Internet Engineering Task Force
INTERNET-DRAFT
draft-ietf-msec-arch-05.txt
January 2004

Thomas Hardjono (VeriSign)
Brian Weis (Cisco)

Expires July 2004

The Multicast Group Security Architecture

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.

Copyright Notice

Copyright (C) The Internet Society (2004). All Rights Reserved.

Abstract

This document provides an overview and rationale of the multicast security architecture used to secure data packets of large multicast groups. The document begins by introducing a Multicast Security Reference Framework, and proceeds to identify the security services that may be part of a secure multicast solution.

Table of Contents

1. Introduction....2
  1.1 Scope....3
  1.2 Summary of Contents of Document....4
  1.3 Audience....4
  1.4 Terminology....4
2. Architectural Design: The Multicast Security Reference Framework...5
  2.1 The Reference Framework....5
  2.2 Elements of the Centralized Reference Framework....6
    2.2.1 Group Controller and Key Server....7
    2.2.2 Sender and Receiver....7
    2.2.3 Policy Server....7
  2.3 Elements of the Distributed Reference Framework....8
3. Functional Areas....9
  3.1 Multicast Data Handling....9
  3.2 Group Key Management....10
  3.3 Multicast Security Policies....11
4. Group Security Associations (GSA)....12
  4.1 The Security Association....12
  4.2 Structure of a GSA: Introduction....12
  4.3 Structure of a GSA: Reasoning....13
  4.4 Definition of GSA....14
  4.5 Typical Compositions of a GSA....16
5. Security Services....16
  5.1 Multicast Data Confidentiality....17
  5.2 Multicast Source Authentication and Data Integrity....17
  5.3 Multicast Group Authentication....18
  5.4 Multicast Group Membership Management....18
  5.5 Multicast Key Management....19
  5.6 Multicast Policy Management....20
6. Security Considerations....20
  6.1 Multicast Data Handling....20
  6.2 Group Key Management....21
  6.3 Multicast Security Policies....21
7. Intellectual Property Rights Statement....21
8. Acknowledgments....21
9. References....22
  9.1 Normative References....22
  9.2 Informative References....22
Authors Addresses....24
Full Copyright Statement....24

1. Introduction

Securing IP multicast group communication is a complex task that involves many aspects. Consequently, a secure IP multicast protocol suite must have a number of functional areas that address different aspects of the solution. This document describes those functional areas, and how they are related.

1.1 Scope

This architecture is concerned with the securing of large multicast groups. Whereas it can also be used for smaller groups, it is not necessarily the most efficient means. Other architectures (e.g., the Cliques architecture [STW]) can be more efficient for small ad-hoc group communication.

This architecture is "end to end", and does not require multicast routing protocols (e.g., PIM [RFC2362]) to participate in this architecture. Inappropriate routing may cause denial of service to application layer groups conforming to this architecture. However the routing cannot affect the authenticity or secrecy of group data or management packets. The multicast routing protocols could themselves use this architecture to protect their own multicast and group packets. However, this would be independent of any secure application layer group.

This architecture does not require IP multicast admission control protocols (e.g., IGMP [RFC3376], MLD [RFC3019]) to be a part of secure multicast groups. As such, a "join" or "leave" operation for a secure group is independent of a "join" or "leave" of an IP multicast group. For example, the process of joining a secure group requires being authenticated and authorized by a security device, while the process of joining an IP multicast group entails contacting a multicast-aware router. Admission control protocols could themselves use this architecture to protect their own multicast packets. However, this would be independent of any secure application layer group.

This architecture does not explicitly describe how secure multicast groups deal with Network Address Translation (NAT) [RFC2663]. Multicast routing protocols generally require the source and destination addresses and ports of an IP multicast packet to remain unchanged. This allows consistent multicast distribution trees to be created throughout the network. If NAT is used in a network, then the connectivity of senders and receivers may be adversely affected. This situation is neither improved or degraded as a result of deploying this architecture.

This architecture does not require the use of reliable mechanisms, for either data or management protocols. The use of reliable multicast routing techniques (e.g., FEC [RFC3453]) enhance the availability of secure multicast groups. However the authenticity or

secrecy of group data or management packets is not affected by the omission of that capability from a deployment.

1.2 Summary of Contents of Document

This document provides an architectural overview that outlines the security services required to secure large multicast groups. It provides a Reference Framework for organizing the various elements within the architecture, and explains the elements of the Reference Framework.

The Reference Framework organizes the elements of the architecture along three Functional Areas pertaining to security. These elements cover the treatment of data when it is to be sent to a group, the management of keying material used to protect the data, and the policies governing a group.

Another important item in this document is the definition and explanation of Group Security Associations (GSA), which is the multicast counterpart of the unicast Security Association (SA). The GSA is specific to multicast security, and is the foundation of the work on group key management.

1.3 Audience

This document is addressed to the technical community, implementers of IP multicast security technology, and others interested in gaining a general background understanding of multicast security. This document assumes that the reader is familiar with the Internet Protocol, the IPsec suite of protocols (e.g. [RFC2401]), related networking technology, and general security terms and concepts.

