MSEC Working Group
Internet-Draft
Expires: April, 2007

B. Weis
Cisco Systems
G. Gross
IdentAware Security
D. Ignjatic
Polycom
October, 2006

Multicast Extensions to the Security Architecture for the Internet Protocol
draft-ietf-msec-ipsec-extensions-04.txt

Status of this Memo

Copyright Notice

Abstract

The Security Architecture for the Internet Protocol [RFC4301] describes security services for traffic at the IP layer. That architecture primarily defines services for Internet Protocol (IP) unicast packets, as well as manually configured IP multicast packets. This document further defines the security services for manually and dynamically keyed IP multicast packets within that Security Architecture.

Table of Contents

1. Introduction.....3
1.1 Scope.....3
1.2 Terminology.....4
2. Overview of IP Multicast Operation.....5
3. Security Association Modes.....6
3.1 Tunnel Mode with Address Preservation.....6
4. Security Association.....7
4.1 Major IPsec Databases.....7
4.1.1 Group Security Policy Database (GSPD).....8
4.1.2 Security Association Database (SAD).....9
4.1.3 Peer Authorization Database (PAD).....9
4.2 Group Security Association (GSA).....10
4.3 Data Origin Authentication.....12
4.4 Group SA and Key Management.....13
4.4.1 Co-Existence of Multiple Key Management Protocols.....13
4.4.2 New Security Association Attributes.....13
5. IP Traffic Processing.....14
5.1 Outbound IP Multicast Traffic Processing.....14
5.2 Inbound IP Multicast Traffic Processing.....14
6. Security Considerations.....14
6.1 Security Issues Solved by IPsec Multicast Extensions.....14
6.2 Security Issues Not Solved by IPsec Multicast Extensions.....15
6.2.1 Outsider Attacks.....15
6.2.2 Insider Attacks.....15
6.3 Implementation or Deployment Issues that Impact Security.....16
6.3.1 Homogeneous Group Cryptographic Algorithm Capabilities.....16
6.3.2 Groups that Span Two or More Security Policy Domains.....16
6.3.3 Network Address Translation.....17
7. IANA Considerations.....19
8. Acknowledgements.....19
9. References.....19
9.1 Normative References.....20
9.2 Informative References.....20
Appendix A - Multicast Application Service Models.....23
A.1 Unidirectional Multicast Applications.....23
A.2 Bi-directional Reliable Multicast Applications.....23
A.3 Any-To-Any Multicast Applications.....24
Author's Address.....25
Intellectual Property Statement.....26
Copyright Statement.....26

1. Introduction

The Security Architecture for the Internet Protocol [RFC4301] provides security services for traffic at the IP layer. It describes an architecture for IPsec compliant systems, and a set of security services for the IP layer. These security services primarily describe services and semantics for IPsec Security Associations (SAs) shared between two IPsec devices. Typically, this includes SAs with traffic selectors that include a unicast address in the IP destination field, and results in an IPsec packet with a unicast address in the IP destination field. The security services defined in RFC 4301 can also be used to tunnel IP multicast packets, where the tunnel is a pairwise association between two IPsec devices. RFC4301 defined manually keyed transport mode IPsec SA support for IP packets with a multicast address in the IP destination address field. However, RFC4301 did not define the interaction of an IPsec subsystem with a Group Key Management protocol or the semantics of a tunnel mode IPsec SA with an IP multicast address in the outer IP header.

This document describes extensions to RFC 4301 that further define the IPsec security architecture for groups of IPsec devices to share SAs. In particular, it supports SAs with traffic selectors that include a multicast address in the IP destination field, and results in an IPsec packet with an IP multicast address in the IP destination field. It also describes additional semantics for IPsec Group Key Management (GKM) subsystems. Note that this document uses the term "GKM protocol" generically and therefore it does not assume a particular GKM protocol.

1.1 Scope

The IPsec extensions described in this document support IPsec Security Associations that result in IPsec packets with IPv4 or IPv6 multicast group addresses as the destination address. Both Any-Source Multicast (ASM) and Source-Specific Multicast (SSM) [RFC3569] [RFC3376] group addresses are supported.

These extensions also support Security Associations with IPv4 Broadcast addresses that result in an IPv4 link-level broadcast packet, and IPv6 Anycast addresses [RFC2526] that result in an IPv6 Anycast packet. These destination address types share many of the same characteristics of multicast addresses because there may be multiple receivers of a packet protected by IPsec.

The IPsec architecture does not make requirements upon entities not participating in IPsec (e.g., network devices between IPsec endpoints). As such, these multicast extensions do not require intermediate systems in a multicast enabled network to participate in IPsec. In particular, no requirements are placed on the use of multicast routing protocols (e.g., PIM-SM [RFC2362]) or multicast admission protocols (e.g., IGMP [RFC3376].

All implementation models of IPsec (e.g., "bump-in-the-stack", "bump-in-the-wire") are supported.

This version of the multicast IPsec extension specification requires that all IPsec devices participating in a Security Association are homogeneous. They MUST share a common set of cryptographic transform and protocol handling capabilities. The semantics of an "IPsec composite group" [COMPGRP], a heterogeneous IPsec cryptographic group formed from the union of two or more sub-groups, is an area for future standardization.

1.2 Terminology

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 RFC 2119 [RFC2119].

The following key terms are used throughout this document.

Any-Source Multicast (ASM)
: The Internet Protocol (IP) multicast service model as defined in RFC 1112 [RFC1112]. In this model one or more senders source packets to a single IP multicast address. When receivers join the group, they receive all packets sent to that IP multicast address. This is known as a (*,G) group.

