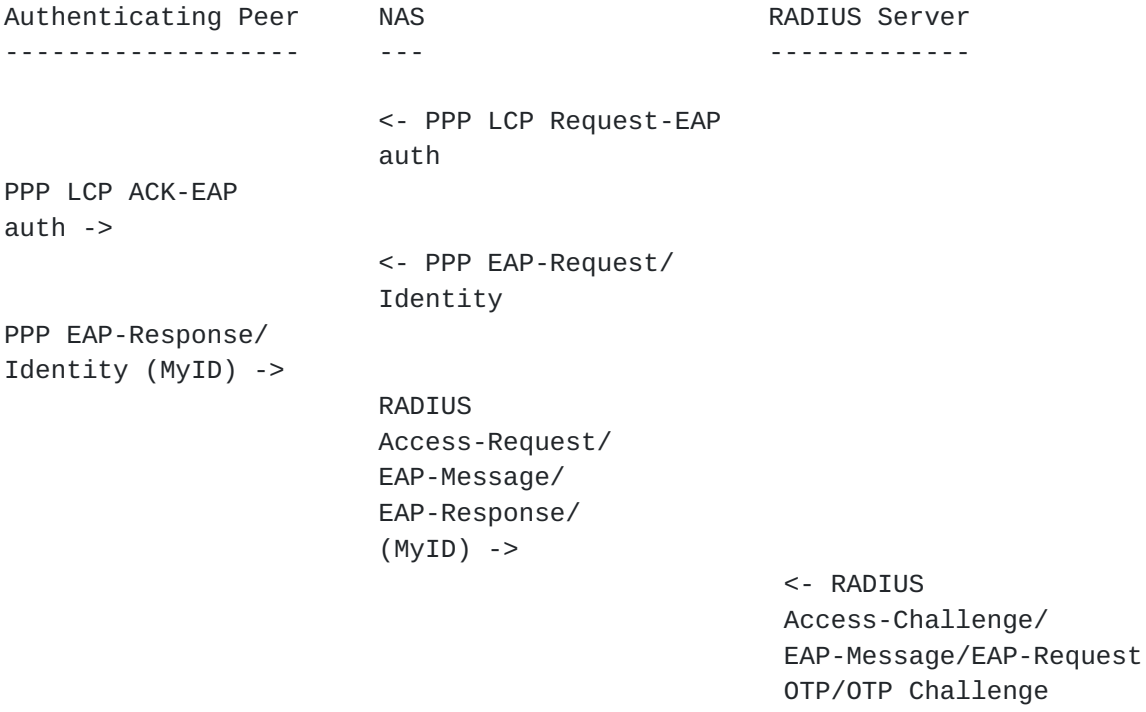
Note that it may be necessary to adjust retransmission strategies and authentication timeouts in certain cases. For example, when a token card is used additional time may be required to allow the user to find the card and enter the token. Since the NAS will typically not have knowledge of the required parameters, these need to be provided by the RADIUS server. This can be accomplished by inclusion of EAP-Timeout and Password-Retry attributes within the Access-Challenge packet.

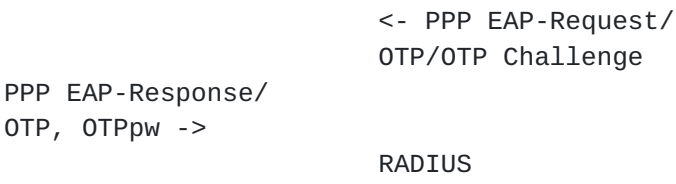
5.2. Fragmentation

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.

5.3. Examples

The example below shows the conversation between the authenticating peer, NAS, and RADIUS server, for the case of a One Time Password (OTP) authentication. OTP is used only for illustrative purposes; other authentication protocols could also have been used, although they might show somewhat different behavior.



