Internet Engineering Task Force
INTERNET-DRAFT (experimental track)

George Gross (IdentAware)
H. Cruickshank
(CCSR, U. of Surrey)

draft-ietf-msec-ipsec-composite-group-00
Expires: May, 2006

November, 2006

Multicast IP Security Composite Cryptographic Groups

Status of this Memo

Copyright Notice

Abstract

The Multicast IP Security extension architecture [Weis] implicitly assumes a basic group endpoint population that shares homogeneous cryptographic capabilities and security policies. In practice, large-scale cryptographic groups may contain a heterogeneous endpoint population that can not be accommodated by that basic multicast IPsec architecture. For example, some endpoints may not have been upgraded to handle the successor algorithm for one that is being retired (e.g. SHA1 transition to SHA-ng). Group deployments that span multiple legal jurisdictions may have a different security policy in each jurisdiction (e.g. key strength). This document defines the "composite cryptographic group" IP security architecture capability. A composite cryptographic group allows multicast IPsec applications to transparently interact with the single logical group that is formed by the union of one or more basic cryptographic groups.

Table of Contents

1. Introduction

In a basic IPsec cryptographic group there is a 1:1 relationship between an IPsec group's data security association, a multicast application, and a multicast IP address. All of the group members share identical cryptographic capabilities and they abide by a common security policy. IPsec subsystems that are compliant to the [Weis] standard by definition support basic IPsec cryptographic groups. For a small-scale cryptographic group, it is operationally feasible to maintain a homogenous endpoint population. In contrast, large-scale cryptographic groups may be heterogeneous in both their cryptographic capabilities and/or their security policies.

- The differences in cryptographic capabilities can arise when subsets of the group's membership are in transition, migrating from one version of a cryptographic algorithm to its successor (e.g. SHA-1 hash function to SHA-ng). It is unreasonable to expect that a large-scale group membership should upgrade to new capabilities in a flash cut operation.

- Heterogeneous security policies can occur when a cryptographic group's membership straddles legal or security domain boundaries. An example is a multi-national cryptographic group, for which some endpoints reside in a country that enforces legislation that specifies weaker cipher key strengths.

The above two requirements motivate the implementation and operation of a "composite IPsec cryptographic group". A composite IPsec cryptographic group is the union of two or more non-overlapping basic IPsec cryptographic sub-groups. For sake of brevity, the terms "Composite IPsec Group" and "Basic IPsec Subgroup" will be used in subsequent text. The goal of a Composite IPsec Group is to accommodate a large-scale group membership population that contains heterogeneous capabilities, policies, or other attributes. Appendix A enumerates additional use cases that can be satisfied by Composite IPsec Groups.

A strong benefit of IPsec is that it applies its security processing at the IP layer. Consequently, upper layer application programs can execute securely without reprogramming or any awareness that IPsec services are present. The additional benefit of a Composite IPsec Group is that it shields the multicast application from the IP layer complexity of the two or more Basic IPsec Subgroups. The application multicasts its messages to what appear to be a single homogeneous multicast group.

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 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.

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.

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 Protocol (GKMP) server that manages IPsec state for a group. A GCKS authenticates and provides the IPsec SA policy and keying material to GKMP group members.

Group Key Management Protocol (GKMP)

> A key management protocol used by a GCKS to distribute IPsec Security Association policy and keying material. A GKMP 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.

GKMP Subsystem

A subsystem in an IPsec device implementing a Group Key Management Protocol. The GKMP Subsystem provides IPsec SAs to the IPsec subsystem on the IPsec device.

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 GKMP Subsystem SAs necessary for a Group Member to receive key updates. A GSA describes the working policy for a group.

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 in order for IP multicast routing to correctly route IP multicast packets that are protected by IPsec.

2. Composite IPsec Group Architecture

The GCKS and the Group Members must support a Group Key Management Protocol (GKMP) that can negotiate a Composite IPsec Group's membership join or leave operation. The group key management subsystem configures one or more IPsec subsystems to reflect the Composite IPsec Group's revised state. In addition, the GCKS configures a supporting Composite Group Distributor component

whenever a new Group Speaker endpoint joins the Composite IPsec Group. The Composite Group Distributor handles the data flowing from a multicast application's Group Speaker endpoint to the IPsec subsystem. When the multicast application requests a message transmission to the Composite IPsec Group's endpoints, the Composite Group Distributor component transparently intercepts and replicates that message for multicast delivery to each Basic IPsec Subgroup. Sections 2.1 and 2.2 define the Composite Group Distributor's architectural role for transport mode and tunnel mode IPsec security associations. Section 3 provides the GKMP requirements for Composite IPsec Group capability.

