IGMP Extension for Authentication of IP Multicast Senders and Receivers

Status of this Memo

This document is an Internet-Draft. 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".

To learn the current status of any Internet-Draft, please check the "id-abstracts.txt" listing contained in the Internet-Drafts Shadow Directories on ftp.is.co.za (Africa), nic.nordu.net (Europe), munnari.oz.au (Pacific Rim), ftp.ietf.org (US East Coast), or ftp.isi.edu (US West Coast).

Abstract

The security enhancement is one of the most important enhancements to IP multicast. IP multicast requires many security functions that include user authentication of IP multicast, encryption of IP multicast datagrams and key management protocols for IP multicast. Among them, the user authentication function for IP multicast is considered one of the most important security functions for IP multicast. This document describes the extension to IGMP, version 2 (IGMPv2) [1] for the authentication of IP multicast senders and receivers, which prevents an unauthorized user from sending and receiving IP multicast datagrams.
1. Introduction

The rapid deployment of IP multicast over the Internet has been realized by MBone, an experimental IP multicast network over the Internet. IP multicast is at the experimental stage. In order to make IP multicast a commercial service, several enhancements to IP multicast are required. Such enhancements include security, accounting, QoS and IP multicast address allocation. Among them, the security enhancement is one of the most important enhancements to IP multicast. IP multicast requires many security functions that include user authentication of IP multicast, encryption of IP multicast datagrams and key management protocols for IP multicast. Among them, the user authentication function for IP multicast is considered one of the most important security functions for IP multicast.

This document describes the extension to IGMPv2 for the authentication of IP multicast senders and receivers, which prevents an unauthorized user from sending and receiving IP multicast datagrams. The term "IP multicast sender/receiver" is extensively used in this document. "IP multicast sender/receiver" is defined as an user entity to be authenticated in a sending/receiving host.

2. Requirements

The design requirements on the user authentication functions for IP multicast are described below.

(1) Authentication of IP Multicast Sender: In the case of IP multicast, IP multicast datagrams sent by a sender will be simultaneously delivered to many receivers distributed over the Internet. If a sender sends IP multicast datagrams erroneously or maliciously, the overall Internet is burdened with the undesirable traffic and receivers may misunderstand that IP multicast datagrams received from the malicious sender are valid. Since anyone can send IP multicast datagrams to the Internet, it is easy to inject such traffic into the Internet. Therefore, it is important to confine only an authorized sender to sending IP multicast datagrams.

(2) Authentication of IP Multicast Receiver: Anyone can receive IP multicast datagrams from the Internet. However, when delivering charged contents to authorized receivers, it is desirable not to deliver them to unauthorized receivers, even if charged contents are encrypted. In addition, the extra traffic caused by delivering them to unauthorized receivers is useless and should be avoidable. Therefore, it is important to confine only an authorized receiver to receiving IP multicast datagrams.

(3) IP Multicast Routing Protocols: IP multicast routing protocols such as DVMRP [2], PIM [3] and CBT [4] have been developed within IETF. The user authentication function for IP multicast should be independent of such IP multicast routing protocols, and hence should not depend on a specific IP multicast routing protocol.
This document describes the extension to IGMPv2, which satisfies the above requirements.

3. Architecture

The overall architecture for the authentication of IP multicast senders and receivers is described below.

An IP multicast sender sends IP multicast datagrams to an ingress router in an IP multicast network. IP multicast datagrams travel egress routers through IP multicast routers within an IP multicast network. An IP multicast routing is controlled by IP multicast routing protocols such as DVMRP, PIM and CBT. An egress router sends IP multicast datagrams to IP multicast receivers which join the host group.

This document describes the user authentication functions of IP multicast, using the Challenge-Response mechanism in a similar way as CHAP [5].

NOTE: Other mechanisms for the user authentication functions of IP Multicast are for further study.

When an IP multicast sender starts to send IP multicast datagrams, an ingress router may optionally authenticate it, using the challenge-response mechanism. An ingress router may optionally use RADIUS as the authentication server, when authenticating the IP multicast sender.

