Group Domain of Interpretation (GDOI)

<draft-ietf-msec-gdoi-04.txt>

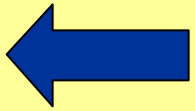
Mark Baugher (Cisco)
Thomas Hardjono (Verisign)
Hugh Harney (SPARTA)
Brian Weis (Cisco)

Group DOI

Comments on Draft 4

Open Issues

Implementation Status



Optional Payloads

Clarify that implementation of some registration exchange payloads is optional:

- KE (used for PFS)
- POP (used for authorization)
- CERT (used for authorization)

Mandatory algorithms

This was needed for interoperability.

- Rekey algorithms:
  - Encryption cipher: 3DES CBC
  - Signature: RSA

Clarification on LKH Processing

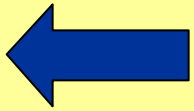
- Declared implementation of LKH to be optional
- Addressed issues of large LKH arrays
  - If the array is very large the rekey message may be broken up into multiple packets.
  - However each rekey message much be fully formed, including SEQ, SA and KD payloads
  - It would be an optimization to omit the SA payload in some cases, but the added complexity isn't worth it

Signaling deletion of SAs in the rekey message

- There were two methods
  - Implicit signaling by sending a KD payload with zero key packets.
    - Deletes all group SAs
  - Pass ISAKMP Delete Payloads in the rekey message
    - Deletes individual TEK SAs (e.g., IPSec SAs).
    - The KEK SA can also be deleted.
- Draft 4 omits the implicit signaling.

Group DOI

Comments on Draft 4
Open Issues
Implementation Status



Issue 1: KEK Encryption Algorithm IV

How to handle the IV for CBC mode?

- A static IV per group is currently specified
- Should have a different IV per packet
  - IKE uses the last ciphertext block from the previous message.
  - The GDI rekey protocol can’t use this approach

Dynamic IV Proposal

- Proposal: Use a counter in the packet combined with a secret in order to provide a per-packet IV.
- The ISAKMP HDR Message ID field could be used as a basis for an IV.
  - The Message ID identifier is within the context of the ISAKMP cookie pair, which is unique to a group.
  - Secret could be the KEK encryption key

Issue 2: Senders & Receiver Roles

- A group member cannot explicitly declare it wants to be a sender.
  - Noted in Alcatel drafts on securing IGMP and PIM.
    - `draft-irtf-gsec-igmpv3-security-issues-01.txt`
    - `draft-irtf-gsec-pim-sm-security-issues-01.txt`
  - We originally said that this was policy which should be determined out of band.
- Proposal: Extend the ID payload definition to declare the requested “role” of the group member.

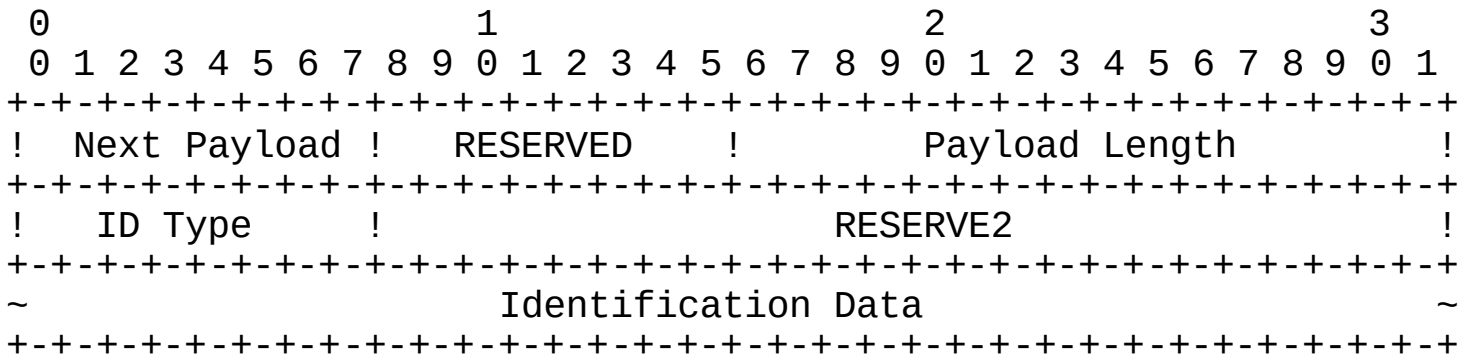
This problem is authorization!

```
Initiator (Member)                    Responder (GCKS)
------------------                    ----------------
HDR*, HASH(1), Ni, ID       -->

                            <--       HDR*, HASH(2), Nr, SA

HDR*, HASH(3) [, KE_I]      -->
        [,CERT] [,POP_I]

                            <--       HDR*, HASH(4), [KE_R,] SEQ, KD
                                                    [,CERT] [,POP_R]
```

- If the GCKS uses ACLs, they are evaluated on receipt of GDOI message 1.
- If the GCKS uses a CERT/POP pair for authorization, he can’t do that until GDOI message 3!

