Fast & Secure Crash Detection in IKEv2

Solving the Problem of Quickly Detecting Dangling SAs.

F. Detienne
Y. Nir
P. Sethi
Crash Detection Problem Statement

- Sometimes SAs get out-of-sync, for example, when one side reboots. Recovery then takes minutes.

- Assume Bob has rebooted:

  Alice → Bob

  ESP (SPI=0x12345678)

  HDR(0,0) N(INVALID_SPI 12345678)

  HDR(A,B) SK{0} - Liveness Check

  HDR(A,B) N(INVALID_IKE_SPI)

  HDR(A,B) SK{0} - Liveness Check

  repeated a dozen times
Proposed Solutions

- **SIR – Stateless IKE Recovery**
  - This involves Alice querying Bob about the lost SA using an unprotected exchange with a stateless cookie. Throttling and dampening prevent this mechanism's use as an attack vector.

- **QCD – Quick Crash Recovery**
  - This involves Alice storing Bob's “token” during the AUTH exchange. Bob can recalculate the token, proving it's really Bob, and authenticating the INVALID_IKE_SPI message.

- **Birth Certificates**
  - These are actually signed timestamps or restart counters. Bob will send the new one to Alice, along with the INVALID_IKE_SPI notification, proving he's rebooted.