Quantum Resistant IKEv2

draft-ietf-ipsecme-qr-ikev2-00
(draft-fluhrer-qr-ikev2)

Scott Fluhrer, David McGrew, Panos Kampanakis
Cisco Systems
Valery Smyslov
ELVIS-PLUS

Background

Currently, IKE-protected traffic can be stored now, and later read by someone with a Quantum Computer (once one is built).

Cryptographers are creating Quantum Safe replacements to DH and ECDH, however those won't be standardized by NIST for a while.

The goal is to create a short-term solution, based on the assumption that both sides can share a high-entropy secret ("PPK").

Changes to the Protocol

- The previous version had a problem if
  - both sides had a PPK, but they weren't the same or
  - the responder did not have a PPK configured for the peer.

  The protocol would fail, with no obvious indication why.

  To address this, we added an optional NO_PPK_AUTH notification. It allows the responder to recognize when there is a PPK mismatch and
  - Fall back to traditional IKEv2 if PPK is configured non mandatory or
  - Abort the exchange.

Change in the Draft Text (Cont'd)

- Expanded Security Considerations
  - responder may wish to cache failed partial initial requests (to address a misconfiguration scenario that may mimic a DoS attack).
  - MUST rekey if sensitive info is exchanged over the initial IKE SA.
  - Downgrade attack if PPK_SUPPORT is non mandatory for both peers.
  - Initiator should wait for more responses when PPK is mandatory, to avoid DoS attack.

Change in the Draft Text (Cont’d 2)

- Added “Operational Considerations”
  - How PPKs are distributed
  - Group PPKs
  - PPK-only authentication (using NULL Authentication method)
- Tweak to PPK_ID format (adjusting the PPK ID type encoding)

Discussion

- Informational or Standards track?
- More reviews and WGLC?
- libreswan implementation (Paul?)