Draft-ietf-msec-gdoi-update-04

Sheela Rowles

IETF 74: San Francisco

March 25, 2009

IPR Disclosure

- The authors are not aware of any IPR associated with this draft

Re-organized doc

- RFC 3547 clarifications
- Authorization: address GDOI attack via update to POP payload
- Sync to RFC5374
- New GDOI attributes

Change to Clarifications

- Deprecate KE Payload
  - Additional encryption of keying material negligible with strong ciphers and authenticated encryption of the GDOI registration.

Updates resulting from RFC5374

- Address Preservation:
  - None
  - SRC: preservation of the original source addr only
  - DST: preservation of the original dest addr only
  - Src-and-Dst: preservation of both src & dst

5374 updates (cont)

- SA Direction:
  - Symmetric: SA TEK policy used by multiple senders in sending and receiving direction.
  - Receiver-only: SA TEK policy for a single sender should be installed in receiving direction by receivers.
  - Sender-only: SA TEK policy for a single sender should be installed in only the sending direction by the sender.
  - Sender-or-Receiver-only: based on the TEK, the GM figures out which direction to install the IPsec SA

5374 updates (cont)

- Rekey Rollover:
  - ATD: time after re-key event that TEK activated
  - DTD: time after re-key event that TEK deactivated

New GDOI Attributes

- Signature hash algorithm: MD5/SHA1 to SHA256
- AH support
- SA GAP payload

```
 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             !
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-!

!                  Group Associated Policy Attributes           ~
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-!
```

SA GAP Payload

- ATD: activation time delay
- DTD: deactivation time delay
- Sender ID: no 2 senders can send a pkt with the same IV with AES counter-based modes. This attribute is used to distribute a unique SID to a GM.

Next Steps

- We would like to go last call.