1.4 Terminology

The following key terms are used throughout this document.

1-to-N

A group which has one sender and many receivers.

Group Security Association (GSA)

A bundling of Security Associations (SAs) that together define how a group communicates securely. The GSA may include an registration protocol SA, a rekey protocol SA, and one or more data security protocol SAs.

M-to-N

A group which has many senders and many receivers, where M and N are not necessarily the same value.

Security Association (SA)

A set of policy and cryptographic keys that provide security services to network traffic that matches that policy.

2. Architectural Design: The Multicast Security Reference Framework

This section considers the complex issues of multicast security in the context of a Reference Framework. This reference framework is used to classify functional areas, functional elements, and interfaces. Two designs of the reference framework are shown: a centralized design, and a distributed design that extends the centralized design for very large groups.

2.1 The Reference Framework

The reference framework is based on three broad functional areas (as shown in Figure 1). The reference framework incorporates the main entities and functions relating to multicast security, and depicts the inter-relations among them. It also expresses multicast security from the perspective of multicast group types (1-to-N and M-to-N), and classes of protocols (the exchanged messages) needed to secure multicast packets.

The aim of the reference framework is to provide some general context around the functional areas, and the relationships between the functional areas. Note that some issues span more than one so-called functional area. In fact, the framework encourages the precise identification and formulation of issues that involve more than one functional area or those which are difficult to express in terms of a single functional area. An example of such a case is the expression of policies concerning group keys, which involves both the functional areas of group key management and multicast policies.

When considering the reference framework diagrams, it is important to realize that the singular "boxes" in the framework do not necessarily imply a corresponding singular entity implementing a given function. Rather, a box in the framework should be interpreted loosely as pertaining to a given function related to a functional area. Whether that function is in reality implemented as one or more physical entities is dependent on the particular solution. As an example, the

box labeled "Key Server" must be interpreted in broad terms as referring to the functions of key management.

Similarly, the reference framework acknowledges that some implementations may in fact merge a number of the "boxes" into a single physical entity. This could be true even across functional areas. For example, an entity in a group could act as both a Group Controller and a Sender to a group.

The protocols to be standardized are depicted in the reference framework diagrams by the arrows that connect the various boxes. See more details in Section 4, below.

2.2 Elements of the Centralized Reference Framework

The Reference Framework diagram of Figure 1 contains boxes and arrows. The boxes are the functional entities and the arrows are the interfaces between them. Standard protocols are needed for the interfaces, which support the multicast services between the functional entities.

In some cases, a system implementing the multicast security architecture may not need to implement protocols to account for every interface. Rather, those interfaces may be satisfied through the use of manual configuration, or even omitted if they are not necessary for the application.

There are three sets of functional entities. Each is discussed below.

```
              +-------------------------------------+
              |                                     |
              |                                     |
              |  FUNCTIONAL                         |
              |    AREAS                            |
              |                                     |
              |             +------+                |
              |  Multicast  |Policy|                |
              |  Security   |Server|                |
              |  Policies   +------+                |
              |                 ^                   |
              |                 |                   |
              |                 |                   |
              |                 v                   |
              |             +------+                |
              |  Group      |Group |                |
              |  Key        |Ctrl/ |<---------+     |
              |  Management |Key   |          |     |
```

```
               |             |Server|          V      |
               |             +------+     +--------+  |
               |                 ^        |        |  |
               |                 |        |Receiver|  |
               |                 |        |        |  |
               |                 v        +--------+  |
               |             +------+          ^      |
               |             |      |          |      |
               |  Multicast  |Sender|----------+      |
               |  Data       |      |                 |
               |  Handling   |      |                 |
               |             +------+                 |
               |                                      |
               +--------------------------------------+
```

Figure 1: Centralized Multicast Security Reference Framework

2.2.1 Group Controller and Key Server

The Group Controller and Key Server (GCKS) represent both the entity and functions relating to the issuance and management of cryptographic keys used by a multicast group, which is subject to the user-authentication and authorization checks conducted on the candidate member of the multicast group.

The Key Server (KS) and the Group Controller (GC) have somewhat different functionality and may in principle be regarded as separate entities. Currently the framework regards the two entities as one "box" in order to simplify the design, and in order not to mandate standardization of the protocol between the KS and the GC. It is stressed that the KS and GC need not be co-located. Furthermore, future designs may choose to standardize the protocol between the GC and the KS, without altering other components.

2.2.2 Sender and Receiver

The Sender is an entity that sends data to the multicast group. In a 1-to-N multicast group only a single sender is authorized to transmit data to the group. In an M-to-N multicast group, two or more group members are authorized to be senders. In some groups all members are authorized as senders.

Both Sender and Receiver must interact with the GCKS entity for the purpose of key management. This includes user and/or device authentication, user and/or device authorization, the obtaining of keying material in accordance with some key management policies for the group, obtaining new keys during key-updates, and obtaining other

messages relating to the management of keying material and security parameters.

