

Internet Engineering Task Force  
INTERNET-DRAFT  
[draft-ietf-msec-ipsec-multicast-issues-01.txt](#)  
Expires: June, 2003

Mark Baugher(Cisco)  
Ran Canetti (IBM)  
Thomas Hardjono (Verisign)  
Brian Weis (Cisco)  
December, 2002

## IP Multicast issues with IPsec

### Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of [Section 10 of RFC2026](#).

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."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/1id-abstracts.txt>

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

### Abstract

The IPsec Architecture [[RFC2401](#)] and IPsec transform RFCs [[RFC2402](#), [RFC2406](#)] define certain mechanisms for IP multicast traffic. The recent revisions to each of the protocol documents [[ESPbis](#), [AHbis](#)] propose changes to those semantics. However, neither the existing nor proposed semantics are sufficiently general such that IPsec can be used to protect the wide variety of IPv4 and IPv6 multicast applications that are expected by the IP multicast community. In particular, they are not compatible with the needs of the protocols developed in the MSEC WG and for Source Specific Multicast [[RFC3376](#), SSM-ARCH]. This document reviews these semantics and proposes some minor changes, which would enable IPsec to be suitable for these uses.

## Table of Contents

<a href="#">1.0</a>	Introduction.....	<a href="#">2</a>
<a href="#">1.1</a>	Addressing Scope.....	<a href="#">3</a>
<a href="#">1.2</a>	Key Words.....	<a href="#">3</a>
<a href="#">2.0</a>	General Issues.....	<a href="#">3</a>
<a href="#">2.1</a>	SPI allocation and SA lookup.....	<a href="#">4</a>
<a href="#">2.2</a>	Multiple sender SAs and replay protection.....	<a href="#">5</a>
<a href="#">2.3</a>	Integrity vs. Authentication.....	<a href="#">5</a>
<a href="#">3.0</a>	Proposed Changes to ESPbis.....	<a href="#">5</a>
<a href="#">3.1</a>	SPI allocation and SA lookup.....	<a href="#">5</a>
<a href="#">3.2</a>	Multiple sender SAs and replay protection.....	<a href="#">6</a>
<a href="#">3.3</a>	Integrity vs. Authentication.....	<a href="#">7</a>
<a href="#">4.0</a>	Proposed Changes to AHbis.....	<a href="#">8</a>
<a href="#">4.1</a>	SPI allocation and SA lookup.....	<a href="#">8</a>
<a href="#">4.2</a>	Multiple sender SAs and replay protection.....	<a href="#">8</a>
<a href="#">4.3</a>	Integrity vs. Authentication.....	<a href="#">9</a>
<a href="#">5.0</a>	Conclusion.....	<a href="#">9</a>
<a href="#">6.0</a>	Security Considerations.....	<a href="#">9</a>
<a href="#">7.0</a>	References.....	<a href="#">9</a>
<a href="#">7.1</a>	Normative References.....	<a href="#">9</a>
<a href="#">7.2</a>	Informative References.....	<a href="#">9</a>
	Authors Addresses.....	<a href="#">10</a>

## [1.0](#) Introduction

At the time RFCs 2401/2402/2406 were written, use of IPsec for multicast was for the most part not deployed. However the authors of those RFCs and the IPsec Working Group had the vision that IPsec would someday be just as useful for IP multicast as IP unicast. At that time there were a number of unsolved problems, and those are candidly listed in [RFC 2401](#).

However, because so little attention had been focused on using IPsec to protect multicast traffic, and because new methods of IP multicast have been invented since that time, it is only natural that what is currently documented in those RFCs do not handle all of the current IP multicast needs. We are thus faced with a situation where the current specification of IPsec is inconsistent with the secure multicast standard that is being developed in the MSEC WG.

Consequently, the IPSEC and MSEC working groups now have to make a decision to take one of the following to standardization paths:

- A. Decide that ESP/AH should not be modified for the purpose of accommodating the needs of MSEC. In this case, MSEC will define its own version of ESP [[MESP](#)]. MESP will be similar to ESP, but will be incompatible with ESP in several ways. In particular, MESP will use a different protocol number than that of ESP.

Baughner, et. al. Expires June, 2003 2  
IP Multicast issues with IPsec December, 2002

- B. Decide that ESP/AH should be modified to accommodate the needs of MSEC. In this case, both MSEC and IPsec will use the same definition of ESP, with the same protocol number. (MESP will define additional authentication protocols for ESP, to obtain source authentication.)

The main advantage of option A is that there is no need to coordinate between the two working groups, and each WG is free to define (and subsequently modify) its own protocols. The main disadvantage of option A is the extra complexity involved in defining, implementing, and maintaining a separate "multicast ESP" protocol. Thus, the decision between options A and B has to weigh the complexity of modifying ESP to accommodate MSEC, against the complexity of having a different "multicast ESP" protocol.

