Internet Engineering Task Force
INTERNET-DRAFT

Thomas Hardjono
Brad Cain
Indermohan Monga
Nortel Networks
November 1998
Expires July 1999

Intra-Domain Group Key Management Protocol

<draft-ietf-ipsec-intragkm-00.txt>

Status of this Memo

Abstract

This document describes a protocol for intra-domain group key management for IP multicast security, based on the framework of [HCD98]. In order to support multicast groups, the domain is divided into a number of administratively-scoped "areas". A host-member of a multicast group is defined to reside within one (and only one) of these areas. The purpose of placing host-members in areas is to achieve flexible and efficient key management, particularly in the face of the problem of changes (joining, leaving, ejections) in the membership of a multicast group. A separate administratively-scoped area control-group is defined for each (data) multicast group, for the express purpose of key management and other control-message delivery.

Table of Contents

1. Introduction

This document describes a protocol for intra-domain group key management for IP multicast security, based on the framework of [HCD98]. In order to support multicast groups, the domain is divided into a number of administratively-scoped "areas". A host-member of a multicast group is defined to reside within one (and only one) of these areas. The purpose of placing host-members in areas is to achieve flexible and efficient key management, particularly in the face of the problem of changes (joining, leaving, ejections) in the membership of a multicast group.

A separate administratively-scoped area control-group is defined for each (data) multicast group, for the express purpose of key management and other control-message delivery. A unique cryptographic key is associated with every (multicast group, control-group) pair in a given area. The control-groups are used for key management, following the re-keying behavior described in

[WGL98] and extending it over several key distributor entities.

2. Background

The current document follows from the group key management framework proposal of [HCD98]. The framework of [HCD98] introduces two planes corresponding to the network entities and functions pertaining to multicasting ("network infrastructure plane") and to security ("key management plane"). Within the key management plane two hierarchies (levels) of regions are introduced, namely one "trunk region" (inter-region) and one or more "leaf regions" (intra-region). These regions are defined to have unique group keys and are open to differing (inter-region or intra-region) group key management protocols.

The current work introduces an "intra-region" (leaf-region) group key management protocol, where the term "domain" in the current work is taken to mean a single leaf region of [HCD98]. Although in practice one leaf region of [HCD98] can consist on one or more of our current "domains", for simplicity we assume that one leaf region corresponds to one current domain.

The definition of a "domain" (leaf) here is viewed more from an administrative perspective, in which the "domain" is administered and controlled by one body. This single-administration perspective is assumed both for multicasting and for key management.

The group key management behavior in the current document is inspired by the work of [WGL98] which is based on a centralized server. The current work extends it to cover multiple entities in a distributed fashion.

The current document addresses group key management for multicast security. The issue of how a cryptographic key is applied to data in a multicast group is not addressed, although the current document points to IPsec (ESP and AH) [KA98a, KA98b, KA98c] as a foremost candidate, depending on the multicast application type. Although in the document a key is used to "encipher" the multicast data to control access by group members, the intent is clear that authentication-only multicast applications may also employ the current design.

The current document seeks to cover both the one-to-many and many-to-many multicast application types. Hence, the protocol has been described is the broadest way possible, without affecting the security of key management in general.

3. Architecture

The current work aims to manage multicast group keys based on well-defined domains. It also distinguishes between multicast groups for the purpose of payload delivery and for the purpose of key management.

The current document is concerned with the correct and secure delivery of keys to members of a multicast group. It does not prescribe how a key is to be used on the data being transmitted in the multicast group. The reader is directed to methods such as IPsec ESP [KA98b] for concrete possibilities.

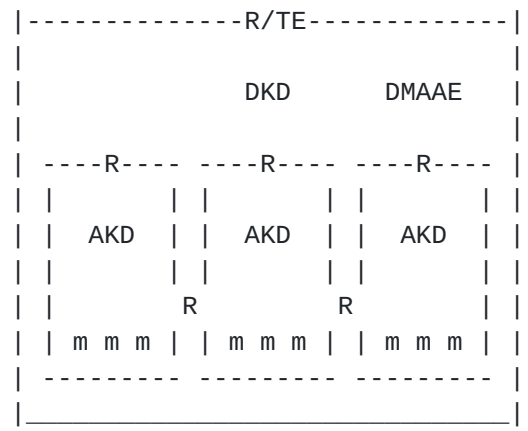

Figure 1: Intra-Domain Group Key Management Elements

3.1 Domains, Areas and Key Distributors

At the domain-level, a Domain Key Distributor (DKD) entity is defined for the domain for the purpose of key management.

In order to support multicast groups, the domain is divided into a number of administratively-scoped "areas" [Mey98]. A host-member of a multicast group is defined to reside within one (and only one) of these areas. The purpose of placing host-members in areas is to achieve flexible and efficient key management, particularly in the face of the problem of changes (joins and leaves) in the membership of a multicast group.

At the area level, an Area Key Distributor (AKD) entity is defined for each area for the purpose of key management.

Depending on the address allocation approach (see Section 3.4), each area may be associated with one Area Multicast Address Allocation Entity (AMAAE), such the MAAS of [HTE98], from which the Area Key Distributor (AKD) of that area obtains area-wide multicast addresses. In addition, at the domain-level, a Domain Multicast Address Allocation Entity (DMAAE) must exist to cater for the domain.

Within the domain, all Key Distributors (the DKD and AKDs) are members of the domain-wide administratively-scoped multicast group, called the "All-KD-group", which does not extend beyond the domain and whose membership consists only of Key Distributors.

The Domain Key Distributor (DKD) communicates to Area Key Distributors (AKD) either through secure one-to-one (unicast) communications or through the All-KD-group. The All-KD-group is independent of other multicast groups and it exists even when there are no host-members of any multicast group in the domain.

The Area Key Distributor (AKD) communicates to host-members residing in its area either through secure one-to-one (unicast) communications or through a special (ie. control) multicast group whose scope is limited to that area.

Should a multicast group originate from outside the domain and should its traffic be enciphered under a foreign key, then Translating Entity(s) (TE), such as a border-router(s), must be specified in the domain. In such a case, the Domain Key Distributor (DKD) is assumed to have a copy of the foreign key through other methods (unspecified). The DKD will then supply the Translating Entity(s) with a copy of the foreign key and a copy of a new multicast key to be used on the traffic in the domain.

