

Internet Engineering Task Force
Internet Draft
[draft-ietf-msec-secure-feedback-00.txt](#)
Expires: Dec 2003

L. Dondeti, T. Hardjono
Nortel Networks, Verisign
Jun 2003

Securing Feedback Messages: Secure and Scalable Many-to-one Communication

STATUS OF THIS MEMO

This document is an Internet-Draft and is in full conformance with all provisions of [Section 10 of RFC2026](#).

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 view the list Internet-Draft Shadow Directories, see <http://www.ietf.org/shadow.html>.

Abstract

Members in a secure group may need to communicate to the GCKS to Deregister from the group, for SA resynchronization, or to request retransmission of a Rekey message. A simple solution is to keep the registration SA around, but that comes at the expense of $O(n)$ SA maintenance, and storage at the GCKS. Each member is also responsible for maintaining an extra SA. We propose an efficient method for members to securely send messages to the GCKS, using the Rekey SA.

Internet Draft [draft-ietf-msec-secure-feedback-00](#)

Table of Contents

- [1](#). Introduction to GSA
- [2](#). Need for Many-to-one Secure communication in Secure Groups
- [3](#). Proposed Solution
 - [3.1](#). Rekey Message
 - [3.2](#). Feedback Message
 - [3.3](#). Integrity Protection of Feedback Message
 - [3.4](#). Processing at the members
 - [3.5](#). Processing at the GCKS
- [4](#). Security Considerations
- [5](#). References
- [6](#). Authors' Contact Information

[1](#) Introduction to GSA

The GKM architecture [[1](#)] proposed by MSEC defines three SAs: Registration SA, Rekey SA and Data Security SA. These three SAs comprise the Group SA (GSA). The Registration SA protects member initialization process, and protects the downloading of Rekey and the Data Security SAs. At this point the GCKS uses a one-to-one secure channel, protected by the Registration SA, for secure communication.

The Rekey SA protects Rekey messages, which contain updates to the Rekey SA or a new Data Security SA. The Data Security SA protects data transmissions to the group.

For scalable operation, it is inefficient to keep the registration SAs alive, especially in large groups. Each registration SA may have to be stored and maintained (rekeyed periodically) from the time the corresponding member joins the group until it leaves. This is

Internet Draft [draft-ietf-msec-secure-feedback-00](#)

expensive due to the large state storage required and the computation and communication overhead due to SA maintenance.

[2](#) Need for many-to-one communication in secure groups

Secure communication in groups as defined in GKM architecture [\[1\]](#) is mostly one-way from the GCKS to the members (sender and receivers), and from the sender to the receivers. As noted earlier, the Rekey and the Data Security SAs are used to protect these communications.

But, from time to time members may need to contact the GCKS, for example, to request retransmission of a rekey message, for GSA synchronization, or to Deregister from the group.

[3](#) Proposed solution

We propose a scalable protocol to send feedback securely using the Rekey SA. Note that in most, if not all, group key management algorithms, the GCKS shares a unique key with each member. For example, in LKH, this key corresponds to the leaf node a member is associated with. We propose to use the unique key to protect the integrity of the feedback message.

The Sequence number from the lost or the most recently received rekey message can be used for replay protection. Such Sequence number use for feedback messages, allows efficient implementation at the GCKS. Specifically, the GCKS does not need to maintain per-member Sequence numbers.

[3.1](#) Rekey message

Our design of the feedback message is based on GDOI Rekey message (although there is no reason to believe that this won't work for GSAKMP rekey messages) or GROUPKEY-PUSH message:

Member	GCKS
-----	-----
<--- HDR*, SEQ, SA, KD, [CERT,] SIG	

* protected by the Rekey SA KEK; Everything after the HDR is encrypted

The HDR is an ISAKMP header. The SEQ payload contains a monotonically increasing sequence number. The SA payload can include one or more SAKEK payloads and zero or more SATEK payloads. The KD payload contains KEKs and TEKs corresponding to SAKEK and SATEK payloads. The

Internet Draft [draft-ietf-msec-secure-feedback-00](#)

SIG payload signs the hash of a message formed by concatenating the string "rekey" with the Rekey message (excluding SIG itself). The message is encrypted (excluding the HDR) using the group KEK.