Senders and Receivers may receive much of their policy from the GCKS entities. The event of joining a multicast group is typically coupled with the Sender/Receiver obtaining keying material from a GCKS entity. This does not preclude the direct interaction between the Sender/Receiver and the Policy Server.

2.2.3 Policy Server

The Policy Server represents both the entity and functions used to create and manage security policies specific to a multicast group. The Policy Server interacts with the GCKS entity in order to install and manage the security policies related to the membership of a given multicast group and those related to keying material for a multicast group.

The interactions between the Policy Server and other entities in the reference framework is dependent to a large extent on the security circumstances being addressed by a given policy.

2.3 Elements of the Distributed Reference Framework

The need for solutions to be scalable to large groups across wide geographic regions of the Internet requires the elements of the framework to also function as a distributed system. Figure 2 shows how distributed designs supporting large group scalability fit into the Reference Framework.

```
 +-------------------------------------------------------------------+
 |                                                                   |
 |                                                                   |
 | FUNCTIONAL                                                        |
 |   AREAS                                                           |
 |            +------+                                +------+       |
 | Multicast  |Policy|<-------------------------------->|Policy|       |
 | Security   |Server|                                |Server|       |
 | Policies   +------+                                +------+       |
 |                ^                                       ^          |
 |                |                                       |          |
 |                |                                       |          |
 |                v                                       v          |
 |            +------+                                +------+       |
 | Group      |Group |<-------------------------------> |Group |       |
 | Key        |Ctrl/ |<---------+                     |Ctlr/ |       |
```

```
 | Management |Key   |          |                      |Key   |   |
 |            |Server|          V                      |Server|   |
 |            +------+     +--------+                  +------+   |
 |                ^        |        |                      ^      |
 |                |        |Receiver|                      |      |
 |                |        |        |                      |      |
 |                v        +--------+                      |      |
 |            +------+          ^                          V      |
 |            |      |          |                     +--------+  |
 | Multicast  |Sender|----------+                     |        |  |
 | Data       |      |--------------------------------->|Receiver|  |
 | Handling   |      |                                 |        |  |
 |            +------+                                 +--------+  |
 +-------------------------------------------------------------------+
```

Figure 2: Distributed Multicast Security Reference Framework

In a distributed design the GCKS entity interacts with other GCKS entities to achieve scalability in the key management related services. GCKS entities will require a means of authenticating their peer GCKS entities, a means of authorization, and a means of interacting securely to pass keys and policy.

Similarly, Policy Servers must interact with each other securely to allow the communication and enforcement of policies across the Internet.

Two Receiver boxes are displayed corresponding to the situation where both the Sender and Receiver employ the same GCKS entity (centralized architecture) and where the Sender and Receiver employ different GCKS entities (distributed architecture). In the distributed design, all Receivers must obtain identical keys and policy. Each member of a multicast group may interact with a primary GCKS entity (e.g., the "nearest" GCKS entity, measured in terms of a well-defined and consistent metric). Similarly, a GCKS entity may interact with one or more Policy Servers, also arranged in a distributed architecture.

3. Functional Areas

The Reference Framework identifies three functional areas. They are:

- Multicast data handling. This area covers the security-related treatments of multicast data by the sender and the receiver. This functional area is further discussed in Section 3.1.

- Group Key Management. This area is concerned with the secure distribution and refreshment of keying material. This functional

area is further discussed in Section 3.2.

- Multicast security policies. This area covers aspects of policy in the context of multicast security, taking into consideration the fact that policies may be expressed in different ways, that they may exist at different levels in a given multicast security architecture, and that they may be interpreted differently according to the context in which they are specified and implemented. This functional area is further discussed in Section 3.3.

3.1 Multicast Data Handling

In a secure multicast group, the data typically needs to be:

1. Encrypted using the group key, mainly for access control and possibly also for confidentiality.

2. Authenticated, for verifying the source and integrity of the data. Authentication takes two flavors:
   a. Source authentication and data integrity. This functionality guarantees that the data originated with the claimed source and was not modified en route (either by a group member or an external attacker).
   b. Group authentication. This type of authentication only guarantees that the data was generated (or last modified) by some group member. It does not guarantee data integrity unless all group members are trusted.

While multicast encryption and group authentication are fairly standard and similar to encrypting and authenticating point-to-point communication, source authentication for multicast is considerably more involved. Consequently, off-the-shelf solutions (e.g., taken

from IPsec [RFC2406]) may be sufficient for encryption and group authentication. For source authentication, however, special-purpose transformations are necessary. See [CCPRRS] for further elaboration on the concerns regarding the data transforms.

Multicast data encrypted and/or authenticated by a sender should be handled the same way by both centralized and distributed receivers, (as shown in Figure 2).

The "Multicast Encapsulating Security Payload" [BCCR] provides the definition for Multicast ESP for data traffic. The "Multicast Source Authentication Transform Specification" [PCW] defines the use of the TESLA algorithm for source authentication in multicast.

