Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: September 11, 2017

B. Weis
Cisco Systems
U. Mangla
Juniper Networks Inc.
T. Karl
Deutsche Telekom
N. Maheshwari

March 10, 2017

GDOI GROUPKEY-PUSH Acknowledgement Message
draft-weis-gdoi-rekey-ack-05

Abstract

The Group Domain of Interpretation (GDOI) includes the ability for a Group Controller/Key Server (GCKS) to provide a set of current Group Member (GM) devices with additional security associations (e.g., to rekey expiring security associations). This memo adds the ability of a GCKS to request the GM devices to return an acknowledgement of receipt of its rekey message, and specifies the acknowledgement method.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

The Group Domain of Interpretation (GDOI) [RFC6407] is a group key management method by which a Group Controller/Key Server (GCKS) distributes security associations (i.e., cryptographic policy and keying material) to a set of Group Member (GM) devices. GDOI meets the requirement of the Multicast Security (MSEC) Group Key Management Architecture [RFC4046], and defines both a Registration Protocol and Rekey Protocol. GDOI describes the Rekey Protocol as a GROUPKEY-PUSH message.

A GDOI GCKS uses a GROUPKEY-PUSH message to alert group members to updates in policy for the group, including new policy and keying material, replacement policy and keying material, and indications of

deleted policy and keying material. Usually the GCKS does not require a notification that the group member actually received the policy. However, in some cases it is beneficial for a GCKS to be told by each receiving GM that it received the rekey message and by implication has reacted to the policy contained within. For example, a GCKS policy can use the acknowledgements to determine which GMs are receiving the current group policy and which members may no longer be members of the group.

This memo introduces a method by which a GM returns an acknowledgment message to the GCKS. Initially a GCKS requests GM to acknowledge GROUPKEY-PUSH messages as part of distributed group policy. Then (shown in Figure 1) when the GCKS delivers a GROUPKEY-PUSH message, each GM that honors the GCKS request returns a GROUPKEY-PUSH Acknowledgement Message. The rest of this memo describes this method in detail.

```
                GCKS                          GM1       GM2
                 |                             |         |
                 |                 +---------->|         |
                 |   GROUPKEY-PUSH |           |         |
                 |-----------------+           |         |
                 |                 |           |         |
                 |                 +-------------------->|
                 |                             |         |
                 |<----------------------------|         |
                 |      GROUPKEY-PUSH ACK      |         |
                 |                             |         |
                 |<--------------------------------------|
                 |      GROUPKEY-PUSH ACK      |         |
```

Figure 1: GROUPKEY-PUSH Rekey Event

Implementation of the GROUPKEY-PUSH Acknowledgement Message is OPTIONAL.

1.1. 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].

1.2. Acronyms and Abbreviations

The following acronyms and abbreviations are used throughout this document.

D	Delete Payload
GCKS	Group Controller/Key Server
GDOI	Group Domain of Interpretation
GM	Group Member
HDR	Header Payload
IV	Initialization Vector
KD	Key Download Payload
KDF	Key Derivation Function
KEK	Key Encryption Key
LKH	Logical Key Hierarchy
MSEC	Multicast Security
SA	Security Association
SEQ	Sequence Number Payload
SIG	Signature Payload
SPI	Security Parameter Index

2. Acknowledgement Message Request

When a GM is ready to join a group, it contacts the GCKS with a GROUPKEY-PULL Registration Protocol. When the GCKS has authenticated and verified that the GM is an authorized member of the group it downloads several sets of policy in a Security Association (SA) payload. If the group includes the use of a GROUPKEY-PUSH Rekey Protocol, the SA payload includes an SA Key Encryption Key (KEK) payload (Section 5.3 of [RFC6407]). When necessary the GROUPKEY-PUSH Rekey Protocol also contains an SA payload that includes SA KEK policy. The SA KEK policy indicates how the GM will be receiving and handling the GROUPKEY-PUSH Rekey Protocol.