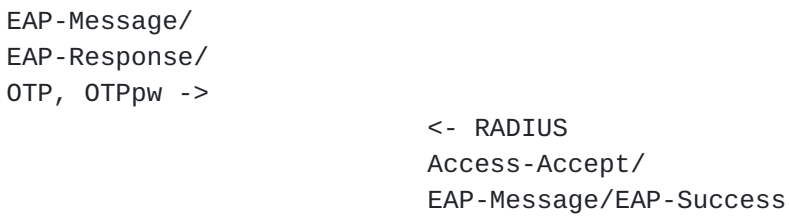

<- PPP EAP-Request/
OTP/OTP Challenge
PPP EAP-Response/
OTP, OTPpw ->
RADIUS

```
                        Access-Request/
                        EAP-Message/
                        EAP-Response/
                        OTP, OTPpw ->
                                                <- RADIUS
                                                Access-Accept/
                                                EAP-Message/EAP-Success
                                                (other attributes)
                        <- PPP EAP-Success
PPP Authentication
Phase complete,
NCP Phase starts
```

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
-------------------     ---                     -------------

                        <- PPP LCP Request-EAP
                        auth
PPP LCP ACK-EAP
auth ->
                        RADIUS
                        Access-Request/
                       EAP-Message/Start ->
                                                <- RADIUS
                                                Access-Challenge/
                                                EAP-Message/Identity
                        <- PPP EA-Request/
                        Identity
PPP EAP-Response/
Identity (MyID) ->
                        RADIUS
                        Access-Request/
                        EAP-Message/
                        EAP-Response/
                        (MyID) ->
                                                <- RADIUS
                                                Access-Challenge/
                                                EAP-Message/EAP-Request
                                                OTP/OTP Challenge
                        <- PPP EAP-Request/
                        OTP/OTP Challenge
PPP EAP-Response/
OTP, OTPpw ->
                        RADIUS
                        Access-Request/
```


EAP-Message/
EAP-Response/
OTP, OTPpw ->
<- RADIUS
Access-Accept/
EAP-Message/EAP-Success

```
                                                  (other attributes)
                        <- PPP EAP-Success
PPP Authentication
Phase complete,
NCP Phase starts
```

In the case where the client fails EAP authentication, the conversation would appear as follows:

```
Autheticating Peer     NAS                      RADIUS Server
-------------------     ---                      -------------

                        <- PPP LCP Request-EAP
                        auth
PPP LCP ACK-EAP
auth ->
                        Access-Request/
                        EAP-Message/Start ->
                                                 <- RADIUS
                                                 Access-Challenge/
                                                 EAP-Message/Identity
                        <- PPP EAP-Request/
                        Identity
PPP EAP-Response/
Identity (MyID) ->
                        RADIUS
                        Access-Request/
                        EAP-Message/
                        EAP-Response/
                        (MyID) ->
                                                  <- RADIUS
                                                  Access-Challenge/
                                                  EAP-Message/EAP-Request
                                                  OTP/OTP Challenge
                        <- PPP EAP-Request/
                        OTP/OTP Challenge
PPP EAP-Response/
OTP, OTPpw ->
                        RADIUS
                        Access-Request/
                        EAP-Message/
                        EAP-Response/
                        OTP, OTPpw ->
                                                  <- RADIUS
                                                  Access-Reject/
                                                  EAP-Message/EAP-Failure
```

<- PPP EAP-Failure
(client disconnected)

In the case that the RADIUS server or proxy does not support EAP-Message, the conversation would appear as follows:

```
Authenticating Peer     NAS                         RADIUS Server
-------------------     ---                         -------------

                        <- PPP LCP Request-EAP
                        auth
PPP LCP ACK-EAP
auth ->
                        RADIUS
                        Access-Request/
                        EAP-Message/Start ->
                                                    <- RADIUS
                                                    Access-Reject
                        <- PPP LCP Terminate
                        (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
-------------------     ---                         -------------

                        <- PPP LCP Request-EAP
                        auth
PPP LCP ACK-EAP
auth ->
                        RADIUS
                        Access-Request/
                        EAP-Message/Start ->
                                                    <- RADIUS
                                                    Access-Challenge/
                                                    EAP-Message/Identity
                        <- PPP EAP-Request/
                        Identity
PPP EAP-Response/
Identity
(MyID) ->
                        RADIUS
                        Access-Request/
                        EAP-Message/EAP-Response/
                        (MyID) ->
                                                    <- RADIUS
                                                    Access-Reject
                                                    (proxied from remote
                                                    RADIUS Server)
                        <- PPP LCP Terminate
                        (User Disconnected)
```

In the case where 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 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)
```

6. Alternative uses

Currently the conversation between the backend security server and the RADIUS server is proprietary because of lack of standardization. In order to increase standardization and provide interoperability between Radius vendors and backend 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 backend security server instead.