3.2 Trust Relationships

The trust relationship in the current work revolves around the Key Distributors and does not extend beyond the domain. All Key Distributors (DKD and AKDs) are configured and maintained by the human administration in the domain. They must be implemented using the most secure technology available, since they represent the best point-of-attack.

All entities trust the Domain Key Distributor (DKD) as the primary source of authentic parameters. The DKD can in fact also take-on the role of a certification authority when the need arises. The public-key of the DKD is well-known to (and/or is configured within) each host and within the Area Key Distributors (AKDs).

A host residing within an area trusts the Area Key Distributor (AKD) in that area.

3.3 Multicast Groups for Data and Control

The current work employs administratively-scoped multicast groups for the purpose of key management.

To distinguish these administratively-scoped multicast groups for control (ie. key management) from the multicast group for data, the latter will be referred to as "data multicast groups", "data-groups" or simply "multicast groups". A control-related group will be referred to as "control-multicast group" or simply "control-group".

A "control-group" is an administratively-scoped multicast group which is area-wide. It is initiated/owned by the Area Key Distributor (AKD) of an area. The purpose of an area control-group is for key management relating to an associated data-multicast group.

An area control-group associated with a data-multicast group exists so long as there are members of the corresponding data-multicast group in the area. Once a data-multicast group ceases to have any members in an area, the Area Key Distributor (AKD) of that area may terminate that corresponding area control-group.

A special control-group is the All-KD-group. This is an administratively-scoped multicast group which is domain-wide and consists only of the Domain Key Distributor (DKD) and Area Key Distributors (AKD). It has a fixed address and is initiated/owned by the Domain Key Distributor (DKD). There is only one All-KD-group in a domain, and it is a permanent group, independent of whether any data multicast group members exists in the domain. Unless specifically mentioned, in the remainder of this document all control-groups are area control-groups.

Note that once a host (in an area within the domain) becomes a member of a multicast group, it also must become a member of one of the area control-groups of the area within which that host resides. This allows the Area Key Distributor (AKD) to communicate with the host-member through the area control-group.

From the perspective of an Area Key Distributor (AKD) of an area, for a multicast group having a host-member in its area, the Key Distributor (AKD) must assign that host-member to one of the area control-groups in that area.

3.4 Keys: Multicast Groups and Control-Multicast Groups

A multicast group is associated with a domain-wide Multicast-Key (MKey). The current work assumes that cryptographic keys are used for the encipherment of the multicast traffic as a method to provide receiver access-control, where only valid members of the multicast group is provided with a copy of the cryptographic key. This is true for data multicast groups and area control-groups.

For each multicast group having a member in the domain, a unique Multicast-Key (MKey) is assigned by the Domain Key Distributor (DKD) for that multicast group.

A multicast group having a member in an area in the domain is associated with one control-group in the area by the Area Key Distributor (AKD) of that area. All traffic within an area control-group is enciphered in such a way that only the AKD of that area and the intended receivers of the traffic will be able to decipher the traffic. The cryptographic key associated with an area control-group is referred to generally as the Area-Group-Key (AreaGroupKey). An Area-Group-Key is selected by the Area Key Distributor (AKD). The Area-Group-Key (AreaGroupKey) is unique for each (multicast group, control-group) pair.

For the special All-KD-group, an All-KD-Key (AllKDKey) is assigned by the Domain Key Distributor (DKD) for the All-KD-group.

Here, it is assumed (initially) that all payload related to a multicast group travelling within a domain is encrypted using the Multicast-Key (MKey). Should the sender of the multicast group be located outside the domain, then a "Translating-Entity" (TE), such as the border-router of the domain, must be employed to decrypt the entering traffic (using some inter-domain cryptographic key) and to re-encrypt it using the Multicast-Key (MKey) assigned in the domain to that multicast group. Similarly, the Translating-Entity must "translate" multicast group traffic (sent from a group member in the current domain) when the traffic leaves the domain.

The "boot-strapping" process of each multicast group and control-group relies on the establishment of a Security Association (SA) and a shared private-key between a (candidate) member of the group with the Key Distributor (DKD or AKDs) that controls the group. It is through this one-to-one secure channel that the parameters for the groups are then given to host-members by the Area Key Distributor in the case of the multicast group and area control groups, or to the Area Key Distributors (AKDs) by the Domain Key Distributor (DKD) in the case of the All-KD-group.

3.5 Control-Multicast Groups: Address Allocation

Three possible approaches are available with regards to the use of area control-groups (corresponding to a given multicast group) for key management by the Area Key Distributor (AKD):

(a) One control-group per area per multicast group:

For each multicast group, having members in an area, a separate control-group is created within the area.

Each separate area control-group is associated with a different Area-Group-Key.

One disadvantage of this approach is the potential lack of multicast addresses within the area. Another disadvantage is the waste of resource related to area-wide multicasting if the area only has very few members of the corresponding multicast group. This approach requires the presence of an Area Multicast Address Allocation Entity (AMAAE) in each area.

(b) One control-group per area for all multicast groups:

In this approach, for each multicast group, having members in an area, only one control-group is created within the area. Hence, the area control-group is shared among members of different multicast groups.

Although there is only one (shared) area control-group, a separate Area-Group-Key is used for each data multicast group. When the AKD wishes to communicate with members of a particular multicast group residing in its area, the AKD will encipher the communications using the appropriate Area-Group-Key. Other non-intended recipients will also receive the enciphered packets, but will drop them since they will not be able to decipher them.

The advantage of this approach is that there is only one control-group which can be long-lived and have a fixed address. Having the fixed address obviates the Area Multicast Address Allocation Entity (AMAAE), thereby simplifying the entire design.

The main disadvantage of this approach is that bandwidth within the area is wasted when the AKD is performing key management communications with only a small subset of group members residing in the area, since all other unconcerned members are receiving the (enciphered) packets and dropping them. Another related disadvantage is increased opportunity for cryptanalysis of enciphered packets of control-groups, since unconcerned members are receiving these packets and may cryptanalyze them.