When the GCKS policy includes the use of the GROUPKEY-PUSH Acknowledgement Message, the GCKS reports this policy to the GM within the SA KEK policy. The GCKS includes a new KEK Attribute with the name KEK_ACK_REQUESTED (value TBD-1), which indicates that the GM is requested to return a GROUPKEY-PUSH Acknowledgement Message. A GM receiving the KEK_ACK_REQUESTED attribute can choose to ignore it, thus appearing as if it does not support the KEK_ACK_REQUESTED attribute. However, GCKS policy may consider a non-responsive GM to no longer desire to be a member of the group.

As part of the SA KEK policy, the GCKS specifies information on the keying material, that is used to protect the GROUPKEY-PUSH Rekey Protocol (e.g. presence of KEK Management Algorithm). Parts of these information are used by a GM to derive the ack_key (defined in Section 3.2), which protects the GROUPKEY-PUSH Acknowledgement Message. There are different types of Rekey Acknowledgement messages, which share an identical message format but differ in the used keying material.

The following values of the KEK_ACK_REQUESTED attribute are defined in this memo.

2.1. REKEY_ACK_KEK Type

This type of Rekey ACK is used when the KEK KD Type (Section 5.6.2 of [RFC6407]) is part of the group policy. The base_key (defined in Section 3.2) is the KEK_ALGORITHM_KEY used to decrypt the GROUPKEY-PUSH message. Note that the KEK_ALGORITHM_KEY may include an explicit Initialization Vector (IV) before the actual key (Section 5.6.2.1 of [RFC6407]), but it is not used in the definition of the base_key.

2.2. REKEY_ACK_LKH Type

This type of Rekey ACK can be used when the KEK_MANAGEMENT_ALGORITHM KEK attribute with a value representing Logical Key Hierarchy (LKH) is part of the group policy (Section 5.3.1.1 of [RFC6407]). The base_key is the Key Data taken from the first LKH Key structure in an LKH_DOWNLOAD_ARRAY attribute (see Section 5.6.3.1 of [RFC6407]). This is a private key that the GCKS shares with the group member. Note that the LKH Key structure may include an explicit IV before the actual key (Section 5.6.3.1 of [RFC6407]), but it is not used in the definition of the base_key.

3. GROUPKEY-PUSH Acknowledgement Message

The GROUPKEY-PUSH message defined in [RFC6407] is reproduced in Figure 2. The SA and Key Download (KD) payloads contain the actual policy and keying material being distributed to the GM. The Sequence Number (SEQ) payload contains a sequence number that is used by the GM for replay protection. This sequence number defines a unique rekey message delivered to that GM. One or more Delete (D) payloads optionally specify the deletion of existing group policy. The Signature (SIG) payload includes a signature of a hash of the entire GROUPKEY-PUSH message (excepting the SIG payload octets) before it has been encrypted

```
            GM                                    GCKS
            --                                    ----
                <---- HDR*, SEQ, [D,] SA, KD, SIG

    * Protected by the Rekey SA KEK; encryption occurs after HDR
```

Figure 2: GROUPKEY-PUSH from RFC 6407

When the GM has received a KEK_ACK_REQUESTED attribute in an SA KEK and it chooses to respond, it returns the value of the Sequence Number taken from the GROUPKEY-PUSH message to the GCKS along with its identity. This tuple alerts the GCKS that the GM has received the GROUPKEY-PUSH message and implemented the policy contained therein. The GROUPKEY-PUSH Acknowledgement Message is shown in Figure 3.

```
                   GM                               GCKS
                   --                               ----
                      HDR, HASH, SEQ, ID   ---->
```

Figure 3: GROUPKEY-PUSH Acknowledgement Message

The IP header for the GROUPKEY-PUSH Acknowledgement Message is constructed as if it were a reply to the GROUPKEY-PUSH message. That is, the Source Address of the GROUPKEY-PUSH message becomes the Destination Address of the GROUPKEY-PUSH Acknowledgement Message and the GM includes its own IP address as the Source Address of the GROUPKEY-PUSH Acknowledgement Message. The Source port in the GROUPKEY-PUSH message UDP header becomes the Destination port of the GROUPKEY-PUSH Acknowledgement Message UDP header, and the Destination port of the GROUPKEY-PUSH message UDP header becomes the Source port of the GROUPKEY-PUSH Acknowledgement Message UDP header.

