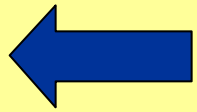
# Group Domain of Interpretation (GDOI)

<draft-ietf-msec-gdoi-01.txt>

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

# Group DOI

Mission of GDOI



Relationship of GDOI to IKE

Protocol Overview

Changes from draft –00

Remaining Issues

Implementation Experience

Future Plans

# Mission of GDOI

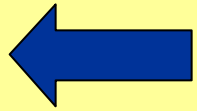
- Provide key management for groups
  - Primarily manages keys for multicast ESP, but also MESP, SRTP as they mature.
- Defines both a registration exchange, and a rekey message.

# Design goals of GDOI

- Expected to co-exist with IKE.
  - There will be a need for systems to protect both IPsec unicast traffic and IPsec multicast traffic.
  - Two independent protocols requires full design and security review of 2 discrete protocols.
- This reduces system-wide complexity
  - Two independent protocols requires an implementer to develop & maintain discrete cryptosystems, with the probable effect of neither getting proper attention.

# Group DOI

Mission of GDOI
Relationship of GDOI to IKE
Protocol Overview
Changes from draft –00
Remaining Issues
Implementation Experience
Future Plans



# Relationship of GDOI to IKE

- IKE Phase 1 is used to provide confidentiality, integrity, and replay protection.
  - IKE Phase 1 is **UNCHANGED**.
- A newly defined phase 2 exchange (called GDOI) is run rather than IKE Phase 2.
  - IKE Phase 2 is **UNUSED** and **UNCHANGED**.

# GDOI co-exists with IKE

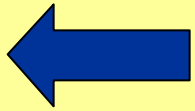
- A new DOI number is used to differentiate GDOI exchanges from IKE Phase 2.
  - At the end of IKE Phase 1 a state machine looks at the DOI number to determine next exchange.
- A GDOI service should listen on a seperate port from IKE.

# Reuse of IKE definitions

- Because GDOI is managing IPsec SAs, RFC 2407 definitions are applicable.
  - ESP Transform Identifiers
  - SA Attributes
  - ID payload & Identification Types
- Because the GDOI exchange is protected by IKE Phase 1 policy, GDOI uses definitions in common with RFC 2409.
  - Hashes are modeled after RFC 2409 hashes.

# Group DOI

Mission of GDOI
Relationship of GDOI to IKE
Protocol Overview
Changes from draft –00
Remaining Issues
Implementation Experience
Future Plans



# Group DOI Overview

- Defines a Registration exchange for initial group key mgmt.
  - Follows the IKE Phase 1
- Defines a Rekey exchange for subsequent key updates.
  - Can be multicasted for efficiency.

# Registration

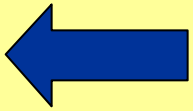
- Four message exchange between group member and GCKS
  - Request
  - Policy Push
  - Ack
  - Key Download
- The group member then has all keys necessary to decrypt and authenticate
  - Data packets
  - Rekey messages

# Rekey

- Single message sent from GCKS to the group member.
- Supplies new SAs and keys for the group.
- Encrypted with keys sent in the registration protocol.
- Signed with a digital signature

# Group DOI

Mission of GDOI
Relationship of GDOI to IKE
Protocol Overview
Changes from draft –00
Remaining Issues
Implementation Experience
Future Plans



# Changes to draft -00

- Section 2.4
  - Text is added requiring that the DOI in the IKE Phase 1 be the GDOI DOI value. This was originally intended , but not fully specified.

# Changes to draft -00

- Section 5.4.
  - Removed 3 reserved bytes from the SA TEK header. They were intended to ensure word alignment but don't actually do that.
  - The protocol list was taken from RFC 2407. That was inappropriate since GDOI supports protocols not defined in RFC 2407. This version contains a new protocol ID value list.

# Changes to draft -00

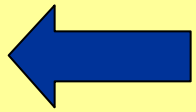
- Section 5.5
  - Removed the implicit semantic that a KD payload with no key packets instructed the group member to delete all keys associated with the group.
  - This was replaced with an explicit delete using a ISAKMP Delete payload.

# Changes to draft -00

- Section 5.5.1.1
  - Specify format of DES and 3DES keys in the KD key packet.
    - Each DES key is 64 bits (inc. the parity bits)
- Section 5.5.1.2
  - Specify format of SHA and MD5 HMAC keys in the KD key packet.
    - 160 bits and 128 bits respectively

# Group DOI

Mission of GDOI
Relationship of GDOI to IKE
Protocol Overview
Changes from draft –00
Remaining Issues
Implementation Experience
Future Plans



# 1. DOI number

Issue: It is inappropriate to define a DOI number in the document when IANA has not yet allocated one.

Proposed action: Make it TBD and define a Vendor-id payload to be included before the SA payload which provides context for interpreting the DOI number.

# 2. KE payloads

Issue: The current draft inadvertently removed the optional KE payloads from the registration exchange.

- An attacker determining the IKE Phase 1 confidentiality keys can access all packets in the group, including key update messages.
- A passive attacker can store the GDOI messages and data packets while attempting to find the IKE Phase 1 keys.

# 2. KE Payloads

Proposed Action: Reinstate the KE payloads.

- KE payloads are used to pass DH public numbers.
- The DH shared number provides keying material for super-encryption of the KD payload.