(c) One control-group per area for several multicast groups:

This approach attempts to bring together the advantages of the previous two. For a fixed number of multicast groups, having members in an area, a single control-group is created within the area.

Thus, within a given area a set of N multicast addresses for N control-groups can be selected and fixed. Each multicast group having (one or more members in an area) is then mapped to one of the N control-groups in that area (eg. by hashing the multicast group address).

In terms of key management, each (multicast group, control-group) pair will be associated with a unique Area-Group-Key (AreaGroupKey).

Thus, for example, a host who is a member of two multicast groups MG1 and MG2 may find that in its area both MG1 and MG2 are mapped into one control-group CG1, with two Area-Group-Keys AGK1 and AGK2 corresponding to the two multicast groups. Hence, for the control-group CG1 the host must maintain the unique triplets (MG1, CG1, AGK1) and (MG2, CG1, AGK2). The host must be able to distinguish control-group packets in CG1 corresponding to the two multicast groups, in order for it to apply the matching keys. Tagging methods within control-packets may be employed to achieve this effect, saving the host the effort of trying the keys.

In this manner, the design is simplified by obviating the Area Multicast Address Allocation Entity (AMAAE) for each area, and the problem of unintended members receiving and dropping (enciphered) messages is also somewhat reduced.

The current work will employ the third approach due to its simplicity. We specify that an Area Key Distributor (AKD) maintains a mapping between a multicast group and its corresponding control-group in the area. How this mapping is established is implementation-specific, and thus outside the scope of the document. Furthermore, we assume that each control-group packet carries sufficient identification information relating to the multicast group to which it corresponds, thereby allowing non-intended receivers of the packets in the shared control-group to drop the packets without attempting to decrypt it.

3.6 Group Security Associations

The IPsec security architecture [KA98a] defines the concept of a Security Association (SA) between two communicating parties. An SA is a simplex connection that affords security services to the traffic carried by it. An SA is uniquely identified by the triple consisting of the Security Parameter Index (SPI), an IP Destination Address and a security protocol identifier. Thus, for a two way communications, two Security Associations must be negotiated and established.

The current work recognizes that for the many-to-many multicast applications the basic IPsec Security Association as a simplex connection does not suffice. Hence, it uses the notion of a Multicast Group Security Association (GSA) derived from the simplex Security Association. Note that the concept of a GSA for multicast has previously been describe, albeit briefly, in the IPsec security architecture document [KA98a] and other related documents.

In the current document we assume that a Group Security Association (GSA) attributes is not negotiated between the communicating parties, but rather selected by one party. The entity that selects the GSA depends on the whether it is a multicast group or a control-group. All members of the group would then use the one same Group Security Parameter Index (GSPI) related to the GSA. Similarly, when a re-keying occurs, a new Group Security Parameter Index (GSPI) must selected for the GSA and a new key must be generated by one entity and delivered to the group members.

The notion of a Group Security Association (GSA) selected by one entity departs from the existing IPsec definition and has implications on the ability of hosts to join multicast groups. Recall that in the two-party communication scenario, each party negotiates the Security Association (SA) depending on their cryptographic capability (eg. cryptographic algorithms available). In the case of a Group Security Association (GSA) selected by one entity, the required capability (eg. minimal algorithms) demanded of a potential member must be announced through other methods, such as through the multicast session description protocol or other protocols. In this way, a multicast group initiator or owner can specify what cryptographic algorithm(s) can be used in the multicast group. This approach is in-line with the one-to-many multicast applications (eg. pay per view service owners) and is deemed reasonable within the many-to-many multicast applications.

3.7 Secure Channels

The general term "secure channel" is used in the remainder of the current document to mean communications between one sender and one receiver (unicast), with authenticity and confidentiality. Secure channels here will be based on IPsec (AH and/or ESP) [KA98a]. The term implies the existence of a Secure Association (SA) and a private-key shared between the sender and receiver before the two begin communicating securely. The IKE protocol [HC98] can be used to establish the Security Association and the shared private-key.

Independent of the Group Security Association (GSA) for the multicast group, each host-member is assumed to have establish a Security Association (SA) and a shared private-key with the Area Key Distributor (AKD) of the area within which that host resides before the host joins any groups. Similarly, each Area Key Distributor (AKD) is assumed to have establish a Security Association (SA) and a shared private-key with the Domain Key Distributor (DKD) before the AKD serves any multicast groups.

A "secure channel" between one sender and one receiver implies that the identity of the one is known to the other. Hence, in communicating via a secure channel with a Key Distributor (AKD or DKD) a host-member is by definition identified and authenticated by the Key Distributor, and vice versa.

3.8 Periodic Re-Keying

It is commonly accepted that the longer a cryptographic key is being employed, the higher the chances of that key being successfully cryptanalyzed by an attacker (who is assumed to have collected ciphertext of messages encrypted using the key). This is particularly true for keys of symmetric cryptosystems.

The current document recognizes the importance of periodic re-keying and attempts to provide a workable solution in the face of the issue of re-keying due to a new host-member joining (backward confidentiality) and the issue of an existing member leaving or being ejected (forward confidentiality).

The approach of re-keying only when the group membership changes suffers from the possibility that the membership does not in fact change over long periods, and thus opening the possibility of cryptanalysis of the multicast key.

Hence, the current design adopts the underlying philosophy that periodic re-keying is necessary (even if the membership of the multicast group does not change), independent of whether or not

immediate re-keying is performed when a host joins/leaves the multicast group. In this way, the design provides flexibility for the implementor to be "strict" (immediate re-key at each membership change) or to be "loose" (wait until next periodic re-key) with regards to multicast key re-keying.

In the following discussions on the group key management protocols, the current work will observe the strict re-keying policy (ie. immediate re-key at each membership change) since it represents a more complex case. The loose re-keying can be established by removing some steps from the protocols and executing other steps only when the designated periodic re-keying occurs. Periodic re-keying in the multicast group will be determined by the Domain Key Distributor (DKD) and implemented with the aid of the Area Key Distributors (AKDs). Periodic re-keying in a control-group (in an area) associated with a multicast group will be determined by the Area Key Distributor (AKD) of that area.