2.1 Transport Mode Composite Group Distributor

For a Composite IPsec Group transport mode security association, it is the responsibility of the Composite Group Distributor to rewrite each message copy's destination IP address before it is multicast to the respective Basic IPsec Subgroup. The IPsec subsystem's SPD traffic selectors then evaluate that message, and apply the Basic IPsec Subgroup's security association transform. Since a single IPsec subsystem supports the Group Speaker, that IPsec subsystem MUST support all of the outbound security transforms required by all of the Basic IPsec Subgroups that form the Composite IPsec Group. Regardless of the Composite Group Distributor's underlying implementation, it is a requirement that the two or more security transforms applied by the IPsec subsystem to the multicast application's replicated data streams MUST remain transparent to that application's Group Speaker endpoint. Each Basic IPsec Subgroup MUST be allocated a unique multicast destination IP address. Appendix B provides non-normative guidance for the implementation of a Composite Group Distributor supporting IPsec transport mode security associations.

2.2 Tunnel Mode Composite Group Distributor

For a Composite IPsec Group tunnel mode security association, the Composite Group Distributor component is simply the multicast routing infrastructure residing on the network path between the Group Speaker endpoint and two or more IPsec subsystems. Typically, the IPsec subsystems are IPsec security gateways. In a tunnel mode configuration, there is a parallel IPsec subsystem instance per Basic IPsec Subgroup. Unlike transport mode, in tunnel mode the Composite Group Distributor does not rewrite the destination IP multicast address for each Basic IPsec Subgroup. Instead, each IPsec subsystem SPD independently recognizes the message addressed to the Composite IPsec Group destination IP address, and applies the IPsec tunnel mode security transform for its respective Basic IPsec Subgroup. Each IPsec subsystem MUST use a unique Security Parameter Index for their security association instance. The GKMP is responsible for allocating the SPI for each tunnel mode security association, so that they are uniquely identified when the replicated messages are distributed to the Composite IPsec Group.

Note that in tunnel mode, there is one multicast distribution tree representing the Composite IPsec Group rather than a multicast distribution tree per Basic IPsec Subgroup. All of the message copies are multicast to the Composite IPsec Group's multicast IP address. Consequently, the Group Receiver IPsec subsystems use the SPI to de-multiplex which one of the message replicas is addressed to its Basic IPsec Subgroup.

2.3 Rationale for Multicast Destination IP Address and SPI Assignment

For Composite Groups in transport mode, each Basic IPsec Subgroup is assigned a distinct multicast destination IP address. This assignment policy assures that the Group Speaker IPsec subsystem's SPD packet matching can direct a packet to the correct sub-group's transport mode IPsec SA instance. In particular, the CGD must not only replicate the transmitted packet for each Basic IPsec Subgroup, it must also alter each copied packet's destination IP address so that the packet will be matched by the SPD and then encrypted by the respective IPsec SAD entry.

In a Composite Group with tunnel mode address preservation, the address assignment policy is to keep the packet's original multicast address, and use only the SPI to distinguish between the Basic IPsec Subgroups. Each Basic IPsec Subgroup has a parallel Security Gateway instance doing an IPsec tunnel mode SA encapsulation. There is no CGD component in these Security Gateways, since the multicast capable trusted network has already replicated the packet. Each such Security Gateway SPD is configured by the GKM protocol to insert the same outer IP header as its peer Security Gateways. However, the SPI assigned to the IPsec SA at each of the Security Gateways must be unique. This allows the Group Receivers to discriminate between the sub-group specific packet arrivals sharing a common destination multicast IP address.

In a Composite Group without tunnel mode address preservation, it is feasible to use any assignment policy that maintains a unique 2-tuple of {destination multicast IP address, SPI} across all of the Basic IPsec subgroups.

3. Group Key Management Protocol Composite IPsec Group Requirements

A Group Key Management Protocol subsystem supporting Composite IPsec Groups is responsible for configuring the Group Speaker's Composite Group Distributor and one or more IPsec SPD/SAD to create and manage a Composite IPsec Group membership. Those GKMP subsystems that choose to implement the optional Composite IPsec Group capability MUST support both Group Receivers and Group Speakers, as defined below in section 3.2 and section 3.3 respectively.