The following sections describe the payloads in the GROUPKEY-PUSH Acknowledgement Message.

3.1. HDR

The message begins with a header as defined for the GDOI GROUPKEY-PUSH message in Section 4.1 of [RFC6407]. The fields in the HDR must be initialized as follows. The Cookies of a GROUPKEY-PUSH message act as a Security Parameter Index (SPI) and are copied to the Acknowledgement Message. Next Payload identifies a Hash payload (8). Major Version is 1 and Minor Version is 0. The Exchange Type has value 35 for the GDOI GROUPKEY-PUSH Acknowledgment Message. Flags are set to 0. Message ID MUST be set to zero. Length is according to Section 4.1 of [RFC6407]).

3.2. HASH

The HASH payload is the same one used in the GDOI GROUPKEY-PULL exchange defined in Section 3.2 of [RFC6407]. The hash data in the HASH payload is created as follows:

```
HASH = prf(ack_key, SEQ | ID)
```

where:

- o prf is PRF-HMAC-SHA-256 [RFC4868].
- o "|" indicates concatenation.
- o SEQ and ID represent the bytes comprising the Sequence Number and Identification Payloads

The ack_key is computed from a Key Derivation Function (KDF) that conforms to KDF in Feedback Mode as defined in NIST SP800-108 [SP800-108] where the length of the derived keying material is the same as the output of the prf, there is no initialization vector, and the optional counter is not used. Note: When the derived ack_key is smaller than the prf block size (i.e., 512 bits for PRF-HMAC-SHA-256), it is zero filled to the right, as specified in Section 2.1.2 of [RFC4868].

```
ack_key = prf(base_key, "GROUPKEY-PUSH ACK" | SPI | L)
```

where:

- o prf is PRF-HMAC-SHA-256 [RFC4868].
- o base_key is specific to the KEK_ACK_REQUESTED value, and is described as part of that description. If the base_key is smaller than the prf block size (i.e., 512 bits for PRF-HMAC-SHA-256),

then it is zero filled to the right, as specified in Section 2.1.2 of [RFC4868].

- o "|" indicates concatenation.

- o "GROUPKEY-PUSH ACK" is a label encoded as a null terminated ASCII string.

- o SPI is the Initiator Cookie followed by the Responder Cookie taken from the GROUPKEY-PUSH message HDR, which describes the Context of the key usage.

- o L is a length field matching the number of bits in the ack_key. L MUST match the length of the base_key (i.e., 512 bits for PRF-HMAC-SHA-256). The value L is represented as two octets

3.3. SEQ

The Sequence Number Payload is defined in [RFC6407]. The value in the GROUPKEY-PUSH SEQ payload is copied to the SEQ payload.

3.4. ID

The Identification payload is used as defined in Section 5.1 of [RFC6407]. The ID payload contains an ID Type of ID_IPV4_ADDR, ID_IPV6_ADDR, or ID_OID as defined for GDOI exchanges [I-D.weis-gdoi-iec62351-9]. Protocol ID and Port fields MUST be set to 0. The address provided in the ID payload represents the IP address of the GM, and MUST match the source IP address used for the most recent GROUPKEY-PULL exchange.

4. Group Member Operations

When a GM receives an SA KEK payload (in a GROUPKEY-PULL exchange or GROUPKEY-PUSH message) including a KEK_ACK_REQUESTED attribute, it records in its group state some indication that it is expected to return a GROUPKEY-PUSH ACK message. A GM SHOULD honor the KEK_ACK_REQUESTED attribute by sending acknowledgments, because it can be expected that the GCKS is likely to take some policy-specific action regarding non-responsive GMs, including ceasing to deliver GROUPKEY-PUSH messages to it.

If a GM does not intend to respond with Acknowledgements, or cannot respond with the requested type of Acknowledgement, it continues with protocol exchange and participates in the group. In any case, if a GM stops receiving GROUPKEY-PUSH messages from a GCKS it will re-register before existing security associations expire, so omitting sending Acknowledgements should not be critical.

