EAP-Only Authentication in IKEv2

draft-ietf-ipsecme-eap-mutual-00

Pasi Eronen, Yaron Sheffer,
Hannes Tschofenig

IETF-77, Anaheim, CA

Motivation

- Client auth using certificates is hard to do
- Even server auth requires some provisioning
- IKE shared secret often abused for password authentication
- EAP-only auth is often more practical
  - E.g. EAP-AKA (long shared secret)
  - EAP-EKE, EAP-PWD (password)

- Current IKEv2 requires authentication of the server cert, even when you're doing EAP
  - Regardless of the assurances of the EAP method
  - AUTH payload in message 4

Proposed Solution

- Prerequisite: a mutual authenticating, key generating EAP method

- Add an EAP_ONLY_AUTHENTICATION notification to message 3
- Responder cert is not required, AUTH payloads computed using the EAP MSK
- If the responder does not understand, initiator validates cert-derived AUTH payload as usual (new in -00)

Message Sequence

Initiator *Responder*

HDR, SAi1, KEi, Ni, [N(NAT_DETECTION_SOURCE_IP), N(NAT_DETECTION_DESTINATION_IP)] →

← HDR, SAr1, KEr, Nr, [CERTREQ], [N(NAT_DETECTION_SOURCE_IP), N(NAT_DETECTION_DESTINATION_IP)]

HDR, SK { IDi, [IDr], SAi2, TSi, TSr, **N(EAP_ONLY_AUTHENTICATION)**, [CP(CFG_REQUEST)] } →

← HDR, SK {IDr, EAP(Request) }

HDR, SK {EAP(Response) } →

← HDR, SK {EAP(Request) }

HDR, SK {EAP(Response) } →

← HDR, SK {EAP(Success) }

HDR, SK {**AUTH**} →

<-- HDR, SK {**AUTH**, SAr2, TSi, TSr, [CP(CFG_REPLY]}

Channel Binding

- EAP should authenticate the identity of the IKE Responder
  - Otherwise a rogue Access Point can masquerade as a VPN gateway
- This means:
  - The EAP method should be mutually authenticating and key generating (MSK)
  - The EAP exchange should include both parties' IKE identities
  - These identities should be crypto-bound into MSK
  - We trust the AAA server to include the correct gateway identity in EAP
- Not (yet) discussed in -00

New in -00

- An explicit list (and IANA registry) of allowed EAP methods
  - Non-expert implementers do not have to sift through available methods
  - The list does *not* include any tunneled (X-in-TLS) methods
- Both peers MUST ensure use of legal methods

Thank You!