MBONED
Internet-Draft
Intended status: Informational
Expires: April 30, 2015

W. Atwood
Concordia University/CSE
B. Li
Normal College of Shenzhen University
S. Islam
North South University

October 27, 2014

Receiver Access Control using PANA in IP Multicast
draft-atwood-mboned-mrac-pana-00

Abstract

Multicast Receiver Access Control must be enforced at both the application level and at the network level. The control at the two levels must be correlated, to ensure that only a legitimate group member at the application level is permitted to join group at the network level. We assume that authentication and authorization at the application level are provided by Extensible Authentication Protocol (EAP) exchanges. We describe how to use Protocol for carrying Authentication for Network Access (PANA) to transport the EAP packets in such a way that authententication and authorization can be easily achieved at the network level and that the necessary coordination is achieved.

Status of This Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

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."

This Internet-Draft will expire on April 30, 2015.

Table of Contents

1. Introduction

This document is part of a series that proposes a solution for Multicast Receiver Access Control (MRAC). The reader is encouraged to read the other documents in the series to gain insight into how the various components of the solution interact.

A list of desirable properties for MRAC is presented in [I-D.atwood-mboned-mrac-req]. A possible architecture for achieving these properties is presented in [I-D.atwood-mboned-mrac-arch]. The use of the keys described in this document by a secure version of IGMP is presented in [I-D.atwood-pim-sigmp]. The corresponding use of the keys for a secure version of MLD will be presented in draft-atwood-pim-smld (not yet published). The required coordination of keys and security associations among the End User(s) and the router(s) on a network segment is described in [I-D.atwood-pim-gsam].

MRAC can be viewed at two levels: the application level and the network level. At the application level, an End User will obtain permission to subscribe to a group session. This permission will

contain at least two components: a description of how the session is to be accessed and a certification that the End User is authorized to access the session.

The certification will be presented at the application level. If it is valid the End User will be permitted to join the group.

At the network level, the session descriptor will be used to issue the network level join, which allows the session data to flow to the End User device.

To prevent the End User from presenting an arbitrary session descriptor, it is necessary to coordinate the application level join and the network level join.

This draft describes how to achieve receiver access control at the application level, using Protocol for carrying Authentication for Network Access (PANA) [RFC5191] in IP multicast. The approach uncouples the receiver access control from the process of joining a multicast group. An End User is authenticated and authorized at the application level while he/she shows his/her interest in a multicast group at the network level.

This draft does not conflict with or intend to replace [RFC3740] published by the Multicast Security (MSEC) working group. Encryption for multicast data could also be implemented in addition to receiver access control if the multicast application requires it.

1.1. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT","SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

2. Framework for Multicast Receiver Access Control

2.1. PANA Role Description

There are four roles in a PANA environment: the PANA client (PaC), the PANA authentication agent (PAA), the AAA server (AAAS) and the enforcement point (EP). They are briefly described as follows:

PaC: It is the client implementation of PANA. A PaC runs on a device operated by an End User that wishes to be authorized to perform some action.

PAA: It is the server implementation of PANA. The PAA interacts with a PaC to convey the EAP exchanges that are necessary for

authentication, authorization and accounting. The location of a PAA may be one or more IP hops away from the PaCs that it is responsible for.

AAAS: It is a server that handles authentication, authorization and accounting service. The AAAS interprets the certification presented by a PaC. According to the interpreted information, the AAAS authenticates and authorizes a PaC to perform the action that it has requested.

EP: It is the point in the network where the limitations on the desired action are enforced.

2.2. MRAC Role Description

In the architecture described in [I-D.atwood-mboned-mrac-arch], the End User is required to obtain a ticket from a multicast service provider, which authorizes him/her to participate in the multicast group. The ticket contains the certification and the session descriptor mentioned in Section 1. The certification is carried as a payload by EAP, and the EAP message is presented to the PaC for transmission to the PAA. The certification will be (in most cases) validated by the AAAS.

The PAA is responsible for managing the negotiation with a PaC, usually with the help of the AAAS, that will authorize the End User to join the multicast group. Once the authorization has been achieved, the PAA is responsible for informing the EP that the access to the multicast group can be permitted, and what its responsibilities are with regard to accounting.

The AAAS is responsible for validating the certification, and determining what accounting information must be collected related to the received multicast traffic.

The EP is responsible for allowing authorized PaCs to receive the multicast data while preventing others from doing so. In the case of controlling access to multicast groups, the EP is actually the access router (AR) that is one hop away from the PaC. In a multicast network, the multicast routing protocol designates one AR, called the Designated Router (DR), to join multicast groups on behalf of an End User device. It is clear that the DR takes the role of the EP to enforce the access to multicast groups. Since any AR is potentially designated as a DR, all ARs are considered as (potential) EPs.

To distinguish the role of the EP in this MRAC case from the role of EPs in general in the PANA environment, we will use the designator

mEP. In the simple case, there is only one mEP in the network segment (on the DR) and the PAA resides on the DR.

