A Quick Crash Discovery Method for IKEv2

draft-nir-ike-qcd-05

Y. Nir

November 2009

What are We Proposing?

- A Quick Crash Discovery Method for IKEv2
- When VPN implementations reboot, or otherwise lose their state, their peers need to discover this in order to quickly re-establish the tunnels
- RFC 4306 and the -bis document describe a method for state loss discovery. However, this method may take several minutes to complete.
  - You need several failed attempts at liveness test before giving up on an IKE SA.

What are We Proposing?

- Our draft proposes an extension to IKEv2 that allows a secure method for an implementation to signal to its peer that it has lost state.
- During IKE_AUTH the peers exchange “tokens” based on IKE SPIs
- When a gateway receives an IKE message with an unknown IKE SPI, it generates an identical token, and sends that along with the INVALID_IKE_SPI
- A peer receiving a clear token with the correct content, silently deletes the IKE SA.

What are We Proposing?

- Design Goals:
  - Minimal persistent state on the gateway that has lost state
  - Resistance to spoofing of "crash proofs"
  - Resistance to DoS
- Non Goals:
  - Re-establish the IKE SAs – this can be done using regular IKEv2 or Session Resumption.
  - Discovering the crash while the peer is still down, and cannot send INVALID_SPI.

Initiation

```
Alice                                                    Bob
----------                                          ----------

                          ---- IKE_AUTH ----

 HDR(A,B), SK {IDi,
    [CERT,] [CERTREQ,]
    [Idr,] AUTH, N(TokenA),
    SAi2, TSi, Tsr}
                                        -->
                                      <-- HDR(A,B), SK{IDr,[CERT,]
                                           AUTH, N(TokenB), SAr2,
                                           TSi, TSr}
```

Presentation

```
Alice                                                    Bob
----------                                          ----------

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

                                <--   HDR(A,B), N(TokenB),
                                        N(INVALID_IKE_SPI)


                    ---- IKE_SA_INIT exchange ----
HDR(A',0), N(COOKIE),
  SAi1, KEi, Ni                 -->

                                <-- HDR(A',B'), SAr1, Ker,
                                        Nr, [CERTREQ]
```

Do gateways actually lose state?

- Easy answer: yes. There are several reasons:
  - Bugs – it's sad, but they do exist.
  - OS failures.
  - Power failures – try running a gateway without UPS in Detroit.
  - Temporary connectivity failures, where only one side is doing regular liveness checks.
  - Scheduled maintenance with or without a backup gateway.
  - The administrator's favorite button for trouble-shooting (and it really helps, too!)

Reset All the Tunnels!

- Every implementation has one:
  - `clear crypto isakmp sa`
  - `clear services ipsec-vpn ike security-associations`
  - `fw tab -t ikev2_sas -x -y`
  - `ipsec restart`
  - `setkey -F ; killall racoon`
- For extra credit, identify these implementations!

Why this should be a WG item?

- Has security implications – needs eyeballs.
- Has interaction with other WG items:
  - Session Resumption
- Has interaction with non-IETF standards:
  - 3GPP
- Two competing proposals (QCD and SIR)
  - We really don't want two competing non-standards
- May fill a need for multiple vendors and users of IKE.

Funny Question Mark Goes Here