Group Controller Key Server (GCKS)
: A Group Key Management (GKM) protocol server that manages IPsec state for a group. A GCKS authenticates and provides the IPsec SA policy and keying material to GKM group members.

Group Key Management (GKM) Protocol
: A key management protocol used by a GCKS to distribute IPsec Security Association policy and keying material. A GKM protocol is used when a group of IPsec devices require the same SAs. For example, when an IPsec SA describes an IP multicast destination, the sender and all receivers must have the group SA.

Group Key Management Subsystem
: A subsystem in an IPsec device implementing a Group Key Management protocol. The GKM subsystem provides IPsec SAs to the IPsec subsystem on the IPsec device. Refer to RFC 3547 [RFC3547] and RFC 4535 [RFC4535] for additional information.

Group Member
: An IPsec device that belongs to a group. A Group Member is authorized to be a Group Speaker and/or a Group Receiver.

Group Owner
An administrative entity that chooses the policy for a group.

Group Security Association (GSA)
A collection of IPsec Security Associations (SAs) and GKM Subsystem SAs necessary for a Group Member to receive key updates. A GSA describes the working policy for a group. Refer to RFC 4046 [RFC4046] for additional information.

Group Security Policy Database (GSPD)
The GSPD is a multicast-capable security policy database, as mentioned in RFC3740 and RFC4301 section 4.4.1.1. Its semantics are a superset of the unicast SPD defined by RFC4301 section 4.4.1. Unlike a unicast SPD-S in which point-to-point security associations are inherently bi-directional, multicast security associations in the GSPD-S introduce a "sender only" or "receiver only" or "symmetric" SA direction attribute. Refer to section 4.1.1 for more details.

Group Receiver
A Group Member that is authorized to receive packets sent to a group by a Group Speaker.

Group Speaker
A Group Member that is authorized to send packets to a group.

Source-Specific Multicast (SSM)
The Internet Protocol (IP) multicast service model as defined in RFC 3569 [RFC3569]. In this model, each combination of a sender and an IP multicast address is considered a group. This is known as an (S,G) group.

Tunnel Mode with Address Preservation
A type of IPsec tunnel mode used by security gateway implementations when encapsulating IP multicast packets such that they remain IP multicast packets. This mode is necessary for IP multicast routing to correctly route IP multicast packets protected by IPsec.

2. Overview of IP Multicast Operation

IP multicasting is a means of sending a single packet to a "host group", a set of zero or more hosts identified by a single IP destination address. IP multicast packets are UDP data packets delivered to all members of the group with either "best-effort" [RFC1112], or reliable delivery (e.g., NORM) [RFC3940].

A sender to an IP multicast group sets the destination of the packet to an IP address that has been allocated for IP multicast. Allocated IP multicast addresses are defined in RFC 3171, RFC 3306, and RFC 3307 [RFC3171] [RFC3306] [RFC3307]. Potential receivers of the packet

"join" the IP multicast group by registering with a network routing device [RFC3376] [RFC3810], signaling its intent to receive packets sent to a particular IP multicast group.

Network routing devices configured to pass IP multicast packets participate in multicast routing protocols (e.g., PIM-SM) [RFC2362]. Multicast routing protocols maintain state regarding which devices have registered to receive packets for a particular IP multicast group. When a router receives an IP multicast packet, it forwards a copy of the packet out each interface for which there are known receivers.

3. Security Association Modes

IPsec supports two modes of use: transport mode and tunnel mode. In transport mode, IP Authentication Header (AH) [RFC4302] and IP Encapsulating Security Payload (ESP) [RFC4303] provide protection primarily for next layer protocols; in tunnel mode, AH and ESP are applied to tunneled IP packets.

A host implementation of IPsec using the multicast extensions MAY use either transport mode and tunnel mode to encapsulate an IP multicast packet. These processing rules are identical to the rules described in [RFC4301, Section 4.1]. However, the destination address for the IPsec packet is an IP multicast address, rather than a unicast host address.

A security gateway implementation of IPsec using the multicast extensions MUST use a tunnel mode SA, for the reasons described in [RFC4301, Section 4.1]. In particular, the security gateway must use tunnel mode to encapsulate incoming fragments, since IPsec cannot directly operate on fragments.

3.1 Tunnel Mode with Address Preservation

New header construction semantics are required when tunnel mode is used to encapsulate IP multicast packets that are to remain IP multicast packets. This is due to the following unique requirements of IP multicast routing protocols (e.g., PIM-SM [RFC2362]).

- IP multicast routing protocols compare the destination address on a packet to the multicast routing state. If the destination of an IP multicast packet is changed it will no longer be properly routed. Therefore, an IPsec security gateway must preserve the multicast IP destination address after IPsec tunnel encapsulation.

  The GKM Subsystem on a security gateway implementing the IPsec multicast extensions preserves the multicast IP address as follows. Firstly, the GKM Subsystem sets the Remote Address PFP flag in the GSPD-S entry for the traffic selectors. This flag causes the remote address of the packet matching IPsec SA traffic

selectors to be propagated to the IPsec tunnel encapsulation. Secondly, the GKM Subsystem needs to signal that destination address preservation is in effect for a particular IPsec SA. The GKM protocol MUST define an attribute that signals destination address preservation to the GKM Subsystem on an IPsec security gateway.

- IP multicast routing protocols also typically create multicast distribution trees based on the source address. If an IPsec security gateway changes the source address of an IP multicast packet (e.g., to its own IP address), the resulting IPsec protected packet may fail Reverse Path Forwarding (RPF) checks on other routers. A failed RPF check may result in the packet being dropped.

