ROAMOPS Working Group
INTERNET-DRAFT
Category: Standards Track
<draft-ietf-roamops-roamsec-02.txt>
20 July 1998

Pat Calhoun
Sun Microsystems
Bernard Aboba
Microsoft

End-to-End Security in Roaming

1. Status of this Memo

This document is an Internet-Draft. Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

To learn the current status of any Internet-Draft, please check the "1id-abstracts.txt" listing contained in the Internet-Drafts Shadow Directories on ftp.ietf.org (US East Coast), nic.nordu.net (Europe), ftp.isi.edu (US West Coast), or munnari.oz.au (Pacific Rim).

The distribution of this memo is unlimited. It is filed as <draft-ietf-roamops-roamsec-02.txt>, and expires January 15, 1999. Please send comments to the authors.

2. Abstract

As noted in Roaming Requirements, there is a need for end-to-end security in roaming, including end-to-end integrity protection, and confidentiality. In roaming implementations based on proxy chaining, packets are routed between the NAS and home server through a series of proxies. Current roaming implementations provide only hop-by-hop security, guarding only against modification of packets in transit between hops. This makes it possible for untrusted proxies to modify packets sent between a NAS and a home server without detection, as well as to decrypt PAP passwords, Tunnel passwords, and other hidden attributes which are available to it in cleartext.

This document provides a framework for end-to-end security in roaming, making it possible to provide end-to-end message integrity and attribute hiding through addition of three new attributes.

3. Introduction

As noted in [2], there is a need for end-to-end security in roaming, including end-to-end integrity protection, and confidentiality. In

roaming implementations based on proxy chaining, packets are routed between the NAS and home server through a series of proxies. Current roaming implementations, as described in [1] provide only hop-by-hop security, guarding only against modification of packets in transit between hops. This makes it possible for untrusted proxies to modify packets sent between a NAS and a home server without detection, as well as to decrypt PAP passwords, Tunnel passwords, and other hidden attributes which are available to proxies in cleartext.

This document provides a framework for end-to-end security in roaming, making it possible to provide end-to-end message integrity and attribute hiding through addition of three new attributes, Security-Parameter-Index, Hidden and End-to-End-Signature. In this document, it is assumed that a key has previously been established between the two endpoints. It is this key which is used in calculation of the message integrity check, as well as in end-to-end encryption of attributes. Future documents will discuss key exchange issues.

The Security-Parameters-Index attribute is used to identify the security association within which the End-to-End-Signature and Hidden attributes are to be evaluated. Note that in the case where an intermediate proxy implements policy, it is possible for a security association to be established between the intermediate proxy and the home server, NAS, or local proxy. For example, an intermediate proxy may immediately send an Access-Reject to the NAS in response to an Access-Request, without having first forwarded it to the home server. In this case, the intermediate proxy and NAS would need to establish a security association in order to permit verification of the authenticity of the Access-Reject.

Using the Hidden attribute, it is possible for the client or server to protect an attribute end-to-end. This is accomplished by encapsulating and then encrypting another attribute within the Hidden attribute.

Using the End-to-End-Signature attribute, it is possible for a client or server to provide a keyed MAC which will allow end-to-end integrity protection. The keyed MAC is calculated over the immutable portions of the packet header, as well as all of the attributes preceeding the End-to-End-Signature attribute. This makes it possible for some or all of the attributes in the packet to be protected, at the sender's discretion.

While a proxy may add, delete or modify unprotected attributes, it MUST NOT add, delete or modify protected attributes so that the validity of the keyed MAC can be maintained. A proxy also MUST NOT modify an End-to-End-Signature or Hidden attribute. On receiving a packet including an End-to-End-Signature attribute, an end system implementing end-to-end security MUST check the validity of the message

integrity check and MUST silently discard the packet if the message integrity check cannot be verified.

By allowing the message integrity check to be applied to a subset of attributes selected by the sender, and by allowing attributes to be hidden individually, these extensions enable end-to-end security

functionality while at the same time enabling proxies to continue to implement policy. As described in [8], policy function is a central part of the roaming architecture since roaming is inherently an inter-domain activity.

4. Requirements language

In this document, the key words "MAY", "MUST, "MUST NOT", "optional", "recommended", "SHOULD", and "SHOULD NOT", are to be interpreted as described in [7].

