Group Key Management using IKEv2

draft-ietf-ipsecme-g-ikev2

Valery Smyslov
ELVIS-PLUS

Brian Weis
Independent

IETF 113

Document Status

- Has been in development for several years
  - few implementations of early draft versions exist
- Has been adopted by IPSECME WG in 2019
- Version -01 (July 2020): major rewrite
- Version -02 (January 2021): minor update
- Version -03 (July 2021): minor update
- Version -04 (January 2022): no changes
- **Version -05 (March 2022): major update as result of WGLC comments**
  - Reviews are needed

Issues Resolved in -05

- Terminology section added
- It is clarified that IKE_AUTH and GSA_AUTH exchanges are treated equally with regard to IKEv2 extensions
- Keys used inside Rekey SA are renamed from SK_a/SK_e/SK_w to GSK_a/GSK_e/GSK_w
- Changing Authentication method and authentication key is prohibited in rekey operations, as well as changing Key Management method
- Using SIDs is clarified (in particular how the GCKS handles the situation when it runs out of available SIDs)
- Consistency of the document is improved, a lot of clarifications is added

Unresolved Issues

- Changing public key in rekey operations
- Using ports
- Unregistration of a GM
- AUTHORIZATION_FAILED vs REGISTRATION_FAILED
- Explicit PSK authentication
- ESN
- Integration with RFC 8784
- Using Tunnel Mode
- UDP encapsulation
- Transport mode signaling

Changing Public Key in Rekey operations

- Changing Authentication method and authentication key is prohibited in rekey operations, including changing public key for digital signatures (if they are used for authentication of multicast rekeys)
  - Is it OK?

Using Ports

- For compatibility with GDOI the draft allows using port 848. Standard IKEv2 ports 500/4500 are also allowed, as well as using TCP.
  - Should the unicast IKE SA switch from port 848 to 4500 if NAT is detected?
    - Yes

Unregistration of GM

- Is it needed?
  - No strict opinion. Explicit unregistering of the GM can save some GCKS's resources, e.g. in case of LKH. On the other hand, in most cases GCKS operations don't depend on the population of the group.

AUTHORIZATION_FAILED vs REGISTRATION_FAILED

- Which notification to use in which case?
  - AUTHORIZATION_FAILED is used when something is wrong with the GM and REGISTRATION_FAILED if something is wrong with the group (e.g. the capacity of the group is exceeded)

Is Explicit PSK Authentication needed?

- The draft defines two authentication modes based on symmetric shared secret for multicast rekey operations (besides authentication with digital signatures). When PSK authentication is explicit, a dedicated shared secret is transferred to GMs at the time of registration and is used across all rekey operations. Implicit authentication relies on the ability for GMs to decrypt and verify ICV of the received multicast packet (i.e. a knowledge of message protection keys which change with every rekey operation).
  - No strict opinion

ESN

- High-order 32 bits of extended sequence numbers are never transmitted in IPsec, it makes using ESN in multicast Data-Security SAs problematic, because GMs that join group long after it was created have to somehow learn the current high order 32 bits of ESN for each sender in the group. The algorithm for doing this described in RFC4302 and RFC4303 is resource-consuming
  - SHOULD NOT be used?
  - MUST NOT be used?

Integration with RFC 8784

- When PPK is used GSK_w is derived from SK_d, so an attacker cannot learn the multicast SA keys, but authentication of the keys is performed on IKE message level, so an attacker can tamper them, if it is able to break DH in real time, and can also see all the other stuff (like group policy). Is it an important threat to justify developing draft-smyslov-ipsecme-ikev2-qr-alt?
  - No strict opinion

Tunnel Mode

- RFC 5374 (Multicast Extensions to the Security Architecture for the Internet Protocol) allows both tunnel and transport modes for multicast SA. However, for tunnel mode it defines a special mode called Tunnel Mode with Address Preservation, when IP addresses from the inner IP header are copied to the outer one.
  - It seems that this mode has little value, but consumes resources; the only reason to use it – if SGW is participating in the group; how GCKS knows if this is the case?
    - Is it preconfigured?
  - Both dst and src addresses can be preserved, however the preservation of src address is optional
    - Who will control it – SGW or GCKS?

UDP Encapsulation

- Is UDP encapsulation needed for multicast Data-Security SAs? If yes, then how to signal it? Explicitly (e.g. add new Transform Type) or implicitly by specifying destination port 4500?
  - No strict opinion

Transport Mode Signaling

GSA may have some IPsec SAs created in tunnel mode and some – in transport mode. How to indicate which SAs are created in which mode?

- Change semantics of USE_TRANSPORT_MODE when it is used in the context of G-IKEv2
  - Protocol and SPI fields are used to indicate which SAs use transport mode
  - multiple instances can be sent if multiple SAs use transport mode
  - no update to RFC7296 is needed, since the context is clear
- Add new notification (e.g. GSA_USE_TRANSPORT_MODE)
- Add new transform (e.g. Encapsulation Mode) in GSA payload
- Prohibit policy when different IPsec SAs have different encapsulation modes in a single GSA payload and use USE_TRANSPORT_MODE without changing its semantics

Thank you!

- Comments?
- Questions?
- Please review the document