3.1 IPsec Security Association Identifier Assignment

Each Basic IPsec Subgroup MUST have a group data IPsec security association identifier allocation from the GKMP subsystem that is unique relative to all other security associations in the Composite IPsec Group. For an any-source multicast group, the security association identifier is the 2-tuple {destination multicast IP address, Security Parameter Index}. If the Composite IPsec Group is using Source-Specific Multicast, then the IPsec security association identifier MUST be composite group-wide unique for the 3-tuple: {source IP address, destination multicast IP address, Security Parameter Index}.

3.2 Group Receiver Composite IPsec Group Membership

A Group Receiver endpoint acquires membership in only one Basic IPsec Subgroup within a Composite IPsec Group. When a Group Receiver endpoint requests to join the Composite IPsec Group, the registration protocol exchange MUST select the Group Receiver's membership in one of the Basic IPsec Subgroups. The Basic IPsec Subgroup selection can be implicit (i.e. pre-configured at the GCKS) or explicitly negotiated by registration protocol exchanges between the candidate Group Receiver and the GCKS. The GKMP specification defines the registration protocol exchange negotiation. When evaluating a candidate Group Receiver's registration request, the GCKS MUST enforce the authentication and membership authorization policies of the Basic IPsec Subgroup that the candidate Group Receiver has requested membership.

3.3 Group Speaker Composite IPsec Group Membership

When a Group Speaker endpoint registers with a GCKS to join a Composite IPsec Group, the Group Speaker implicitly joins all of the Basic IPsec Subgroups as a speaker in each subgroup. The GCKS sets up the Composite IPsec Group such that when the multicast application Group Speaker endpoint sends a single message to the Composite IPsec Group, it is received once at each Group Receiver endpoint within the two or more Basic IPsec Groups. The GCKS and GKMP is responsible for the following actions:

- The GCKS MUST authenticate and authorize the candidate Group Speaker endpoint before allowing it to become a Composite IPsec Group Speaker. The speaker authorization is contingent on the approval of both the Composite IPsec Group policy and the logical-AND authorization of all of the Basic IPsec Group policies.

- For each Basic IPsec Group, the GCKS allocates a new group IPsec security association instance representing the new Group Speaker. The GCKS uses the GKMP to distribute and then activate that IPsec security association's configuration in the IPsec subsystem SPD/SAD of every Group Receiver endpoint within the subgroup. In addition, the GCKS chooses one IPsec subsystem to be the Group Speaker's representative in that Basic IPsec Group, and configures its SPD/SAD for that role.

- o For an IPsec transport mode security association, the GCKS explicitly directs the Group Speaker's Composite Group Distributor to intercept and replicate the Group Speaker's data traffic before multicasting it to each Basic IPsec Group. The trusted control interface between the GCKS and Composite Group Distributor is implementation specific and it is outside the scope of this specification.

5. IANA Considerations

This document does not require any IANA action.

6. Security Considerations

This document describes a large-scale Composite IPsec Group architecture. Consequently, it inherits all of the security considerations previously discussed in [Weis] for Basic IPsec Groups. The reader is encouraged to review those security considerations in addition to those discussed herein for Composite IPsec Groups.

6.1 Security Issues Solved by Composite IPsec Groups

Composite IPsec Groups accommodate the natural heterogeneity often found in large-scale cryptographic groups. Two common motivations for Composite IPsec Groups are easing the migration to new cryptographic algorithms and handling country-specific cryptographic policies. Appendix A enumerates a variety of other potential use cases.

Regardless of the motive, the primary benefit of composite groups is that a group multicast application can interact without change with a single virtual homogeneous cryptographic group. The Composite Group Distributor and its supporting IPsec subsystems transparently apply the correct IPsec transforms at the IP layer for each sub-group. An operational benefit of Composite IPsec Groups is that it centralizes the security policy management for multiple group multicast applications into a single Security Officer role.

In contrast, in the scenario without the Composite Group capability, a group multicast application must be re-programmed and re-configured to correctly interact with the two or more Basic IPsec Groups. Alternatively, the group multicast application must be re-programmed to support an application layer security service equivalent to that offered by the IPsec subsystem at the network layer. In either case, the group multicast application incurs complexity and cost that could have been avoided.

6.2 Security Issues Not Solved by Composite IPsec Groups

Similar as is the case for Basic IPsec Groups, the security issues not solved by a Composite IPsec Group divide into two categories:

outsider attacks, and insider attacks. The discussion will focus on the security issues that arise only in Composite IPsec Groups.