From the perspective of multicast reliability, the approach of using periodic re-keying allows each Key Distributor (AKD and DKD) to prepare for the re-keying, hence providing them with a window of opportunity to obtain the next key. Having this window of opportunity provides a context within which reliability mechanisms for key delivery can be established, either through existing reliable multicast protocols or through mechanisms specific to key management. In either case, the current document recognizes that reliability is paramount to group key management if multicast security is to be achieved.

3.9 Arrangement of Keys in the Domain

The current protocol aims at delivering a multicast key, in the form of a private-key (symmetric cryptography), to members of a multicast group or a control-group. The fact that a host holds a copy of the multicast key is taken to mean that the host has previously been correctly identified by its Area Key Distributor (AKD) and that it has established a Security Association with its AKD. The private-key used in a multicast group or a control-group affords confidentiality and "group authentication" in the sense that the source of any information enciphered under the key is a valid member of the group. Note, that this level of authentication (group authentication) is implicit and does not provide irrefutable proof of the singular identity of the sender.

The current document recognizes the benefits of a public key certification infrastructure and is open to such an infrastructure being deployed, with each entity being assigned a public key.

However, in order to render the protocol immediately deployable in the near future, we assume that public keys are assigned only to the Key Distributors (DKD and AKDs) and the Domain Multicast Address Allocation Entity (DMAAE) to allow them to digitally-sign information that is to be sent through the multicast group or the control-groups. These public keys are valid only within the domain, and may not be recognized outside the domain (unless a certification infrastructure is employed).

3.9.1 Public Keys

The current protocol assumes that all Key Distributors (DKD and AKDs) are assigned public-keys (asymmetric cryptography) in order for these Key Distributors to digitally-sign certain information in such a way that it is verifiable by all hosts in the domain.

A host-member residing in area is assumed to have a copy of the public-key of its Area Key Distributor (AKD) and the public-key of the Domain Key Distributor (DKD).

An Area Key Distributor (AKD) is assumed to have a copy of the public-key of the Domain Key Distributor (DKD). An Area Key Distributor (AKD) may obtain the public-keys of other Area Key Distributors from the Domain Key Distributor (DKD), with the DKD acting as a domain-wide certification authority.

Al the very least, the public key of the Domain Key Distributor (DKD) must be advertised in a tamper-proof manner (eg. printed or manually configured) to allow it to be used to vouch for the public keys of the Area Key Distributors (AKDs).

3.9.2 Shared Private-Keys

Three types of group-oriented (ie. shared by a group) private-keys (symmetric cryptography) are used:

- Multicast-Key (MKey): this is the private-key associated with a multicast group that is used by all the group members in the domain to encrypt/decrypt the multicast traffic in the multicast group. This key is generated by the Domain Key Distributor (DKD) of the domain.

  This key is delivered securely to each Area Key Distributor (AKD), who will in turn deliver the key securely to each group member in their area.

- Area-Group-Key (AreaGroupKey): this is the private-key associated with the (multicast group, control-group) pair, and used to encipher the communications in the control-group. An Area-Group-Key is generated by the Area Key Distributor (AKD) of that area and delivered to each member through a secure-channel. An Area-Group-Key is known only to the AKD of an area and the members (of the corresponding multicast group) residing in that area.

- All-KD-Key (AllKDKey): this is the private-key associated with the special All-KD-group. All the Area Key Distributors (AKDs) and the Domain Key Distributor (DKD) hold a copy of the All-KD-Key. This key is generated by the Domain Key Distributor (DKD) and delivered to each AKD through a secure-channel. This key is used to encipher the communications within the All-KD-group.

Two types of pair-oriented private-key are used in the current work:

- Member-Private-Key (MbrPKey): Each host-member in an area pair-wise shares a Security Association (SA) and a Member-Private-Key (MbrPKey) with the Area Key Distributor (AKD) of that area. The Security Association (SA) and the Member-Private-Key (MbrPKey) are long-term and must be established before the host-member joins (or initiates) any multicast groups and is given a copy of that group's Multicast-Key (MKey). There is only one SA and one MbrPKey shared between the host-member and the Area Key Distributor (AKD), independent of the number of multicast groups to which that host-member belongs.

- AKD-Private-Key (AKDPKey): Each Area Key Distributor (AKD) of an area pair-wise shares a Security Association (SA) and a AKD-Private-Key with the Domain Key Distributor (DKD). The Security Association and the AKD-Private-Key (AKDPKey) are long-term and must be established before any multicast group exists in the domain.

In summary, the private-key arrangement from the point of view of entities is as follows.

Hosts:

A host-member of a multicast group residing in an area holds a copy of the Multicast-Key (MKey) and a copy of the Area-Group-Key (AreaGroupKey) corresponding to the (multicast group, control-group) pair. In addition, the host-member also holds its own Member Private-Key (MbrPKey) independent of any multicast groups.

Area Key Distributors (AKD):
For each multicast group having a member in an area, the Area Key Distributor (AKD) of the area holds a copy of the Multicast-Key (MKey) of the multicast group and holds a unique Area-Group-Key (AreaGroupKey) corresponding to each (multicast group, control-group) pair.

In addition, an AKD also holds a copy of the current All-KD-Key (AllKDKey), its own AKD-Private-Key (AKDPKey) and a copy of the Member Private-Key (MbrPKey) of each member residing in its area. These (the AllKDKey, AKDPKey and MbrPKeys) are independent of any multicast groups to which a resident host-member belongs.

Domain Key Distributor (DKD):
The Domain Key Distributor (DKD) of a given domain holds the Multicast-Key (MKey) for each multicast group, a copy of the current All-KD-Key (AllKDKey), and a copy of the AKD-Private-Key (AKDPKey) of each Area Key Distributor (AKD) in the domain.

	Multicast access purposes: Multicast Key (MKey)	
	Control purposes:	
	Pair-wise Shared	Group-wise shared
DKD with AKD	Key: AKD-Private-Key - Long-term - Independent of groups	Key: All-KD-Key - Medium-term - Independent of groups
AKD with Hosts	Key: Member-Private-Key - Long-term - Independent of groups	Key: Area-Group-Key - Medium-term - N per area

Table 1: Key arrangement

Note that the Domain Key Distributor (DKD) does not hold copies of the Member-Private-Keys (MbrPKey). This is in contrast to the approach in [WGL98] in which a central server holds the private-keys of all members in the multicast group. If a host is in need of communicating directly through a secure channel to the Domain Key Distributor (DKD) or any other entity, then the host must establish a Security Association and a shared private-key with the DKD or entity.