Issue 3: Group Identification

- Current ID payload

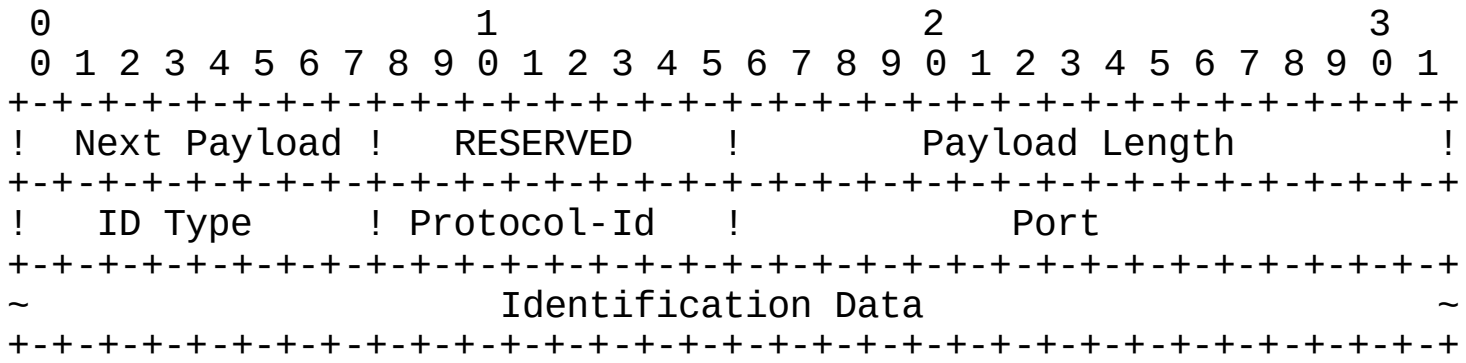


ID Type	Value
RESERVED	0 - 10
ID_KEY_ID	11
RESERVED	12 - 127
Private Use	128 - 255

Need more group id types!

- In some cases the group identities are well-defined addr/port/protocol types:
  - E.g., IGMPv3
    - address=224.0.0.1, protocol=IGMP
    - address=224.0.0.22, protocol =IGMP
    - address=<any multicast>, protocol=IGMP
- A GDOI group id could be constructed from these values in the ID payload

Proposed ID Payload



ID Type	Value
RESERVED	0
ID_IPV4_ADDR	1
RESERVED	2-3
ID_IPV4_ADDR_SUBNET	4
ID_IPV6_ADDR	5
ID_IPV6_ADDR_SUBNET	6
ID_IPV4_ADDR_RANGE	7
ID_IPV6_ADDR_RANGE	8
RESERVED	9-10
ID_KEY_ID	11

Issue 4: Support for AH

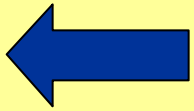
- The current GDOI TEK protocol list only includes ESP.
- IGMPv3 specifies use of AH as a way of protecting multicast messages.
  - This is commonly specified by IETF groups for control channel protocol integrity
- Proposal: Add AH to the list

Group DOI

Comments on Draft 4

Open Issues

Implementation Status



Interoperability

- Two implementations:
  - Nortel (Linux)
  - Cisco (Linux/OpenBSD)
- Interop of registration protocol continues this week.

Reference Implementation

- To be released shortly after IETF 53
  - Registration & Rekey exchanges
  - Tested on Linux and OpenBSD
    - IPSec SA's can be loaded into the OpenBSD kernel and used
    - Still looking for a Linux IPSec implementation that will support multicast
  - Web site for the source is TBD

Questions?

