Internet Engineering Task Force
MSEC Working Group
INTERNET-DRAFT

EXPIRES: September 2003

Mark Baugher (Cisco Systems)
Ran Canetti (IBM Watson)
Pau-Chen Cheng (IBM Watson)
Pankaj Rohatgi (IBM Watson)

March 2003

MESP: A Multicast Framework for the IPsec ESP
<draft-ietf-msec-mesp-01.txt>

Status of this memo

Abstract

Multicast ESP (MESP) is a framework for multicast data-origin authentication using the IPsec Encapsulating Security Payload (ESP) protocol. The MESP framework combines group-secrecy, group-authentication, and source-authentication transforms in an ESP packet. MESP uses a message authentication code for group authentication to protect a digital signature, TESLA timed MAC, or other multicast source-authentication transform.

TABLE OF CONTENTS

1.0 Notational Conventions

The key words "MUST", "MUST NOT", "REQUIRED", "MUST", "MUST NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].
The terminology conforms to [RFC2828].

2.0 Introduction

The IPsec Encapsulation Security Payload (ESP) provides a set of security services that include data origin authentication, which enables an IPsec receiver to validate that a received packet

originated from a peer-sender in a pairwise security association [Section 3.1, RFC2401]. A Message Authentication Code (MAC), such as the hash-based message authentication code [RFC2104, RFC2404] (HMAC), is the common means to provide data-origin authentication for pairwise IPsec security associations. For secure groups such as IP multicast groups, however, a MAC supports only "group authentication" and not data-origin authentication [CP]. This Internet-Draft document (I-D) defines a framework for ESP data-

origin authentication that is suitable for IP multicast groups of ESP receivers.

2.1 Changes from the Previous Version

This version is not a protocol, unlike the previous version, but is a transform framework for ESP and realizes all of its functions within the ESP protocol. MESP now imposes an additional structure and usage on IPsec ESP Initialization Vector (IV) and Integrity Check Value (ICV) fields [ESPbis].

A smaller change that appears in this version of MESP is the requirement that TESLA authentication be protected by external authentication transform such as a MAC.

2.2 Overview

This I-D assumes that the reader is familiar with the "Security Architecture for Internet Protocol" [RFC2401] and the "IP Encapsulating Security Payload (ESP)" [ESPBIS] RFCs. Section 3 reviews the functionalities of group data-security transforms for applications such as media streaming, process control, and reliable multicast applications. Section 3 describes the problem of authenticating the source when the data-authentication key is shared by more than two IPsec endpoints. Section 4 describes the MESP framework in terms of the extensions and use of the ESP IV and integrity-check-value fields. The three functionalities of the MESP framework are realized in cryptographic transforms that are secure for various uses, and Section 5 recites the security considerations for each MESP transform. Section 5 considers IP multicast risks, the transforms that address a particular risk, and the suitability of a transform for various applications and environments.

3.0 IP Multicast Security Functionalities

The security requirements for multicast have been discussed in [CP]. In general, group security has different requirements and characteristics than pairwise security. In particular, data-origin authentication using a MAC will not prevent one member from impersonating another when a group of three or more members share the symmetric authentication key. There are three new functionalities needed to add data-origin authentication to ESP.

a) Group Secrecy (GS)

The GS functionality is ESP confidentiality applied to a group . It ensures that transmitted data are accessible only to group members (i.e. two or more hosts in possession of a shared symmetric key). This can also be viewed as a way to enforce access control. A typical realization of GS is to encrypt data using a key known only to group members. Essentially, the solution for multicast is the

same as the solution for unicast confidentiality. It is important to note, however, that some encryption transforms have special considerations when a key is shared among multiple senders. An MESP encryption or authentication transform SHOULD describe any potential risks of multicast operation and how those risks are averted.

b) Group Authentication (GA)

The GA functionality enables a group member to verify that the received data originated from someone in the group and was not modified en-route by a non-group member. Note that group authentication by itself does not identify the source of the data. For example, the data might have been forged by any malicious group member. GA can be efficiently realized using standard shared key authentication mechanisms such as Message Authentication Codes (MACs), e.g., CBC-MAC, HMAC, or UMAC.