5. Transition

Since NAS devices will not initially implement the End-to-End-Signature and Hidden attributes, it is envisaged that these attributes will initially be deployed on local proxies and home servers. In this scenario, the local proxy will be configured to employ end-to-end security for those NAS devices that do not support this. In this case, the local proxy would add End-to-End security attributes to Access-Requests destined for the home server and would process End-to-End security attributes in an Access-Accept, Access-Reject or Access-Challenge originated by the home server.

Note that if a NAS is end-to-end security enabled, then the local proxy will receive an Access-Request from the NAS with an End-to-End-Signature and will not need to add its own. As a result, a packet should include at most one End-to-End-Signature attribute. A packet may contain more than one Hidden attribute.

6. Proposed attributes

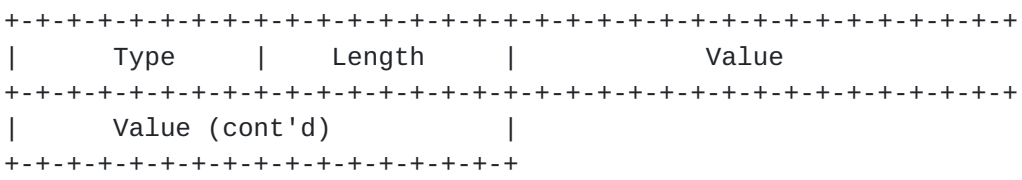
6.1. Security-Parameter-Index

Description

The purpose of the Security-Parameter-Index attribute is to identify the security association within which the End-to-End-Signature and Hidden attributes should be evaluated.

A summary of the Security-Parameter-Index attribute is shown below. The fields are transmitted from left to right.

```
0                   1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2
```


Type
Length
Value
Value (cont'd)

Type

? for Security-Parameter-Index

Length

6

Value

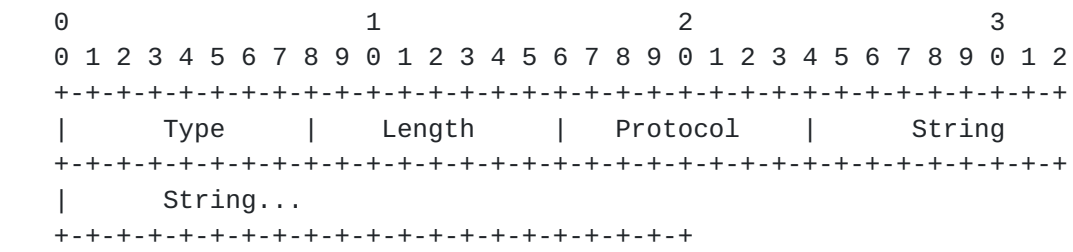
The Value field is four octets. This serves as an index identifying the security association established between the two end-points.

6.2. End-to-End-Signature

Description

This attribute provides for the use of a keyed-MAC to be verified end-to-end.

A summary of the End-to-End Signature attribute is shown below. The fields are transmitted from left to right.



Type

? for End-to-End-Signature

Length

19 (protocol 1)

Protocol

The protocol field specifies the authentication algorithm to be used in computing the message authentication code (MAC) which is placed in the string field.

If the protocol field is 1, the HMAC protocol, described in [6] is used, along with the MD5 algorithm described in [5]. All implementations MUST support HMAC-MD5. No other protocol values

are defined.

String

The End-to-End-Signature is an calculated using the algorithm

specified in the protocol field. The MAC is computed over the portion of the RADIUS packet from the beginning until the end of the End-to-End-Signature attribute, including Type, ID, Length and authenticator. In calculating the End-to-End-Signature, the authenticator should be considered to be filled with zeroes, and the End-to-End-Signature string should be considered to be six-teen octets of zero.

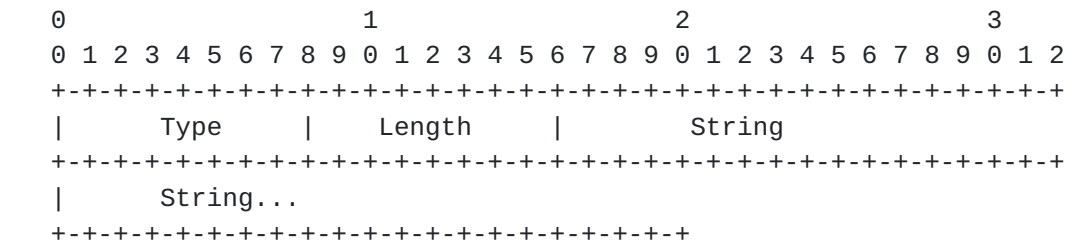
The portion of the RADIUS packet after the End-to-End-Signature attribute is not included in the calculation of the MAC. This makes it possible for a proxy to add, modify, or delete attributes placed after the End-to-End-Signature attribute. As a result, attributes placed prior to the End-to-End-Signature attribute can be considered "protected" and those placed after the attribute can be considered to be "unprotected." Note that in order for the End-to-End-Signature to be verified, the proxy MUST maintain attribute order.

