Secure Failure Detection
Decision Process

IPsecME WG
IETF 78, Maastricht
The basic scenario

• Alice and Bob have SAs up and ESP traffic is flowing, but then Bob crashes
• Alice keeps sending ESP to Bob
• When Bob finally comes back up, he replies to Alice’s ESP with INVALID_SPI notifications
• Alice starts sending IKE liveness checks until she is “sure” that the INVALID_SPI responses are not a DoS attack; this could be “at least several minutes” according to RFC 4306
• Then Alice rekeys the IKE SA
What we want

• As soon as Bob starts sending INVALID_SPI responses to Alice’s ESP traffic, the two parties should be able to quickly determine that this is not an attack and therefore they probably want to rekey right away

• It is still incumbent upon Alice and Bob to do the rekeying, but at least they know they can do it now
Why this is important

- Without a protocol extension, it can take a long time before Alice knows that she should really rekey.
- Bob may have time-critical traffic he wants to send on an SA, but he can’t convince Alice to rekey now.
Two proposed solutions

- **QCD**
  - Bob gives Alice a token in the AUTH exchange
  - Bob puts the token in his INVALID_SPI response as a way to say “this SPI is gone”

- **SIR**
  - Alice sends a new Check_SPI query with a stateless cookie
  - Bob responds “I’m sure I don’t know that SPI”
QCD overview

- draft-nir-ike-qcd
- Bob generates a per-peer token using a master secret
  - The secret is remembered across reboots, and is used with all SA partners
- Alice must remember the token (or a hash of it) for each SA
SIR overview

- draft-detienne-ikev2-recovery (expired)
- Alice asks “do you really not know about this SPI?”, Bob confirms
- Nothing is stored on either side
- A man-in-the-middle can attack this to cause an unnecessary rekey just as they can normal IKE
- IPR statement filed 2010-03-09
Criteria for choosing

- Support for different scenarios (load-balancer, active cluster, failover)
- Security from man-in-the-middle DoS attacks
- Resources used
- IPR
Moving forward in the WG

• Last year, people wanted this added to the charter, and five people agreed to review drafts
• Recently, Yaron and I have asked the group a few times how people want to proceed, but there has been no reply
• So ..... ?
Backup
Some other problem cases

• Bob has two gateways in some failover architecture
  – One gateway goes down, the other gateway detects this and wants to tell Alice to rekey

• Bob has a bunch of gateways in some load-balancing or cluster architecture
  – One gateway is taken down on purpose, and the system wants to tell Alice to rekey

• Protocol robustness
  – Bob’s gateway loses the SA without going down