c) Source and Data Authentication (SrA)

The SrA functionality enables a group member to verify that the received data originated from the claimed source and was not modified en-route by anyone (including other malicious group

members). Unlike Group Authentication, SrA provides the IPsec data-origin authentication function [RFC2401, ESPbis]. Source and Data Authentication provides a much stronger security guarantee than Group Authentication in that a particular group member can be identified as a source of a packet. Group and multicast source authentication requires stronger cryptographic techniques such as digital signatures, stream signatures [GR], flow signatures [WL], hybrid signatures [R], timed MACs, e.g. TESLA [TESLA, Ch,PCTS],asymmetric MACs [CGIMNP], etc.

3.1 Composition of the Functionalities

A secure multicast solution is likely to utilize all three of the basic functionalities. Due to the diversity of the various application and deployment scenarios for multicast, several issues arise with respect to the composition and ordering of these functionalities.

In ESP, encryption precedes authentication when both are applied and a "combined-mode" confidentiality/integrity operation is not used [Section 3.3.2 of ESPBIS]. Combined modes of encryption and authentication are supported in ESP [ESPbis] but are not considered in this version of MESP. Encryption first is an efficient ordering that allows the receiver to apply a message authentication code (MAC) before it runs a more computationally-intensive decryption; fast authentication before decryption offers a better defense against bogus packets from a denial of service attack. In MESP, therefore, the group secrecy (GS) transform MUST precede group authentication (GA) when GS is used. In other words, the sender

applies GS prior to GA and the receiver applies GA prior to GS. Krawczyk has shown that it is more secure to authenticate encrypted data rather than encrypt authenticated data [K], but this ordering does not provide non-repudiation. The latter is usually not needed or even desirable for IPsec applications.

MESP uses the same ordering for SrA: SrA MUST follow GS. Digital signatures offer the simplest method for multicast source authentication (SrA) but are computationally expensive, greatly expand the packet size and impractical for many, if not most, packet flows. Given the relatively high cost of signature verification, a digital signature leaves the receiver vulnerable to denial of

service attack when an attacker succeeds in getting the receiver to perform signature validation of bad packets.

MESP partially protects the receiver from denial-of-service attacks from bogus digitally-signed packets by applying a MAC to the packet after signing it. MESP calls this MAC "external authentication" and applies it in an identical fashion to ESP. The digital signature is called "internal authentication," which the sender applies to the packet payload before the MAC. MAC authentication, therefore, is applied first by the receiver. If the attacker is not a member of the group, or otherwise has not obtained the group key, the MAC will fail before the receiver incurs the burden of a signature validation.

SrA transforms such as TESLA timed-MAC can be more efficient than digital signatures for many applications. But like a digital signature, it is REQUIRED that TESLA and other SrA transforms use internal authentication in MESP and be protected by an external-authentication MAC. Thus, a digital signature or TESLA MAC MUST be applied prior to GA at the sender and after GA at the receiver. MAC-based GA is an external-authentication transform that MUST be applied last at the sender and first at the receiver. As in ESP, encryption (GS) is applied before any authentication and is optional.

3.2 MESP Security Association Database

The MESP framework applies up to three transforms to a multicast ESP packet in the order described above: Group Secrecy (GS) is OPTIONAL, Source Authentication (SrA) SHOULD be applied next, and Group Authentication (GA) SHOULD be applied last. The IPsec SAD MUST be extended to store the additional transform information if MESP is to be supported.

There are no changes to ESP SA lookup beyond what is specified for multicast SAs in the IPsec specifications [AHbis, ESPbis].