3.2 Group Key Management

The term "keying material" refers to the cryptographic keys belonging to a group, the state associated with the keys, and the other security parameters related to the keys. Hence, the management of the cryptographic keys belonging to a group necessarily requires the management of their associated state and parameters. A number of solutions for specific issues must be addressed. These may include the following:

- Methods for member identification and authentication.
- Methods to verify the membership to groups.
- Methods to establish a secure channel between a GCKS entity and the member, for the purpose of delivery of shorter-term keying material pertaining to a group.
- Methods to establish a long-term secure channel between one GCKS entity and another, for the purpose of distributing shorter-term keying material pertaining to a group.
- Methods to effect the changing of keys and keying material
- Methods to detect and signal failures and perceived compromises to keys and keying material

The requirements related to the management of keying material must be seen in the context of the policies that prevail within the given circumstance.

Core to the area of key management is Security Association (SA) Management, which will be discussed further below.

A "Group Key Management Architecture" document [BCDL] further defines the key management architecture for multicast security. It builds on the Group Security Association (GSA) concept, and further defines the roles of the Key Server and Group Controller.

"The Group Domain of Interpretation" [RFC3547], "GSAKMP" [GSAKMP], and "MIKEY" [ACLNM] are three instances of protocols implementing the group key management function.

3.3 Multicast Security Policies

Multicast Security Policies must provide the rules for operation for the other elements of the Reference Framework. Security Policies may be distributed in an ad-hoc fashion in some instances. However, better coordination and higher levels of assurance are achieved if a Policy Controller distributes Security Policies policy to the group.

Multicast security policies must represent, or contain, more

information than a traditional peer-to-peer policy. In addition to representing the security mechanisms for the group communication, the policy must also represent the rules for the governance of the secure group. For example, policy would specify the authorization level necessary in order for an entity to join a group. More advanced operations would include the conditions when a group member must be forcibly removed from the group, and what to do if the group members need to resynchronize because of lost key management messages.

The application of policy at the Group Controller element and the member (sender and receiver) elements must be described. While there is already a basis for security policy management in the IETF, multicast security policy management extends the concepts developed for unicast communication in the areas of:

- Policy creation,
- High-level policy translation, and
- Policy representation.

Examples of work in multicast security policies include the Dynamic Cryptographic Context Management project [Din], Group Key Management Protocol [Har1, Har2], and Antigone [McD].

Policy creation for secure multicast has several more dimensions than the single administrator specified policy assumed in the existing unicast policy frameworks. Secure multicast groups are usually large and by their very nature extend over several administrative domains, if not spanning a different domain for each user. There are several methods that need to be considered in the creation of a single, coherent group security policy. They include a top-down specification of the group policy from the group initiator and negotiation of the policy between the group members (or prospective members). Negotiation can be as simple as a strict intersection of the policies of the members or extremely complicated using weighted voting systems.

The translation of policy rules from one data model to another is much more difficult in a multicast group environment. This is especially true when group membership spans multiple administrative domains. Policies specified at a high level with a Policy Management tool must be translated into more precise rules that the available security policy mechanisms can both understand and implement. When dealing with multicast communication and its multiple participants, it is essential that the individual translation performed for each

participant result in the use of a mechanism that is interoperable with the results of all of the other translations. Typically, the

translation from high-level policy to specific policy objects must result in the same objects in order to achieve communication between all of the group members. The requirement that policy translation results in the same objects places constraints on the use and representations in the high-level policies.

It is also important that policy negotiation and translation be performed as an integral part of joining a group. Adding a member to a group is meaningless if they will not be able to participate in the group communications.

4. Group Security Associations (GSA)

4.1 The Security Association

A security association is a commonly used term in cryptographic systems (e.g., [RFC2401, RFC2406bis, RFC2409]). This document uses the term to mean any set of policy and cryptographic keys that provide security services for the network traffic matching that policy. A Security Association usually contains the following attributes:

- selectors, such as source and destination transport addresses.
- properties, such as an security parameter index (SPI) or cookie pair, and identities.
- cryptographic policy, such as the algorithms, modes, key lifetimes, and key lengths used for authentication or confidentiality.
- keys, such as authentication, encryption and signing keys.

Group key management uses a different set of abstractions than point-to-point key management systems (such as IKE [RFC2409]). Notwithstanding, the abstractions used in the Group Key Management functional area may be built from the point-to-point key management abstractions.

4.2 Structure of a GSA: Introduction

Security associations (SAs) for group key management are more complex, and are usually more numerous, than for point-to-point key management algorithms. The latter establishes a key management SA to protect application SAs (usually one or two, depending on the protocol). However, group key management may require up to three or more SAs. These SAs are described in later sections.

A GSA contains all of the SA attributes identified in the previous section, as well some additional attributes pertaining to the group. As shown in Figure 3, the GSA builds on the SA in two distinct ways.

- First, the GSA is a superset of an SA (Figure 3(a)). A GSA has group policy attributes. For example, the kind of signed

credential needed for group membership, whether group members will be given new keys when a member is added (called "backward re-key" below), or whether group members will be given new key when a member is removed from the group ("forward re-key"). A GSA also includes an SA as an attribute of itself.

