draft-yeung-g-ikev2-13

Group Key Management using IKEv2

Brian Weis
Yoav Nir
Valery Smyslov

IP Multicast Security in the IETF

- The Multicast Security (MSEC) WG was alive in 2001-2011, which looked at the needs of securing IP multicast traffic
- This included:
  - RFC 3740: The Multicast Group Security Architecture
  - RFC 4046: MSEC Group Key Mgmt. Architecture
  - RFC 5374: Multicast Extensions to the Security Architecture for the Internet Protocol
  - RFC 6407: The Group Domain of Interpretation
- Platforms supporting IP multicast security take advantage of IKEv2 benefits by replacing GDOI with G-IKEv2

Securing IP Multicast

- IP multicast applications
  - Contain at least 1 sender, and N receivers
  - Take advantage of the network to route and replicate IP packets, such that the same packet reaches all N receivers.
- This requires senders and receivers to share setup an IPsec SA using the same keys.
  - The IPsec policy and keys cannot be individually negotiated, but instead of distributed by a controller/ key server (GCKS) to group members (GMs)
  - A GM invokes a Registration protocol which requires it to authenticate to the GCKS. The GCKS then authorizes the GM, and distributes IPsec policy and keys to the GM.
  - A Rekey protocol enforces a time-based key rollover strategy.

G-IKEv2 Registration

- GSA_AUTH exchange
  - Preceded with an IKE_SA_INIT exchange

```
Initiator (GM)                                  Responder (GCKS)
------------------                              ---------------
HDR, SK {IDi, [CERT,] [CERTREQ, ]
        [IDr,] AUTH, IDg, [SAg,] [N ]} -->
                                        <-- HDR, SK {IDr, [CERT,] AUTH,
                                                 [GSA, KD,] [D,]}
```

- GSA_REGISTRATION Exchange
  - Used when the IKEv2 SA has already been created

```
Initiator (GM)                      Responder (GCKS)
------------------                  ----------------
HDR, SK {IDg,[SAg,][N]}     -->
                            <--     HDR, SK {GSA, KD, [D]}
```

G-IKEv2 Rekey

- GSA_REKEY exchange
  - Usually a multicast message, Intended for large groups, pushed by the GCKS to all GMs, protected by policy previously distributed by the GCKS

```
Responder (GM)                  Initiator (GCKS)
--------------                  ----------------
                          <-- HDR, SK {GSA, KD, [D,] AUTH}
```

- GSA_INBAND_REKEY exchange
  - Distributed within each IKEv2 SA setup for G-IKEv2 registration, intended for small groups

```
Responder (GM)                  Initiator (GCKS)
--------------                  ----------------
                          <-- HDR, SK {GSA, KD, [D,]}
                  HDR, SK {} -->
```

GSA Payload

Contains policy necessary to participating in the group

- Traffic Encryption Key (TEK)
  - ESP SPI, traffic selectors, single set of transforms, attributes
- Key Encrypting Key (KEK) policy
  - IKE Header SPI, traffic selectors, attributes
- Group Associated Policy (GAP) (other group-wide policy)
  - IPsec SA Activation time, deactivation time

KD payload

- Contains keying material necessary for the policy in the GSA payload
  - TEK (IPsec SPI, keying material)
  - KEK (Rekey SA SPI, keying material)
  - LKH (Logical Key Hierarchy key arrays)
  - SID (Sender-ID (SID) values for a GM)

Reuse of IKEv2 payloads (1)

- IDg (Group Identification payload)
  - ID_KEY_ID MUST be supported.
  - ID_IPV4_ADDR, ID_FQDN, ID_RFC822_ADDR, ID_IPV6_ADDR SHOULD be supported
- SAg (GM Supported Transforms)
  - Declares which Transforms a GM is willing to accept
- D (Delete Payload)
  - Used when the GCKS may want to signal to group members to delete policy (e.g., data flows finished, change of policy)

Reuse of IKEv2 payloads (2)

- N (Notify Payload)
  - INVALID_GROUP_ID (error notify)
    - GCKS informs GM that the requested Group ID in a registration protocol is invalid
  - AUTHORIZATION_FAILED (error notify)
    - GCKS informs GM that it is not authorized to join the requested Group ID
  - SENDER_ID_REQUEST (status notify)
    - GM requests Sender IDs from the GCKS, used as part of a counter-mode transform nonce (RFC 6054)

Draft Maturity & Implementations

- The draft has been in development for several years
- Implementations
  - One known full implementation
  - A couple of known partial implementations, including the "Minimal G-IKEv2" work presented at IETF 99
  - Initial Interop results (Ludwig-Maximilians-Universität München & Cisco):
    - http://mnm-team.org/pub/Fopras/enge18/PDF-Version/enge18.pdf
- The authors request consideration as a WG item.