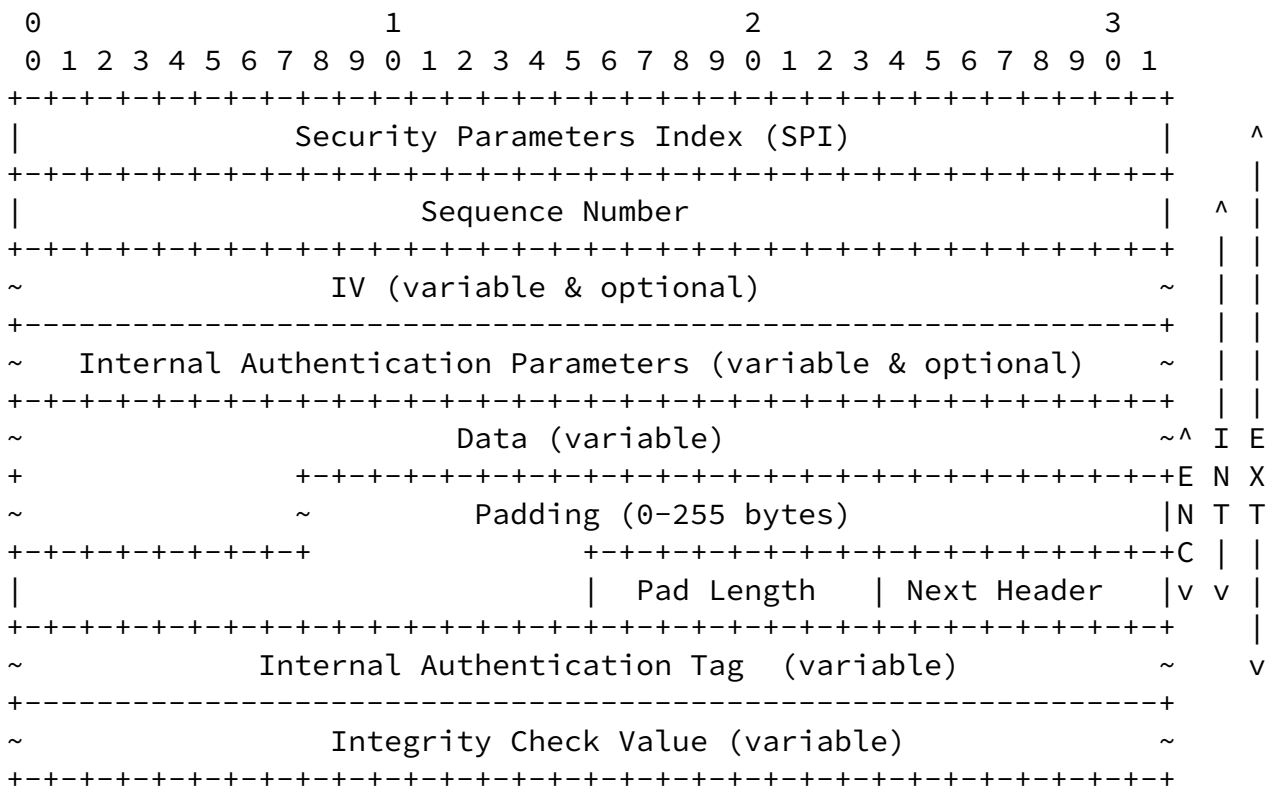
4.0 MESP Packet Format

The ESP Packet format is illustrated in Figure 4-1:

* Internal Authentication Parameters (variable). The length and contents of this field are defined by the SrA transform. Certain internal authentication transforms have a zero length SrA Transform Parameters fields (Section 5.1).

* Internal Authentication Tag (Variable). The length and contents of this field are defined by the internal authentication transform. Certain SrA transforms have a zero length Internal Authentication Tag field.

Figure 4-1: MESP Transforms in an ESP Packet



Encryption (ENC), when applied, covers the ESP data, padding and next header fields. Internal Authentication (INT) covers the ESP sequence number through the next header field, inclusive. External authentication (EXT) covers the entire ESP packet except for the Integrity Check Value (ICV) field.

A sender MAY use an encryption-transform (ENC) as done in any other ESP packet.

When INT is applied to the packet, its output (if any) is placed in the Internal Authentication Tag. Section 4.1 identifies the INT transforms, which the sender MUST perform prior to the encryption transform.

A sender of an MESP packet SHOULD use an external-authentication transform (EXT). Section 4.1 identifies the EXT transforms, which the sender MUST perform last (and the receiver performs first).

The sender MUST perform the MESP transforms in the order of ENC, INT, and EXT while the receiver MUST perform them in the order of EXT, INT and ENC.