6.3. Hidden

Description

The purpose of the Hidden attribute is to make possible end-to-end encryption of individual attributes. This would make it possible for attributes such as User-Password or Tunnel-Password to be sent securely between a RADIUS client and a server, without risk of com-promise by an untrusted proxy.

A summary of the Hidden attribute is shown below. The fields are transmitted from left to right.



Type

? for Hidden

Length

>=4

String

The String field includes the encapsulated ciphertext of the attribute which is to be hidden end-to-end. The hidden attribute is encrypted using a key and encryption algorithm which had previously been established between the two endstations. Note that

due to the 253 octet limitation on the size of RADIUS attributes, the encapsulated attribute may be a maximum of 251 octets in length.

7. Table of Attributes

The following table provides a guide to which attributes may be found in which kind of packets.

Request	Accept	Reject	Challenge	#	Attribute
0-1	0-1	0-1	0-1	?	End-to-End-Signature
0+	0+	0	0+	?	Hidden
0-1	0-1	0-1	0-1	?	SPI

8. Security issues

The following security threats have been identified in roaming systems:

Rogue proxies
Theft of passwords
Theft of accounting data
Replay attacks
Connection hijacking
Fraudulent accounting

8.1. Rogue proxies

In conventional ISP application, the NAS, proxy, and home server exist within a single administrative entity. As a result, the proxy may be considered a trusted component.

However, in a roaming system implemented with proxy chaining, the NAS, proxies, and home server may be managed by different administrative entities. Through the use of shared secrets it is possible for proxies operating in different domains to establish a trust relationship. However, if packets are only authenticated on a hop-by-hop basis, then untrusted proxies are capable of perpetrating a number of man-in-the-middle attacks.

These attacks typically involve the editing of attributes, or the modification or insertion of messages, such as the substitution of an Access-Accept for an Access-Reject. For example, a proxy may modify an Access-Accept sent by the home server so as to lessen the security obtained by the client. For example, EAP attributes might be removed or modified so as to cause a client to authenticate with EAP MD5 or

PAP, instead of a stronger authentication method. Alternatively, tunnel attributes might be removed or modified so as to remove encryption, redirect the tunnel to a rogue tunnel server, or otherwise lessen the security provided to the client.

Through implementation of the End-to-End-Signature attribute, it is possible to detect unauthorized addition, deletion, or modification of protected attributes. Note that it is still possible for a rogue proxy to add, delete, or modify unprotected attributes.

While a proxy MUST NOT send an Access-Accept to the NAS after receiving an Access-Reject from the home server, a proxy MAY send an Access-Reject to the NAS after receiving an Access-Accept from the home server. Note that in the latter case, a Security-Parameter-Index attribute should be used denoting the security association between the proxy and the NAS, rather than that between the home server and the NAS, since the proxy has originated the packet. This will allow the NAS to verify the End-to-End-Signature attribute within the packet, and decide whether to silently discard the packet. As noted earlier, an Access-Accept originated by a proxy MUST be silently discarded by the NAS, even if the End-to-End-Signature attribute can be verified.

The determination of whether end-to-end security is to be used in a conversation is made using out-of-band mechanisms. Typically this is based either on static configuration or on the outcome of a key exchange conversation between the two endpoints. However, once it is determined that the end systems wish to use end-to-end security, all packets sent MUST include an End-to-End-Signature attribute and packets received without an End-to-End-Signature attribute MUST be silently discarded. Note that policy determination using an out-of-band mechanism rather than a proxied conversation limits the ability of a rogue proxy to interfere with the security negotiation between the two end systems.

8.2. Theft of passwords or keys

Unless the Hidden attribute is used, where clients authenticate using PAP, or where the Tunnel-Password attribute is included with the Access-Accept, each proxy along the path between the local NAS and the home server will have access to the cleartext password or key. In many circumstances, this represents an unacceptable security risk. As a result, the Hidden attribute SHOULD be used to provide end-to-end confidentiality for User-Password or Tunnel-Password attributes.

