IKE Session Resumption

draft-ietf-ipsecme-ikev2-resumption-03

Yaron Sheffer, Hannes Tschofenig,
Lakshminath Dondeti, Vidya Narayanan

Main Changes in -03

- Changed from 1 round trip resumption for 2 round trips
- This is the big one, but also:
  - Clarified which state is resumed from ticket and which is renegotiated
  - Clarified use of identities
  - Added discussion of ticket lifetime and reissue, as discussed in SFO
  - Discussed NAT and IP address change
  - And several more…

2 Round Trips

- 1 RT barebones IKE_SESSION_RESUME followed by a regular IKE_AUTH
  - IKE_SESSION_RESUME behaves like IKE_SA_INIT

```
HDR, Ni, N(TICKET_OPAQUE) [,N+] →
                                ← HDR, Nr [,N+]
```

- The new IKE SA is created at this point
  - Derivation similar to IKE SA rekey

```
SKEYSEED = prf(SK_d_old, "Resumption" | Ni | Nr)
```

Resumed vs. New State (1/2)

- Very little state in the ticket
- 2 round trips means that most (non-IKE SA) state can be exchanged normally
- Some stuff left unspecified
  - Next slide
- Internal IP address is another important special case

Resumed vs. New State (2/2)

IDi
IDr
Authentication method
Certificates (when applicable)
Local IP address/port, peer IP address/port
NAT detection status
SPIs
Which peer is the "original initiator"?
IKE SA sequence numbers
IKE SA algorithms (SAr)
IKE SA keys (SK_*)

IKE SA window size
Child SAs (ESP/AH)
Internal IP address
Other Configuration Payload information
Peer vendor IDs
Peer supports MOBIKE
MOBIKE additional addresses
Time until re-authentication [RFC4478]
Peer supports redirects

Source IP Address and NAT

- Client can resume from a new address
  - Return routability ensured by 2nd RT
- NAT is detected (again) upon resumption

Identities

- IDr is renegotiated
  - But gateway should store IDr in ticket, and may use it for policy decisions on resumption
- IDi is included in the ticket *and* in the exchange
  - Protected in IKE_AUTH
  - Both occurrences MUST be identical

Thank You!