When a GM receives a GROUPKEY-PUSH message that contains a KEK_ACK_REQUESTED attribute in the SA KEK payload, it processes the message according to RFC 6407. When it concludes successful processing of the message, it formulates the GROUPKEY-PUSH ACK messages as described in Section 3 and delivers the message to the GCKS from which the GROUPKEY-PUSH message was received. A GROUPKEY-PUSH ACK message is sent even if the GROUPKEY-PUSH message contains a Delete payload for the KEK used to protect the GROUPKEY-PUSH message.

5. GCKS Operations

When a GCKS policy includes requesting a GROUPKEY-PUSH ACK message from Group Members, it includes the KEK_ACK_REQUESTED attribute in the SA KEK payload. It does this each time the SA KEK is delivered, in both GROUPKEY-PULL exchanges and GROUPKEY-PUSH messages. The value of the KEK_ACK_REQUESTED attribute will depend upon the type SA KEK, as described in Section 2.

When a GCKS receives a GROUPKEY-PUSH ACK message (identified by an Exchange type of GROUPKEY-PUSH-ACK), it first verifies that the group policy includes receiving GROUPKEY-PUSH ACK messages. If not, the message is discarded.

If the message is expected, the GCKS validates the format of the message, and verifies that the HASH has been properly constructed as described in Section 3.2. If validation fails, the message is discarded. The GCKS extracts the sequence number and identity of the GM from the SEQ and ID payloads respectively, and records the fact that the GM received the GROUPKEY-PUSH message represented by its serial number.

6. Management Considerations

The GCKS manages both group policy and group membership of a group. Group membership policy includes a strategy to ensure that rekey messages with current group policy reach all live group members. This is discussed briefly in Section 5.3 of the MSEC Group Key Management Architecture [RFC4046]. The GROUPKEY-PUSH Acknowledgement message specified in this memo provides the GCKS an additional method to assess if a group member is live and has received the current group policy. But it is possible for a rekey message or GROUPKEY-PUSH Acknowledgement message to be discarded in the network, which results in a live GM to appear unresponsive. Also a GM may be willing or able to respond with an GROUPKEY-PUSH ACK. So the GCKS should use caution in using a lack of Acknowledgment as the only factor in determining whether a GM is live.

Some management considerations determining how a Group Member handle Acknowledgement messages is as follows:

- A GM SHOULD respond with Acknowledgement messages when requested, as a GCKS can subsequently determine when a GM becomes unexpectedly non-responsive.

- A GM MAY introduce a jitter to the timing of its Acknowledgement message to help the GCKS better manage replies from group members. The jitter SHOULD be no more than a few seconds.

Some management considerations determining how the GCKS handles Acknowledgement messages is as follows:

- A non-receipt of an Acknowledgement is an indication that a GM is either unable or unwilling to respond. A GCKS SHOULD wait at least several seconds before determining non-receipt, as GMs could add jitter to the response time before sending an acknowledgement.

- If the GCKS is aware that GMs are expected to respond, then a non-receipt of an Acknowledgement SHOULD trigger a logging event. The GCKS MAY be configured with additional policy actions such as alerting its administrators of GMs that do not return several consecutive acknowledgement messages or even removing unresponsive GMs from the group. However, a GCKS with a policy of removing GMs from the group needs to be aware that a GM that has chosen not to respond will not receive newer group policy until it initiates contact with the GCKS again.

- When a GROUPKEY-PUSH message includes a Delete payload for the KEK used to protect the GROUPKEY-PUSH message, the GCKS should not itself delete the KEK until it has given GMs the opportunity to acknowledge receipt of the GROUPKEY-PUSH message. This could be several seconds, as GMs could add jitter to the response time before sending an acknowledgement.

- A GCKS SHOULD log failure events, such as receiving Acknowledgement messages for a group in which the GCKS has not requested Acknowledgements, receiving malformed Acknowledgement, and Acknowledgements that fail validation.