- Second, the GSA is an aggregation of SAs (Figure 3(b)). A GSA is comprised of multiple SAs, and these SAs may be used for several independent purposes.

```
+---------------+              +-------------------+
|     GSA       |              |        GSA        |
|               |              | +-----+   +-----+ |
|               |              | | SA1 |   | SA2 | |
|    +----+     |              | +-----+   +-----+ |
|    | SA |     |              |      +-----+      |
|    +----+     |              |      | SA3 |      |
|               |              |      +-----+      |
+---------------+              +-------------------+

   (a) superset                  (b) aggregation
```

Figure 3: Relationship of GSA to SA

4.3 Structure of a GSA: Reasoning

Figure 4 shows three categories of SAs that can be aggregated into a GSA.

```
+-------------------------------------------------------------+
|                                                             |
|                   +------------------+                      |
|                   |       GCKS       |                      |
|                   |                  |                      |
|                   |   REG      REG   |                      |
|                   |    /  REKEY \    |                      |
|                   +---/-----|----\---+                      |
|                      /      |     \                        |
|                     /       |      \                       |
|                    /        |       \                      |
|                   /         |        \                     |
|                  /          |         \                    |
|       +----------/------+   |   +------\----------+        |
|       |        REG      |   |   |      REG         |        |
|       |            REKEY-----+----REKEY              |        |
|       |     SENDER      |       |      RECEIVER    |        |
|       |             DATA----------DATA               |        |
```

```
|       +-----------------+        +-----------------+       |
|                                                             |
|                                                             |
+-------------------------------------------------------------+
```

Figure 4: GSA Structure and 3 categories of SAs

The three categories of SAs are:

- Registration SA (REG): A separate unicast SA between the GCKS and each group member, regardless of whether the group member is a sender or a receiver or acting in both roles.

- Re-key SA (REKEY): A single multicast SA between the GCKS and all of the group members.

- Data Security SA (DATA): A multicast SA between each multicast source speaker and the group's receivers. There are as many data SA as there are multicast sources allowed by the group's policy.

Each of these SAs are defined in more detail in the next section.

4.4 Definition of GSA

The three categories of SAs correspond to three different kinds of communications commonly required for group communications. This section describes the SAs depicted in Figure 4 in detail.

- Registration SA (REG):
  An SA is required for (bi-directional) unicast communications between the GCKS and a group member (be it a Sender or Receiver). This SA is established only between the GCKS and a Member. The GCKS entity is charged with access control to the group keys, with policy distribution to members (or prospective members), and with group key dissemination to Sender and Receiver members. This use of a (unicast) SA as a starting point for key management is common in a number of group key management environments [RFC3547, GSAKMP, CCPRRS, RFC2627, BMS,].

  The Registration SA is initiated by the member to pull GSA information from the GCKS. This is how the member requests to join the secure group, or has its GSA keys re-initialized after being disconnected from the group (e.g., when its host computer has been turned off during re-key operations). The GSA information pulled down from the GCKS is related to the other two SAs defined as part of the GSA.

Note that this (unicast) SA is used to protect the other elements of the GSA. As such, the Registration SA is crucial and is inseparable from the other two SAs in the definition of a GSA.

However, the requirement of a registration SA does not imply the need of a registration protocol to create that Registration SA. The registration SA could instead be setup through some manual means, such as distributed on a smart card. Thus, what is important is that a Registration SA exists, and is used to protect the other SAs.

From the perspective of one given GCKS, there are as many unique registration SAs as there are members (Senders and/or Receivers) in the group. This may constitute a scalability concern for some applications. A registration SA may be established on-demand with a short lifetime, whereas re-key and data security SAs are established at least for the life of the sessions that they support.

Conversely the registration SA could be left in place for the duration of the group lifetime, if scalability is not an issue. Such a long term registration SA would be useful for re-synchronization or deregistration purposes.

- Re-key SA (REKEY):
  In some cases, a GCKS needs the ability to "push" new SAs as part of the GSA. These new SAs must be sent to all group members. In other cases, the GCKS needs the ability to quickly revoke access to one or more group members. Both of these needs are satisfied with the Re-key SA.

  This Re-key SA is a unidirectional multicast transmission of key management messages from the GCKS to all group members. As such, this SA is known by the GCKS and by all members of the group.

  This SA is not negotiated, since all the group members must share it. Thus, the GCKS must be the authentic source and act as the sole point of contact for the group members to obtain this SA.

  A rekey SA is not absolutely required to be part of a GSA. For example, the lifetime of some groups may be short enough such that a rekey is not necessary. Conversely, the policy for the group could specify multiple rekey SAs of different types. For example, if the GC and KS are separate entities, the GC may deliver rekey messages that adjust the group membership, and the KS may deliver rekey messages with new DATA SAs.

- Data Security SA (DATA):
  The Data Security SA protects data between member senders and member receivers.

  One or more SAs are required for the multicast transmission of data-messages from the Sender to other group members. This SA is known by the GCKS and by all members of the group.