In the case where RADIUS-encapsulated EAP is used in a conversation between a RADIUS server and a backend security server, the security server will typically return an Access-Accept/EAP-Success 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/EAP-Success message to the NAS.

7. Attributes

7.1. EAP-Message

Description

This attribute encapsulates Extensible Authentication Protocol [1] packets so as to allow the NAS to authenticate dial-in users via EAP without having to understand the protocol.

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-Messages 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. Access-Accept and Access-Reject packets SHOULD only have ONE EAP-Message attribute in them, containing EAP-Success or EAP-Failure.

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 the EAP-Success o EAP-Failure packets) it is necessary that RADIUS/EAP provide integrity protection at least as strong as those used in the EAP methods themselves.

The Signature attribute specified in [4] MUST be used to protect all Access-Request, Access-Challenge, Access-Accept, and Access-Reject packets containing an EAP-Message attribute. For Access-Accepts the Signature is calculated as specified in [4]. For Access-Challenge, Access-Accept, and Access-Reject packets, the Signature is calculated as follows:

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

The Signature attribute is zeroed for the purposes of the calculation and the shared secret is used as the key for the HMAC-MD5

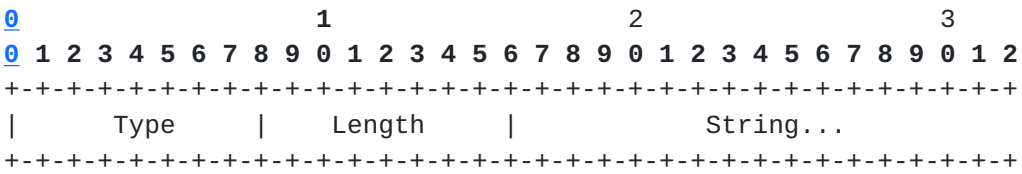
hash. The Signature is calculated and inserted in the packet before the Authenticator is calculated.

Access-Request packets including an EAP-Message attribute without a Signature attribute SHOULD be silently discarded by the RADIUS server. A RADIUS Server supporting EAP-Message MUST calculate the

correct value of the Signature and silently discard the packet if it does not match the value sent. A RADIUS Server not supporting EAP-Message MUST return an Access-Reject if it receives an Access-Request containing an EAP-Message attribute. A RADIUS Server receiving an EAP-Message attribute that it does not understand MUST return an Access-Reject.

Access-Challenge, Access-Accept, or Access-Reject packets including an EAP-Message attribute without a Signature attribute SHOULD be silently discarded by the NAS. A NAS supporting EAP-Message MUST calculate the correct value of the Signature and 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

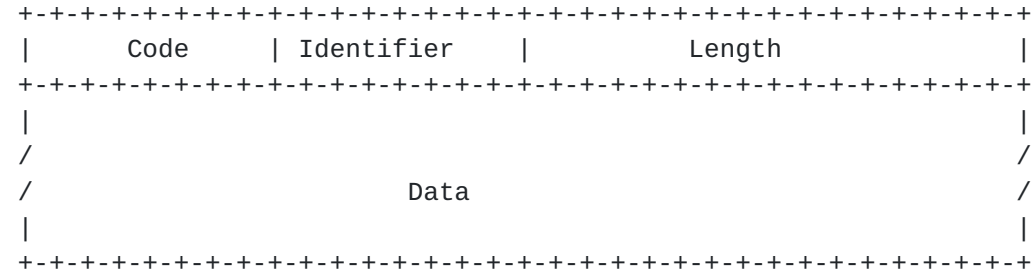
79 for EAP-Message

Length

>=3 (EAP packet enclosed)
=2 (EAP-Start message)

String

The String field includes EAP packets, as defined in [1]. 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 passed by RADIUS.



