AH/ESP Multicast Issues

<draft-ietf-msec-ipsec-multicast-issues-01.txt>

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

ESP/AH Background

- RFC 2406 (ESP) and RFC 2402 (AH) were intended to protect both unicast *and* multicast traffic.
  - But we've since found limitations with multicast which were documented in our draft
- ESP and AH are currently being revised.
  - ESPbis and AHbis IPsec WG documents
- Our hope was that the new revisions could handle all multicast scenarios
  - MESP could then be based on ESP

Identified Issues

1. SPI allocation/SA Lookup
2. Anti-Replay Protection for Multiple sender SAs
3. Integrity vs. Authentication

1. SPI allocation

- RFC 2401 assumes that SPIs for multicast traffic will be coordinated by a group controller
  - That works fine for Any Source Multicast (ASM), which defines an *ASM group* as an IP multicast address.
  - Group members join {G} using IGMPv2
- Since the time RFC 2401 was published Source-Specific Multicast (SSM) was developed
  - An *SSM group* is defined to be a particular source on an IP multicast address
  - A group member joins {S,G} using IGMPv3.
  - Sources are not necessarily coordinated! Therefore we cannot require a group controller to coordinate SPIs for all sources.

SA Lookup

- RFCs 2406/2402 specify a 3-tuple SA lookup
  - {SPI, protocol, destination}
- Older ESPbis/AHbis drafts specified multicast SA lookup
  - {SPI, destination}, or {SPI, protocol, destination}

These are both sufficient for a single group controller allocating SPIs to an ASM group.

But neither support SSM.

ESPbis-04/AHbis-02 Changes

- The SA basic SA lookup would remain as specified in the bis drafts for unicast SA lookups
  - SPI alone, or {SPI, protocol}
- A bit can be set in the SA to indicate that the *destination* address must also be used in the SA lookup. This should be used for ASM
  - {SPI, destination} or {SPI, protocol, destination}
- Another bit can be set in the SA to indicate that the *source* address must also be used in the SA lookup.
- The *source bit* combined with the *destination bit* in the SA lookup should be used for SSM
  - {SPI, source, destination} or
    {SPI, protocol, source, destination}

2. Anti-Replay Protection for Multiple Sender SAs

- An ASM group with multiple senders can share a single SA.
  - E.g., a small group using an IP multicast address to share data
- However, the anti-replay method defined in RFC 2402 and RFC2406 is *not* suitable for multiple senders.

IPsec Sequence Number Field

```
 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+ ----
|               Security Parameters Index (SPI)                 | ^Auth.
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+ |Cov-
|                      Sequence Number                          |erage
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+ | ----
|                    Payload Data* (variable)                   | |   ^
~                                                               ~ |   |
|                                                               | |Conf.
+               +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+ |Cov-
|               |     Padding (0-255 bytes)                     | |erage*
+-+-+-+-+-+-+-+-+               +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+ |   |
|                               |  Pad Length   | Next Header   | v   v
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+ ------
|                 Authentication Data (variable)                |
~                                                               ~
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

IPsec sequence number verification

- For each SA, receivers maintain a sliding *receive window* of recently received packets
- Sequence numbers in newly received packets are compared with the receive window state
  - If an authenticated packet with this sequence number has already been handled, the new packet is immediately discarded

The issue

- Multiple senders cannot coordinate sequence numbers to share a single receive window.
  - When two senders use the same sequence number one of the packets will be discarded.
- Because of this, AH and ESP recommend that receivers turn off the anti-replay service in this situation.
  - But what if the group really does want to protect themselves from replay attacks?

A Possible Solution

- Receivers could maintain a receive window per sender.
- BUT the value of this method has been questioned:
  - Is the size of the per-sender state small enough to be worthwhile?
  - ESP does not include the sending IP address in the integrity check, which makes per-sender state questionable for ESP.
  - IPsec implementations should not be required to implement such a complex method

ESPbis-04/AHbis-02 Changes

- No specific solution is specified
- A statement that the "… anti-replay service SHOULD NOT be used …" for multi-sender SAs was removed.
- Senders to multi-sender SAs are given the recommendation to increment the sequence number "… unless anti-replay mechanisms outside the scope of this standard are negotiated between the sender and receiver ….".

3. Integrity vs. Authentication

- The term “Authentication Data” used in RFC 2402 and RFC 2406 was generally changed to “Integrity Check Value”.

```
  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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+ ----
|               Security Parameters Index (SPI)                 | ^Integ.
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+ |Cov-
|                      Sequence Number                          | |erage
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+ | ----
|                    Payload Data* (variable)                   | |   ^
~                                                               ~ |   |
|                                                               | |Conf.
+               +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+ |Cov-
|               |     Padding (0-255 bytes)                     | |erage*
+-+-+-+-+-+-+-+-+               +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+ |   |
|                               |  Pad Length   | Next Header   | v   v
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+ ------
|                                                               |
~           Integrity Check Value-ICV                           ~
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

No Changes Made

- We were concerned that “Integrity Check value” implied some limitations on how the field could be used.
  - Was Source Origin Authentication excluded?
- It turns out no limitations were intended
  - So the language seems acceptable.

Summary of Changes

- SPI allocation/SA Lookup
  - Good to go for supporting SSM!
- Anti-Replay Protection for Multiple sender SAs
  - Methods of an anti-replay service are possible, but not specified in the standard
- Integrity vs. Authentication
  - No changes were necessary

Thanks go to Steve Kent for working with us to improve the usability of ESP and AH for multicast!