8.3. Integrity and confidentiality of accounting data

Typically in roaming systems, accounting packets are provided to all the participants along the roaming relationship path, in order to allow them to audit subsequent invoices. In order to prevent modification of accounting packets by untrusted proxies, the End-to-End-Signature attribute MAY be used. If it is desired that accounting data be kept confidential from a proxy, the Hidden attribute MAY be used. If

the objective is to prevent snooping of accounting data on the wire, then IPSEC ESP MAY be used.

8.4. Replay attacks

In this attack, a man in the middle or rogue proxy collects CHAP-Challenge and CHAP-Response attributes, and later replays them. If this attack is performed in collaboration with an unscrupulous ISP, it can be used to subsequently submit fraudulent accounting records to the accounting agent for payment. The system performing the replay need not necessarily be the one that initially captured the CHAP Challenge/Response pair.

While such an attack has always been possible, without roaming the threat is restricted to proxies operating in the home server's domain. With roaming, such an attack can be mounted by any proxy capable of reaching the home server.

In order to protect against replay attacks, CHAP-Challenge and CHAP-Response attributes MAY be protected using the Hidden attribute. CHAP replay attacks can also be defeated by means of an end-to-end challenge-response exchange. For example, if the home server returns an Access-Challenge packet containing a CHAP-Challenge attribute and maintains state with respect to outstanding challenges, replay attacks cannot succeed.

However, it should also be noted that end-to-end challenges (as practiced within the EAP MD5 authentication method, or in the CHAP-Challenge method described above) are also subject to attacks by rogue proxies. In such an attack a proxy substitutes a static challenge for the challenge sent by the home server, and on receiving the response, checks it against a databases of hashes applied against a dictionary. This attack may be prevented through use of the End-to-End-Signature attribute.

8.5. Connection hijacking

In this form of attack, the attacker attempts to inject packets into the conversation between the NAS and the home server. RADIUS as described in [3] is vulnerable to such attacks since only Access-Reply and Access-Challenge packets are authenticated. This attack may be defeated via use of an End-to-End-Signature attribute.

8.6. Fraudulent accounting

In this form of attack, a local proxy transmits fraudulent accounting packets or session records in an effort to collect fees to which they are not entitled. This includes submission of packets or session records for non-existent sessions, or submission of exaggerated session times for actual sessions.

Such behavior will only be easily detectable in the event that roaming users are making use of voluntary or compulsory tunneling, in which case the tunnel server will generate its own accounting record, which may be compared to that generated by the local ISP. However, tunneling

is expected to represent only a small percentage of roaming use.

In order to detect submisson of fraudulent accounting packets or session records, the the accounting gateway SHOULD send copies of session records to all parties with a financial interest in the session. Parties receiving copies of these session records SHOULD reconcile them with logs of proxied authentications.

In order to make it easier to match authentication logs with accounting records, home servers involved in roaming SHOULD include a Class attribute in the Access-Accept. The Class attribute should uniquely identify a session, so as to allow an authentication log entry to be matched with a corresponding accounting log.

In order to be able to match accounting logs with logs of proxied authentications, accounting agents SHOULD require that they act as an authentication proxy for all sessions for which an accounting record will subsequently be submitted.

9. Acknowledgments

Thanks to Glen Zorn of Microsoft for useful discussions of this problem space.

10. References

[1] B. Aboba, J. Lu, J. Alsop, J. Ding, W. Wang. "Review of Roaming Implementations." RFC 2194, Microsoft, Aimnet, i-Pass Alliance, Asiainfo, Merit, September 1997.

[2] B. Aboba, G. Zorn. "Roaming Requirements." Internet-Draft (work in progress) draft-ietf-roamops-romreq-09.txt, Microsoft, April 1998.

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

[4] C. Rigney. "RADIUS Accounting." RFC 2139, Livingston, April 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] Krawczyk H., M. Bellare and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication," Internet Draft (work in progress), draft-ietf-ipsec-hmac-md5-01.txt, August 1996.

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

[8] B. Aboba, J.R. Vollbrecht, "Proxy Chaining and Policy

Implementation in Roaming," Internet Draft (work in progress), draft-ietf-roamops-auth-05.txt, Microsoft, MERIT, July 1998.

11. Authors' Addresses

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

Phone: 650-786-7733
Fax: 650-786-6445
EMail: pcalhoun@eng.sun.com

Bernard Aboba
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052

Phone: 206-936-6605
EMail: bernarda@microsoft.com