  To accommodate routing protocol RPF checks, the GKM Subsystem on a security gateway implementation implementing the IPsec multicast extensions must preserve the original packet IP source address as follows. Firstly, the GSPD-S entry for the traffic selectors must have the Source Address PFP flag set. This flag causes the remote address to be propagated to the IPsec SA. Secondly, the GKM Subsystem needs to signal that source address preservation is in effect for a particular IPsec SA. The GKM Subsystem MUST define a protocol attribute that signals source address preservation to the GKM Subsystem on an IPsec security gateway.

Some applications of address preservation may only require the destination address to be preserved. For this reason, the specification of destination address preservation and source address preservation are separated in the above description.

Address preservation is applicable only for tunnel mode IPsec SAs that specify the IP version of the encapsulating header to be the same version as that of the inner header. When the IP versions are different, tunnel processing semantics described in RFC 4301 MUST be followed.

In summary, retaining both the IP source and destination addresses of the inner IP header allow IP multicast routing protocols to route the packet irrespective of the packet being protected by IPsec. This result is necessary in order for the multicast extensions to allow a security gateway to provide IPsec services for IP multicast packets. This method of RFC 4301 tunnel mode is known as "tunnel mode with address preservation".

4. Security Association

4.1 Major IPsec Databases

The following sections describe the GKM Subsystem and IPsec extension interactions with the major IPsec databases. The major IPsec databases needed expanded semantics to fully support multicast.

4.1.1 Group Security Policy Database (GSPD)

The Group Security Policy Database is a security policy database capable of implementing both unicast security associations as defined by RFC4301 and the multicast extensions defined by this specification. A new Group Security Policy Database (GSPD) attribute is introduced: GSPD entry directionality. Directionality can take three types. Each GSPD entry can be marked "symmetric", "sender only" or "receiver only". "Symmetric" GSPD entries are the common entries as specified by RFC 4301. "Symmetric" SHOULD be the default directionality unless specified otherwise. GSPD entries marked as "sender only" or "receiver only" SHOULD support multicast IP addresses in their destination address selectors. If the processing requested is bypass or discard and a "sender only" type is configured the entry SHOULD be put in GSPD-O only. Reciprocally, if the type is "receiver only", the entry SHOULD go to GSPD-I only. SSM is supported by the use of unicast IP address selectors as documented in RFC 4301.

GSPD entries created by a GCKS may be assigned identical SPIs to SPD entries created by IKEv2 [RFC4306]. This is not a problem for the inbound traffic as the appropriate SAs can be matched using the algorithm described in RFC 4301 section 4.1. In addition, SAs with identical SPI values but not manually keyed can be differentiated because they contain a link to their parent SPD entries. However, the outbound traffic needs to be matched against the GSPD selectors so that the appropriate SA can be created on packet arrival. IPsec implementations that support multicast MUST use the destination address as the additional selector and match it against the GSPD entries marked "sender only".

To facilitate dynamic group keying, the outbound GSPD MUST implement a policy action capability that triggers a GKM protocol registration exchange (as per [RFC4301] section 5.1). For example, the Group Speaker GSPD policy might trigger on a match with a specified multicast application packet. The ensuing Group Speaker registration exchange would setup the Group Speaker's outbound SAD entry that encrypts the multicast application's data stream. In the inverse direction, group policy may also setup an inbound IPsec SA.

At the Group Receiver endpoint(s), the GSPD policy might trigger on a match with the multicast application packet sent from the Group Speaker. The ensuing Group Receiver registration exchange would setup the Group Receiver's inbound SAD entry that decrypts the multicast application's data stream. In the inverse direction, the group policy may also setup an outbound IPsec SA (e.g. when supporting an ASM service model).

The IPsec subsystem MAY provide GSPD policy mechanisms (e.g. trigger on detection of IGMP/MLD leave group exchange) that automatically initiate a GKM protocol de-registration exchange. De-registration minimizes exposure of the group's secret key. It also minimizes cost for those groups that incur cost on the basis of membership duration.

Additionally, the GKM subsystem MAY setup the GSPD/SAD state information independent of the multicast application's state. In this scenario, the group's Group Owner issues management directives that tells the GKM subsystem when it should start GKM registration and de-registration protocol exchanges. Typically the registration policy strives to make sure that the group's IPsec subsystem state is "always ready" in anticipation of the multicast application starting its execution.

4.1.2 Security Association Database (SAD)

The Security Association Database (SAD) can support multicast SAs, if manually configured. An outbound multicast SA has the same structure as a unicast SA. The source address is that of the Group Speaker and the destination address is the multicast group address. An inbound multicast SA must be configured with the source addresses of each Group Speaker peer authorized to transmit to the multicast SA in question. The SPI value for a multicast SA is provided by a GCKS, not by the receiver as occurs for a unicast SA. Other than the SPI assignment and the inbound packet de-multiplexing described in RFC4301 section 4.1, the SAD behaves identically for unicast and multicast security associations.

4.1.3 Peer Authorization Database (PAD)

The Peer Authorization Database (PAD) needs to be extended in order to accommodate peers that may take on specific roles in the group. Such roles can be GCKS, Group Speaker (in case of SSM) or a Group Receiver. A peer can have multiple roles. The PAD may also contain root certificates for PKI used by the group.

