IPsecME WG Rechartering

IETF 100, Singapore

ipsec@ietf.org
Tero Kivinen
David Waltermire

Why

- Our chartered current work items are almost done
- We have to recharter or close down by the end of this year

Items in charter already done

- DDoS protection
- Updating MTI algorithm documents
- Adding new algorithms
  - Curve25519, Curve448, EdDSA (almost done).
- TCP Encapsulation

Items left in charter

- Quantum resistant IKEv2
- Split-DNS
- Implicit IV

Charter

The IPsec suite of protocols includes IKEv1 (RFC 2409 and associated RFCs), IKEv2 (RFC 7296), and the IPsec security architecture (RFC 4301). IPsec is widely deployed in VPN gateways, VPN remote access clients, and as a substrate for host-to-host, host-to-network, and network-to-network security.

The IPsec Maintenance and Extensions Working Group continues the work of the earlier IPsec Working Group which was concluded in 2005. Its purpose is to maintain the IPsec standard and to facilitate discussion of clarifications, improvements, and extensions to IPsec, mostly to IKEv2. The working group also serves as a focus point for other IETF Working Groups who use IPsec in their own protocols.

Quantum resistant IKEv2 (old)

IKEv1 using shared secret authentication was partially resistant to quantum computers. IKEv2 removed this feature to make the protocol more usable. The working group will add a mode to IKEv2 or otherwise modify IKEv2 to have similar quantum resistant properties than IKEv1 had.

Split DNS (old)

Split-DNS is a common configuration for VPN deployments, in which only one or a few private DNS domains are accessible and resolvable via the tunnel. Adding new configuration attributes to IKEv2 for configuring Split-DNS would allow more deployments to adopt IKEv2. This configuration should also allow verification of the domains using DNSSEC. Working group will specify needed configuration attributes for IKEv2.

Implicit IV (old)

Currently, widely used counter mode based ciphers send both the ESP sequence number and IV in form of counter, as they are very commonly the same. There has been interest to work on a document that will compress the packet and derive IV from the sequence number instead of sending it in separate field. The working group will specify how this compression can be negotiated in the IKEv2, and specify how the encryption algorithm and ESP format is used in this case.

Group DOI (new)

The Group Domain of Interpretation (GDOI - RFC 6407) is an IKEv1-based protocol for negotiating group keys for both multicast and unicast uses. The Working Group will develop an IKEv2-based alternative that will include cryptographic updates. A possible starting point is draft-yeung-g-ikev2.

Responder MOBIKE (new)

MOBIKE protocol [RFC4555] is used to move existing IKE/IPsec SA from one IP address to another. However, in MOBIKE it is the initiator of the IKE SA (i.e. remote access client) that controls this process. If there are several responders each having own IP address and acting together as a load sharing cluster, then it is desirable for them to have ability to request initiator to switch to a particular member. The working group will analyze the possibility to extend MOBIKE protocol or to develop new IKE extension that will allow to build load sharing clusters in an interoperable way.

Postquantum IKEv2 (new)

Postquantum Cryptography brings new key exchange methods. Most of these methods that are known to date have much larger public keys then conventional Diffie-Hellman public keys. Direct using these methods in IKEv2 might lead to a number of problems due to the increased size of initial IKEv2 messages. The working group will analyze the possible problems and develop a solution, that will make adding Postquantum key exchange methods more easy. The solution will allow post quantum key exchange to be performed in parallel with (or instead of) the existing Diffie-Hellman key exchange.

Diet ESP (new)

A growing number of use cases for constraint network - but not limited to - have shown interest in reducing ESP (resp. IKEv2) overhead by compressing ESP (resp IKEv2) fields. The WG will define extensions of ESP and IKEv2 to enable ESP header compression.

draft-mglt-ipsecme-diet-esp and draft-mglt-ipsecme-ikev2-diet-esp-extension are expected to be good starting points for ESP compression. draft-smyslov-ipsecme-ikev2-compression and draft-smyslov-ipsecme-ikev2-compact are good starting point for IKEv2 compression.

Signature algorithm neg. (new)

RFC7427 allows peers to indicate hash algorithms they support, thus eliminating ambiguity in selecting a hash function for digital signature authentication. However, recent advances in cryptography lead to a situation when some signature algorithms have several signature formats. A prominent example is RSASSA-PKCS#1 and RSASSA-PSS, however it is envisioned that the same situation may repeat in future with other signature algorithms. Currently IKE peers have no explicit way to indicate each other which signature format(s) the support, that leads to ineroperability problems. The WG will investigate the situation and come up with a solution that allows peers to deal with the problem in an interoperable way.

Other items (no charter text yet)

- IPv4 & IPv6 address failure errors
- Labeled IPsec
- Others?