Group Key Management using IKEv2

draft-yeung-g-ikev2-16

Brian Weis
Independent

Valery Smyslov
ELVIS-PLUS

IETF 105
IP Multicast Security in the IETF

- The Multicast Security (MSEC) WG was active in 2001-2011, which looked at the needs of securing IP multicast traffic
  - RFC 3740: The Multicast Group Security Architecture
  - RFC 4046: MSEC Group Key Management 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 are not individually negotiated, but instead of distributed by a Group Controller / Key Server (GCKS) to Group Members (GMs)
  - A GM invokes a unicast Registration protocol 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

• Initial registration (no IKE SA between GM and GCKS)

Initiator (GM) | Responder (GCKS)

**IKE_SA_INIT**
HDR, SAi1, KEi, Ni

**GSA_AUTH**
HDR, SK{IDi, [CERT,] [CERTREQ,] [IDr,] AUTH, IDg, [SAg,] [N]}

**IKE_SA_INIT**
HDR, SARl, KEr, Nr, [CERTREQ]

**GSA_AUTH**
HDR, SK{IDr, [CERT,] AUTH, [GSA, KD,] [D]}

• Subsequent registration (IKE SA has already been created)

Initiator (GM) | Responder (GCKS)

**GSA_REGISTRATION**
HDR, SK{IDg, [SAg,] [N]}

**GSA_REGISTRATION**
HDR, SK{[GSA, KD,] [D]}
G-IKEv2 Rekey

- Multicast rekey: intended for large groups, protected by policy previously distributed by the GCKS

Responder (GM)-------------------------------------------------------------Initiator (GCKS)

\[\text{GSA\_REKEY} \]
\[\text{HDR, SK}\{[\text{GSA, KD}, [D], [AUTH]]}\]

- Unicast rekey: intended for small groups, used registration IKE SAs with each GM

Responder (GM)-------------------------------------------------------------Initiator (GCKS)

\[\text{GSA\_INBAND\_REKEY} \]
\[\text{HDR, SK}\{[\text{GSA, KD}, [D], ]}\]

\[\text{GSA\_INBAND\_REKEY} \]
\[\text{HDR, SK}\{\}\]
GSA Payload

Contains policy necessary to participating in the group:

• Traffic Encryption Key (TEK) policy
  – AH/ESP SPI, traffic selectors, single set of AH/ESP SA related transforms, additional attributes

• Key Encrypting Key (KEK) policy
  – Rekey SA SPI, traffic selectors, single set of IKE SA related transforms, additional attributes

• Group Associated Policy (GAP) (other group-wide policy)
  – SA Activation time, SA deactivation time
KD Payload

Contains keying material necessary for the policy in the GSA payload

- **TEK**
  - AH/ESP SPI, keying material

- **KEK**
  - Rekey SA SPI, keying material

- **LKH**
  - Logical Key Hierarchy key arrays

- **SID**
  - Sender-ID (SID) values for a GM acting as a sender
IDg Payload

Contains identity of the group a GM wants to join
• has the same format as IKEv2 ID payload
• only some ID types are expected to be used
  – ID_KEY_ID MUST be supported
  – ID_IPV4_ADDR, ID_IPV6_ADDR, ID_FQDN, ID_RFC822_ADDR SHOULD be supported
Reuse of IKEv2 payloads

Payloads that have the same types as in IKEv2, but slightly different semantics

• SAg (GM Supported Transforms)
  – has the same format as IKEv2 SA payload
  – 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)
New Notifications

- **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
- **REGISTRATION_FAILED** (error notify)
  - GCKS informs GM that for some reason the GM cannot join the group
  - GM sends to GCKS to unregister from the group
- **SENDER** (status notify)
  - GM informs the GCKS about its intention to be a sender in the group
  - requests a number of Sender-ID values, that are used as part of a counter-mode transform nonce (RFC 6054)
Draft Maturity & Implementations

• The draft has been in development for several years
  – last version of the draft received quite a lot of changes

• Implementations
  – One known full implementation (older version of the draft)
  – A couple of known partial implementations, including the “Minimal G-IKEv2” work presented at IETF 99
  – Initial Interop results (Ludwig-Maximilians-Universität München & Cisco):
Thank you!

- Comments?
- Questions?
- Document adoption?