Quantum Resistant IKEv2

The shortterm solution

Scott Fluhrer
Cisco Systems
sfluhrer@cisco.com

Background

Currently, IKE depends on the security of DH or ECDH for privacy

Both DH and ECDH are believed to be breakable by someone with a Quantum Computer

No one has a nontoy Quantum Computer currently; however if someone does develop one in the future, they can decrypt recordings of old IKE and IPsec sessions

What do we do about this?

Short term strategy: have both sides have a shared secret; stir that into the derived key.

Long term strategy: extend IKE to allow the use of postquantum key agreement protocols.

This discussion is about the short term strategy.

Previous WG Meeting

We agreed on the basic approach, with the following tweaks:

- Simplified how it is negotiated
- Simplified how the PPK were stirred in
  - We modify the initial SK_d, SK_pi, SK_pr values
  - Initial IKE SAs were not protected
- Suggested how PPK were to be transported out-of-band

Current Status

We’ve updated the draft.

draft-fluhrer-qr-ikev2-04

We have a test implementation.

Comments???


CISCO