4.1.3.1 GKM/IPsec Interactions with the PAD

The RFC 4301 section 4.4.3 introduced the PAD. In summary, the PAD manages the IPsec entity authentication mechanism(s) and authorization of each such peer identity to negotiate modifications to the GSPD/SAD. Within the context of the GKM/IPsec subsystem, the PAD defines for each group:

. For those groups that authenticate identities using a Public Key Infrastructure, the PAD contains the group's set of one or more trusted root public key certificates. The PAD may also include the PKI configuration data needed to retrieve supporting certificates needed for an end entity's certificate path validation.

. A set of one or more group membership authorization rules. The GCKS examines these rules to determine a candidate group member's acceptable authentication mechanism and to decide whether that candidate has the authority to join the group.

. A set of one or more GCKS role authorization rules. A group member uses these rules to decide which systems are authorized to act as a GCKS for a given group. These rules also declare the permitted GCKS authentication mechanism(s).

. A set of one or more Group Speaker role authorization rules. In some groups the group members allowed to send protected packets is restricted.

Some GKM protocols (e.g. GSAKMP [RFC4535]) distribute their group's PAD configuration in a security policy token [RFC4534] signed by the group's policy authority, also known as the Group Owner (GO). Each group member receives the policy token (using a method not described in this memo) and verifies the Group Owner's signature on the policy token. If that GO signature is accepted, then the group member dynamically updates its PAD with the policy token's contents.

The PAD MUST provide a management interface capability that allows an administrator to enforce that the scope of a GKM group's policy specified GSPD/SAD modifications are restricted to only those traffic data flows that belong to that group. This authorization MUST be configurable at GKM group granularity. In the inverse direction, the PAD management interface MUST provide a mechanism(s) to enforce that IKEv2 security associations do not negotiate traffic selectors that conflict or override GKM group policies. An implementation SHOULD offer PAD configuration capabilities that authorize the GKM policy configuration mechanism to set security policy for other aspects of an endpoint's GSPD/SAD configuration, not confined to its group security associations. This capability allows the group's policy to inhibit the creation of back channels that might otherwise leak confidential group application data.

This document refers to re-key mechanisms as being multicast because of the inherent scalability of IP multicast distribution. However, there is no particular reason that re-key mechanisms must be multicast. For example, [ZLLY03] describes a method of re-key employing both unicast and multicast messages.

4.2 Group Security Association (GSA)

An IPsec implementation supporting these extensions has a number of security associations: one or more IPsec SAs, and one or more GKM SAs used to download IPsec SAs [RFC3740, Section 4]. These SAs are collectively referred to as a Group Security Association (GSA).

4.2.4.1 Concurrent IPsec SA Life Spans and Re-key Rollover

During a cryptographic group's lifetime, multiple IPsec group security associations can exist concurrently. This occurs principally due to two reasons:

- There are multiple Group Speakers authorized in the group, each with its own IPsec SA that maintains anti-replay state. A group that does not rely on IP Security anti-replay services can share one IPsec SA for all of its Group Speakers.

- The life spans of a Group Speaker's two (or more) IPsec SAs are allowed to overlap in time, so that there is continuity in the multicast data stream across group re-key events. This capability is referred to as "re-key rollover continuity".

Each group re-key multicast message sent by a GCKS signals the start of a new Group Speaker time epoch, with each such epoch having an associated IPsec SA. The group membership interacts with these IPsec SAs as follows:

- As a precursor to the Group Speaker beginning its re-key rollover continuity processing, the GCKS periodically multicasts a Re-Key Event (RKE) message to the group. The RKE multicast contains group policy directives, and new IPsec SA policy and keying material. In the absence of a reliable multicast transport protocol, the GCKS may re-transmit the RKE a policy defined number of times to improve the availability of re-key information.

- The RKE multicast configures the group's GSPD/SAD with the new IPsec SAs. Each IPsec SA that replaces an existing SA is called a "leading edge" IPsec SA. The leading edge IPsec SA has a new Security Parameter Index (SPI) and its associated keying material keys it. For a short period after the GCKS multicasts the RKE, a Group Speaker does not yet transmit data using the leading edge IPsec SA. Meanwhile, other Group Members prepare to use this IPsec SA by installing the new IPsec SAs to their respective GSPD/SAD.

- After waiting a sufficiently long enough period such that all of the Group Members have processed the RKE multicast, the Group Speaker begins to transmit using the leading edge IPsec SA with its data encrypted by the new keying material. Only authorized Group Members can decrypt these IPsec SA multicast transmissions. The time delay that a Group Speaker waits before starting its first leading edge SA transmission is a GKM/IPsec policy parameter. This value SHOULD be configurable at the Group Owner management interface on a per group basis.

- The Group Speaker's "trailing edge" SA is the oldest security association in use by the group for that speaker. All authorized

> Group Members can receive and decrypt data for this SA, but the Group Speaker does not transmit new data using the "trailing edge" SA after it has transitioned to the "leading edge SA". The trailing edge SA is deleted by the group's endpoints according to group policy (e.g., after a defined period has elapsed)"

This re-key rollover strategy allows the group to drain its in transit datagrams from the network while transitioning to the leading edge SA. Staggering the roles of each respective IPsec SA as described above improves the group's synchronization even when there are high network propagation delays. Note that due to group membership joins and leaves, each Group Speaker time epoch may have a different group membership set.

It is a group policy decision whether the re-key event transition between epochs provides forward and backward secrecy. The group's re-key protocol keying material and algorithm (e.g. Logical Key Hierarchy) enforces this policy. Implementations MAY offer a Group Owner management interface option to enable/disable re-key rollover continuity for a particular group. This specification requires that a GKM/IPsec implementation MUST support at least two concurrent IPsec SA per Group Speaker and this re-key rollover continuity algorithm.