4.1 MESP Transforms

This version of MESP defines a minimal number of transforms. In the future, new transforms MAY be added through the publication of an Internet RFC. The transforms of the MESP framework are listed below and classified according to MESP type.

4.1.1 Group Secrecy

MESP supports 3DES, AES-CBC, and AES-CTR.

4.1.2 Internal Authentication

MESP internal authentication is either RSA-SHA1 or TESLA.

4.1.3 External Authentication

MESP external authentication uses HMAC-SHA1.

4.2 MESP Signaling

MESP parameters are signaled through a key management protocol or interface such as GDOI, GSAKMP, GKMP, or SDP.

4.2.1 GDOI

GDOI MUST signal use of the MESP framework using PROTO_ESP_MESP with the TRANSFORM ID set to the MESP transform ID value (see IANA Section below). MESP extends the RFC 2407 attributes ["IPsec Security Association Attributes," IANA] with the three new classes, "ENC_Transform, "INT_Transform," and "EXT_Transform" (see IANA Section below).

The ENC Transform MUST be one of the transforms from 4.1.1. Additional ENC transforms MAY be added to this suite through the

publication of an Internet RFC.

The INT Transform MUST be non-null and MUST be one of the values from 4.1.2. Additional INT transforms MAY be added to this suite through the publication of an Internet RFC.

The EXT Transform MUST be one of the transforms from 4.1.3. Additional EXT transforms MAY be added to this suite through the publication of an Internet RFC.

The IANA Considerations section of this document describes value assignments for the EXT, INT and ENC attributes.

The SA Life Type and Life Duration as defined in RFC 2407 [RFC2407, IANA] apply to all keys used for the session, including the Signature PubKey, which MUST NOT be sent if the INT Transform is not a digital signature algorithm. The length of the encoding is determined by INT. {Editor: Need to define the Signature PubKey format and should make it a GDOI KD payload item instead.}

4.2.2 GSAKMP

TBD

4.2.3 MIKEY

TBD

5.0 Security Considerations

MESP is a framework for IPsec ESP authentication and encryption transforms to support IP multicast delivery. IPsec ESP provides access control, rejection of replayed packets, confidentiality (encryption), limited traffic-flow confidentiality and connectionless integrity. ESP supports a datagram environment where each IP packet is cryptographically independent of other IP packets and can be decrypted, authenticated, and integrity checked when delayed, reordered, or when other packets from the flow are lost. ESP provides rejection of replayed packets for pairwise security

associations and for multicast security associations under certain circumstances [ESPbis]. MESP has the same replay mechanism for the single-sender case; the multi-sender case is for further study. ESP provides data origin authentication for pairwise security associations using symmetric message authentication codes, which are not sufficient for group security applications where more than two members share a symmetric key.

5.1 MESP Authentication

The MESP framework for ESP provides data-origin authentication services to multicast ESP packets. Secure groups, such as secure multicast groups, cannot use a symmetric-key MAC to uniquely identify the sender; any group member that is in possession of the group authentication key is capable of replacing the source address of the packet with that of another group member and applying the symmetric key to authenticate the packet. To uniquely identify a sender among a group of members, digital signature, public key

encryption, or specialized source-authentication techniques such as timed MACs are needed. This version of MESP defines a general ESP packet structure for accommodating a digital signature or TESLA timed MAC.

5.2 MESP Denial-of-Service Protection

As discussed above, a group member cannot authenticate the source of the packet for a multicast group where multiple members share the MAC key. Thus, a rogue member of the group has all the keying material needed to impersonate a sender of the group if that attacker is able to inject packets into the network using that sender's IP address. The MESP framework addresses this problem by augmenting the MAC with an "internal authentication" transform, which MAY be an RSA-SHA1 digital signature or a TESLA timed MAC. Digital signatures leave multicast receivers vulnerable to denial-of-service attack if the receiver is duped into performing computationally-expensive signature validation of bogus packets. An external message authentication SHOULD accompany a digital signature so as to limit the effectiveness of bogus digitally signed packets by non-group members. TESLA is also vulnerable to a denial of service attack if the receiver is duped into storing bogus packets awaiting MAC verification. An external message authentication

transform SHOULD accompany a TESLA authentication transform so as to limit the effectiveness of bogus TESLA packets by non-group members.