The purpose of this draft is to explain and clarify the changes needed to ESP/AH in order to make it compatible with MSEC, and thus start a discussion on the MSEC and IPsec working groups. In a nutshell, three modifications to the IPsec protocol suite are necessary:

1. Allow parties to further refine the SA lookup. (That is, allow a party to have two different SA's, with the same destination address, same IPSEC protocol, and same SPI, but with different source addresses.
2. Allow parties a wider range of replay protection possibilities for ESP/AH.
3. Better describe that a variety of authentication methods can be used within the IPsec protocols.

It is our impression that the changes required of ESP/AH to accommodate the needs of MSEC are minor, and in no case will existing IPsec implementations be affected. Thus, option B is the better one. We solicit discussion of this question on the IPSEC and MSEC WGs.

## [1.1](#) Addressing Scope

Although this document is primarily concerned with IP multicast, the issues raised are not restricted to multicast; IPv4 or IPv6 broadcast and anycast groups are similarly affected.

## 1.2 Key Words

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [[RFC2119](#)].

## 2.0 General Issues

There are two distinct unrelated problems which have been discovered, first by the SMuG IRTF WG and then by the IETF MSEC WG

Baughner, et. al.	Expires June, 2003	3
IP Multicast issues with IPsec	December, 2002	

which was formed to focus on the security of IP multicast groups. One other issue has arisen specifically with new wording in the [[ESPbis](#)] and [[AHbis](#)] drafts.

## 2.1 SPI allocation and SA lookup

[RFC 2401](#) states an SA will use the 3-tuple (destination address, IPsec protocol, and SPI) to look up the SA in the SAD. That is sufficient and satisfactory in many IP multicast cases. It can be accomplished in those cases by using a multicast key management scheme which is built around a centralized group controller. As long as a single group controller synchronizes SPI values, this 3-tuple is sufficient -- even as the authors of [RFC 2401](#) predicted in [Section 4.7 of RFC 2401](#):

So some system or person will need to coordinate among all multicast groups to select an SPI or SPIs on behalf of each multicast group and then communicate the group's IPsec information to all of the legitimate members of that multicast group via mechanisms not defined here.

The text quoted above from [RFC 2401](#) does not say that there MUST be a single controller, but appears to be giving clarifying text based on the expectations of the time.

Since the time [RFC 2401](#) was written, Source-Specific Multicast (SSM) has been specified. SSM allows for sender-specific SAs. An SSM "group" is composed of a particular sender and its receivers. Multiple SSM groups may use that same multicast address, but no coordination between senders is assumed. Similarly, IGMP version 3 also operates on the basis of (Source, Group) pairs. Therefore, when we wish to protect this traffic with IPsec we cannot assume any security coordination between the senders. A 3-tuple is no longer

sufficient.

[Section 4.7 of RFC 2401](#) also says

Specifications for other, more general multicast cases are deferred to later IPsec documents.

Given the above two quotes it would seem that we should be able to accommodate multiple multicast group controllers within the existing architecture.

[RFC 2402](#) and [RFC 2406](#) did not further restrict the SA lookup as described in [RFC 2401](#). They also describe the 3-tuple to be used in all cases (unicast and multicast).

The proposed new ESP [[ESPbis](#)] and AH [[AHbis](#)] do change the semantics of SA lookup. It makes them less specific in both the unicast and multicast cases. For the IP multicast case, the lookup has been changed to a SPI lookup (and optionally the protocol ID) in combination with the destination address. This is fine except in the

Baughner, et. al.	Expires June, 2003	4
IP Multicast issues with IPsec	December, 2002	

case when multiple multicast group controllers are used for the group.

In order to effectively differentiate between SAs administered by different group controllers, we need a MORE specific SA lookup than [RFC 2406](#) rather than the less specific lookup as proposed in [[ESPbis](#)].

## [2.2](#) Multiple sender SAs and replay protection

[RFC 2401](#) points out that having senders share a single SA is useful under some circumstances (see [Section 4.7](#) of [RFC2401]). It acknowledges that the anti-replay service provided by a sequence number in the AH or ESP packet is not possible with present semantics.

[RFC 2406](#) agrees with this, and further states that anti-replay SHOULD NOT be used with a multi-sender SA in [Section 3.4.3](#):

(Note that there are no provisions for managing transmitted Sequence Number values among multiple senders directing traffic to a single SA (irrespective of whether the destination address is unicast, broadcast, or multicast). Thus the anti-replay service SHOULD NOT be used in a multi-sender environment that employs a single SA.) [[RFC2406](#)].

The new ESP [[ESPbis](#)] goes even further to deprecate multiple sender

SAs in [Section 2.2](#). However, there are multicast applications with very large numbers of senders to the same IP multicast group, where the receivers are low end devices which cannot store a single SA per sender.