# 3. Optional SEQ payload

Issue: The SEQ payload is only required if a KEK is included in the rekey SA.

- KEK is not needed unless the group policy includes use of rekey messages.
- SEQ is used as a replay protection for rekey mess ages

Proposed Action: Make the SEQ optional in the exchange, and also in HASH(4).

# 4. CERT/POP payloads

Issue: As specified the registration messages include a POP (proof-of-possession) payload which accompanies a CERT (attribute cert).

- PKIX attributes certs don't contain a public key, so no verification can be made using this CERT alone.
- Other methods of POP are not supported.

# 4. CERT/POP payloads

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

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

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

We’ve considered several alternatives ….

# 4. CERT/POP payloads

Alternative A: POP only. Use the authentication keypair for authorization.

- PRO: Simpler protocol
- CON: Doesn’t allow a different authorization
- CON: Doesn’t allow methods other than public key.

# 4. CERT/POP payloads

Alternative B: Require an authentication CERT, authorization CERT, POP.

- PRO: Allows authorization system to be different from authentication.
- CON: Really clutters up the protocol.
- CON: Doesn't allow methods other than public key based.

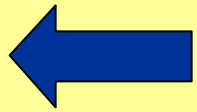
# 4. CERT/POP payloads

Alternative C: Replace CERT and POP with an AUTH payload that specifies different sorts of authorizations.

- PRO: Allows authorization system to be different from authentication.
- PRO: Opens up other types of authorization.
- PRO: Pushes specification down into a payload specification.

# Group DOI

Mission of GDOI
Relationship of GDOI to IKE
Protocol Overview
Changes from draft –00
Remaining Issues
Implementation Experience
Future Plans



# Proofs of Concept

- A proof of concept implementation was done using *isakmpd* to test the assertion that GDOI could co-exist with IKE.
- Another implementation was done using FreeS/WAN.
- Results: In both cases GDOI was added with minor changes to the original code.

# *Isakmpd* Implementation Experience

Source file changes:

- Original number: 133 files
- Changes: 14 files
- Additional : 7 files

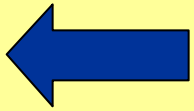
# *isakmpd* Implementation Experience

Lines of code:

- Original size: 35,000
- Changes: 759 (2%)
- Additions: 3,639 (+10%)

# Group DOI

Mission of GDOI
Relationship of GDOI to IKE
Protocol Overview
Changes from draft –00
Remaining Issues
Implementation Experience
Future Plans



# Next steps: Implementation

- Interoperability testing between Cisco and Nortel implementations.
  - Beginning late August.
  - Focus on the registration message.
- Implement & test rekey message, including use of LKH.

# Next steps: Protocol

- Resolve the mentioned issues.
- Other issues to consider:
  - The GCKS (or delegate) public key used to verify the rekey message should be downloaded in the registration message SAT payload.
  - Consider using hashes conforming to Tero's draft `draft-ietf-ipsec-ike-hash-revised-02.txt`
- Resolve problems discovered from interop testing.

# 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]
```

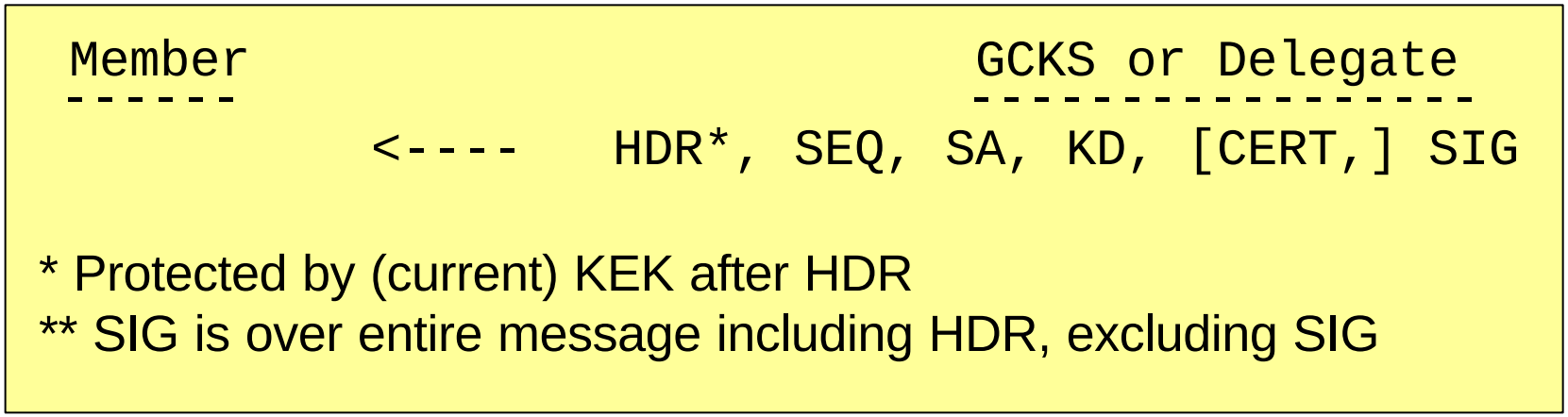
```
  HASH(4) = prf(SKEYID_a, M-ID | Ni_b | Nr_b [ | KE_R ] | SEQ | KD [| POP_R])
```

- 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