Privacy Addition to the IKEv2 IKE_SA_INIT Exchange

draft-dschinazi-ipsecme-sa-init-privacy-addition-00

David Schinazi — dschinazi@apple.com
Problem Statement: Privacy

- IKEv2 is robust and secure after AUTH check
- Some information is leaked before then
  - Initiator identity
  - Fact that IKEv2 responder is running
- Important: this discusses an addition that does NOT replace any existing IKEv2 security mechanisms
Case 1: Initiator Identity

- **Initiator Identity (IDi) sent before responder has been authenticated**
- **Leaked to on-path active attacker**

Initiator: HDR, SAi1, KEi, Ni  -->

Responder: HDR, SAr1, KEr, Nr, [CERTREQ]  

Initiator: HDR, SK {IDi, [CERT,] [CERTREQ,] [IDr,] AUTH, SAi2, TSi, TSr}  -->

Responder: HDR, SK {IDr, [CERT,] AUTH, SAr2, TSi, TSr}  -->

- Initiator Identity (IDi) sent before responder has been authenticated
- Leaked to on-path active attacker
Case 1: Initiator Identity

- Initiator Identity (IDi) sent before responder has been authenticated
- Leaked to on-path active attacker
Case 2: Hidden Server

- Some users wish to hide the fact that they use a VPN
- Solution: IKEv2 over TLS/TCP/443 — RFC 8229
- Evil operator can observe traffic to server and probe for IKEv2 support by sending IKE_SA_INIT
Proposed Solution:
Initialization Authentication Code

- Add to configuration:
  - Shared secret (IAC)
  - Pseudo-random function (prf)
- Added optional notify on IKE_SA_INIT messages
Proposed Solution: Initialization Authentication Code

- Initiator sends IAC_i with IKE_SA_INIT request
- Responder verifies IAC_i and drops silently if fail
- Responder sends IAC_r with IKE_SA_INIT reply
- Initiator verifies IAC_r and fails exchange if fail
Proposed Solution: Initialization Authentication Code

- Computed as follows:

\[
\text{IAC}_i = \text{prf}_i( \text{prf}_i(\text{IASS}_i, \text{"Initialization Authentication Key Pad for IKEv2 Initiator"}), Ni)
\]

\[
\text{IAC}_r = \text{prf}_r( \text{prf}_r(\text{IASS}_r, \text{"Initialization Authentication Key Pad for IKEv2 Responder"}), Ni \mid Nr)
\]
Replay Attacks

• This design does not prevent replay attacks on IKE_SA_INIT

• Case 2 can leverage TLS to prevent on-path attackers and prevent replay of IKE_SA_INIT messages
Privacy Addition to the IKEv2
IKE_SA_INIT Exchange

draft-dschinazi-ipsecme-sa-init-privacy-addition-00

David Schinazi — dschinazi@apple.com