Although currently not prescribed, depending on the reliability mechanism to be employed, the Domain Key Distributor (DKD) may hold copies of the Area-Group-Key (AreaGroupKey) within each area in the domain. However, the intent is clear that the Domain Key Distributor (DKD) is not to replace any Area Key Distributor (AKD).

Each key is assumed to be associated with a Key Identifier which uniquely identifies the cryptographic key is question.

4. Creation of New Multicast Groups

Two possible scenarios with respect to new multicast groups exist. In the first case, the new multicast group is initiated from the current domain. In the second case, the multicast group was initiated from outside the domain and has existed before a host in the current domain joins it.

4.1 Initiation of New Internal-Origin Groups

When a host ("Initiator") in the current domain wishes to commence a new multicast group, it must first initiate the creation of the multicast group via the underlying multicast routing protocol and some membership protocol (eg. IGMP).

If it has not already done so, the initiator host must establish a Security Association (SA) and a shared Member Private-Key (MbrPKey) with its Area Key Distributor (AKD).

The commencement of a new multicast group from the perspective of group key management is described as follows, consisting two inseparable parts. The first part is the generation and distribution of the multicast-key, while the second part is the generation and distribution of the Area-Group-Key.

Protocol-I: Generation and distribution of the multicast key

Step N1: The initiator in an area within the current domain creates a new domain-wide multicast group (method unspecified) with the aid of the Domain Multicast Address Allocation Entity (DMAAE) at the domain level. The DMAAE returns to the initiator the following parameters, digitally signed by the DMAAE:

- a multicast group address
- a multicast group identity
- the identity of the initiator (as group owner)

Step N2: The initiator selects the Multicast Group Security Association (MGSA) attributes (without the GSPI). The initiator then authentically notifies its Area Key Distributor (AKD) about the new multicast group and requests a new multicast key for the new multicast group. The message is sent through a secure channel and contains the signed parameters from the DMAAE, the MGSA and an Access Control List (ACL):

- the multicast group address
- the multicast group identity
- the identity of the initiator
- the Multicast Group Security Association (MGSA)
- the time-period for re-keying cycle
- an Access Control List (ACL) generated by the initiator

Step N3: The Area Key Distributor (AKD) of the initiator receives the request from the initiator, notifies the Domain Key Distributor (DKD) about the new multicast group and passes the request message to the DKD through a secure channel.

Step N4: The Domain Key Distributor (DKD) receives the request and performs the following steps:

Step N4.1: The Domain Key Distributor (DKD) verifies the digital signature of the Domain Multicast Address Allocation Entity (DMAAE).

Step N4.2: The Domain Key Distributor (DKD) generates:

- a Group Security Parameter Index (GSPI) for the MGSA
- a Multicast-Key (MKey)
- a multicast key identifier MKeyID

based on the MGSA selected by the initiator.

Step N4.3: The Domain Key Distributor (DKD) digitally-signs the multicast group parameters:

- the multicast group address
- the multicast group identity
- the identity of the initiator
- the time-period for re-keying cycle
- the Access Control List (ACL)
- the Multicast Group Security Association (MGSA)
- the Multicast-Key (MKey)
- the multicast key identifier MKeyID
- a timestamp

Step N4.4: The Domain Key Distributor (DKD) securely delivers the signed multicast group parameters to each Area Key Distributor (AKD), either through the All-KD-group (encrypted under the All-KD-Key) or through a one-to-one secure channel to each Area Key Distributor (AKD). This message also serves as an acknowledgment to the Area Key Distributor (AKD) of the initiator.

The process of the creation of the All-KD-group is similar to Protocol-I, with the exception that the multicast address is fixed and the DKD selects the Group Security Association (GSA) for the All-KD-group. The DKD also generates the All-KD-Key (AllKDKey) and the All-KD-Key identifier AllKDKeyID for the multicast group, based on the MGSA selected by the DKD.

Protocol-II Generation and distribution of the area key

Step N5: Upon receiving the signed multicast group parameters from the DKD, the Area Key Distributor (AKD) of the initiator performs the following steps:

Step N5.1: The Area Key Distributor (AKD) maps the multicast group address to one of the area control-group addresses. The AKD maintains the following information for the given multicast group:
- an area control-group address
- an area control-group identity
- the identity of the AKD (as group owner)

Step N5.2: The Area Key Distributor (AKD) selects the Area Group Security Association (AGSA) attributes and generates:
- a Group Security Parameter Index (GSPI) for the AGSA
- an Area-Group-Key (AreaGroupKey)
- an area key identifier AkeyID

based on the AGSA selected by the AKD.

Step N5.3: The Area Key Distributor (AKD) digitally-signs the area control-group parameters:
- the multicast group address
- the multicast group identity
- the area control-group address
- the area control-group identity
- the identity of the AKD
- the time-period for re-keying cycle
- the Area Group Security Association (AGSA)
- the Area-Group-Key (AreaGroupKey)
- the area key identifier AKeyID

- a timestamp

Step N6: The Area Key Distributor (AKD) of the initiator returns to the initiator, through a secure channel:
- the multicast group parameters (from Step N4) without the ACL, signed by the AKD
- the area control-group parameters (from Step N5) signed by the AKD

Step N7: The initiator joins the area control-group (method unspecified).

Note that Step N4 above effectively provides each and every Area Key Distributor (AKD) in the domain with the necessary parameters related to the multicast group, regardless of whether or not the area of an AKD actually contains any members of the multicast group. This approach is chosen to allow for quick response by an AKD should other hosts in other areas wish to join the multicast group. In addition, the approach leaves open the possibility of the AKDs to participate in the reliability mechanisms to be employed (ie. as backups), since each of the AKDs holds the parameters related to every multicast group in the domain.

The multicast group parameters are digitally signed by Domain Key Distributor (DKD) in order to aid reliability protocols. That is, in the case that the DKD goes down, the parameters can be obtained by one AKD from another AKD through a one-to-one secure channel, with the recipient being able to verify the authenticity of the parameters as signed by the DKD.