NOTE: The interaction between a multicast router and a RADIUS server is described in Appendix A. The separate document [6] describes the extensions to RADIUS [7] for the authentication of IP multicast senders and receivers.

When the result of the authentication is successful, IP multicast datagrams sent by the IP multicast sender travel towards egress routers through IP multicast routers. When the result of the authentication is not successful, the ingress router silently discards IP multicast datagrams sent by the IP multicast sender. This mechanism prevents an unauthorized user from sending IP multicast datagrams to the Internet.

When an IP multicast receiver starts to receive IP multicast datagrams, an egress router may optionally authenticate it, using the challenge-response mechanism. An egress router may optionally use RADIUS as the authentication server, when authenticating the IP multicast receiver. When the result of the authentication is successful, the egress router starts to transmit IP multicast datagrams to the IP multicast receiver. When the result of the authentication is not successful, the egress router does not transmit IP multicast datagrams to the IP multicast receiver. This mechanism prevents an unauthorized user from receiving IP multicast datagrams from the Internet.
There are two levels of multicast routers.

(1) Level 1: Unsecure Multicast Router
The multicast router complies with IGMPv2.

(2) Level 2: Secure Multicast Router
The multicast router complies with both IGMPv2 and this document.

All multicast routers in a subnetwork must be either secure or
unsecure. In other words, unsecure multicast routers and secure
multicast routers must not coexist in the same subnetwork.

4. Protocol Description

This section describes the mechanisms for the user authentication
functions of IP multicast.

4.1 Procedures for Authentication of IP Multicast Senders

4.1.1 Operation of Sending hosts

When an IP multicast sender wants to send IP multicast datagrams, a
sending host sends a Sender Start message to a multicast router.
When [Retry Interval] expires, a sending host resends a Sender Start
message to a multicast router, until a Challenge message is received,
or [Retry Count] expires.

When a Challenge message is received, A sending host sends a Response
message to a multicast router. When [Retry Interval] expires, a
sending host resends a Response message to a multicast router, until
a Success or Failure message is received, or [Retry Count] expires.

When a Success message is received, a sending host starts to send IP
multicast datagrams. When a Failure message is received, a sending
host is not allowed to send IP multicast datagrams.

After a sending host starts to send IP multicast datagrams, it may
receive a Challenge message. When a Challenge message is received,
a sending host sends a Response message to a multicast router. After a
sending host sends a Response message, it may receive the same
Challenge message. In this case, a sending host resends the same
Response message.

NOTE: This is the case where a Response message was lost.
When [Retry Interval] expires, a sending host resends a Response message to a multicast router, until a Success or Failure message is received, or [Retry Count] expires.

When a Success message is received, a sending host can continue to send IP multicast datagrams. When a Failure message is received, a sending host stops to send IP multicast datagrams.

### 4.1.2 Operation of Multicast Routers

When a multicast router receives a Sender Start message, it sends a Challenge message to the sending host which sent the Sender Start message. After a multicast router sent the Challenge message, it may receive the same Sender Start message. In this case, a multicast router resends the same Challenge message.

**NOTE:** This is the case where a Challenge message was lost.

When a Response message is received, a multicast router compares the response value with the expected value for the authentication of the IP multicast sender. Alternatively, a multicast router may ask a RADIUS server to authenticate the IP multicast sender.

If the result of the authentication is successful, a multicast router sends a Success message to the sending host. If the result of the authentication is not successful, a multicast router sends a Failure message to the sending host. After a multicast router sent the Success message, it may receive the same Response message. In this case, a multicast router resends the same Success message.

**NOTE:** This is the case where a Success message was lost.

A multicast router manages a list of IP addresses of authenticated IP multicast senders regarding each host group with a destination port. When the authentication of the IP multicast sender is successful, a multicast router adds its IP address to the list.

When a multicast router receives an IP multicast datagram from a sending host, it checks the source IP address of the received IP multicast datagram. If the source IP address was registered in the list of IP addresses of authenticated IP multicast senders, a multicast router forwards the received IP multicast datagrams. If the source IP address was not registered in the list of IP addresses of authenticated IP multicast senders, a multicast router silently discards the received IP multicast datagrams.