### [2.3](#) Integrity vs. Authentication

[RFC 2402](#) and [RFC 2406](#) described an "Authentication Data" section as providing connectionless integrity and data origin authentication. However [\[ESPbis\]](#) and [\[AHbis\]](#) replaced the name of that field with "Integrity Check Value" which doesn't really accurately describe the field when group data origin authentication algorithms are used. This is described more fully in following sections.

### [3.0](#) Proposed Changes to ESPbis

The following sections propose changes to [\[ESPbis\]](#) to address the above general issues.

#### [3.1](#) SPI allocation and SA lookup

[Section 2.1](#) (Security Parameters Index) specifies exactly how the SPI should be dealt with:

For multicast SAs, the SPI (and optionally the protocol ID) in combination with the destination address is used to select an SA. This is because multicast SAs are defined by a multicast

Baughner, et. al.	Expires June, 2003	5
IP Multicast issues with IPsec	December, 2002	

controller, not by each IPsec receiver. (See the Security Architecture document for more details) [\[ESPbis\]](#).

As noted above, this is not sufficient for IP multicast in the case of multiple multicast group controllers. We propose this section to be replaced with the following wording:

For broadcast, multicast, and anycast SAs, the SPI and protocol ID (ESP) in combination with the destination address is used to select an SA. In some cases, other parameters (such as a source address) MAY be used by a receiver to further identify the correct SA. This is because multicast SAs may be defined by more than one multicast group controller.

[Section 3.4.2](#) (Security Association Lookup) of [\[ESPbis\]](#) would also need to discuss these semantics. It currently states:

Upon receipt of a packet containing an ESP Header, the receiver determines the appropriate (unidirectional) SA, based on the SPI alone (unicast) or SPI combined with destination IP address

(multicast). (This process is described in more detail in the Security Architecture document) [[ESPbis](#)].

We propose this text be replaced as follows.

Upon receipt of a unicast packet containing an ESP Header, the receiver determines the appropriate (unidirectional) SA, based on the SPI alone. (This process is described in more detail in the Security Architecture document.)

If the packet is a broadcast, multicast, or anycast packet, there may be more than one SA pointed to by the combination of SPI, security protocol and destination address. This can happen if multiple non-cooperating multicast controllers are present in the network. In this case the receiver MAY use other parameters (such as a source address) to identify the correct SA. Key management MAY indicate (e.g., with an SA attribute) that such processing is necessary in order for a receiver to properly process the ESP packets for a group if that is known a priori.

### [3.2](#) Multiple sender SAs and replay protection

[Section 2.2](#) (Sequence Number) states:

Sharing an SA among multiple senders is deprecated, since there is no general means of synchronizing packet counters among the senders or meaningfully managing a receiver packet counter and window in the context of multiple senders [[ESPbis](#)].

It is true that with the current semantics that synchronizing packet counters across multiple senders is not possible. However, there is a need to provide anti-replay in this situation and there is ongoing research into methods which allow anti-replay in this situation.

Baughner, et. al. Expires June, 2003  
IP Multicast issues with IPsec

6  
December, 2002

Therefore, rather than forbid the use of multiple-sender SAs we propose relaxing the multiple-sender SA restriction found in [RFC 2406](#) to accommodate new methods of replay detection as they become available. We propose the following replacement for the above text in [[ESPbis](#)].

For a multi-sender multicast SA, the anti-replay service MUST NOT be used unless key management signals its use. If the anti-replay service is used in this case, each receiver must keep a replay window per sender.

This text intentionally restricts any new anti-replay functionality being used unless it has been negotiated in or downloaded from key

management. In this way, older IPsec and hardware implementations of IPsec will be shielded from having to implement or understand the new semantics.

### [3.3](#) Integrity vs. Authentication

The name associated with the authentication portion of ESP is "Authentication Data". However, [\[ESPbis\]](#) changed the name to "Integrity Check Value". The rationale for this change is described in [Section 1](#):

Data origin authentication and connectionless integrity are joint services, hereafter referred to jointly as "integrity." (This term is employed because, on a per-packet basis, the computation being performed provides connectionless integrity directly; data origin authentication is provided indirectly as a result of binding the key used to verify the integrity to the identity of the IPsec peer [\[ESPbis\]](#)).

This is certainly true for a pairwise unicast connection. However when ESP is used with multicast, data origin authentication can be an authentication feature distinct from identity checks. At least two forms of data origin authentication have been proposed: digital signatures and TESLA.

Since this field can provide more than just integrity it is more accurately named as "Authentication Data". We propose the following wording changes to [\[ESPbis\]](#).

1. The text quoted above from [Section 1](#) should be replaced with:

Data origin authentication and connectionless integrity are joint services, hereafter referred to jointly as "authentication."