4.2 Membership to External-Origin Groups

Although the current design focuses on intra-domain group key management, it does not preclude the possibility of a multicast group originated by a host external to the domain. However, unlike multicast groups which originate from a host within the domain and which is therefore known to the Domain Key Distributor (DKD), multicast groups which originate from outside a domain must be explicitly made known to the DKD.

Since the current protocol views the multicast distribution tree used by a multicast routing protocol as a construct outside its control, the Domain Key Distributor (DKD) can be notified (when a host in domain joins the external-origin multicast group) through a number of ways, among others:
- The joining host can explicitly notify its Area Key Distributor (AKD) or the Domain Key Distributor (DKD).

- A domain border-router can notify the Domain Key Distributor (DKD) when it senses a request from a host to join the distribution tree
- The Domain Key Distributor (DKD) can by default be a member of all external-origin multicast groups whose distribution tree extend into the domain.

However, from the perspective of group key management, the Domain Key Distributor (DKD) only plays a role when the external-origin multicast traffic is enciphered for access control and the owner of the group requires the aid of the DKD to enforce access control. Hence, in this situation the DKD must obtain a copy of the key used to encipher the multicast traffic as it enters the domain and assign a new multicast key for that same traffic within its domain (method unspecified).

The current document leaves the precise description and specification of the group key management for external-origin multicast groups to a later date.

5. Re-Keying Approach

The basic approach to re-keying is discussed first in order to simplify later discussions on re-keying due to membership changes and due to periodic re-keying. For simplicity, the process is view from the perspective of the Domain Key Distributor (DKD) and one Area Key Distributor (AKD).

It is the DKD who initiates and controls all re-keying events in the domain related to multicast groups. Re-keying of Area-Group-Keys of area control-groups are initiated and controlled by the respective Area Key Distributors (AKD).

Note that it is important to have "cycle-over" period in which all host-members are in possession of the new re-key parameters, but is still employing the existing/old parameters.

5.1 Re-Keying of Multicast Keys

In the following, all re-key steps are related to a given multicast group. The protocol is initiated and controlled by the Domain Key Distributor (DKD).

Protocol-III: Re-keying the multicast key

Step RM1: The Domain Key Distributor (DKD) issues an authentic prepare-to-rekey message to all Area Key Distributors (AKD) through the All-KD-group. The message contains:
- an existing multicast group address
- a existing multicast group identity

of the multicast group being re-keyed

Step RM2: The Domain Key Distributor (DKD) generates:
- a new Group Security Parameter Index (GSPI) for the MGSA
- a new Multicast-Key (MKey)
- a new multicast key identifier MKeyID

based on the MGSA selected by the initiator.

Step RM3: The Domain Key Distributor (DKD) digitally-signs the multicast group parameters:
- the existing multicast group address
- the existing multicast group identity
- the Multicast Group Security Association (MGSA)
- the new Multicast-Key (MKey)
- the new multicast key identifier MKeyID
- a timestamp

Step RM4: The Domain Key Distributor (DKD) securely delivers the signed parameters to each Area Key Distributor (AKD), either through the All-KD-group (encrypted under the All-KD-Key) or through a one-to-one secure channel to each Area Key Distributor (AKD).

Step RM5: The Area Key Distributor (AKD) securely delivers the signed multicast group parameters to each host-member (of the multicast group) in its area using one of the following methods (depending on the cause of the re-keying event):
(a) through the area control-group related to the multicast group (encrypted under the AreaGroupKey)
(b) through a one-to-one secure channel to each concerned host-member.

5.2 Re-Keying of Area Keys

In the following, all re-key steps by the Area Key Distributor (AKD) are related to a given multicast group. The protocol is initiated and controlled by the Area Key Distributor (AKD).

Protocol-IV: Re-keying the area key

Step RA1: The Area Key Distributor (AKD) issues an authentic prepare-to-rekey message to all members of the multicast group within the area through the relevant area control-group. The message contains:
- an existing area control-group address
- an existing area control-group identity

of the area control-group being re-keyed

Step RA2: The Area Key Distributor (AKD) generates:
- a new Group Security Parameter Index (GSPI) for the AGSA
- a new Area-Group-Key (AreaGroupKey)
- a new area key identifier AkeyID

based on the AGSA selected by the AKD.

Step RA3: The Area Key Distributor (AKD) digitally-signs the area control-group parameters:
- the existing area control-group address
- the existing area control-group identity
- the Area Group Security Association (AGSA)
- the new Area-Group-Key (AreaGroupKey)
- the new area key identifier AKeyID
- a timestamp

Step RA4: The Area Key Distributor (AKD) securely delivers the signed control-group parameters to each host-member (of the multicast group) in its area, using one of the following methods (depending on the cause of the re-keying event):
(a) through the area control-group related to the multicast group (encrypted under the old/current AreaGroupKey)
(b) through a one-to-one secure channel to each concerned host-member.

5.3 Re-Keying of the All-KD-Key

The following describes the protocol to be employed when the All-KD-Key (AllKDKey) is to be re-keyed. All the Area Key Distributors (AKDs) and the Domain Key Distributor (DKD) share an All-KD-Key. This key is used to encrypt traffic within the All-KD-group. Note, that unlike host-members, Key Distributors never leave the All-KD-group, and hence its membership is static.

Protocol-V: Re-keying the All-KD-Key

Step RK1: The Domain Key Distributor (DKD) issues an authentic prepare-to-rekey message to all Area Key Distributors (AKD) through the All-KD-group. The message contains:
- the existing All-KD-group address
- the existing All-KD-group identity

Step RK2: The Domain Key Distributor (DKD) generates:
- a new Group Security Parameter Index (GSPI) for the MGSA
- a new All-KD-Key (AllKDKey)
- a new All-KD-Key identifier AllKDKeyID

based on the MGSA selected by the DKD

Step RK3: The Domain Key Distributor (DKD) digitally-signs the All-KD-group parameters:
- the existing multicast group address
- the existing multicast group identity
- the Multicast Group Security Association (MGSA)
- the new All-KD-Key (AllKDKey)
- the new All-KD-Key identifier (AllKDKeyID)
- a timestamp

Step RK4: The Domain Key Distributor (DKD) securely delivers the signed All-KD-group parameters to each Area Key Distributor (AKD) using one of the following methods, depending on the status of the AKD and the network condition:
(a) through the All-KD-group (encrypted under the existing/old All-KD-Key)
(b) through a one-to-one secure channel to each Area Key Distributor (AKD).