4.3 Data Origin Authentication

As defined in [RFC4301], data origin authentication is a security service that verifies the identity of the claimed source of data. A Message Authentication Code (MAC) is often used to achieve data origin authentication for connections shared between two parties. But MAC authentication methods are not sufficient to provide data origin authentication for groups with more than two parties. With a MAC algorithm, every group member can use the MAC key to create a valid MAC tag, whether or not they are the authentic originator of the group application's data.

When the property of data origin authentication is required for an IPsec SA distributed from a GKCS, an authentication transform where the originator keeps a secret should be used. Two possible algorithms are TESLA [RFC4082] or RSA digital signature [RFC4359].

In some cases, (e.g., digital signature authentication transforms) the processing cost of the algorithm is significantly greater than an HMAC authentication method. To protect against denial of service attacks from device that is not authorized to join the group, the IPsec SA using this algorithm may be encapsulated with an IPsec SA using a MAC authentication algorithm. However, doing so requires the packet to be sent across the IPsec boundary for additional inbound processing [RFC4301, Section 5.2]. This use of ESP encapsulated within ESP accommodates the constraint that an ESP trailer defines an Integrity Check Value (ICV) for only a single authenticator

transform. Relaxing this constraint on the use of the ICV field is an area for future standardization.

4.4 Group SA and Key Management

4.4.1 Co-Existence of Multiple Key Management Protocols

Often, the GKM subsystem will be introduced to an existent IPsec subsystem as a companion key management protocol to IKEv2 [RFC4306]. A fundamental GKM protocol IP Security subsystem requirement is that both the GKM protocol and IKEv2 can simultaneously share access to a common Group Security Policy Database and Security Association Database. The mechanisms that provide mutually exclusive access to the common GSPD/SAD data structures are a local matter. This includes the GSPD-outbound cache and the GSPD-inbound cache. However, implementers should note that IKEv2 SPI allocation is entirely independent from GKM SPI allocation because group security associations are qualified by a destination multicast IP address and may optionally have a source IP address qualifier. See [RFC4303, Section 2.1] for further explanation.

The Peer Authorization Database does require explicit coordination between the GKM protocol and IKEv2. Section 4.1.3 describes these interactions.

4.4.2 New Security Association Attributes

A number of new security association attributes are defined in this document. Each GKM protocol supporting this architecture MUST support the following list of attributes described elsewhere in this document.

- Address Preservation (Section 3.1). This attribute describes whether address preservation is to be applied to the SA on the source address, destination address, or both source and destination addresses.

- Direction attribute (Section 4.1.1). This attribute describes whether the GSPD direction is to be "symmetric", "receiver only", or "sender only".

- Any of the cryptographic transform-specific parameters and keys that are sent from the GCKS to the Group Members (e.g. data origin authentication parameters as described in section 4.3).

- Re-key rollover procedure time intervals (section 4.2.4.1). The time that the Group Receiver IPsec subsystems will wait after creating the leading edge IPsec SA before they will retire the trailing edge IPsec SA. Also, the time that the Group Speaker will delay before it starts transmitting on the leading edges IPsec SA.

5. IP Traffic Processing

Processing of traffic follows [RFC4301, Section 5], with the additions described below when these IP multicast extensions are supported.

5.1 Outbound IP Multicast Traffic Processing

If an IPsec SA is marked as supporting tunnel mode with address preservation (as described in Section 3.1), either or both of the outer header source or destination addresses is marked as being preserved. If the source address is marked as being preserved, during header construction the "src address" header field MUST be "copied from inner hdr" rather than "constructed" as described in [RFC4301]. Similarly, if the destination address is marked as being preserved, during header construction the "dest address" header field MUST be "copied from inner hdr" rather than "constructed".

5.2 Inbound IP Multicast Traffic Processing

If an IPsec SA is marked as supporting tunnel mode with address preservation (as described in Section 3.1), the marked address (i.e., source and/or destination address) on the outer IP header MUST be verified to be the same value as the inner IP header. If the addresses are not consistent, the IPsec system MUST treat the error in the same manner as other invalid selectors, as described in [RFC4301, Section 5.2]. In particular the IPsec system MUST discard the packet, as well as treat the inconsistency as an auditable event.

6. Security Considerations

The IP security multicast extensions defined by this specification build on the unicast-oriented IP security architecture [RFC4301]. Consequently, this specification inherits many of the RFC4301 security considerations and the reader is advised to review it as companion guidance.

6.1 Security Issues Solved by IPsec Multicast Extensions

The IP security multicast extension service provides the following network layer mechanisms for secure group communications:

- Confidentiality using a group shared encryption key.

- Group source authentication and integrity protection using a group shared authentication key.

- Group Speaker data origin authentication using a digital signature, TESLA, or other mechanism.

- Anti-replay protection for a limited number of Group Speakers using the ESP (or AH) sequence number facility.

- Filtering of multicast transmissions by those group members who are not authorized by group policy to be Group Speakers. This feature leverages the IPsec state-less firewall service.

In support of the above services, this specification enhances the definition of the SPD, PAD, and SAD databases to facilitate the automated group key management of large-scale cryptographic groups.

6.2 Security Issues Not Solved by IPsec Multicast Extensions

As noted in RFC4301 section 2.2, it is out of scope of this architecture to defend the group's keys or its application data against those attacks that do not originate in the network. However, it should be noted that the risk of these attacks is magnified to the extent that the group keys are shared across a large number of systems.

The security issues that are left unsolved by the IPsec multicast extension service divide into two broad categories: outsider attacks, and insider attacks.