The [Validity Period] of the authentication of an IP multicast sender is set in the authentication parameter of a Success message. If the [Validity Period] expires, a multicast router may reauthenticate the IP multicast sender.
When a multicast router reauthenticates the IP multicast sender, it sends a Challenge message. When a [Retry Interval] expires, the multicast router resends a Challenge message, until a Response message is received, or [Retry Count] expires.

When a Response message is received, a multicast router compares the response value with the expected value for the authentication of the IP multicast sender. Alternatively, a multicast router may ask a RADIUS server to authenticate the IP multicast sender.

If the result of the authentication is successful, a multicast router sends a Success message to the sending host. If the result of the authentication is not successful, a multicast router sends a Failure message to the sending host. After a multicast router sent the Success message, it may receive the same Response message. In this case, a multicast router resends the same Success message.

NOTE: This is the case where a Success message was lost.

A multicast router deletes the IP address of an IP multicast sender from a list of IP addresses of authenticated IP multicast senders, in the following cases.

- When the [Validity Period] of the authentication of an IP multicast sender expires, a multicast router does not want to reauthenticate it.
- The reauthentication of an IP multicast sender is not successful.

4.2 Procedures for Authentication of IP multicast Receivers

4.2.1 Operation of Receiving Hosts

When an IP multicast receiver wants to receive IP multicast datagrams, a receiving host sends a Membership Report message with an authentication parameter to a multicast router. When [Retry Interval] expires, a receiving host resends a Membership Report message to a multicast router, until a Challenge message is received, or [Retry Count] expires.

When a Challenge message is received, a receiving host sends a Response message to a multicast router. When [Retry Interval] expires, a receiving host resends a Response message to a multicast router, until a Success or Failure message is received, or [Retry Count] expires.

When a Success message is received, a receiving host starts to receive IP multicast datagrams. When a Failure message is received, a receiving host is not allowed to receive IP multicast datagrams.
After a receiving host starts to receive IP multicast datagrams, it may receive a Group-Specific Query message with a reason parameter (reason = "reauthentication is required"). When a Group-Specific Query message with a reason parameter (reason = "reauthentication is required") is received, a receiving host sets a delay timer to a random value selected from the range (0, Max Response Time) for the host group being queried. Max Response Time is specified in the Group-Specific Query message. If the receiving host receives another Membership Report message with an authentication parameter while the timer is running, it stops the timer for the host group and does not send a Membership Report message with an authentication parameter, in order to suppress duplicate Membership Report messages.

When the timer expires, the receiving host sends a Membership Report message with an authentication parameter to a multicast router. When [Retry Interval] expires, a receiving host resends a Membership Report message to a multicast router, until a Challenge message is received, or [Retry Count] expires.

When a Challenge message is received, a receiving host sends a Response message to a multicast router. When [Retry Interval] expires, a receiving host resends a Response message to a multicast router, until a Success or Failure message is received, or [Retry Count] expires.

When a Success message is received, a receiving host can continue to receive IP multicast datagrams. When a Failure message is received, a receiving host stops to receive IP multicast datagrams.

4.2.2 Operation of Multicast Routers

When a multicast router receives a Membership Report message with an authentication parameter, it sends a Challenge message to the receiving host which sent the Membership Report message. After a multicast router sent the Challenge message, it may receive the same Membership Report message. In this case, a multicast router resends the same Challenge message. 

NOTE: This is the case where a Challenge message was lost.

When a Response message is received, a multicast router compares the response value with the expected value for the authentication of the IP multicast receiver. Alternatively, a multicast router may ask a RADIUS server to authenticate the IP multicast receiver.

If the result of the authentication is successful, a multicast router sends a Success message to the receiving host. If the result of the authentication is not successful, a multicast router sends a Failure message to the receiving host. After a multicast router sent the Success message, it may receive the same Response message. In this case, a multicast router resends the same Success message.