2. All occurrences of "Integrity-only ESP" should be "Authentication-only ESP".
3. The "Integrity Check Value" field in AH should be named "Authentication Data", and all references to that section should be updated.

### [4.0](#) Proposed Changes to AHbis

The following sections propose changes to [\[AHbis\]](#) to address the above general issues.

#### [4.1](#) SPI allocation and SA lookup



[Section 2.4](#) (Security Parameters Index) specifies exactly how the SPI should be dealt with. It is identical to [\[ESPbis\]](#) wording.

For multicast SAs, the SPI (and optionally the protocol ID) in combination with the destination address is used to select an SA. This is because multicast SAs are defined by a multicast controller, not by each IPsec receiver. (See the Security Architecture document for more details) [\[AHbis\]](#).

As in the case with [\[ESPbis\]](#), we propose this section to be replaced with the following wording:

For broadcast, multicast, and anycast SAs, the SPI and protocol ID (AH) in combination with the destination address is used to select an SA. In some cases other parameters (such as a source address) MAY be used by a receiver to further identify the correct SA. This is because multicast SAs may be defined by more than one multicast group controller.

[Section 3.4.2](#) (Security Association Lookup) of [\[AHbis\]](#) also needs to be modified to reflect these semantics. It currently states:

Upon receipt of a packet containing an IP Authentication Header, the receiver determines the appropriate (unidirectional) SA, based on the destination IP address, security protocol (AH), and the SPI [\[AHbis\]](#).

No change to this text is necessary. We propose that the following text be appended to it.

If the packet is a broadcast, multicast, or anycast packet, there may be more than one SA pointed to by the combination of SPI, security protocol and destination address. This can happen if multiple non-cooperating multicast controllers are present in the network. In this case the receiver MAY use other parameters (such as a source address) to identify the correct SA. Key management MAY indicate (e.g., with an SA attribute) that such processing is necessary in order for a receiver to properly process the AH packets for a group if that is known a priori.

#### [4.2](#) Multiple sender SAs and replay protection

[Section 2.5](#) (Sequence Number) states the same text as [\[ESPbis\]](#) [Section 2.2](#). We propose the same text here as is proposed in [Section 3.2](#).

### [4.3](#) Integrity vs. Authentication

AH has the same issue as ESP regarding the use of the term "Integrity" over "Authentication". We propose the "Integrity Check Value" field in AHbis be named "Authentication Data", and all references to that section should be updated.

### [5.0](#) Conclusion

The IPsec architecture is capable of accommodating multicast applications, including source specific multicast applications, with minor revisions in SA lookup and replay protection, which are described in this memo. These minor changes will enable new transforms for source authentication of multicast messages as well as group authentication of multicast messages.

### [6.0](#) Security Considerations

This entire document discusses how multicast data packets can be effectively protected within the IPsec architecture.

### [7.0](#) References

#### [7.1](#) Normative References

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

[RFC2402] Kent, S., and R. Atkinson, "IP Authentication Header", [RFC 2402](#), November 1998.

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

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

[RFC3376] Cain, B., et. al., "Internet Group Management Protocol, Version 3", [RFC 3376](#), October 2002.

#### [7.2](#) Informative References

[ESPbis] Kent, S., "IP Encapsulating Security Payload (ESP)", <http://www.ietf.org/internet-drafts/draft-ietf-ipsec-esp-v3-03.txt>, Work in progress 2002.

[AHbis] Kent, S., "IP Authentication Header", <http://www.ietf.org/internet-drafts/draft-ietf-ipsec-rfc2402bis-01.txt>, Work in progress 2002.

[MESP] Baugher, M., et. al., "MESP: Multicast Encapsulating Security

Payload?, <http://www.ietf.org/internet-drafts/draft-ietf-msec-mesp-00.txt>, Work in progress 2002.

Baughner, et. al.	Expires June, 2003	9
IP Multicast issues with IPsec	December, 2002	

[SSM-ARCH] Holbrook, H., Cain, B., ?Source-Specific Multicast for IP?, <http://www.ietf.org/internet-drafts/draft-ietf-ssm-arch-01.txt>, Work in progress 2002.

#### Authors Addresses

Mark Baughner  
Cisco Systems  
5510 SW Orchid Street  
Portland, OR 97219, USA  
(503) 245-4543  
mbaughner@cisco.com

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

Thomas Hardjono  
VeriSign  
401 Edgewater Place, Suite 280  
Wakefield, MA 01880  
Tel: 781-245-6996  
thardjono@verisign.com

Brian Weis  
Cisco Systems  
170 W. Tasman Drive,  
San Jose, CA 95134-1706, USA  
(408) 526-4796  
bew@cisco.com

Baughner, et. al.	Expires June, 2003	10
-------------------	--------------------	----