IKE and QR Requirements

Scott Fluhrer, David McGrew

Cisco Systems

11/15/16

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

Background

What do we do about this:

- Option 1: replace (EC)DH with a Quantum Resistant Key Exchange
  - Issue with that: large change, no Quantum Resistant Key Exchange is universal accepted
- Option 2: have both sides have a shared secret (ppk); stir that into the derived key
  - The idea is that, even if someone breaks the DH shared secret, the ppk still protects us

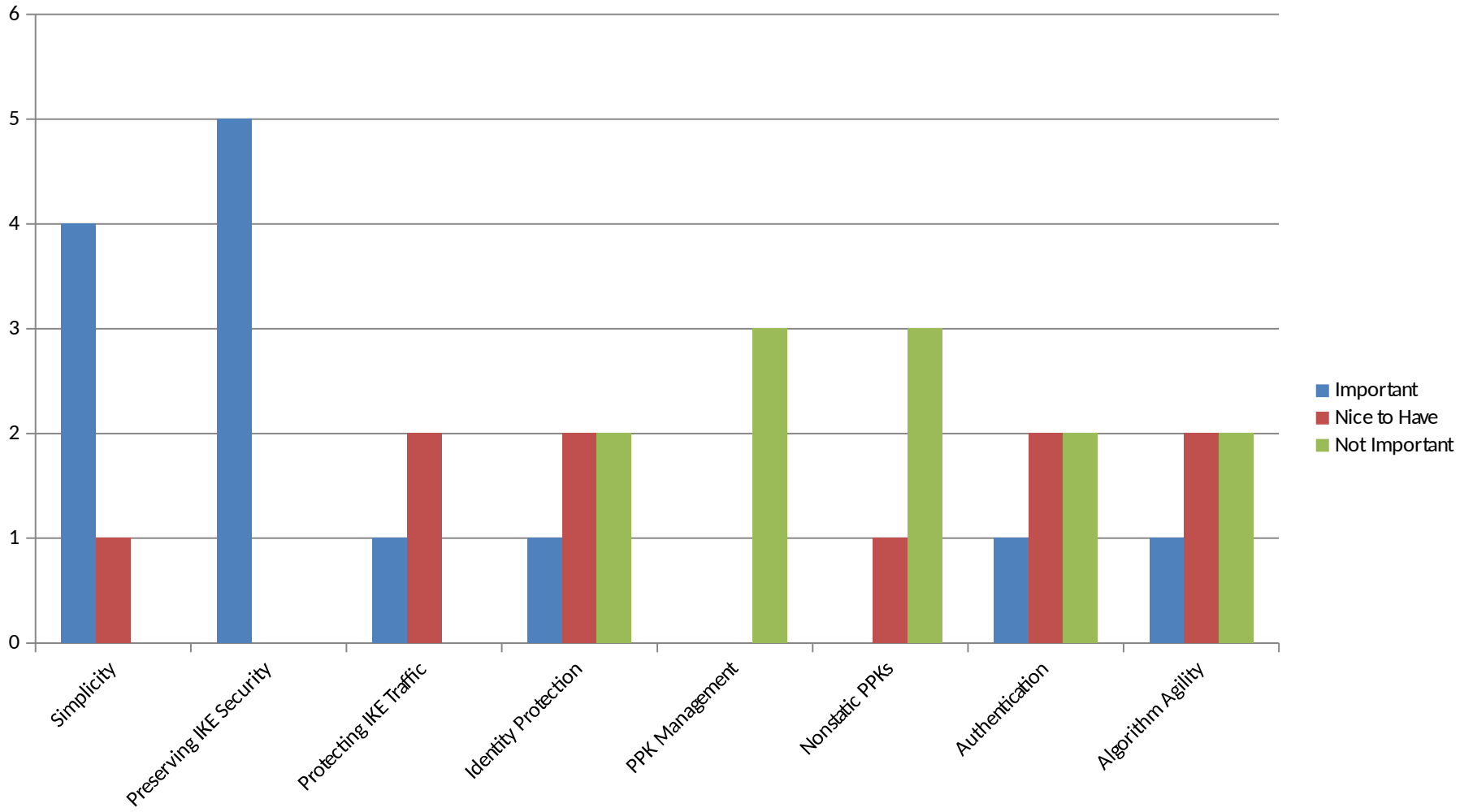
Previous WG Meeting

We agreed to make working on this as a WG item

We decided to gather requirements for a solution

We agreed to have a poll of the WG for the important of various requirements

Results of the WG Poll



Interpretation of the Results

Preserving IKE security properties against a conventional adversary considered the most critical

> "First rule: do no harm"

Simplicity was the second most important goal

Protecting IKE traffic, and identities were considered less important

Updates to draft-fluhrer-qr-ikev2-03 to reflect these priorities

There are now three differences from the standard IKE protocol

- We exchange notifications on the first encrypted exchange
  - This is to deal with the brownfield scenario
- We stir in the PPK when generating IPsec KEYMAT
  - This means that all IPsec keys are protected
- We stir in the PPK when generating child SAs
  - This means that child IKE traffic is protected

Changes from the previous version

- We simplified the protocol
- We do not attempt to protect identities from an adversary with a QC
- We do not protect the initial IKE exchange from an adversary with a QC
  - However, since we can immediately create a child IKE SA (which is protected), an implementation can protect the traffic selectors

How we score against the requirements

Requirement (ordered by importance)	
Preserving IKE security	✓
Simplicity	✓
Protecting IKE traffic	At additional cost
Authentication	✓
Algorithm Agility	✓
Identity Protection	✗
Nonstatic PPKs	Not addressed
PPK Management	Not addressed

Thank you.