NOTE: This is the case where a Success message was lost.
A multicast router manages a list of group addresses of host groups which have at least one authenticated IP multicast receiver for each of its attached networks. When the authentication of the IP multicast receiver is successful, a multicast router adds the address of the host group which the receiving host wants to join to the list, unless the address is already registered in the list.

The [Validity Period] of the authentication of an IP multicast receiver is set in the authentication parameter of a Success message. If the [Validity Period] expires, a multicast router may reauthenticate the IP multicast receiver.

When a multicast router reauthenticates the IP multicast receiver, it sends a Group-Specific Query message with a reason parameter (reason = "reauthentication is required"). The Group-Specific Query message has the Max Response Time set to [Reauthentication Query Interval]. When a [Reauthentication Query Interval] expires, the multicast router resends the Group-Specific Query message, until a Membership Report message with an authentication parameter is received, or a [Retry Count] expires.

When a multicast router receives a Membership Report message with an authentication parameter, it sends a Challenge message to the receiving host which sent the Membership Report message. After a multicast router sent the Challenge message, it may receive the same Membership Report message. In this case, a multicast router resends the same Challenge message.

NOTE: This is the case where a Challenge message was lost.

When a Response message is received, a multicast router compares the response value with the expected value for the authentication of the IP multicast receiver. Alternatively, a multicast router may ask a RADIUS server to authenticate the IP multicast receiver.

If the result of the authentication is successful, a multicast router sends a Success message to the receiving host. If the result of the authentication is not successful, a multicast router sends a Failure message to the receiving host. When the result of the authentication is not successful, the multicast router resends a Group-Specific Query message with a reason parameter (reason = "reauthentication is required"), until the authentication succeeds, or [Retry Count] expires.

After a multicast router sent the Success message, it may receive the same Response message. In this case, a multicast router resends the same Success message.

NOTE: This is the case where a Success message was lost.
A multicast router deletes the address of the host group from a list of the addresses of host groups which have at least one authenticated IP multicast receiver, in the following cases.

- When the [Validity Period] of the authentication of an IP multicast receiver expires, a multicast router does not want to reauthenticate it.
- The reauthentication of an IP multicast receiver host is not successful.
- A multicast router finds that there are no local members for the host group in accordance with IGMPv2.

When a multicast router receives a Membership Report message without an authentication parameter, it silently discards the received Membership Report message, if the group address set in the Membership Report message is not registered in the list of the addresses of host groups which have at least one authenticated IP multicast receiver.

**NOTE:** A multicast router receives a Membership Report message without an authentication parameter as the response to a Membership Query, in accordance with IGMPv2.

### 5. Compatibility with IGMPv2 Hosts

#### 5.1 Compatibility with IGMPv2 Sending Hosts

A sending host which only complies with IGMPv2 sends IP multicast datagrams without having any authentication procedures. To keep the compatibility with IGMPv2 compliant sending hosts, a sending host may send IP multicast datagrams to a host group with a destination port without having any authentication procedures, unless it is explicitly stated that only an authenticated IP multicast sender may send IP multicast datagrams to the host group with the destination port. An ingress router must manage the access control list for host groups with destination ports. If the host group with the destination port is included in the access control list, only an authenticated IP multicast sender may send IP multicast datagrams to the host group with the destination port. Otherwise, a sending host may send IP multicast datagrams to the host group with the destination port without having any authentication procedures.

#### 5.2 Compatibility with IGMPv2 Receiving Hosts

A receiving host which only complies with IGMPv2 may receive IP multicast datagrams without having any authentication procedures. To keep the compatibility with IGMPv2 compliant receiving hosts, a receiving host may join a host group without having any authentication procedures, unless it is explicitly stated that only an authenticated IP multicast receiver may join the host group. An egress router must manage the access control list for host groups. If the host group is included in the access control list, only an authenticated IP multicast
receiver may join the host group and receive IP multicast datagrams
sent to the host group. Otherwise, a receiving host may join the host
group and receive IP multicast datagrams sent to the host group,
without having any authentication procedures.

6. Extensions to IGMPv2 Messages

The following messages and parameters are added to IGMPv2 for the
authentication of IP multicast senders and receivers.