2.3. Framework

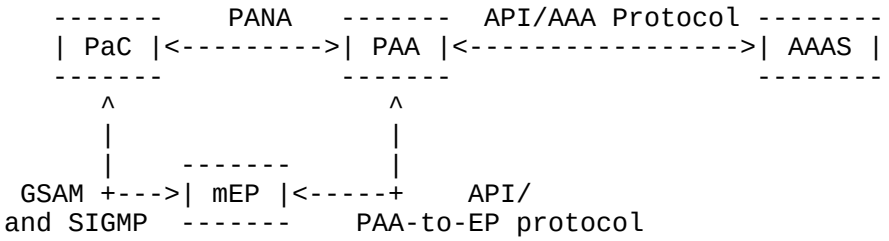

Figure 1: Receiver Access Control Framework

In an IP multicast network, the MRAC framework is as shown in Figure 1. A PaC interacts with a PAA using PANA, which carries the EAP authentication method to request the authorization for a multicast group. A PAA consults a AAAS for authentication and authorization of a PaC according to the EAP method carried in PANA. Moreover a PAA also communicates with the pertinent mEPs to forward the authorization attributes (mainly including the key derived from the EAP authentication method) of a PaC to the pertinent mEPs if a PaC is authorized. The mEPs establish IPsec SAs [RFC4301] with the authorized PaC according to the authorized attributes using a protocol called group security association management (GSAM) [I-D.atwood-pim-gsam]. A PaC then shows its interest in a multicast group to its mEP using the Secure IGMP (SIGMP) protocol [I-D.atwood-pim-sigmp] in an IPv4 network or using the Secure MLD (SMLD) protocol in an IPv6 network. The SIGMP packet or the SMLD packet is secured by an IPsec SA established during the GSAM negotiations. The mEP will join the multicast group on behalf of the authenticated and authorized PaCs and then send the multicast data to them. Usually the PaC is not allowed to forward the multicast data to any other device. The way to prevent forwarding is out of scope for this document.

If the PAA and the AAAS reside in the same device, an API is used to communicate between the PAA and the AAAS. Otherwise, a AAA protocol is usually needed, e.g., Diameter. Similarly, if the PAA and the mEP reside in the same device, an API is used to communicate between the PAA and the mEP. Otherwise, a PAA-to-EP protocol is needed. Possible candidates include, but are not limited to, COPS, SNMP, Diameter, etc.

This draft shows how to share the authorization attributions between a PaC and its mEP. The creation of the IPsec SAs and the protocols SIGMP and SMLD are out-of-scope for this draft. These topics are discussed in [I-D.atwood-pim-gsam], [I-D.atwood-pim-sigmp] and draft-atwood-pim-smld (not yet published) respectively.

3. Receiver Access Control Process in IP Multicast

As defined in [RFC5191], a PANA session has five phases. In our MRAC system, the five phases are explained as follows.

3.1. Handshake Phase

The handshake phase is triggered when a PaC receives the request to establish IPsec SAs in its local GSAM instance. In this phase, a PaC sends a PANA-Client-Initiation message to the PAA to initiate a PANA session. In MRAC, only PaC may initiate a PANA session rather than both a PAA and a PaC as described in [RFC5191]. A PaC may use its local configuration or DHCP to discover its PAA.

3.2. Authentication and Authorization Phase

Immediately following the handshake phase, a PAA and a PaC interact using both PANA-Auth-Request message and PANA-Auth-Answer message in the authentication and authorization phase. The EAP method is carried in the PANA message. The certification that the PaC possesses is encapsulated in one of the EAP packets and is delivered from a PaC to a PAA. A PAA will consult the AAAS using an API or a AAA protocol for authentication and authorization based on the EAP method and then convey the result to a PaC.

On successful authentication, a PANA Master Session Key (PANA MSK) becomes known to the PAA and the PaC as a result of the EAP exchanges. At the network side, the PAA must combine the PANA MSK with EP-specific information to produce the PaC-EP Master Key (PEMK), which is then forwarded (securely) to the pertinent mEP(s) using an API (when the PAA and the mEP are located in the same device) or a PAA-to-EP protocol (when the PAA and mEP are located in different devices). The rules for doing this are specified in [RFC5807]. The mEP must, in turn, combine this PEMK with group-specific information to produce the Multicast Session-Specific Key (MSSK), which will be used in GSAM to establish an IPsec SA to permit the network-level joining of the End User. On the End User device, the PaC must store the PANA MSK itself, since it does not know the identification of its mEP at this time. On the End User device, the work to calculate the MSSK based on the PANA MSK is assigned to GSAM. The details of how to calculate the PEMK and the MSSK will be shown in Section 4.

In order to achieve strong security, the EAP method carried in the PANA messages is required to provide the function of dynamic key exchange. Here the EAP-FAST method is recommended.