6. Hosts Joining a Multicast Group

When a host within a domain wishes to join a multicast group having already (at least) a member in the domain, the two possible approaches can be adopted in admitting the host to become a group member. In the first case, the host is disallowed from accessing (reading) traffic previous to its joining the group. In the second case, no such access restriction apply. The choice between the two approaches is dictated by policy, and hence beyond the scope of the current document.

In the following, the strict re-keying policy is adopted, in which a re-keying of the Multicast-Key and the re-keying of the AreaGroupKey (of the area within which the new host joins) is conducted

immediately. In the loose re-keying policy, the task is postponed until the next periodic re-keying, at which point the new member is able access (decipher) the data of the multicast group.

In the following, it is assumed that when a host in an area (first member or otherwise) joins a multicast group the Area Key Distributor (AKD) has already created the necessary area control-groups in its area. To conserve resources, an AKD may postpone the control-group creation (corresponding to a given multicast group) until such time that a first member of the multicast group appears in its area.

6.1 Joining with Backward Confidentiality

When a new host joining a multicast group is to be prevented from accessing (reading) previous traffic (which it may have intercepted and stored), then Multicast-Key (MKey) of the multicast group in the domain must be re-keyed each time a host joins the multicast group.

Note that even when a host is the first member of a multicast group in its area, all the other areas having a member must be re-keyed to reduce the possibility of that new host having access to previous traffic which it obtained (intercepted) in other areas.

Protocol-VI: Host joining with backward confidentiality

Step JB1: The host sends an authentic join-request message for the multicast group to its Area Key Distributor (AKD).

Step JB2: The Area Key Distributor (AKD) checks the host against the Access Control List (ACL) of the multicast group. If the host is permitted to join, then the Area Key Distributor (AKD) authentically notifies the Domain Key Distributor (DKD) and the other Area Key Distributors (AKD) of the membership change (new host-member). Otherwise, the AKD returns a join-reject message to the host

Step JB3: The Domain Key Distributor (DKD) initiates an immediate re-keying (Protocol-III: Re-keying the multicast key). This results in all Area Key Distributor (AKD) and all existing members of the multicast group obtaining the following multicast group parameters:

- the existing multicast group address
- the existing multicast group identity
- the Multicast Group Security Association (MGSA)
- the new Multicast-Key (MKey)
- the new multicast key identifier MKeyID
- a timestamp

Step JB4: The Area Key Distributor (AKD) of the area (within which the host resides) must re-key its Area-Group-Key, and thus generates:
- a new Group Security Parameter Index (GSPI) for the AGSA
- a new Area-Group-Key (AreaGroupKey)
- a new area key identifier AkeyID

based on the AGSA selected by the AKD.

Step JB5: The Area Key Distributor (AKD) digitally signs the area control-group parameters:
- the existing area control-group address
- the existing area control-group identity
- the Multicast Group Security Association (MGSA)
- the new Area-Group-Key (AreaGroupKey)
- the new area key identifier AKeyID
- a timestamp

Step JB6: If there are existing host-members in the area, the Area Key Distributor (AKD) securely delivers the signed control-group parameters to each existing host-member (of the multicast group) in its area, using one of the following methods:
(a) through the area control-group related to the multicast group (encrypted under the old/current AreaGroupKey)
(b) through a one-to-one secure channel to each existing host-member.

Step JB7: The Area Key Distributor (AKD) of the new host-member securely delivers the signed multicast group parameters (from Step JB3) and the signed control-group parameters (from Step JB5) to the new host-member through a one-to-one secure channel to the new host-member.

Step JB8: The new host joins the multicast group (method unspecified).

Step JB9: The new host joins the area control-group (method unspecified).

6.2 Joining Without Backward Confidentiality

Here, when a host joins a multicast group, the Multicast-Key need not be re-keyed since backward confidentiality is not required. The Area Key Distributor (AKD) of the host is already in possession of all the parameters related to the multicast group.

Protocol-VII: Host joining without backward confidentiality

Step JW1: The host sends an authentic join-request message for the multicast group to its Area Key Distributor (AKD).

Step JW2: The Area Key Distributor (AKD) checks the host against the Access Control List (ACL) of the multicast group. If the host is permitted to join, then the Area Key Distributor (AKD) proceeds with the next step, otherwise it returns a join-reject message to the host.

Step JW3: The Area Key Distributor (AKD) looks-up the following multicast group parameters which it previously digitally-signed:
- the existing multicast group address
- the existing multicast group identity
- the Multicast Group Security Association (MGSA)
- the new Multicast-Key (MKey)
- the new multicast key identifier MKeyID
- a timestamp

Step JW4: The Area Key Distributor (AKD) looks-up the following control-group parameters which it previously digitally-signed:
- the existing area control-group address
- the existing area control-group identity
- the Multicast Group Security Association (MGSA)
- the existing Area-Group-Key (AreaGroupKey)
- the existing area key identifier AKeyID
- a timestamp

Step JW5: The Area Key Distributor (AKD) of the new host-member securely delivers the signed multicast group parameters (from Step JW3) and the signed control-group parameters (from Step JW4) to the new host-member through a one-to-one secure channel to the new host-member.

Step JW6: The new host joins the multicast group (method unspecified).

Step JW7: The new host joins the area control-group (method unspecified).

7. Host Leaving a Multicast Group

The case of a host leaving a multicast group can be caused by a number of reasons depending on the policy dictating group membership and on the multicast application in question.

From the perspective of the current design, re-keying must be conducted to preserve forward confidentiality. That is, re-keying must be conducted to prevent the ex-member from further accessing (deciphering) the data in the multicast group, even if the ex-member persists in being a part of the multicast distribution tree.

In the following, the strict re-keying policy is adopted, in which a re-keying of the Multicast-Key and the re-keying of the Area-Group-Key (AreaGroupKey) of the area within which the new host joins are conducted immediately. In the loose re-keying policy, the task is postponed until the next periodic re-keying, at which point the ex-member ceases to be able to decipher traffic in the multicast group and its corresponding control-group in the area.