6.2.1 Outsider Attacks

The IPsec multicast extension service does not defend against an Adversary outside of the group who has:

- The capability to launch a multicast flooding denial-of-service attack against the group, originating from a system whose IPsec subsystem does not filter the unauthorized multicast transmissions.

- Compromised a multicast router, allowing the Adversary to corrupt or delete all multicast packets destined for the group endpoints downstream from that router.

- Captured a copy of an earlier multicast packet transmission and then replays it to a group that does not have the anti-replay service enabled. Note that for a large-scale any source multicast group, it is impractical for the Group Receivers to maintain an anti-replay state for every potential Group Speaker. Group policies that require anti-replay protection for a large-scale any-source-multicast group should consider an application layer total order multicast protocol.

6.2.2 Insider Attacks

For large-scale groups, the IP security multicast extensions are dependent on an automated Group Key Management protocol to correctly authenticate and authorize trustworthy members in compliance to the

group's policies. Inherent in the concept of a cryptographic group is a set of one or more shared secrets entrusted to all of the group's members. Consequently, the service's security guarantees are no stronger than the weakest member admitted to the group by the GKM system. The GKM system is responsible for responding to compromised group member detection by executing a group key recovery procedure. The GKM re-keying protocol will expel the compromised group members and distribute new group keying material to the trusted members. Alternatively, the group policy may require the GKM system to terminate the group.

In the event that an Adversary has been admitted into the group by the GKM system, the following attacks are possible and they can not be solved by the IPsec multicast extension service:

- The Adversary can disclose the secret group key or group data to an unauthorized party outside of the group. After a group key or data compromise, cryptographic methods such as traitor tracing or watermarking can assist in the forensics process. However, these methods are outside the scope of this specification.

- The insider Adversary can forge packet transmissions that appear to be from a peer group member. To defend against this attack for those Group Speaker transmissions that warrant the overhead, the group policy can require the Group Speaker to multicast packets using the data origin authentication service.

- If the group's data origin authentication service uses digital signatures, then the insider Adversary can launch a computational resource denial of service attack by multicasting bogus signed packets.

6.3 Implementation or Deployment Issues that Impact Security

6.3.1 Homogeneous Group Cryptographic Algorithm Capabilities

The IP security multicast extensions service can not defend against a poorly considered group security policy that allows a weaker cryptographic algorithm simply because all of the group's endpoints are known to support it. Unfortunately, large-scale groups can be difficult to upgrade to the current best in class cryptographic algorithms. One possible approach is the deployment of composite groups that can straddle heterogeneous groups [COMPGRP]. A standard solution for heterogeneous groups is an activity for future standardization. In the interim, synchronization of a group's cryptographic capabilities could be achieved using a secure and scalable software distribution management tool.

6.3.2 Groups that Span Two or More Security Policy Domains

Large-scale groups may span multiple legal jurisdictions (e.g countries) that enforce limits on cryptographic algorithms or key strengths. As currently defined, the IPsec multicast extension service requires a single group policy per group. As noted above, this problem remains an area for future standardization.

6.3.3 Network Address Translation

With the advent of NAT and mobile nodes, IPsec multicast applications must overcome several architectural barriers to their successful deployment. This section surveys those problems and identifies the GSPD/SAD state information that the GKM protocol must synchronize across the group membership.

6.3.3.1 GSPD Losses Synchronization with Internet Layer's State

The most prominent problem facing GKM protocols supporting IPsec is that the GKM protocol's group security policy mechanism can inadvertently configure the group's GSPD traffic selectors with unreliable transient IP addresses. The IP addresses are transient because of either node mobility or Network Address Translation (NAT), both of which can unilaterally change a Group Speaker's source IP address without signaling the GKM protocol. The absence of a GSPD synchronization mechanism can cause the group's data traffic to be discarded rather than processed correctly.

6.3.3.2 Mobile Multicast Care-Of Address Route Optimization

Both Mobile IPv4 [RFC3344] and Mobile IPv6 provide transparent unicast communications to a mobile Node. However, comparable support for secure multicast mobility management is not specified by these standards. The goal is the ability to maintain an end-to-end transport mode group SA between a Group Speaker mobile node that has a volatile care-of-address and a Group Receiver membership that also may have mobile endpoints. In particular, there is no secure mechanism for route optimization of the triangular multicast path between the correspondent Group Receiver nodes, the home agent, and the mobile node. Any proposed solution must be secure against hostile re-direct and flooding attacks.

6.3.3.3 NAT Translation Mappings Are Not Predictable

The following spontaneous NAT behaviors adversely impact source-specific secure multicast groups. When a NAT gateway is on the path between a Group Speaker residing behind a NAT and a public IPv4 multicast Group Receiver, the NAT gateway alters the private source address to a public IPv4 address. This translation must be coordinated with every Group Receiver's inbound GSPD multicast entries that depend on that source address as a traffic selector. One might mistakenly assume that the GCKS could set up the Group Members

with a GSPD entry that anticipates the value(s) that the NAT translates the packet's source address. However, there are known cases where this address translation can spontaneously change without warning:

- NAT gateways may re-boot and lose their address translation state information.

- The NAT gateway may de-allocate its address translation state after an inactivity timer expires. The address translation used by the NAT gateway after the resumption of data flow may differ than that known to the GSPD selectors at the group endpoints.

- The GCKS may not have global consistent knowledge of a group endpoint's current public and private address mappings due to network errors or race conditions. For example, a Group Member's address may change due to a DHCP assigned address lease expiration.

- Alternate paths may exist between a given pair of Group Members. If there are parallel NAT gateways along those paths, then the address translation state information at each NAT gateway may produce different translations on a per packet basis.

