GDOI Update v5

Sheela Rowles

Motivation

- Changes getting unwieldy
  - Algorithm agility
  - ESP & AH support
  - Clarifications
  - Harmonization with RFC 5374 & AES counter mode draft
- Revamped draft : updated to independent draft

Refresher on GDOI

- Protocol runs between group member (GM) and Group Controller Key Server (GCKS)
- GDOI protected by ISAKMP phase 1
- GDOI downloads policy & keys using the GROUPKEY-PULL mechanism
- And refreshes keys from the GCKS to the GM using the GROUPKEY-PUSH mechanism

GDOI Exchanges

- **GROUPKEY-PULL**

  Initiator (Member) Responder (GCKS)

  ---------- ----------

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

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

  HDR*, HASH(3) -->

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

- **GROUPKEY-PUSH**

  Member GCKS

  ------ ----------

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

Significant Changes from RFC 3547

- Removal of POP and associated CERT payload
- Removal of KE Payload
- Removal of ID Payload Definition (duplicate of RFC 2408)
- MUST support AES-128 bit keys for rekey encryption.
- MUST support SHA-256 for signatures
- Discourage use of weak algorithms (DES)
- Added support for the PSS encoding method for RSA signatures.
- AH support
- RFC 5374 Support
- Support of ietf-msec-ipsec-group-counter-modes

Updates resulting from RFC 5374

- Multicast Extensions to Security Architecture
  - Group Security Policy Database
  - Address Preservation: None, source, dest, both
  - SA Direction: Symmetric, Receiver-only, Sender-only
  - Rekey Rollover: ATD, DTD

Group Associated Policy Payload

Need for a different category than TEK (specific to IPsec SA) or KEK (Rekey SA)

- GAP Payload
  - Sender ID (ietf-msec-ipsec-group-counter-modes)
  - ATD: delay after rekey to activate new TEKs
  - DTD: delay after rekey to deactivate existing TEKs

New Registries-SA GAP

- GDOI-REG

Attribute Type	Value	Type
RESERVED	0	
ACTIVATION_TIME_DELAY	1	B
DEACTIVATION_TIME_DELAY	2	B
SENDER_ID	3	V
Reserved to IANA	2-127	
Private Use	128-255	

New Registries: Addr Preservation

- ISAKMP-REG

Name	Value
Reserved	0
None	1
Source-Only	2
Destination-Only	3
Source-And-Destination	4
Reserved to IANA	5-61439

New Registries: SA Direction

- Add to ISAKMP-REG

Name	Value
----	-----
Reserved	0
Sender-Only	1
Receiver-Only	2
Symmetric	3
Reserved to IANA	4-61439
Private Use	61440-65535