# Quantum Resistant IKEv2

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?

We have both sides have a shared secret; stir that into the derived key.

The idea is that, even if someone breaks the DH shared secret, the shared secret still protects us.

If the shared secret has 256 bits of entropy, then Grover's algorithm with a Quantum Computer would require $O(2^{128})$ operations, which is considered infeasible.

# Previous WG Meeting

We (mostly) agreed on the requirements for this:

- Simplicity, Algorithm Agility important
- IPsec traffic needs to be protected
- IKE traffic less important

draft-fluhrer-qr-ikev2-03 is the current proposal

# Open Issues

How do we stir in the shared secret (“ppk”)

- Draft stirs it in on all child SA key generation operations
- Valery Smyslov suggested modifying the SK_d after identities were exchanged
- Dan Harkins suggested modifying only the KEYMAT (IPsec keys)

Opinions?

# Open Issues

IKE Security and Anonymity

- Should we initially negotiate with pseudonyms, and then rekey once we are Quantum Secure?
- Is this something that should be in a follow-up RFC?

Opinions?

# Open Issues

How do we distribute these PPKs?

- Draft doesn’t address it
  - Current IKE RFCs do not recommend how to distribute preshared keys
- Is this something that should be in a follow-up RFC?

Opinions?

# Other Issues???