The consequence of this problem is that the GCKS can not be pre-configured with NAT mappings, as the GSPD at the Group Members will lose synchronization as soon as a NAT mapping changes due to any of the above events. In the worst case, Group Members in different sections of the network will see different NAT mappings, because the multicast packet traversed multiple NAT gateways.

6.3.3.4 SSM Routing Dependency on Source IP Address

Source-Specific Multicast (SSM) routing depends on a multicast packet's source IP address and multicast destination IP address to make a correct forwarding decision. However, a NAT gateway alters that packet's source IP address as its passes from a private network into the public network. Mobility changes a Group Member's point of attachment to the Internet, and this will change the packet's source IP address. Regardless of why it happened, this alteration in the source IP address makes it infeasible for transit multicast routers in the public Internet to know which SSM speaker originated the multicast packet, which in turn selects the correct multicast forwarding policy.

6.3.3.5 ESP Cloaks Its Payloads from NAT Gateway

When traversing NAT, application layer protocols that contain IPv4 addresses in their payload need the intervention of an Application Layer Gateway (ALG) that understands that application layer protocol [RFC3027] [RFC3235]. The ALG massages the payload's private IPv4

addresses into equivalent public IPv4 addresses. However, when encrypted by end-to-end ESP, such payloads are opaque to application layer gateways.

When multiple Group Speakers reside behind a NAT with a single public IPv4 address, the NAT gateway can not do UDP or TCP protocol port translation (i.e. NAPT) because the ESP encryption conceals the transport layer protocol headers. The use of UDP encapsulated ESP [RFC3948] avoids this problem. However, this capability must be configured at the GCKS as a group policy, and it must be supported in unison by all of the group endpoints within the group, even those that reside in the public Internet.

6.3.3.6 UDP Checksum Dependency on Source IP Address

An IPsec subsystem using UDP within an ESP payload will encounter NAT induced problems. The original IPv4 source address is an input parameter into a receiver's UDP pseudo-header checksum verification, yet that value is lost after the IP header's address translation by a transit NAT gateway. The UDP header checksum is opaque within the encrypted ESP payload. Consequently, the checksum can not be manipulated by the transit NAT gateways. UDP checksum verification needs a mechanism that recovers the original source IPv4 address at the Group Receiver endpoints.

In a transport mode multicast application GSA, the UDP checksum operation requires the origin endpoint's IP address to complete successfully. In IKEv2, this information is exchanged between the endpoints by a NAT-OA payload (NAT original address). See also reference [RFC3947]. A comparable facility must exist in a GKM protocol payload that defines the multicast application GSA attributes for each Group Speaker.

6.3.3.7 Cannot Use AH with NAT Gateway

The presence of a NAT gateway makes it impossible to use an Authentication Header, keyed by a group-wide key, to protect the integrity of the IP header for transmissions between members of the cryptographic group.

7. IANA Considerations

This document has no actions for IANA.

8. Acknowledgements

[TBD]

9. References

9.1 Normative References

[RFC1112] Deering, S., "Host Extensions for IP Multicasting," RFC 1112, August 1989.

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

[RFC3552] Rescorla, E., et. al., "Guidelines for Writing RFC Text on Security Considerations", RFC 3552, July 2003.

[RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, December 2005.

[RFC4302] Kent, S., "IP Authentication Header", RFC 4302, December 2005.

[RFC4303] Kent, S., "IP Encapsulating Security Payload (ESP)", RFC 4303, December 2004.

9.2 Informative References

[COMPGRP] Gross G. and H. Cruickshank, "Multicast IP Security Composite Cryptographic Groups", draft-gross-msec-ipsec-composite-group-01.txt, work in progress, September 2006.

[RFC2362] Estrin, D., et. al., "Protocol Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification", RFC 2362, June 1998.

[RFC2526] Johnson, D., and S. Deering., "Reserved IPv6 Subnet Anycast Addresses", RFC 2526, March 1999.

[RFC2914] Floyd, S., "Congestion Control Principles", RFC 2914, September 2000.

[RFC3027] Holdrege, M., and P. Srisuresh, "Protocol Complications with the IP Network Address Translator", RFC 3027, January 2001.

[RFC3171] Albanni, Z., et. al., "IANA Guidelines for IPv4 Multicast Address Assignments", RFC 3171, August 2001.

[RFC3235] Senie, D., "Network Address Translator (NAT)-Friendly Application Design Guidelines", RFC 3235, January 2002.

[RFC3306] Haberman B. and D. Thaler, " Unicast-Prefix-based IPv6 Multicast Addresses", RFC3306, August 2002.

[RFC3307] Haberman B., " Allocation Guidelines for IPv6 Multicast Addresses", RFC3307, August 2002.

[RFC3344] Perkins, C., "IP Mobility Support for IPv4", RFC 3344, August 2002.

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

[RFC3547] Baugher, M., Weis, B., Hardjono, T., and H. Harney, "The Group Domain of Interpretation", RFC 3547, December 2002.

[RFC3569] Bhattacharyya, S., "An Overview of Source-Specific Multicast (SSM)", RFC 3569, July 2003.

[RFC3810] Vida, R., and L. Costa, "Multicast Listener Discovery Version 2 (MLDv2) for IPv6", RFC 3810, June 2004.

[RFC3940] Adamson, B., et. al., "Negative-acknowledgment (NACK)-Oriented Reliable Multicast (NORM) Protocol", RFC 3940, November 2004.

[RFC3947] Kivinen, T., et. al., "Negotiation of NAT-Traversal in the IKE", RFC 3947, January 2005.