BACKUP SLIDES

Message 1: Request

```
Initiator (Member)                  Responder (GCKS)
------------------                  ----------------
HDR*, HASH(1), Ni, ID      -->

* Protected by IKE Phase 1 SA Hashes, encryption occurs after HDR
```

```
  HASH(1) = prf(SKEYID_a, M-ID | Ni | ID)
```

- HASH provides message authentication
- NONCE is used for replay protection
- ID indicates the desired group to join

Message 2: Policy Push

```
Initiator (Member)                    Responder (GCKS)
------------------                    ----------------
                            <--       HDR*, HASH(2), Nr, SA
```

```
  HASH(2) = prf(SKEYID_a, M-ID | Ni_b | Nr | SA)
```

- SA contains specific policy for the Category-2 and Category-3 SAs. E.g., which crypto algorithms to use.

Message 3: Ack

```
Initiator (Member)                  Responder (GCKS)
------------------                  ----------------
HDR*, HASH(3) [, KE_I]     -->

          [,CERT] [,POP_I]
```

```
  HASH(3) = prf(SKEYID_a, M-ID | Ni_b | Nr_b [ | KE_I ] [| POP_I])
```

- KE_I obtains perfect forward secrecy (if desired)
- CERT send a public key used for authorization (if needed for POP_I)
- POP_I provides evidence that the client has possession of a private or secret key

Message 4: Key Download

```
Initiator (Member)                    Responder (GCKS)
------------------                    ----------------
                          <--          HDR*, HASH(4), [KE_R,] SEQ, KD
                                                        [,CERT] [,POP_R]
```

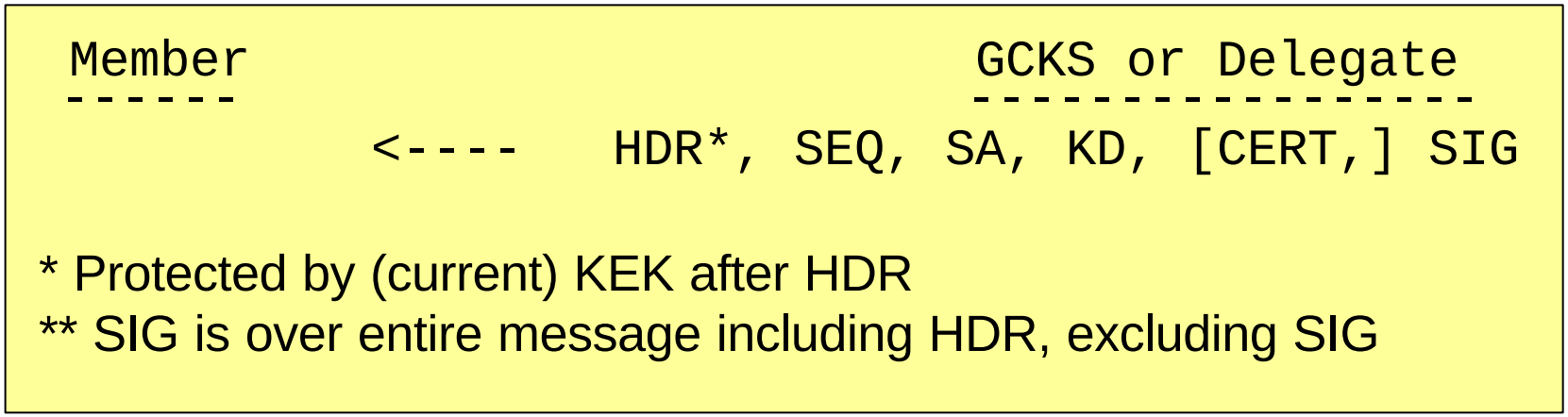
```
  HASH(4) = prf(SKEYID_a, M-ID | Ni_b | Nr_b [ | KE_R ] | SEQ | KD [| POP_R])
```

- SEQ provides the sequence number which will be used for the next rekey message.
- KD provides the keys for the policy delivered in the SA payload

Registration Protocol

```
Initiator (Member)                  Responder (GCKS)
-----------------                   ----------------

HDR*, HASH(1), Ni, ID       -->

                            <--     HDR*, HASH(2), Nr, SA

HDR*, HASH(3) [, KE_I]      -->
         [,CERT] [,POP_I]

                            <--     HDR*, HASH(4), [KE_R,] SEQ, KD
                                                   [,CERT] [,POP_R]

* Protected by IKE Phase 1 SA Hashes, encryption occurs after HDR
```

Rekey Message



- The “cookie pair” in the ISAKMP HDR acts as a SPI which identifies the group.
- SEQ contains a counter used for replay protection
- SIG contains a digital signature of the packet for authentication