6.2.1 Outsider Attacks

A Composite IPsec Group using a weak cryptographic algorithm or key strength in one of its Basic IPsec groups is vulnerable to an Adversary that knows (or guesses) which sub-group uses that algorithm. The Adversary can narrow its eavesdropping effort to only the traffic sent to that sub-group and apply cryptoanalysis on that sub-group's cipher-text.

The Composite Group Distributor can inadvertently leak the composite group security policy to an Adversary that records the transmission time of an IP packet, as each copy is encrypted and multicast for a Basic IPsec Group. The Adversary could use that encryption processing delay information to infer the cryptographic algorithm being applied to a given Basic IPsec Group (e.g. AES encrypts at a faster rate than triple-DES). The Composite Group Distributor can avoid this attack by delaying each packet's transmission by a random dither.

If two Basic IPsec groups use the same encryption key but different encryption algorithms for the same plain-text transmissions, then the cipher-text may become vulnerable to differential analysis attacks. This vulnerability exists only to the extent that comparing the output of the encryption algorithms could disclose hints about the plain text or the encryption key. Requiring the GKM protocol to distribute a distinct encryption key for each Basic IPsec Group can help mitigate this attack. Changing the keys more frequently is another strategy.

6.2.2 Insider Attacks

Composite IPsec Groups are vulnerable to a registration time bid down attack unless the GKM protocol has an accurate database describing each group member's cryptographic capabilities. In the absence of GKM enforcement at registration time, an insider Adversary could pretend to support only a weak cryptographic algorithm. An accomplice to the Adversary could eavesdrop and apply cryptoanalysis on the weakened transmissions without the insider Adversary risking detection by explicitly disclosing the key or plain text. To avoid this attack, a Composite IPsec Group depends on the Group Owner designing a membership authorization policy that forces each candidate Group Receiver member to only join the Basic IPsec Group that implements the strongest algorithms that their IPsec subsystem is known to support. Special care must be taken when authorizing a Group Speaker, as a group member in that role becomes a member of every Basic IPsec Group.

A Composite Group Distributor under the control of an insider Adversary could create a covert channel by altering the order in which it multicast an IP packet to each Basic IP Group. An accomplice

to the Adversary who observed a long sequence of IP packet multicasts could assemble the covert message from a codebook. Each symbol would be represented by a different sequence of Basic IPsec Group transmissions.

6.3 Implementation or Deployment Issues that Impact Security

The most prominent barrier to a successful Composite IPsec Group deployment is the complexity of designing a composite group security policy. Factors that should be considered when designing such policies include:

- For each Basic IPsec Group, the policy should delegate the subordinate GCKS role to the group member with the highest trustworthiness amongst all members of that sub-group.
- A Group Receiver identity should be an authorised member of only one Basic IPsec Group and that sub-group should represent the strongest cryptographic algorithm that the member is capable of supporting.
- The Group Speaker role is endowed with a membership in every sub-group, and therefore this role should be authorised for only the group's most trustworthy members.
- The weakest Basic IPsec Group should be the focal point for retirement efforts, with the goal of moving its membership to better cryptographic algorithms.
- A host system implementing the Composite Group Distributor component will necessarily incur substantially more encryption processing overhead, in proportion to the number of Basic IPsec Groups that form the Composite IPsec Group. Consequently, care should be exercised to minimise the number of Basic IPsec Groups.
- The use of ESP padding, frequent key changes, and a separate key for each IPsec SA can help mitigate traffic analysis attacks that compare the cipher-texts sent to multiple Basic IPsec Groups.

7. Acknowledgements

[TBD]

8. References

8.1 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.

[Weis] Weis B., Gross G., Ignjatic D., "Multicast Extensions to the Security Architecture for the Internet", draft-ietf-msec-extensions-03.txt, October 2006, work in progress.

8.2 Informative References

[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.

[RFC3171] Albanni, Z., et. al., "IANA G uidelines fo r IPv4 Multic ast Address Assignments", RFC 3171, August 2001.

[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] Bhatta charyya, S., "An Ov erview of So urce-Specifi c Multic ast (SSM)", RFC 3569, July 2003.

[RFC3940] Adamso n, B., et. a l., "Negative-a cknowledgmen t (NACK)-Orient ed Reliable Multicast (N ORM) Protoco l", RFC 3940, November 2004.

[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.

[RFC3451] Luby, M., et al, "Layered Coding Transport (LCT) Building Block", RFC3451, December 2002.

