MSEC Working Group
Internet-Draft
Intended status: Standards Track
Expires: March 15, 2012

B. Weis
S. Rowles
Cisco Systems

September 12, 2011

GDOI Generic Message Authentication Code Policy
draft-weis-gdoi-mac-tek-03

Abstract

A number of IETF signaling and routing applications require a set of devices to share the same policy and keying material and include a message authentication code in their protocols packets for authentication . It is often beneficial for this keying material to be chosen dynamically using a group key management protocol. This memo describes the policy required for the Group Domain of Interpretation (GDOI) group key management system to distribute a message authentication code key and associated policy.

Status of this Memo

This Internet-Draft is submitted 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 March 15, 2012.

Table of Contents

1. Introduction

The Group Domain of Interpretation (GDOI) [I-D.ietf-msec-gdoi-update] is a group key management protocol fitting into the Multicast Security Group Key Management Architecture [RFC3740]. GDOI is used to disseminate group security policy and keying material to group members for use with a particular cryptographic system. GDOI describes the distribution of group security policy and keying material for network traffic protected by IPsec [RFC4301], however group security policy and keying material for other types of cryptographic systems can also be distributed by GDOI as well.

A number of transport and routing protocol specifications specify a MAC to provide packet authentication between devices. When the protocol instantiation includes a group of devices, they all need to share a common set of authentication policy and keying material to create and validate the Message Authentication Code (MAC) included in protocol packets. The requirements for each of the protocol specifications are generally similar. This document describes how GDOI can be used to distribute the group authentication policy and keying material for these protocols.

This memo refers to candidate protocol specifications as "applications" of the GDOI Generic Message Authentication Code Policy. Policy distribution for two applications is described: Resource reSerVation Protocol (RSVP) and Network Layer Signaling (NLS).

1.1. Scope

This memo is intended to provide policy for applications not specifying the use of ESP [RFC4303] or AH [RFC4302] for authentication. Such applications SHOULD use the relevant payload definitions described in [I-D.ietf-msec-gdoi-update]. Group applications requiring the use of encryption MUST NOT use payloads described in this memo, and are encouraged to use ESP.

1.2. Requirements notation

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. GDOI Discussion

This section provides a short informative discussion of the GDOI group key management protocol. For definitive information regarding the GDOI protocol, please refer to [I-D.ietf-msec-gdoi-update]. For more information on group security, please refer to RFC 3740.

The GDOI group key management protocol actively manages security policy and keying material for a set of group members. GDOI begins operation when a client application on the group member initiates a request to the GDOI subsystem on the group member. The GDOI subsystem "registers" to a GDOI Group Controller/Key Server (GCKS) device using the GROUPKEY_PULL protocol. The group member and GCKS setup a private and authenticated exchange. After successful authentication and authorization, the GCKS provides group security policy and keying material to the GDOI subsystem on the group member. When the GDOI subsystem on the group member receives both security policy and keying material, it makes it available to the client application on the device that originally requested the MAC policy.

The GDOI key server also distributes policy and keys that describe how it will distribute updates to group policy over time. Described in GDOI as the GROUPKEY_PUSH message, it is more generally known as a "rekey" message. Rekey messages are typically distributed as IP multicast packets. They provide replacement security policy and keying material to group members (e.g., prior to a key expiration) or to revoke group members in a manner that is non-disruptive to the extant group members.

3. New GDOI Payload Definitions

The following sections describe how the GDOI Generic Message Authentication Code Policy is applied to GDOI protocol payloads. There are two affected payloads: the Security Association (SA) payload and the Key Download (KD) payload.

The GDOI SA payload includes a set of SA attribute payloads, including an SA attribute payload which distributes a definition of the traffic to be secured. This payload is known as the SA TEK. This memo describes a new type of SA TEK for distributing GDOI Generic Message Authentication Code Policy. For more information on the SA TEK attribute payload, please refer to Section 5.5 of [I-D.ietf-msec-gdoi-update].