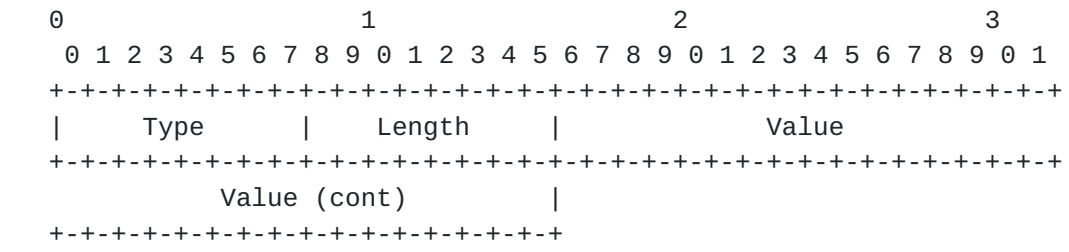
7.2. EAP-Timeout

Description

This attribute is used only in Access-Challenge packets and

provides the NAS with the timeout interval to apply during EAP authentication.

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



Type

? for EAP-Timeout

Length

6

Value

The field is 4 octets, containing a 32-bit unsigned integer with the maximum number of seconds the NAS should wait for an EAP-Response before retransmitting.

8. Security considerations

Since the purpose of EAP is to provide enhanced security for PPP authentication, it is critical that RADIUS support for EAP be secure. In particular, the following issues must be addressed:

Separation of the EAP server and PPP authenticator
Connection hijacking
Man in the middle attacks
Multiple databases
Negotiation attacks

8.1. Separation of the EAP server and PPP authenticator

As described in [8] and [9], it is possible for the EAP endpoints to mutually authenticate, negotiate a ciphersuite, and derive a session key for subsequent use in PPP encryption.

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 pass the session key to the PPP encryption module.

The situation may be more complex when EAP/RADIUS is used, since the PPP authenticator will typically not reside on the same machine as the

EAP server. For example, the EAP server may be a backend security server, or a module residing on the RADIUS server.

In the case where the EAP server and PPP authenticator reside on different machines, there are several implications for security. Firstly, mutual authentication will occur between the peer and the EAP 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.

As described earlier, when EAP/RADIUS is used to encapsulate EAP packets, the Signature attribute is required in EAP/RADIUS Access-Requests sent from the NAS or tunnel server to the RADIUS server. Since the Signature attribute involves a HMAC-MD5 hash, 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. Similarly, Access-Challenge packets sent from the RADIUS server to the NAS are also authenticated and integrity protected using an HMAC-MD5 hash, enabling the NAS or tunnel server to determine the integrity of the packet and verify the identity of the RADIUS server. Morever, EAP packets sent via the methods described in [8] and [9] contain their own integrity protection, so that they cannot be successfully modified by a rogue NAS or tunnel server.

The second issue that arises in the case of an EAP server and PPP authenticator residing on different machines is that the session key negotiated between the peer and EAP server will need to be transmitted to the authenticator. Therefore a mechanism needs to be provided to transmit the session key from the EAP server to the authenticator or tunnel server that needs to use the key. The specification of this transit mechanism is outside the scope of this document.

8.2. Connection hijacking

In this form of attack, the attacker attempts to inject packets into the conversation between the NAS and the RADIUS server, or between the RADIUS server and the backend security server. RADIUS does not support encryption, and as described in [2], only Access-Reply and Access-Challenge packets are integrity protected. Moreover, the integrity protection mechanism described in [2] is weaker than that likely to be used by some EAP methods, making it possible to subvert those methods by attacking EAP/RADIUS.

In order to provide for authentication of all packets in the EAP exchange, all EAP/RADIUS packets MUST be authenticated using the Signature attribute, as described previously.