Note that in the current design, when a host leaves a multicast group it must also (by default) depart from the associated control-group. In general, it makes no sense for a host to join a control-group without joining the corresponding multicast group.

Protocol VIII: Host leaving a multicast group and control-group

Step LB1: The leaving-host sends an authentic leave-request message for the multicast group to its Area Key Distributor (AKD). Alternatively, the Domain Key Distributor (DKD) notifies the AKD through an authentic eject-host-request message to the AKD.

Step LB2: The Domain Key Distributor (DKD) of the affected area authentically notifies the other Area Key Distributors (AKD) of the membership change (host-member leaving).

Step LB3: The Domain Key Distributor (DKD) initiates an immediate re-keying (Protocol-III: Re-keying the multicast key). This results in all Area Key Distributors (AKDs) and all host-members of the multicast group, except host-members in the affected area, obtaining the following multicast group parameters:

- the existing multicast group address
- the existing multicast group identity
- the Multicast Group Security Association (MGSA)
- the new Multicast-Key (MKey)
- the new multicast key identifier MKeyID
- a timestamp

Step LB4: The Area Key Distributor (AKD) of the affected area (within which the leaving-host resides) must re-key its Area-Group-Key, and thus generates:
- a new Group Security Parameter Index (GSPI) for the AGSA
- a new Area-Group-Key (AreaGroupKey)
- a new area key identifier AkeyID

based on the AGSA selected by the AKD.

Step LB5: The Area Key Distributor (AKD) digitally signs the area control-group parameters:
- the existing area control-group address
- the existing area control-group identity
- the Multicast Group Security Association (MGSA)
- the new Area-Group-Key (AreaGroupKey)
- the new area key identifier AKeyID
- a timestamp

and digitally-signs the multicast group parameters that the AKD received from the DKD in Step LB3:
- the existing multicast group address
- the existing multicast group identity
- the Multicast Group Security Association (MGSA)
- the new Multicast-Key (MKey)
- the new multicast key identifier MKeyID
- a timestamp

Step LB6: The Area Key Distributor (AKD) securely delivers the signed multicast group parameters and control-group parameters to each remaining host-member (of the multicast group) in its area, through a one-to-one secure channel to each existing host-member.

Step LB7: The leaving-host leaves the multicast group (method unspecified).

Step LB8: The leaving-host leaves the area control-group (method unspecified).

8. Reliability in Key Management

The current document recognizes that key management be conducted in a reliable manner, due to the sensitivity of cryptographic keys and the basic necessity that a host-member obtain the multicast key before it can access (decipher) the multicast data. Reliability is also important in the re-keying of the keys used in the multicast group and in the area control-groups. This is true particularly if in the re-keying process, the control-group itself is used to

transmit the new parameters (for either the multicast group or the same control-group) to the members of the group.

However, the current document views reliability of transmission, particularly in the control-groups, as more of a multicast-reliability issue. That is, reliability should not be expected from and should not be part of key management. This is also true for the one-to-one "secure channels", in which confidential and authentic communications is created between a sender and a receiver through the previously-established Security Association (SA) and the shared private-key.

Note that in the re-keying of a Multicast-Key (MKey), it is important that each Area Key Distributor (AKD) first reliably obtains the new parameters (including the new key) of the multicast group. This is because without the new parameters, the AKD will not be able to even begin to re-key its area. Once each AKD obtains the new parameters of the multicast group, the re-key of the Multicast-Key in each area is independent of one another.

The current work currently does not specify how or what manner reliability in key management is to be achieved. However, when a control-group (either the All-KD-group or an area control-group) is used for key management from a sender to a number of recipients (eg. delivery of new key and new parameters) several basic approaches can be used:

(a) ACKs from members

When a control-group is used to transmit re-keying parameters, the recipients simply return an acknowledgment (ACK) to the Key Distributor through the secure channel previously established with the Key Distributor. Should the Key Distributor fail to receive such an ACK from a recipient within specified time, it will then query the recipient through the secure channel previously established. Depending on the frequency of key management and the number of host-members, this approach may cause an ACK-implosion on the AKDs.

(b) Timeouts

When some period after a prepare-to-rekey message is received, some recipients fail to receive the actual new key and parameters through the control-group, those recipients query the sender (AKD or DKD).

When nothing is heard after both the due time for the prepare-to-rekey message and due time for the actual key/parameters to be received, the recipients query the sender (AKD or DKD).

(c) Explicit Reliable Multicast (RM) protocol

Employ a specific RM protocol to establish reliability within the All-KD-group and/or the area control-groups. Each control-group can in fact employ different RM protocols.

9. Packet Formats

To be decided.

10. References

[HCD98] T. Hardjono, B. Cain and N. Doraswamy, "A Framework for Group Key Management for Multicast Security", Internet Draft, July 1998.

[HC98] D. Harkins and D. Carrel, "The Internet Key Exchange (IKE)", Internet Draft, June 1998.

[WGL98] C. K. Wong, M. Gouda and S. Lam, "Secure Group Communications Using Key Graphs", in Proceedings of SIGCOMM'98.

[KA98a] S. Kent and R. Atkinson, "Security Architecture for the Internet Protocol", IETF, RFC 1825, 1998.

[KA98b] S. Kent and R. Atkinson, "IP Encapsulating Security Payload (ESP)", Internet Draft, July 1998.

[KA98c] S. Kent and R. Atkinson, "IP Authentication Header", Internet Draft, July 1998.

[Mey98] D. Meyer, "Administratively Scoped IP Multicast", IETF, RFC 2365, July 1998.

[HTE98] M. Handley, D. Thaler, and D. Estrin, "The Internet Multicast Address Allocation Architecture", Internet Draft, June 1998.

11. Author Addresses

Thomas Hardjono
Email: thardjono@baynetworks.com

Brad Cain
Email: bcain@baynetworks.com

Inder Monga
Email: imonga@baynetworks.com

Nortel Networks
3 Federal Street, Bl3-03
Billerica, MA 01821, USA
Tel: +1-978-916-4538

12. Full Copyright Statement