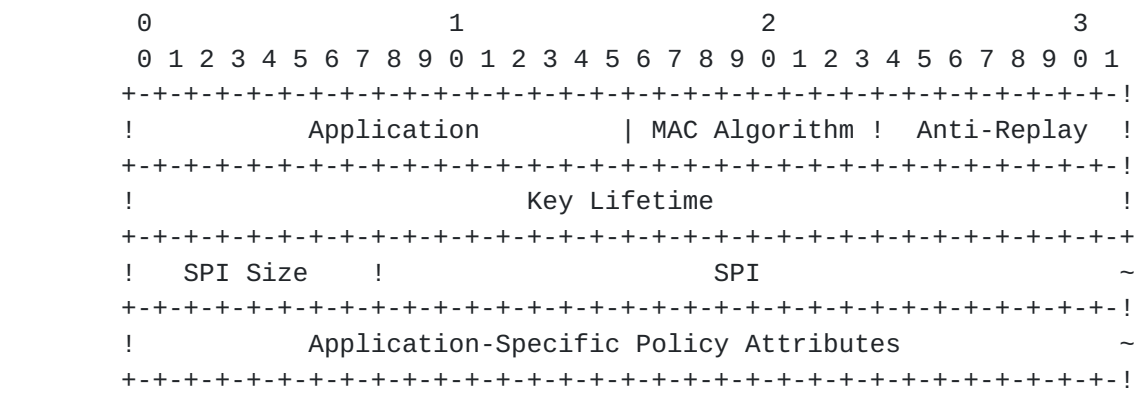
The GDOI KD payload carries keying material associated with policy previously distributed in SA attribute payloads. This memo does not define any new types of key policy for the Message Authentication Protocol Policy, but does place restrictions on the types of keys that can be distributed.

3.1. Message Authentication Code Policy SA TEK

This section describes the SA TEK payload used to distribute MAC policy. Protocols that use a MAC typically define a limited number of policy attributes associated with the MAC. These policy attributes are described in the MAC SA TEK.

The GDOI subsystem on a group member must maintain separation between client applications, and as such needs to know what application requested a particular set of policy. Thus, the SA TEK includes an Application field naming the correct application with the group member. In some instances, client applications define additional policy, and this policy is described in a set of application-specific policy attributes attached to the SA TEK.

A GDOI key server may distribute more than on SA TEK for a particular Application. In particular, the Application-Specific Policy Attributes may describe discrete instances of an application.



The SA TEK Payload fields are defined as follows:

- Application (2 octets -- Value describing the client application. Application types are defined below. Values are defined in the IANA Considerations section.

- MAC Algorithm (1 octet) -- Value specifying which Message Authentication Code (MAC) used to generate MAC. MAC Algorithm types are defined below. Values are defined in the IANA Considerations section.

- Anti-Replay (1 octet) -- Value specifying the type of anti-replay protection that is used with this application. Anti-replay types are defined below. Values are defined in the IANA Considerations section.

- Key Lifetime (4 octets) -- Value specifying the remaining lifetime of the SA TEK, in seconds. A time of zero indicates that the use of this policy does not terminate based on time.

- SPI Size (1 octet) -- Length (in octets) of the SPI associated with this SA TEK.

- SPI (Variable) -- Value describing the identity of the key. The key identifier uniquely defines an SA TEK.

- Application-Specific Policy Attributes (Variable) -- TLV policy attributes specific to this application. These attributes are defined by client application-specific policy.

3.1.1. Application Types

The following Client Applications are defined for use with the MAC SA TEK.

- RSVP. The Resource reSerVation Protocol [RFC3097]

- NLS. Network Layer Signaling protocol [I-D.shore-nls-tl]

Other protocols may be defined for use with the Generic Message Authentication Code Policy SA TEK. However, they must first satisfy the requirements described in Section 4.

3.1.2. MAC Algorithm Types

The following MAC algorithms are defined for use with this TEK.

- HMAC-MD5. The MD5 algorithm used with an HMAC construction [RFC2104]. This MAC algorithm is considered weak, but is required by some protocols.

- HMAC-SHA1-96. The SHA1 algorithm used with an HMAC construction, with a length truncated to 96 bits.[RFC2104].

3.1.3. Anti-Replay Types

The following methods of constructing sequence numbers is defined for use with this TEK.

- NONE. This value indicates that no anti-replay protection is used with this TEK.

- COUNTER. Counters (also known as sequence numbers) provide anti-replay protection in an application-specific manner.

- TIME. Values from a clock are used for replay protection in an application-specific manner.

3.1.4. Application-Specific Policy Attributes

Application-Specific Attributes are defined for each application that requires them. The attributes must follow the format defined in ISAKMP [RFC2408] Section 3.3. In the table, attributes that are defined as TV are marked as Basic (B); attributes that are defined as TLV are marked as Variable (V). Values are defined in the IANA Considerations section.

3.2. Key Packet definition for MACs

Keying material is distributed in a Key Packet as part of the GDOI KD payload. The Key packet is formed as follows.

- KD Type. The type of KD MUST be TEK.
- SPI. The SPI from the SA TEK is placed in the SPI field.
- Key. The keying material for the MAC algorithm is placed in a TEK_INTEGRITY_KEY attribute.