8.3. Man in the middle attacks

Since RADIUS security is based on shared secrets, end-to-end security is not provided in the case where authentication or accounting packets are forwarded along a proxy chain. As a result, attackers gaining

control of a RADIUS proxy will be able to modify EAP packets in transit without fear of detection.

This represents a weakness of RADIUS which cannot be remedied without providing end-to-end data object security.

8.4. Multiple databases

In many cases a backend security server will be deployed along with a RADIUS server in order to provide EAP services. Unless the backend 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 backend 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 backend security server store information in the same backend database; by having the backend security server provide a full RADIUS implementation; or by consolidating both the backend security server and the RADIUS server onto the same machine.

8.5. Negotiation attacks

In a negotiation attack, a rogue NAS, tunnel server, RADIUS proxy or RADIUS server causes the authenticating peer to choose a less secure authentication method so as to make it easier to obtain the user's password. For example, a session that would normally be authenticated with EAP would instead authenticated via CHAP or PAP; alternatively, a connection that would normally be authenticated via one EAP type occurs via a less secure EAP type, such as MD5. 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 [7].

Protection against negotiation attacks requires the elimination of downward negotiations. This can be achieved via implementation of per-connection policy on the part of the authenticating peer, and per-user 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 EAP when calling one service, while negotiating CHAP for another service, even if both services are accessible via the same phone number.

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 CHAP or PAP.

For a NAS, it may not be possible to determine whether a user is required to authenticate with EAP until the user's identity is known. For example, for shared-uses NASes it is possible for one reseller to implement EAP while another does not. In such cases, if any users of the NAS MUST do EAP, then the NAS MUST attempt to negotiate EAP for every call. This avoids forcing an EAP-capable client to do more than one authentication, which weakens 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 user 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, the NAS MUST send an LCP-Terminate and disconnect the user. 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 user dialing in from one location (with an EAP-capable proxy) might be able to successfully authenticate via EAP, while the same user dialing into another location (and encountering an EAP-incapable proxy) might be consistently disconnected.

9. Acknowledgments

Thanks to Dave Dawson and Karl Fox of Ascend, and Glen Zorn and Narendra Gidwani of Microsoft for useful discussions of this problem space.

10. References

[1] L. Blunk, J. Vollbrecht. "PPP Extensible Authentication Protocol (EAP)." RFC 2284, Merit Network, Inc., March 1998.

[2] C. Rigney, A. Rubens, W. Simpson, S. Willens. "Remote Authentication Dial In User Service (RADIUS)." RFC 2138, Livingston, Merit, Daydreamer, April 1997.

[3] C. Rigney. "RADIUS Accounting." RFC 2139, Livingston, April 1997.

[4] C. Rigney, W. Willats. "RADIUS Extensions." Work in progress, draft-ietf-radius-ext-01.txt, Livingston, June, 1997.

[5] R. Rivest, S. Dusse. "The MD5 Message-Digest Algorithm." RFC 1321, MIT Laboratory for Computer Science, RSA Data Security Inc., April 1992.

[6] S. Bradner. "Key words for use in RFCs to Indicate Requirement Levels." RFC 2119, Harvard University, March, 1997.

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

[8] B. Aboba, D. Simon. "PPP EAP TLS Authentication Protocol." Work in progress, draft-ietf-pppext-eaptls-03.txt, Microsoft, April 1998.

[9] G. Carter. "PPP EAP ISAKMP Authentication Protocol." Work in progress, draft-ietf-pppext-eapisakmp-00.txt, Entrust, November 1997.

11. Authors' Addresses

Pat R. Calhoun
Technology Development
Sun Microsystems, Inc.
15 Network Circle
Menlo Park, CA 94025

Phone: 847-548-0926
Fax: 650-786-6445
EMail: pcalhoun@toast.net

Allan C. Rubens
Merit Network, Inc.
4251 Plymouth Rd.
Ann Arbor, MI 48105-2785

Phone: 313-647-0417
EMail: acr@merit.edu

Bernard Aboba

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052

Phone: 425-936-6605

EMail: bernarda@microsoft.com

r