Unfortunately, group members are still capable of sending packets with a valid external-authenticating MAC and invalid digital signature, i.e. a group member can launch a DoS attack on the group using invalid digital signatures. And group members are still capable of sending packets with a valid external-authentication MAC but an invalid TESLA MAC. In both the TESLA and digital-signature cases, the external authentication will succeed only to have the internal authentication fail. MESP includes the ESP sequence number in the internal authentication to protect against a replay attack by a group member. When the RECOMMENDED external authentication code is use, however, the ESP receiver MUST validate both the internal authentication as well as the external authentication before updating the ESP replay window.

The value of MESP authentication transforms is to enable the receiver to greatly reduce the effect of an attack by non-group members, to reduce the effects of a denial of service attack by a group member, to detect an attack by a group member, and to support the integration of multicast source-authentication transforms into IPsec ESP for data-origin authentication.

5.3 MESP Encryption

The value of MESP encryption is to validate individual encryption transforms for multicast operation. It is possible that a

particular cipher and mode are suitable for pairwise security associations but not for multicast security associations, such as one where multiple senders share the key. For example, a stream or hybrid stream/block cipher has special risks of keystream reuse when its key is shared by multiple senders. Although IPsec encryption transforms are generally suitable for multicast operation, many have not been evaluated, tested or used in IP multicast environments. This I-D has considered the suitability of several IPsec ESP encryption transforms for inclusion in the MESP framework. It is RECOMMENDED that all future IPsec encryption transforms be analyzed as to their security for multicast and group security as well as for pairwise security.

6.0 IANA Considerations

This I-D extends the RFC 2407 attributes for IPsec ESP, PROTO_IPSEC_ESP [RFC2407]. Within PROTO_IPSEC_ESP, MESP reserves the transform identifier value 13 [See IANA, "IPSEC ESP Transform Identifiers"]. MESP also adds new type/length/value attributes to RFC 2407. For the MESP transform ID security association attributes, the ENC Transform has type number 11, the INT transform has type number 12, and the EXT transform has type number 13 [see IANA, "Security Association Attributes"].

class	value	type
ENC-Transform	11	B
INT-Transform	12	B
EXT-Transform	13	B

The ENC-Transform has the following values.

name	value
Reserved	0
3DES	1
AES-CBC	2
AES-CTR	3

The INT-Transform has the following values.

name	value
Reserved	0
RSA-SHA	1
TESLA	2

The EXT-Transform has the following values.

name	value
Reserved	0
HMAC-SHA1	1

7.0 Acknowledgements

The authors wish to thank Scott Fluhrer, Thomas Hardjono, Steve Kent

and Brian Weis for their thoughtful comments and suggestions.

8.0 Author's Address

Mark Baugher
Cisco Systems, Inc.
5510 SW Orchid Street
Portland, Oregon
mbaugher@cisco.com
+1-503-245-4543

Ran Canetti
IBM T.J. Watson Research Center
30 Saw Mill River Road
Hawthorne, NY 10598, USA
canetti@watson.ibm.com
Tel: +1-914-784-6692

Pau-Chen Cheng
IBM T.J. Watson Research Center
30 Saw Mill River Road
Hawthorne, NY 10598, USA
pau@watson.ibm.com
Tel: +1-914-784-6692

Pankaj Rohatgi
IBM T.J. Watson Research Center
30 Saw Mill River Road
Hawthorne, NY 10598, USA
rohatgi@watson.ibm.com
Tel: +1-914-784-6692

9.0 References

9.1 Normative References

[AHBIS] S. Kent, IP Authentication Header (AH), IETF, Work in Progress, March 2003, http://www.ietf.org/internet-drafts/draft-ietf-ipsec-rfc2402bis-02.txt

[ESPBIS] S. Kent, IP Encapsulated Security Payload (ESP), IETF, Work in Progress, March 2003, http://www.ietf.org/internet-drafts/draft-ietf-ipsec-esp-v3-04.txt.