The Key Packet MUST NOT contain a TEK_ALGORITHM_KEY or TEK_SOURCE_AUTH_KEY attribute.

4. RSVP

The RSVP protocol provides a means for establishing resource reservations between cooperating systems. To ensure the integrity of the associated reservation and admission control mechanisms, the RSVP INTEGRITY Option defined in [RFC2747] and [RFC3097] may be used. These protect RSVP message integrity hop-by-hop and provide node authentication as well as replay protection, thereby protecting against corruption and spoofing of RSVP messages. In some network configurations, a group of cooperating devices exchange RSVP packets such that the sender of an RSVP packet cannot determine a priori which RSVP device will be receiving it. These cooperating devices can benefit from sharing the same group policy and keying material. [I-D.ietf-tsvwg-rsvp-security-groupkeying] presents a framework for RSVP security using dynamic group keying and discusses its applicability. In line with this framework, this section describes extensions to GDOI for distribution of security policy and keying material for RSVP.

The policy distributed in this section meets the key management assumptions made by the RSVP Security Properties memo [RFC4230].

4.1. RSVP SA TEK Policy

The following describes how the RSVP Integrity object policy is represented in the MAC SA TEK payload.

- MAC Algorithm. This field maps to the Keyed Message Digest field of the RFC 2747 INTEGRITY Object. Supported algorithms are: HMAC-MD5 and HMAC-SHA1-96.

- Anti-Replay. COUNTER and TIME types are both valid types of anti-replay protection. See a discussion of how they are used below.

- Key Lifetime. If the KeyStartValid optional attribute is included in the SA TEK, this lifetime specifies the entire lifetime of the SA TEK. Otherwise, it represents the partial remaining lifetime.

- SPI. This field matches the Key Identifier in the RFC 2747 INTEGRITY Object, and

- SPI Size. The length of the SPI MUST be 1 to 6 octets.

4.2. Anti-Replay Discussion

COUNTER corresponds to the Simple Sequence Numbers method defined in Section 3.1 of RFC 2747. When COUNTER based sequence numbers are used, each group member maintains its own sequence number for a given

group in order to set the sequence number field in RSVP messages generated in this group. Therefore, an RSVP receiver MUST track received sequence numbers separately for each RSVP neighbour in order to reliably distinguish between new and replay messages.

TIME corresponds to the Sequence Numbers Based on a Real Time Clock method described in Section 3.2 of RFC 2747 or the Sequence Numbers Based on a Network Recovered Clock method described in Section 3.3 or RFC 2747.

4.3. Application-specific attributes

- KeyStartValid (V). This attribute specifies an real time in the future when the TEK will take effect [RFC2747]. Note that the corresponding KeyEndValid time defined in RFC 2747 is not distributed by GDOI, but is computed by adding the Key Lifetime value to KeyStartValid. The KeyStartValid value is represented as the number of seconds since 0 hours, 0 minutes, 0 seconds, January 1, 1970.

5. NLS

NLS [I-D.shore-nls-tl] is a core protocol for a generalized on-path request protocol that is being used today to carry topology discovery and other requests. NLS specifies the use of group security, where group members share a MAC key. A MAC result is carried in the NLS A_RESPONSE and B_RESPONSE TLVs, which consummate authenticated nonce exchanges. A MAC result is also carried in the NLS AUTHENTICATION TLV, which is used to ensure integrity of NLS messages. This TLV also includes a Sequence Number for anti-replay protection. NLS associates a set of Application Group IDs (AGIDs) with a particular MAC key. Each AGID represents a unique authorization, within the context of a particular NLS group.

5.1. NLS SA TEK Policy

The following describes how NLS policy is represented in the MAC SA TEK payload.

- MAC Algorithm. This field maps to the Keyed Message Digest field of the RFC 2747 INTEGRITY Object. Supported algorithms are: HMAC-SHA1-96.

- Anti-Replay. The COUNTER type of anti-replay protection is supported.

- Key Lifetime. NLS does not specify a validity period for policy. This field MUST be set to zero.

- SPI. NLS does not specify a key identifier, but this field is used by GDOI to synchronize policy distributed in an MAC SA TEK and KD payloads.

- SPI Size. The length of the SPI MUST be 4 octets.

5.2. Application-specific attributes

- AGID (V). This attribute specifies a single NLS AGID that is associated with this policy. Multiple AGIDs attributes (each specifying a unique AGID) MAY be included in the SA TEK.

- Authz (V). This attribute contains a token used for authorization. The format and usage of this authorization token is outside of the scope of this memo.