APPENDIX A: Examples of Composite Cryptographic Group Use Cases

The following is a non-exhaustive list that identifies other representative use cases where a Composite Group could be applied:

- A group policy that allows the use of both IETF standard and vendor-specific cryptographic algorithms.

- A group straddling both IP-v4 and IP-v6 endpoints. For a group spanning IP-v4 and IP-v6, the Group Speaker endpoint's Node must be dual stack capable.

- A single group using a Reliable Multicast Transport protocol (RTMP) that has a heterogeneous deployment of error recovery algorithms (e.g. Forward Error Correction codes) at its endpoint population. Each RMTP version is configured as a sub-group at a distinct multicast destination IP address. In this case, the application's payload is replicated within the Group Speaker before being distributed to each RMTP version-specific subsystem. The Group Speaker endpoint's system must implement all of the RMTP sub-group versions.

- There are multiple multicast routing domains supporting the IPsec group, each routing domain imposing its own policy defined multicast IP address. The Composite Group Distributor must alter the multicast destination IP address for each copy of the multicast packet before it is sent to its respective routing domain.

- A multicast application wherein the Composite Group is the union of multiple source-specific IP multicast groups. For example, a multi-homed Group Speaker might require this configuration.

In principal, each of the above examples could be decomposed into multiple independent basic IPsec cryptographic groups. However, that incurs a commensurate increase in the multicast application's overhead to discover, join, and manage each of those groups. A preferable solution is for the multicast application to join one Composite Group

Figures A-1, A-2, and A-3 illustrate several representative composite group use cases.

Multicast IPsec Composite Cryptographic Groups

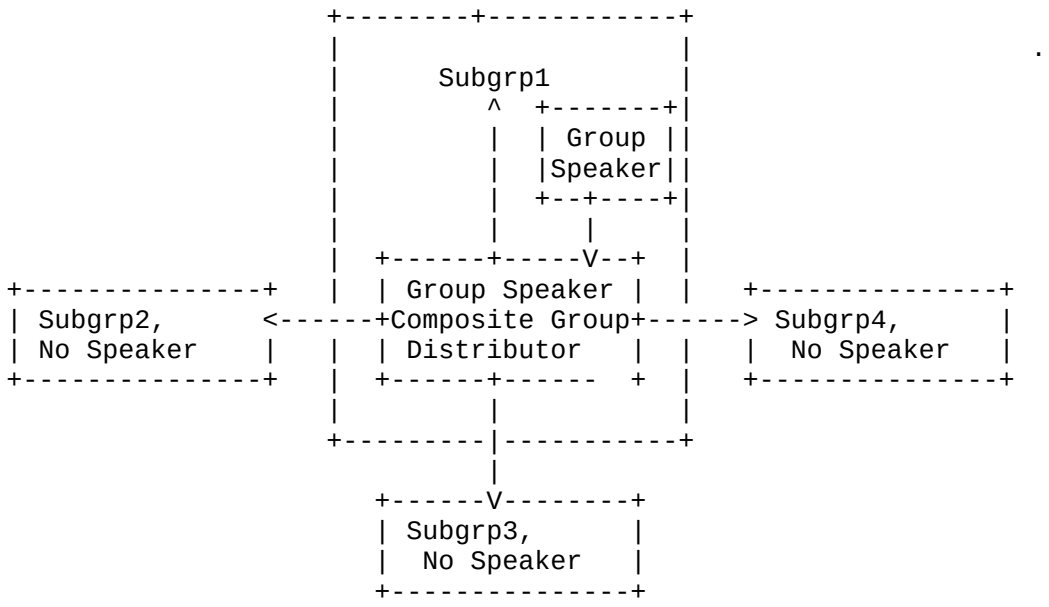

Figure A-1: A simple Composite Group with a single Group Speaker multicasting to 4 Basic IPsec Subgroups, each subgroup having a different group security policy. The Group Speaker multicasts to all four subgroups but it will receive its multicast traffic from only from "Subgrp1". The Group Speaker's Composite Group Distributor (CGD) replicates each of the Group Speaker's IP packets, transforms each copied packet according to its respective Basic IPsec Subgroup's security policy, and sends that copied packet to its subgroup. The Composite Group's security policy specifies each Basic IPsec Subgroup's membership authorization.