7. Security Considerations

There are three areas of security considerations to consider: the protection of the GROUPKEY-PUSH ACK message, whether the GM should transmit a GROUPKEY-PUSH ACK, and whether a GCKS should accept a GROUPKEY-PUSH ACK. These are addressed in the following subsections.

The construction of the HASH defined in this memo uses PRF-HMAC-SHA-256. The strength of this PRF was unquestioned at the time this memo was developed. When a HASH construction is necessary using a different prf (i.e., providing algorithm agility), a new KEK_ACK_REQUESTED value will be defined in a new specification.

7.1. Protection of the GROUPKEY-PUSH ACK

The GROUPKEY-PUSH ACK message is an ISAKMP [RFC2408] message. Message authentication and Man-in-the-Middle Attack Protection is provided by the inclusion of a HASH payload, which includes the output of an HMAC computation (PRF-HMAC-SHA-256) over the bytes of the message.

When the value of REKEY_ACK_KEK is specified, because the KEK is a group secret impersonation of a victim GM by another authorized GM is possible. However, security considerations of the impersonation are limited to a false claim that a victim GM has received a GROUPKEY-PUSH when the victim GM has in fact not received it (e.g., because an active attacker has discarded the GROUPKEY-PUSH). If a GCKS policy includes sending retransmissions of the GROUPKEY-PUSH message to that victim GM, then the victim GM may not receive replacement security associations. However, this adds no additional threats over a use case where the GROUPKEY-PUSH ACK is not deployed and GROUPKEY-PUSH messages are withheld from a victim GM by an active attacker. These threats can be mitigated by using a value of REKEY_ACK_LKH, due to the use of a secret pairwise key shared between the GCKS and individual GM.

Confidentiality is not provided for the GROUPKEY-PUSH ACK message. The contents of the message can be observed by a passive attacker, which includes the hash value, the sequence number of in the GROUPKEY-PUSH message to which it is acknowledging receipt, and the identity of the GM. Observation of a hash value or set of hash values will not compromise the hash key. The identity of the GM is also available to the passive attacker as the source IP address of the packet. The sequence number does reveal the sequence number that was included in the GROUPKEY-PUSH, which was previously not available to the attacker. However, the attacker is assumed to not be in possession of the key used to encrypt the message, and thus cannot create a spoofed GROUPKEY-PUSH message. Therefore, there is no direct value that the attacker derives from the knowledge of the sequence number.

7.2. Transmitting a GROUPKEY-PUSH ACK

A GM transmits an ACK only when the policy of the most recently received SA KEK includes a request by the GCKS for ACKs, and only is returned after processing the GROUPKEY-PUSH message according to Section 4.4 of [RFC6407]. In other words, the form of the GROUPKEY-PUSH message will have been validated, replay protection completed, and the digital signature verified as being genuine. Therefore, the threats of a GM responding to a spoofed or resent GROUPKEY-PUSH message, and the possibility of the GM being used to propagate a Distributed Denial of Service (DDoS) attack on a GCKS are mitigated. For more information, see the security considerations of a GROUPKEY-PUSH message described in Section 7.3 of [RFC6407].

7.3. Receiving a GROUPKEY-PUSH ACK

A GCKS receiving ACK messages will follow the validation steps described in Section 5 before interpreting the contents of the message. The GCKS will then be sure to operate only on messages that have been sent by an authorized GM.

A GCKS SHOULD be prepared to receive GROUPKEY-PUSH ACK messages from each GM to which it was sent. That is, needs to ensure it has sufficient resources (e.g., receive queue size) so that it does not unnecessarily drop ACK messages. An GCKS should be aware that a large number of replayed or invalid GROUPKEY-PUSH messages could be addressed to it. However, this is no worse a threat than if it received a large number of other types of replayed or invalid GDOI or other messages containing a HASH payload.

GCKS implementations SHOULD keep a record (e.g., a hash value) of recently received GROUPKEY-PUSH Acknowledgment messages and reject duplicate messages prior to performing cryptographic operations. This enables an early discard of the replayed messages.

How a GCKS processes the serial number and identity included in an ACK message is a matter of local policy and is outside the scope of this memo.