  Regardless of the number of instances of this third category of SA, this SA is not negotiated. Rather, all group members obtain it from the GCKS. The GCKS itself does not use this category of SA.

  From the perspective of the Receivers, there is at least one data security SA for the member sender (one or more) in the group. If the group has more than one data security SA, the data security

protocol must have a means of differentiating the SAs (e.g., with a SPI).

There are a number of possibilities with respect to the number of data security SAs:

1. Each sender in the group could be assigned a unique data security SA, thereby resulting in each receiver having to maintain as many data security SAs as there are senders in the group. In this case, each sender may be verified using source origin authentication techniques.

2. The entire group deploys a single data security SA for all senders. Receivers would then be able to maintain only one data security SA.

3. A combination of 1. and 2.

4.5 Typical Compositions of a GSA

Depending on the multicast group policy, many compositions of a GSA are possible. For illustrative purposes, this section describes a few possible compositions.

- A group of memory-constrained members may require only a REG SA, and a single DATA SA.
- A "pay-per-session" application, where all of the SA information needed for the session may be distributed over a REG SA. Re-key and re-initialization of DATA SAs may not be necessary, so there is no REKEY SA.
- A subscription group, where keying material is changed as

membership changes. A REG SA is needed to distribute other SAs; a REKEY SA is needed to re-initialize a DATA SA at the time membership changes.

5. Security Services

This section identifies security services for designated interfaces of Figure 2. Distinct security services are assigned to specific interfaces. For example, multicast source authentication, data authentication, and confidentiality occur on the multicast data interface between Senders and Receivers in Figure 2. Authentication and confidentiality services may also be needed between the Key Server and key clients (i.e., the Senders and Receivers of Figure 2), but the services that are needed for multicast key management may be unicast as well as multicast. A security service in the Multicast Security Reference Framework therefore identifies a specific function along one or more Figure 2 interfaces.

This paper does not attempt to analyze the trust relationships, detailed functional requirements, performance requirements, suitable algorithms, and protocol specifications for IP multicast and application-layer multicast security. Instead, that work will occur

as the security services are further defined and realized in algorithms and protocols.

5.1 Multicast Data Confidentiality

This security service handles the encryption of multicast data at the Sender's end and the decryption at the Receiver's end. This security service may also apply the keying material that is provided by Multicast Key Management in accordance with Multicast Policy Management, but it is independent of both.

An important part of the Multicast Data Confidentiality security service is in the identification of and motivation for specific ciphers that should be used for multicast data. Obviously, not all ciphers will be suitable for IP multicast and application-layer multicast traffic. Since this traffic will usually be connectionless UDP flows, stream ciphers may be unsuitable, though hybrid stream/block ciphers may have advantages over some block ciphers.

Regarding application-layer multicast, some consideration is needed to consider the effects of sending encrypted data in a multicast environment lacking admission-control, where practically any application program can join a multicast event independently of its participation in a multicast security protocol. Thus, this security service is also concerned with the effects of multicast

confidentiality services (intended and otherwise) on application programs. Effects to both senders and receivers is considered.

In Figure 2, the Multicast Data Confidentiality security service is placed in Multicast Data Handling Area along the interface between Senders and Receivers. The algorithms and protocols that are realized from work on this security service may be applied to other interfaces and areas of Figure 2 when multicast data confidentiality is needed.

5.2 Multicast Source Authentication and Data Integrity

This security service handles source authentication and integrity verification of multicast data. It includes the transforms to be made both at the Sender's end and at the Receiver's end. It assumes that the appropriate signature and verification keys are provided via Multicast Key Management in accordance with Multicast Policy Management as described below. This is one of the harder areas of multicast security due to the connectionless and real-time requirements of many IP multicast applications. There are classes of application-layer multicast security, however, where offline source and data authentication will suffice. As discussed previously, not all multicast applications require real-time authentication and data-packet integrity. A robust solution to multicast source and data authentication, however, is necessary for a complete solution to multicast security.

In Figure 2, the Multicast Source and Data Authentication security service is placed in Multicast Data Handling Area along the interface between Senders and Receivers. The algorithms and protocols that are produced for this functional area may have applicability to security services in other functional area that use multicast services such as Group Key Management.

5.3 Multicast Group Authentication

This security service provides a limited amount of authenticity of the transmitted data: It only guarantees that the data originated with (or was last modified by) one of the group members. It does not guarantee authenticity of the data in case that other group members are not trusted.

The advantage of group authentication is that it is guaranteed via relatively simple and efficient cryptographic transforms. Therefore, when source authentication is not paramount, group authentication becomes useful. In addition, performing group authentication is useful even when source authentication is later performed: it

provides a simple-to-verify weak integrity check that is useful as a measure against denial-of-service attacks.

The Multicast Group Authentication security service is placed in the Multicast Data Handling Area along the interface between Senders and Receivers.

5.4 Multicast Group Membership Management

This security service describes the functionality of registration of members with the Group Controller, and de-registration of members from the Group Controller. These are security functions, which are independent from IP multicast group "join" and "leave" operations that the member may need to perform as a part of group admission control protocols (i.e., IGMP [RFC3376], MLD [RFC3019]).