[RFC3948] Huttunen, A., et. al., "UDP Encapsulation of IPsec ESP Packets", RFC 3948, January 2005.

[RFC4046] Baugher, M., Dondeti, L., Canetti, R., and F. Lindholm, "Multicast Security (MSEC) Group Key Management Architecture", RFC4046, April 2005.

[RFC4082] Perrig, A., et. al., "Timed Efficient Stream Loss-Tolerant Authentication (TESLA): Multicast Source Authentication Transform Introduction", RFC 4082, June 2005.

[RFC4306] Kaufman, C., "Internet Key Exchange (IKEv2) Protocol", RFC 4306, December 2005.

[RFC4359] Weis, B., "The Use of RSA/SHA-1 Signatures within Encapsulating Security Payload (ESP) and Authentication Header (AH)", RFC 4359, January 2006.

[RFC4534] Colegrove, A., and H. Harney, "Group Security Policy Token v1", RFC 4534, June 2006.

[RFC4535] Harney, H., Meth, U., Colegrove, A., and G. Gross, "GSAKMP: Group Secure Association Key Management Protocol", RFC 4535, June 2006.

[ZLLY03] Zhang, X., et. al., "Protocol Design for Scalable and Reliable Group Rekeying", IEEE/ACM Transactions on

Networking (TON), Volume 11, Issue 6, December 2003. See
http://www.cs.utexas.edu/users/lam/Vita/Cpapers/ZLLY01.pdf.

Appendix A - Multicast Application Service Models

The vast majority of secure multicast applications can be catalogued by their service model and accompanying intra-group communication patterns. Both the Group Key Management (GKM) Subsystem and the IPsec subsystem MUST be able to configure the GSPD/SAD security policies to match these dominant usage scenarios. The GSPD/SAD policies MUST include the ability to configure both Any-Source-Multicast groups and Source-Specific-Multicast groups for each of these service models. The GKM Subsystem management interface MAY include mechanisms to configure the security policies for service models not identified by this standard.

A.1 Unidirectional Multicast Applications

Multi-media content delivery multicast applications that do not have congestion notification or retransmission error recovery mechanisms are inherently unidirectional. RFC 4301 only defines bi-directional unicast security associations (as per sections 4.4.1 and 5.1 with respect to security association directionality). The GKM Subsystem requires that the IPsec subsystem MUST support unidirectional Group Security Associations (GSA). Multicast applications that have only one group member authorized to transmit can use this type of group security association to enforce that group policy. In the inverse direction, the GSA does not have a SAD entry, and the GSPD configuration is optionally setup to discard unauthorized attempts to transmit unicast or multicast packets to the group.

The GKM Subsystem's management interface MUST have the ability to setup a GKM Subsystem group having a unidirectional GSA security policy.

A.2 Bi-directional Reliable Multicast Applications

Some secure multicast applications are characterized as one group speaker to many receivers, but with inverse data flows required by a reliable multicast transport protocol (e.g. NORM). In such applications, the data flow from the speaker is multicast, and the inverse flow from the group's receivers is unicast to the speaker. Typically, the inverse data flows carry error repair requests and congestion control status.

For such applications, the GSA SHOULD use IPsec anti-replay protection service for the speaker's multicast data flow to the group's receivers. Because of the scalability problem described in the next section, it is not practical to use the IPsec anti-replay service for the unicast inverse flows. Consequently, in the inverse direction the IPsec anti-replay protection MUST be disabled. However, the unicast inverse flows can use the group's IPsec group authentication mechanism. The group receiver's GSPD entry for this

GSA SHOULD be configured to only allow a unicast transmission to the speaker Node rather than a multicast transmission to the whole group.

If an ESP digital signature authentication is available (E.g., RFC 4359), source authentication MAY be used to authenticate a receiver Node's transmission to the speaker. The GKM protocol MUST define a key management mechanism for the group speaker to validate the asserted signature public key of any receiver Node without requiring that the speaker maintain state about every group receiver.

This multicast application service model is RECOMMENDED because it includes congestion control feedback capabilities. Refer to [RFC2914] for additional background information.

The GKM Subsystem's Group Owner management interface MUST have the ability to setup a GKM Subsystem GSA having a bi-directional GSA security policy and one group speaker. The management interface SHOULD be able to configure a group to have at least 16 concurrent authorized speakers, each with their own GSA anti-replay state.

A.3 Any-To-Any Multicast Applications

Another family of secure multicast applications exhibits a "any to many" communications pattern. A representative example of such an application is a videoconference combined with an electronic whiteboard.

For such applications, all (or a large subset) of the Group Members are authorized multicast speakers. In such service models, creating a distinct IPsec SA with anti-replay state for every potential speaker does not scale to large groups. The group SHOULD share one IPsec SA for all of its speakers. The IPsec SA SHOULD NOT use the IPsec anti-replay protection service for the speaker's multicast data flow to the Group Receivers.

The GKM Subsystem's management interface MUST have the ability to setup a group having an Any-To-Many Multicast GSA security policy.

Author's Address

Brian Weis
Cisco Systems
170 W. Tasman Drive,
San Jose, CA 95134-1706
USA

Phone: 408-526-4796
Email: bew@cisco.com

George Gross
IdentAware Security
82 Old Mountain Road
Lebanon, NJ 08833
USA

Phone: 908-268-1629
Email: gmgross@identaware.com

Dragan Ignjatic
Polycom
1000 W. 14th Street
North Vancouver, BC V7P 3P3
Canada

Phone: 604-982-3424
Email: dignjatic@polycom.com

Intellectual Property Statement

Disclaimer of Validity

Copyright Statement

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.