Multicast IPsec Composite Cryptographic Groups

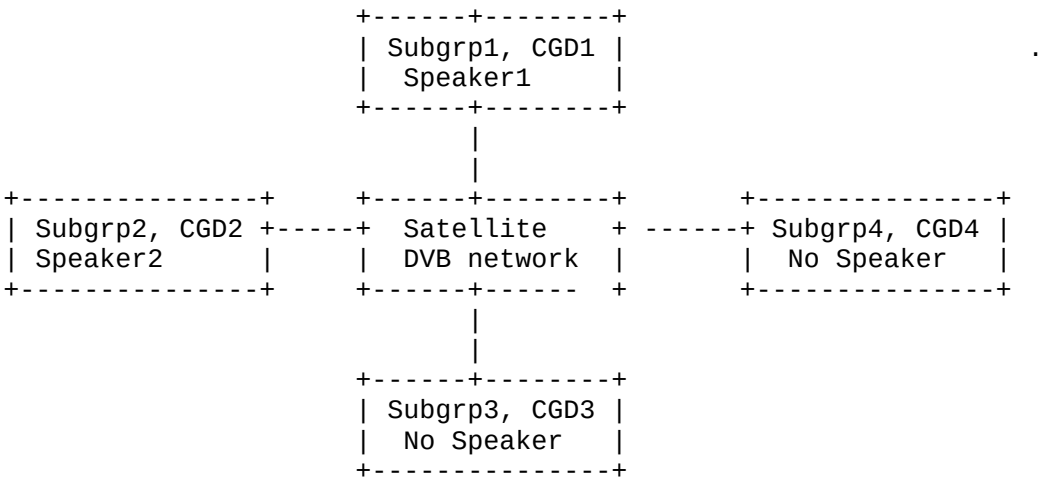

Figure A-2: A Composite Group containing 4 Basic IPsec Subgroups, with each subgroup having its own S-GCKS. There are 5 LKH trees, one for each subgroup managed by a S-GCKS and one LKH tree managed by the primary GCKS for the set of S-GCKS.

Figure A-3 illustrates a reliable multicast scenario using Layered Coding Transport (LCT) as specified in RFC 3451 [RFC3451]. Each subgroup corresponds to a LCT layer. Reliable content delivery and streaming applications could leverage this type of configuration.

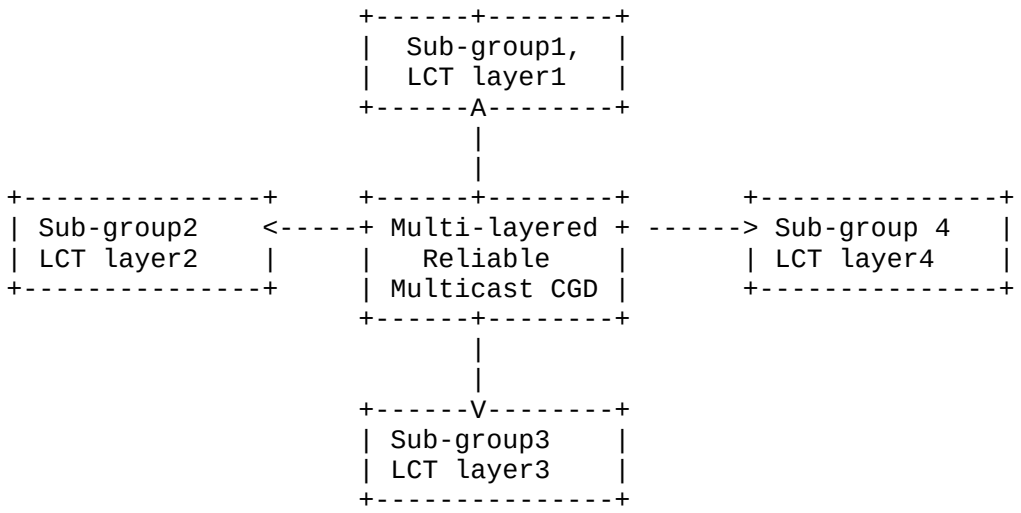

Figure A-3: 4 The LCT groups are organized as Basic IPsec Subgroups managed by a centralized GCKS.

Author's Address

George Gross
IdentAware Security
82 Old Mountain Road
Lebanon, NJ 08833, USA
908-268-1629
gmgross@identaware.com

Haitham Cruickshank
Centre for Communications System Research (CCSR)
University of Surrey
Guildford, Surrey, GU2 7XH
UK
Email: h.cruickshank@surrey.ac.uk

Intellectual Property Statement

Disclaimer of Validity

Copyright Statement

Acknowledgement

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