Registration includes member authentication, notification and negotiation of security parameters, and logging of information according to the policies of the group controller and the would-be member. (Typically, an out-of-band advertisement of group information would occur before the registration takes place. The registration process will typically be invoked by the would-be member.)

De-registration may occur either at the initiative of the member or at the initiative of the group controller. It would result in logging of the de-registration event by the group controller and an invocation of the appropriate mechanism for terminating the membership of the de-registering member (see Section 5.5).

This security service also describes the functionality of the communication related to group membership among different GCKS servers in a distributed group design.

In Figure 2, the Multicast Group Membership security service is placed in the Group Key Management Area and has interfaces to Senders and Receivers.

5.5 Multicast Key Management

This security service describes the functionality of distributing and updating the cryptographic keying material throughout the life of the group. Components of this security service may include:

- GCKS to Client (Sender or Receiver) notification regarding current keying material (e.g. group encryption and authentication keys, auxiliary keys used for group management, keys for source authentication, etc).

- Updating of current keying material, depending on circumstances and policies.
- Termination of groups in a secure manner, including the multicast group itself and the associated keying material.

Among the responsibilities of this security service is the secure management of keys between Key Servers and Clients, the addressing issues for the multicast distribution of keying material, and the scalability or other performance requirements for multicast key management [RFC2627, BMS]. Key Servers and Clients may take advantage of a common Public Key Infrastructure (PKI) for increased scalability of authentication and authorization.

To allow for an interoperable and secure IP multicast security protocol, this security service may need to specify host abstractions such as a group security association database (GSAD) and a group security policy database (GSPD) for IP multicast security. The degree of overlap between IP multicast and application-layer multicast key management needs to be considered. Thus, this security service takes into account the key management requirements for IP multicast, the key management requirements for application-layer multicast, and to what degree specific realizations of a Multicast Key Management security service can satisfy both. ISAKMP, moreover, has been designed to be extensible to multicast key management for both IP multicast and application-layer multicast security [RFC2408]. Thus, multicast key management protocols may use the existing ISAKMP standard's Phase 1 and Phase 2 protocols, possibly with needed extensions (such as GDOI [RFC3547] or application-layer multicast security).

This security service also describes the functionality of the communication related to key management among different GCKS servers in a distributed group design.

Multicast Key Management appears in both the centralized and distributed designs as shown in Figure 2 and is placed in the Group Key Management Area.

5.6 Multicast Policy Management

This security service handles all matters related to multicast group policy including membership policy and multicast key management policy. Indeed, one of the first tasks in further defining this security service is identifying the different areas of multicast policy. Multicast Policy Management includes the design of the policy server for multicast security, the particular policy definitions that

will be used for IP multicast and application-layer multicast security, and the communication protocols between the Policy Server and the Key Server. This security service may be realized using a standard policy infrastructure such as a Policy Decision Point (PDP) and Policy Enforcement Point (PEP) architecture [RFC2748]. Thus, it may not be necessary to re-invent a separate architecture for multicast security policy. At minimum, however, this security service will be realized in a set of policy definitions, such as multicast security conditions and actions.

The Multicast Policy Management security service describes the functionality of the communication between an instance of a GCKS to an instance the Policy Server. The information transmitted may include policies concerning groups, memberships, keying material definition and their permissible uses, and other information. This security service also describes communication between and among Policy Servers. Group members are not expected to directly participate in this security service. However, this option is not ruled out.

6. Security Considerations

This document describes an architectural framework for protecting multicast and group traffic with cryptographic protocols. Three functional areas are identified within the framework. Each functional area has unique security considerations, and these are discussed below.

This architectural framework is end-to-end, and does not rely upon the network that connects group controllers and group members. It also does not attempt to resolve security issues in the unicast or multicast routing infrastructures, or in multicast admission control protocols. As such, denial of service, message deletion, and other active attacks against the unicast or multicast routing infrastructures are not addressed by this framework. Section 1.1 describes the relationship of the network infrastructure to the multicast group security architecture.

6.1 Multicast Data Handling

Cryptographic protocols protecting multicast data are responsible for providing confidentiality and group authentication. They should also be able to provide source authentication to uniquely identify senders to the group. Replay protection of multicast data is also desirable, but may not always be possible. This is due to the complexity of

maintaining replay protection state for multiple senders. Section 3.1

elaborates on the security requirements for this area.

6.2 Group Key Management

Group key management protocols provide cryptographic keys and policy to group members. They are responsible for authenticating and authorizing group members before revealing those keys, and for providing confidentiality and authentication of those keys during transit. They are also responsible for providing a means for rekeying the group, in the case that the policy specifies a lifetime for the keys. They also are responsible for revocation of group membership, once one or more group members have had their authorization to be a group member revoked. Section 3.2 describes the security requirements of this area in more detail.