8. IANA Considerations

The following additions are made to the GDOI Payloads [GDOI-REG] registry.

A new attribute is added to the SA KEK Payload Values - KEK Attributes registry. The ID Class name is KEK_ACK_REQUESTED with a value of TBD-1, and is a Basic attribute.

A new registry defining values for KEK_ACK_REQUESTED is needed, and these values are shown in the following table. The terms Reserved, Unassigned, and Private Use are to be applied as defined in [RFC5226]. The registration procedure is Specification Required.

Value	Type
0	Reserved
1	REKEY_ACK_KEK
2	REKEY_ACK_LKH
3-128	Unassigned
129-255	Private Use

A new registry describing ISAKMP Exchange Types for GDOI is added to GDOI Payloads [GDOI-REG]. This registry defines DOI Specific Use values [ISAKMP-REG], which are Exchange type values used with the ISAKMP GDOI DOI. Its name is "GDOI DOI Exchange Types". The registration procedure is Specification Required. The terms Reserved and Unassigned are to be applied as defined in [RFC5226].

Value	Phase	Reference
GROUPKEY-PULL	32	RFC 6407
GROUPKEY-PUSH	33	RFC 6407
Reserved	34	
GROUPKEY-PUSH-ACK	35	RFC XXXX
Unassigned	36-239	

[Note to RFC Editor: Please replace XXXX with the number of the RFC resulting from this memo, and delete this note.]

9. Acknowledgements

Mike Hamada and Adrian Farrel provided many useful technical and editorial comments and suggestions for improvement.

10. References

10.1. Normative References

[I-D.weis-gdoi-iec62351-9]
Weis, B., Seewald, M., and H. Falk, "GDOI Protocol Support for IEC 62351 Security Services", draft-weis-gdoi-iec62351-9-10 (work in progress), October 2016.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

[RFC4868] Kelly, S. and S. Frankel, "Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec", RFC 4868, DOI 10.17487/RFC4868, May 2007, <http://www.rfc-editor.org/info/rfc4868>.

[RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 5226, DOI 10.17487/RFC5226, May 2008, <http://www.rfc-editor.org/info/rfc5226>.

[RFC6407] Weis, B., Rowles, S., and T. Hardjono, "The Group Domain of Interpretation", RFC 6407, DOI 10.17487/RFC6407, October 2011, <http://www.rfc-editor.org/info/rfc6407>.

10.2. Informative References

[GDOI-REG] Internet Assigned Numbers Authority, "Group Domain of Interpretation (GDOI) Payload Type Values", IANA Registry, November 2016, <http://www.iana.org/assignments/gdoi-payloads/gdoi-payloads.xml>.

[ISAKMP-REG] Internet Assigned Numbers Authority, "Internet Key Exchange (IKE) Attributes Exchange Type Values", IANA Registry, May 2013, <http://www.iana.org/assignments/ipsec-registry/ipsec-registry.xhtml#ipsec-registry-17>.

[RFC2408] Maughan, D., Schertler, M., Schneider, M., and J. Turner, "Internet Security Association and Key Management Protocol (ISAKMP)", RFC 2408, DOI 10.17487/RFC2408, November 1998, <http://www.rfc-editor.org/info/rfc2408>.

[RFC4046] Baugher, M., Canetti, R., Dondeti, L., and F. Lindholm, "Multicast Security (MSEC) Group Key Management Architecture", RFC 4046, DOI 10.17487/RFC4046, April 2005, <http://www.rfc-editor.org/info/rfc4046>.

[SP800-108]
Chen, L., "Recommendation for Key Derivation Using Pseudorandom Functions", United States of America, National Institute of Science and Technology, NIST Special Publication 800-108, October 2009, <http://dx.doi.org/10.6028/NIST.SP.800-108>.

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

Umesh Mangla
Juniper Networks Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA

Phone: +1-408-936-1022
Email: umangla@juniper.net

Thomas Karl
Deutsche Telekom
Landgrabenweg 151
Bonn 53227
Germany

Phone: +49 228 18138122
Email: thomas.karl@telekom.de

Nilesh Maheshwari

Email: nileshm@gmail.com