6.1 New Messages

The format of new messages is as follows.

```
0                   1                   2                   3
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Type       | Max Resp Time |     Checksum                  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                     Group    Address                          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Destination Port          |     Unused                    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

(1) Type

The types of new messages are as follows:

0x21 = Sender Start
0x22 = Challenge
0x23 = Response
0x24 = Success
0x25 = Failure

(2) Max Response Time

The use of this field is same as specified in IGMPv2.

(3) Checksum

The use of this field is same as specified in IGMPv2.

(4) Group Address

In a Sender Start message, the address of the host group to which
an IP multicast sender wants to send IP multicast datagrams is set
to the group address field.

In a Challenge, Response, Success or Failure message, the group
address field is set to zero.
(5) Destination Port

In a Sender Start message, the destination port combined with the host group to which an IP multicast sender wants to send IP multicast datagrams is set to the destination port field. The value all "1"s has a special meaning. If this value is set to the destination port field, it means that the IP multicast sender wants to send IP multicast datagrams to the host group with any destination port.

In a Challenge, Response, Success or Failure message, the group address field is set to zero.

6.2 Optional Parameters

The following optional parameters may be set following the fixed fields of IGMP messages.

The format of the optional parameters is as follows:

```
+--------------------------------------+
| Option1 | Option2 | ... | Padding |
+--------------------------------------+
```

Thus, padding is added in the end, in order to complete them in 32-bit boundary. The value of padding is zero.

```
+--------------------------------------+
| Option Type | Option Data Length | Option Data |
+--------------------------------------+
```

- Option Type: An 8-bit identifier of the option type
- Option Data Length: Length of the option data in octet (8 bits)
- Option Data: Data specific to each option with variable length

6.2.1 Optional Parameters for the Group-Specific Query Message

(1) Reason

This parameter specifies the reason why the Group-Specific Query message is sent by a multicast router.

Option Type: 1

The format of the option data is as follows:

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

Reason: This field is one octet (8 bits). This field specifies the reason why the Group-Specific Query message is sent by a multicast router.
1 = a Leave Group message is received by a multicast router
2 = a reauthentication is required

NOTE: If this parameter is omitted, the value "1" (a Leave Group message is received) is assumed.

6.2.2 Optional Parameters for the Version 2 Membership Report Message and the Sender Start Message

(1) Authentication

This parameter of a Version 2 Membership Report message is used to authenticate an user on a receiving host which wants to receive IP multicast datagrams. This parameter of a Sender Start message is used to authenticate an user on a sending host which wants to send IP multicast datagrams.

Option Type: 1

The format of the option data is as follows:

```
+-----------------------------+
| Mechanism | Identifier | User-ID |
+-----------------------------+
```

Mechanism: An 8-bit identifier of the mechanism for the authentication of a receiving or sending host.

1 = the authentication mechanism specified in this document

NOTE: Other authentication mechanisms are for further study.

Identifier: This field is one octet (8 bits). This field is used to identify the sequence for the authentication of an IP multicast receiver or sender. When a new authentication starts, this field must be changed.

User-ID: The User-ID field is one or more octets representing the identification of an user on a receiving or sending host to be authenticated. An User-ID may be ASCII character strings or an e-mail address of an user.

6.2.3 Optional Parameters for the Challenge Message and the Response Message

(1) Authentication

This parameter of is used to authenticate an user on a receiving host which wants to receive IP multicast datagrams and an user on a sending host which wants to send IP multicast datagrams.
Option Type: 1

The format of the option data is as follows:

```
<table>
<thead>
<tr>
<th>Identifier</th>
<th>Value-Size</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User-ID</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

**Identifier:** This field is one octet (8 bits). When a Challenge message is sent, this field must be copied from the Identifier field of the preceding Version 2 Membership Report or Sender Start message. When a Response message is sent, this field must be copied from the Identifier field of the preceding Challenge message.

**Value-Size:** This field is one octet and indicates the length of the Value field.

**Value:** The Value field is one or more octets.

The Challenge Value is a variable stream of octets. Each Challenge Value should be unique, since repetition of a challenge value in conjunction with the same secret would permit an attacker to reply with a previously intercepted response. The Challenge Value must be changed each time a Challenge message is sent. The length of the Challenge Value depends upon the method used to generate the octets, and is independent of the hash algorithm used.

