Group Domain of Interpretation (GDOI) Status

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

Draft -06

- Latest draft:
  <draft-ietf-msec-gdoi-06.txt>
- Contains no protocol changes

Draft -06 (cont.)

- Clarifies the role of GDOI as a “phase 2” exchange protected by a “phase 1” exchange
- No change to the definition of the IKE Phase 1 “phase 1” protocols defined by previous drafts.
- However, GDOI is not dependent on that “phase 1” protocol

Draft -06 (cont.)

- "Phase 1" requirements in Section 2.0:
  - Peer Authentication
  - Confidentiality
  - Message Integrity
- Appendix A outlines how GDOI *could* be used under other "phase 1" protocols. These protocols are *not* normative.
  - IKEv2
  - KINK

Status of the draft

- In IESG Review
- IESG has asked for clarification on providing key management for other protocols:
  - Need to add advice specifying when GDOI should and should *not* be used
  - This will affect Sections 1.2 and Section 5.4.2.

Proposed Clarification

- GDOI is meant to protect group traffic
  - But there is no restricton as to the address type (unicast, multicast, anycast, etc.)
- GDOI *must not* be used for private communication between a pair of hosts
- It *may* be used between a pair of hosts if they believe a third party may join them later.

Future GDOI Support: MESP

- MESP draft defines:
  - A new SA-TEK Protocol-ID
  - A list of MESP SA Attributes

Future GDOI Support: TESLA (SA Attributes)

Values from TESLA section 2.3.1.1:

- Time interval identifier (j)
- Time synchronization data
  - NTP timestamps, l_ j
- Key Chain PRFs (F, F')
- Key policy
  - disclosure interval (d, d_n)
  - value of final key (n)
  - HMAC key type
- l flag

Future GDOI Support: TESLA (KD Attributes)

Values from TESLA section 2.3.1.1:

- Disclosed key k_ i
- Length of k_ i