6.3 Multicast Security Policies

Cryptographic protocols providing multicast security policies are responsible for distributing that policy such that the integrity of the policy is maintained. If the policy itself is confidential, they also are responsible for authenticating group controllers and group members, and providing confidentiality of the policy during transit.

7. Intellectual Property Rights Statement

The IETF takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on the IETF's procedures with respect to rights in standards-track and standards-related documentation can be found in BCP-11. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementors or users of this specification can be obtained from the IETF Secretariat.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights which may cover technology that may be required to practice this standard. Please address the information to the IETF Executive Director.

8. Acknowledgments

Much of the text in this document was derived from two research papers. The framework for this document came from a paper co-authored by Thomas Hardjono, Ran Canetti, Mark Baugher, and Pete Dinsmore. Description of the GSA came from a document co-authored by Hugh Harney, Mark Baugher, and Thomas Hardjono. George Gross suggested a

number of improvements that were included in later versions of this document.

9. References

9.1 Normative References

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

[RFC2408] D. Maughan, M. Shertler, M. Schneider, J. Turner, Internet Security Association and Key Management Protocol, November 1998.

9.2 Informative References

[ACLNM] J. Arkko, et. al., MIKEY: Multimedia Internet KEYing, draft-ietf-msec-mikey-08.txt, December, 2003. Work in Progress.

[BCCR] M. Baugher, R. Canetti, P. Cheng, P. Rohatgi, MESP: A Multicast Framework for the IPsec ESP, draft-ietf-msec-mesp-01.txt. October 2002. Work in Progress.

[BCDL] M. Baugher, R. Canetti, L. Dondeti, F. Lindholm, Group Key Management Architecture, draft-ietf-msec-gkmarch-06.txt. September 08, 2003. Work in Progress.

[BMS] D. Balenson, D. McGrew, A. Sherman, Key Management for Large Dynamic Groups: One-Way Function Trees and Amortized Initialization, http://www.securemulticast.org/draft-balenson-groupkeymgmt-oft-00.txt, February 1999, Work in Progress.

[CCPRRS] Canetti, R., Cheng P. C., Pendarakis D., Rao, J., Rohatgi P., Saha D., "An IPSec-based Host Architecture for Secure Internet Multicast", http://www.isoc.org/isoc/conferences/ndss/2000/proceedings/028.pdf, NDSS 2000.

[Din] Dinsmore, P., Balenson, D., Heyman, M., Kruus, P., Scace, C., and Sherman, A., "Policy-Based Security Management for Large Dynamic Groups: An Overview of the DCCM Project," DARPA Information Survivability Conference and Exposition, http://download.nai.com/products/media/nai/doc/discex-110199.doc.

[GSAKMP] H. Harney, et. al., GSAKMP. draft-ietf-msec-gsakmp-sec-04.txt. October 2003. Work in Progress.

[Har1] Harney, H., and Muckenhirn, C., "Group Key Management Protocol (GKMP) Specification," RFC 2093, July 1997.

[Har2] Harney, H., and Muckenhirn, C., "Group Key Management Protocol (GKMP) Architecture," RFC 2094, July 1997.

[McD] McDaniel, P., Honeyman, P., and Prakash, A., "Antigone: A Flexible Framework for Secure Group Communication," Proceedings of the Eight USENIX Security Symposium, pp 99-113, August, 1999.

[PCW] A. Perrig, R. Canetti, B. Whillock, TESLA: Multicast Source Authentication Transform Specification. draft-ietf-msec-tesla-spec-00.txt. IETF, October 2002. Work in Progress.

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

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

[RFC2406bis] S. Kent, IP Encapsulating Security Payload (ESP), draft-ietf-ipsec-esp-v3-04.txt, March 2003. Work In Progress.

[RFC2409] D. Harkins, D. Carrel, The Internet Key Exchange (IKE), November, 1998.

[RFC2627] D. M. Wallner, E. Harder, R. C. Agee, Key Management for Multicast: Issues and Architectures, RFC 2627, September 1998.

[RFC2663] P. Srisuresh, M. Holdrege, IP Network Address Translator (NAT) Terminology and Considerations, RFC 2663, August 1999.

[RFC2748] D. Durham, et. al., The COPS (Common Open Policy Service) Protocol, RFC 2748, January, 2000.

[RFC3019] B. Haberman, Worzella, R., IP Version 6 Management Information Base for The Multicast Listener Discovery Protocol, RFC 3019, January, 2001.

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

[RFC3453] M. Luby, et. al., The Use of Forward Error Correction (FEC) in Reliable Multicast, RFC 3453, December 2002.

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

[STW] M. Steiner, Tsudik, G., Waidner, M., CLIQUES: A New Approach to Group key Agreement, IEEE ICDCS'98 , May 1998.

Authors Addresses

Thomas Hardjono
VeriSign
487 E. Middlefield Rd.
Mountain View, CA 94043, USA

Phone:(650) 426-3204
EMail: thardjono@verisign.com

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

Phone: (408) 526-4796
EMail: bew@cisco.com

Full Copyright Statement

Copyright (C) The Internet Society (2003). All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING

BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Acknowledgement

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