[3.2](#) Feedback message

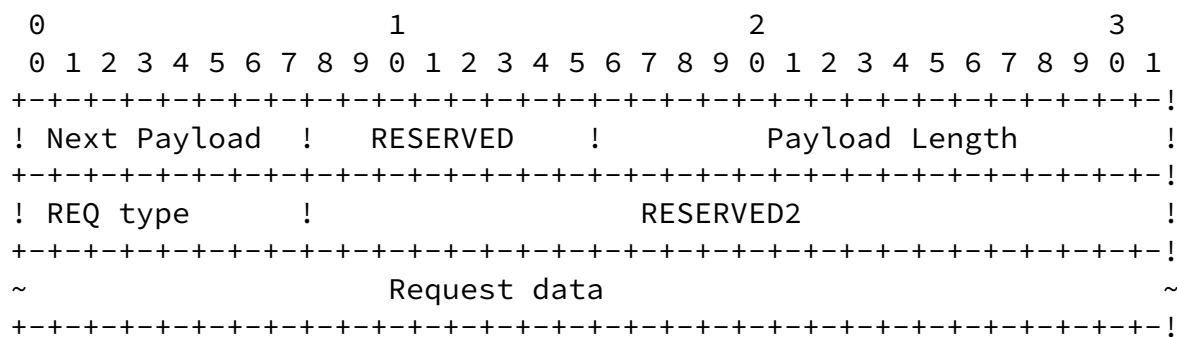
Member	GCKS
-----	-----
HDR*, SEQ, REQ, AUTH -->	

* protected by the leaf/unique KEK of member;
 Everything between the HDR and the AUTH payload is encrypted

The HDR is ISAKMP header payload (see [RFC2408](#) [2]) and is formed similar to that in GDOI (see Section 4.5 in [3]). The cookie pair is the same as in the recently received Rekey message. The next payload is the SEQ payload. The Exchange Type has a value for FEEDBACK-MESSAGE (to be assigned a number). Length is computed as specified in [RFC2408](#). The rest of the fields are the same as in the received message.

The SEQ payload contains the SEQ message in the most recently received GROUPKEY-PUSH message.

The REQ payload is new (to be assigned a payload number) and contains the Feedback message.



REQ type	value
-----	-----

Internet Draft [draft-ietf-msec-secure-feedback-00](#)

RESERVED	0
DE-REGISTER	1
RESYNC	2
NACKs	3
Future Use	
Private Use	

When REQ type is DE-REGISTER or RESYNC, there is no associated Request data. When REQ type is NACKs, Request data contains either a sequence of NACKs, or a range of NACKs, or a combination.

Note: We may need a separate payload definition for the various types of Request data.

[3.3](#) Integrity protection of FEEDBACK messages

The AUTH payload is also new and defined as follows. The LKH ID is defined as in GDOI spec . The AUTH data is a MAC computed over the entire FEEDBACK message excluding the AUTH payload itself.

```

      0               1               2               3
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+!
! Next Payload !   RESERVED   !           Payload Length           !
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+!
!               LKH ID         !           RESERVED2                !
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+!
~                               AUTH data                            ~
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+!

```

[3.4](#) Processing at the members

Members are aware of the Sequence number window maintained by the GCKS. Thus a member can send FEEDBACK messages only before the GCKS has used a Sequence number within the Sequence window of the Sequence number it received. Members may not know the Sequence number being used by the GCKS. Therefore, a member must maintain a timer waiting for a response to the FEEDBACK message. If the member does not receive a response before the time expires, it may have to restart with the Registration protocol.

[3.5](#) Processing at the GCKS

To process the FEEDBACK messages, the GCKS needs to allow them to have a Sequence number within a pre-defined window of the current Sequence number in the latest Rekey message from the GCKS.

[4](#) Security Considerations

The FEEDBACK message is encrypted, and authenticated. It provides replay protection within a window of the Sequence number in the Rekey messages. FEEDBACK messages are integrity protected using a MAC, which is not computationally intensive; thus, there is no threat of denial-of-service attacks using them. The number of FEEDBACK messages can be large, which is a potential problem (open to DoS attacks).

[5](#) Bibliography

- [1] M. Baugher, R. Canetti, L. Dondeti, and F. Lindholm, "Group key management architecture," Internet Draft, Internet Engineering Task Force, Mar. 2003. Work in progress.
- [2] D. Maughan, M. Schertler, M. Schneider, and J. Turner, "Internet security association and key management protocol (ISAKMP)," [RFC 2408](#) (Proposed Standard), IETF, Nov. 1998.
- [3] M. Baugher, T. Hardjono, H. Harney, and B. Weis, "Group domain of interpretation for isakmp," Internet Draft, IETF, Dec. 2002. Work in progress.

[6](#) Authors' contact information

Lakshminath R. Dondeti
Nortel Networks
[600](#) Technology Park Drive
Billerica, MA 01821, USA
(978) 288-6406
ldondeti@nortelnetworks.com

Thomas Hardjono
Verisign Inc.
[401](#) Edgewater Place, Suite 280
Wakefield, MA 01880, USA
thardjono@verisign.com