At the end of this phase, both a PaC and its mEP have calculated the keys (PaC calculates PANA MSK and mEP calculates MSSK) for authentication and authorization at the network layer. For the network layer join, the PaC will use an SIGMP message protected by an IPsec SA to show its interest in a specific group that has been authorized at the application layer. The details of the network layer interactions may be found in [I-D.atwood-pim-sigmp] and [I-D.atwood-pim-gsam].

3.3. Access Phase

On the one hand, a PaC and a PAA use the PANA message to test peer liveness in a PANA session. On the other hand, the multicast data is distributed from the mEP to the network on which the PaC resides.

3.4. Re-authentication Phase

The re-authentication phase is triggered when the access lifetime specified as the PANA session lifetime needs to be extended. In this phase, the EAP authentication carried in PANA messages is re-executed between a PaC and a PAA.

Upon successful re-authentication, access control re-enters the access phase. The lifetime of the PANA session is extended. Moreover a PAA notifies the pertinent mEPs to extend the lifetime of the authentication attributes of the PaC. However, if re-authentication fails, the PANA session must be terminated. Moreover, a PAA notifies mEPs to revoke the access authorization of a PaC.

3.5. Termination Phase

Either a PaC (i.e., disconnect indication) or a PAA (i.e., session revocation) may initiate the termination of the access authorization at any time. On the one hand, they use PANA-Termination-Request and PANA-Termination-Answer message exchanges to terminate the PANA session between them. On the the other hand, a PAA uses an API or a PAA-to-EP protocol to notify mEPs to revoke the access authentication of a PaC.

4. Cryptographic Keys

At the end of the authentication and authorization phase, a PaC and a PAA share the same secret key (PANA MSK). A PAA will derive a separate PaC-EP-Master-Key (PEMK) as follows [RFC5807]:

PEMK = prf+(MSK,"IETF PEMK"|SID|KID|mEPID)

Here, "|" means concatenation of different fields and prf+ is a pseudo-random function defined in [RFC5996]. "IETF PEMK" is the ASCII code representation, SID is a four-octet Session Identifier, KID is associated with the MSK and mEPID is the identifier of the mEP.

A PaC may be authorized to join more than one multicast group in one PANA session. For each multicast group, a separate Multicast Group-Specific Key (MSSK) is derived from the PEMK using the following method:

MSSK = HMAC-SHA-1(PEMK,"MSSK"|MSSInf|SID|KID|mEPID).

Here, "MSSK" is the ASCII code representation, SID is a four-octet Session Identifier, KID is associated with the PEMK and mEPID is the identifier of the mEP. MSSInf is the multicast group-specific information.

5. IANA Considerations

This document has no actions for IANA.

6. References

6.1. Normative References

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

[RFC5191] Forsberg, D., Ohba, Y., Patil, B., Tschofenig, H., and A. Yegin, "Protocol for Carrying Authentication for Network Access (PANA)", RFC 5191, May 2008.

[RFC5807] Ohba, Y. and A. Yegin, "Definition of Master Key between PANA Client and Enforcement Point", RFC 5807, March 2010.

6.2. Informative References

[I-D.atwood-mboned-mrac-arch] Atwood, B., Li, B., and S. Islam, "Architecture for IP Multicast Receiver Access Control", draft-atwood-mboned-mrac-arch-01 (work in progress), July 2014.

[I-D.atwood-mboned-mrac-req]
Atwood, B., Islam, S., and B. Li, "Requirements for IP Multicast Receiver Access Control", draft-atwood-mboned-mrac-req-01 (work in progress), July 2014.

[I-D.atwood-pim-gsam]
Atwood, B. and B. Li, "Group Security Association Management Protocol", draft-atwood-pim-gsam-00 (work in progress), July 2014.

[I-D.atwood-pim-sigmp]
Atwood, B. and B. Li, "Secure Internet Group Management Protocol", draft-atwood-pim-sigmp-01 (work in progress), July 2014.

[RFC3740] Hardjono, T. and B. Weis, "The Multicast Group Security Architecture", RFC 3740, March 2004.

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

[RFC5996] Kaufman, C., Hoffman, P., Nir, Y., and P. Eronen, "Internet Key Exchange Protocol Version 2 (IKEv2)", RFC 5996, September 2010.

Authors' Addresses

William Atwood
Concordia University/CSE
1455 de Maisonneuve Blvd, West
Montreal, QC H3G 1M8
Canada

Phone: +1(514)848-2424 ext3046
Email: william.atwood@concordia.ca
URI: http://users.encs.concordia.ca/~bill

Bing Li
Normal College of Shenzhen University
Nanhai Ave 3688
Shenzhen, Guangdong 518060
China

Phone: +86(0755)26558364
Email: libingice@szu.edu.cn

Salekul Islam
North South University
House 80, Road 8/A, Mirza Golam Hafiz Road
Dhanmondi, Dhaka 1209
Bangladesh

Email: salekul@northsouth.edu