6. Requirements for adding additional application support

Any memo supporting the definitions in the memo MUST include the following information relating to the application:

- Define an Application Type mnemonic, and provide a reference to a document describing the protocol specification.
- Define a set of MAC algorithms.
- Define anti-replay types.
- Define key lifetime parameters.
- Define valid SPI values and lengths.
- Description of Optional Attributes.

7. IANA Considerations

A new GDOI SA TEK type Protocol-ID type [GDOI-REG] should be assigned from the Unassigned space. The new algorithm id should be called GDOI_PROTO_MAC, and refers to the Message Authentication Code Policy SA TEK described in Section 3.1 of this memo.

Terms describing policies for allocating new name space types below are defined in [RFC5226].

The following applications are defined as part of this memo.

Application Type	Value
RESERVED	0
RSVP	1
NLS	2
Specification Required	3-127
Private Use	128-255

The following MAC Algorithms are defined as a part of this memo.

MAC Algorithm Type	Value
RESERVED	0
HMAC-MD5	1
HMAC-SHA1-96	2
Specification Required	3-127
Private Use	128-255

The following Sequence Number Types are defined as a part of this memo.

Sequence Number Type	Value
RESERVED	0
COUNTER	1
TIME	2
Specification Required	3-127
Private Use	128-255

The following Optional Attributes are defined as part of this memo, used with an Application of type RSVP.

RSVP Optional Attribute	Value
RESERVED	0
KeyStartValid	1
Specification Required	2-127
Private Use	128-255

The following Optional Attributes are defined as part of this memo, used with an Application of type NLS.

NLS Optional Attribute	Value
RESERVED	0
AGID	1
Authz	2
Specification Required	3-127
Private Use	128-255

8. Security Considerations

This memo describes the passing of policy and keying material used by two applications: an RSVP speaker producing an RFC 2747 INTEGRITY Object, and an NLS speaker producing A_RESPONSE, B_RESPONSE, and AUTHENTICATION TLVs. This policy and keying material is protected by the GDOI protocol described in [I-D.ietf-msec-gdoi-update]. The security considerations in that memo apply fully to this memo as well.

The use of the MAC SA TEK to distribute policy and keys is only appropriate when the application is using a group security model. [I-D.ietf-tsvwg-rsvp-security-groupkeying] describes the circumstances when a group security model may be used with RSVP. NLS always uses a group security model.

9. References

9.1. Normative References

[I-D.ietf-msec-gdoi-update]
Weis, B., Rowles, S., and T. Hardjono, "The Group Domain of Interpretation", draft-ietf-msec-gdoi-update-11 (work in progress), August 2011.

9.2. Informative References

[GDOI-REG]
Internet Assigned Numbers Authority, "Group Domain of Interpretation (GDOI) Payload Type Values", IANA Registry, December 2004, <http://www.iana.org/assignments/gdoi-payloads>.

[I-D.ietf-tsvwg-rsvp-security-groupkeying]
Behringer, M., Faucheur, F., and B. Weis, "Applicability of Keying Methods for RSVP Security", draft-ietf-tsvwg-rsvp-security-groupkeying-11 (work in progress), September 2011.

[I-D.shore-nls-tl]
Shore, M., McGrew, D., and K. Biswas, "Network-Layer Signaling: Transport Layer", draft-shore-nls-tl-06 (work in progress), July 2008.

[RFC2104] Krawczyk, H., Bellare, M., and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication", RFC 2104, February 1997.

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

[RFC2408] Maughan, D., Schneider, M., and M. Schertler, "Internet Security Association and Key Management Protocol (ISAKMP)", RFC 2408, November 1998.

[RFC2747] Baker, F., Lindell, B., and M. Talwar, "RSVP Cryptographic Authentication", RFC 2747, January 2000.

[RFC3097] Braden, R. and L. Zhang, "RSVP Cryptographic Authentication -- Updated Message Type Value", RFC 3097, April 2001.

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

[RFC4230] Tschofenig, H. and R. Graveman, "RSVP Security Properties", RFC 4230, December 2005.

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

[RFC4302] Kent, S., "IP Authentication Header", RFC 4302, December 2005.

[RFC4303] Kent, S., "IP Encapsulating Security Payload (ESP)", RFC 4303, December 2005.

[RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 5226, May 2008.

Authors' Addresses

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

Phone: +1-408-526-4796
Email: bew@cisco.com

Sheela Rowles
Cisco Systems
170 W. Tasman Drive
San Jose, California 95134-1706
USA

Phone: +1-408-527-7677
Email: srowles@cisco.com