[GDOI] M. Baugher, H. Harjono, H. Harney, B. Weis, The Group Domain of Interpretation, IETF, Work in Progress, October 2002, http://www.ietf.org/internet-drafts/draft-ietf-msec-gdoi-06.txt.

[GSAKMP] H. Harney, A. Schuett, A. Colegrove, GSAKMP Light, IETF, Work in Progress, July 2002, http://www.ietf.org/internet-drafts/draft-ietf-msec-gsakmp-light-sec-01.txt

[IANA] http://www.iana.org/assignments/isakmp-registry

[MIKEY] J. Arkko, E. Carrara, F. Lindholm, M. Naslund, K. Normann, MIKEY: Multimedia Internet KEYing, IETF, Work in Progress, September 2002, http://www.ietf.org/internet-drafts/draft-ietf-msec-mikey-04.txt

[PKCS1] PKCS #1 v2.1: RSA Cryptography Standard, RSA Laboratories, ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-1/pkcs-1v2-1.pdf, June 2002.

[RFC2104] H. Krawczyk, M. Bellare, R. Canetti, HMAC: Keyed-Hashing for Message Authentication, Internet Request for Comments 2104, IETF, November 1997, ftp://ftp.rfc-editor.org/in-notes/rfc2104.txt.

[RFC2401] S.Kent, R.Atkinson, Security Architecture for the Internet Protocol, Internet Request for Comments 2401, IETF, November 1998, http://www.ietf.org/rfc/tfc2401.txt.

[RFC2404] C. Madson, R. Glenn, The Use of HMAC-SHA-1-96 within ESP and AH, Internet Request for Comments 2404, IETF, November 1998, http://www.ietf.org/rfc/rfc2404.txt.

[RFC2407] D. Piper, The Internet IP Security Domain of Interpretation for ISAKMP, Internet Request for Comments 2407, IETF, November 1998, http://www.ietf.org/rfc/rfc2407.txt.

[RFC2451] Pereira, R., and R. Adams, "The ESP CBC-Mode Cipher Algorithms", Internet Request For Comments 2451, IETF, November 1998, ftp://ftp.rfc-editor.org/in-notes/rfc2451.txt.

[RFC3376] B.Cain, S.Deering, B.Fenner, I. Kouvelas, A. Thyagarajan, Internet Group Management Protocol, Version 3, Internet Request for Comments 3376, IETF, October 2002, http://www.ietf.org/rfc/rfc3376.txt.

[SSM]H.Holbrook, B.Cain, Source Specific Multicast for IP, http://www.ietf.org/internet-drafts/draft-ietf-ssm-arch-00.txt, Work in Progress

[TESLA]

9.2 Informative References

[CGIMNP] Canetti R., J. Garay, G. Itkis, D. Micciancio, M. Naor, B. Pinkas, "Multicast Security: A Taxonomy and Efficient Authentication", INFOCOM '99.

[CP] R. Canetti, B. Pinkas, "A taxonomy of multicast security issues",draft-canetti-secure-multicast-taxonomy-01.txt, Nov. 1998.

[Ch] S. Cheung, An Efficient Message Authentication Scheme for Link State Routing, Proceedings of the 13th Annual Computer Security Applications Conference, San Diego, December 8-12, 1997, pp.90-98.

[GR] R. Gennaro, P. Rohatgi, "How to Sign Digital Streams", Advances in Cryptology - Crypto '97, Springer-Verlag LNCS 1294, pp. 180-197, 1997.

[K] H. Krawczyk, The order of encryption and authentication for protecting communications (or: How secure is SSL?). In J. Kilian, editor, CRYPTO 2001.

[PCTS] A. Perrig, R. Canetti, D. Tygar, D. Song, Efficient Authentication and Signature of Multicast Streams over Lossy Channels, IEEE Symposium on Security and Privacy, Oakland, CA, May 2000.

[R] P. Rohatgi, A Compact and Fast Signature Scheme for Multicast Packet Authentication, In 6th ACM Computer and Communications Security Conference (CCS) , Nov 1999.

[WL] C. K. Wong and S. S. Lam, Digital Signatures for Flows and Multicasts, IEEE ICNP '98. See also University of Texas at Austin, Computer Science Technical report TR 98-15.