The Response Value is the one-way hash calculated over a stream of octets consisting of the Identifier, followed by (concatenated with) the "secret", followed by (concatenated with) the Challenge Value. The length of the Response Value depends upon the hash algorithm used. MD5 [8] is used as the hash algorithm. In the case of MD5, The length of the Response Value is 16 octets.

The length of "secret" must be at least 1 octet. The "secret" should be at least as large and unguessable as a well-chosen password.

**User-ID:** The User-ID field is one or more octets representing the identification of an user on a receiving or sending host to be authenticated. An User-ID may be ASCII character strings or an e-mail address of an user.
6.2.4 Optional Parameters for the Success Message

(1) Authentication

This parameter is used to authenticate an user on a receiving host which wants to receive IP multicast datagrams and an user on a sending host which wants to send IP multicast datagrams.

Option Type: 1

The format of the option data is as follows:

```
+----------+--------------+-----------+
| Identifier| Validity-Period| Message   |
+----------+--------------+-----------+
```

Identifier: This field is one octet (8 bits). When a Success or Failure message is sent, this field must be copied from the Identifier field of the preceding Response message.

Validity-Period: This field is four octets (32 bits). This field specifies the period of the validity for the authentication of an user on a receiving or sending host in units of second. When a Success message is sent, a multicast router specifies the validity period for the authentication.

Message: The Message field is zero or more octets, and its contents are implementation dependent. It is intended to be human readable, and must not affect the operation of the protocol.

6.2.5 Optional Parameters for the Failure Message

(1) Authentication

This parameter is used to authenticate an user on a receiving host which wants to receive IP multicast datagrams and an user on a sending host which wants to send IP multicast datagrams.

Option Type: 1

The format of the option data is as follows:

```
+----------+--------+
| Identifier| Message |
+----------+--------+
```

Ishikawa, Yamanouchi, Takahashi  Expires February 1999  [Page 14]
Identifier: This field is one octet (8 bits). When a Success or Failure message is sent, this field must be copied from the Identifier field of the preceding Response message.

Message: The Message field is zero or more octets, and its contents are implementation dependent. It is intended to be human readable, and must not affect the operation of the protocol.

7. List of Timers and Default Values

This document defines the following timers and their default values, in addition to those defined in IGMPv2.

7.1 Retry Interval

The Retry Interval is the time between repetitions of a Sender Start message, a Membership Report message, a Challenge message or a Response message during the authentication phase. Default: 10 seconds ?.

7.2 Retry Count

The Retry Count is the number of Sender Start messages, Membership Report messages, Group-Specific Query message, Challenge messages or Response messages sent before the authentication procedure is abandoned. Default: the Robustness Variable.

NOTE: The Robustness Variable is defined in IGMPv2.

7.3 Validity Period

The Validity Period of the authentication of an IP multicast sender or receiver set in a Success message.

7.4 Reauthentication Query Interval

The Reauthentication Query Interval is the Max Response Time set in a Group-Specific Query message sent when the [Validity Period] of the authentication of an IP multicast receiver expires. Default: 10 seconds ?.
8. Message Destinations

The destinations of messages defined in this document are summarized below.

<table>
<thead>
<tr>
<th>Message Type</th>
<th>Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sender Start</td>
<td>ALL-ROUTERS (224.0.0.2)</td>
</tr>
<tr>
<td>Challenge</td>
<td>The sending host which sent a Sender Start message, or the receiving host which sent a Membership Report message with an authentication parameter</td>
</tr>
<tr>
<td>Response</td>
<td>The multicast router which sent a Challenge message</td>
</tr>
<tr>
<td>Success</td>
<td>The sending or receiving host which sent a Response message</td>
</tr>
<tr>
<td>Failure</td>
<td>The sending or receiving host which sent a Response message</td>
</tr>
</tbody>
</table>

9. Security Considerations

This document describes the IGMPv2 extension for authentication of IP multicast senders and receivers.
Appendix A. Interaction with the RADIUS Server

This appendix gives an outline of the interaction between a secure multicast router and a RADIUS server. The detailed specifications of the interaction between them are described in [6].

A.1 Interaction with the RADIUS Server for the Authentication of IP Multicast Senders and Receivers

A.1.1 Interaction with the RADIUS Server for the Authentication of IP Multicast Senders

When a multicast router receives a Response message from a sending host, it sends an Access-Request message in RADIUS to a RADIUS server.

When the multicast router receives an Access-Accept message in RADIUS from the RADIUS server, it sends a Success message to the sending host. When the multicast router receives an Access-Reject message in RADIUS, it sends a Failure message to the sending host.

A.1.2 Interaction with the RADIUS Server for the Authentication of IP Multicast Receivers

When a multicast router receives a Response message from a receiving host, it sends an Access-Request message in RADIUS to a RADIUS server.

When the multicast router receives an Access-Accept message in RADIUS from the RADIUS server, it sends a Success message to the receiving host. When the multicast router receives an Access-Reject message in RADIUS, it sends a Failure message to the receiving host.
Appendix B. Issues

B.1 IP Multicast Receivers on Shared Media Networks

Once one IP multicast receiver on a shared media network such as Ethernet is authenticated, a multicast router starts to send IP multicast datagrams to the network. As a result, other IP multicast receivers on the network can receive IP multicast datagrams, even if they are not authenticated.

The most straightforward solution on this issue is the use of encryption. One possible scenario for the solution is as follows.

When the authentication of an IP multicast sender is successful, an ingress router sends a group key (i.e. symmetric key) to the IP multicast sender, as the parameter of a Success message. The key is encrypted with the public key of the IP multicast sender. The IP multicast sender encrypts IP multicast datagrams with the group key and sends them to the ingress router.

Similarly, when the authentication of an IP multicast receiver is successful, an egress router sends a group key to the IP multicast receiver, as the parameter of a Success message. The key is encrypted with the public key of the IP multicast receiver. The egress router transmits IP multicast datagrams encrypted with the group key to the IP multicast receiver. The IP multicast receiver decrypts IP multicast datagrams received, using the group key.

It is assumed that a group key for the host group is generated when the address of the host group is assigned to the host group. Protocols for group key management and distribution are for further study.

B.2 Granularity on Filtering of IP multicast Datagrams

An ingress router drops IP multicast datagrams sent from unauthenticated IP multicast senders, based on only their source IP addresses, even if user-IDs are used for authenticating IP multicast senders.

B.3 Quick detection of Sender Leave

When the reauthentication of an IP multicast sender fails, a multicast router detects the leave of the IP multicast sender.

To detect the leave of an IP multicast sender more quickly, it is necessary to define a new message (i.e. Sender Stop message). When an IP multicast sender stops sending IP multicast datagrams, a sending host sends a Sender Stop message to a multicast router. When a multicast router receives a Sender Stop message from a sending host, the multicast router detects the leave of the IP multicast sender. This mechanism allows a multicast router to detect the leave of an IP multicast sender more quickly.
References


Acknowledgements

Authors' Address:

Norihiro Ishikawa
NTT Information and Communication Systems Laboratory
1-1 Hikarino-oka Yokosuka-Shi
Kanagawa 239 Japan
isic@isl.ntt.co.jp
+81 468 59 2434 (tel)
+81 468 59 3796 (fax)
Nagatsugu Yamanouchi  
IBM Research, Tokyo Research Laboratory  
IBM Japan, Ltd.  
1623-14, Shimotsuruma, Yamato-shi,  
Kanagawa 242, Japan  
yamanouc@trl.ibm.co.jp  
+81 462 73 5150 (tel)  
+81 462 74 4282 (fax)

Osamu Takahashi  
NTT Information and Communication Systems Laboratory  
1-1 Hikarino-oka Yokosuka-Shi  
Kanagawa 239 Japan  
osamu@isl.ntt.co.jp  
+81 468 59 2415 (tel)  
+81 468 59 3796 (fax)