Announcing Supported Authentication Methods in IKEv2

draft-smyslov-ipsecme-ikev2-auth-announce

Valery Smyslov
svan@elvis.ru

IETF 112
Authentication in IKEv2

- Unlike IKEv1, authentication method in IKEv2 is not negotiated, each peer is free to use whichever method it thinks is appropriate.
- Generally works well if there is only one way of doing authentication or there is no ambiguity in choosing among several of them.
- If peers can use several methods to authenticate each other, it is possible that initiator selects authentication method unsupported by the responder.
  - Less likely in the opposite direction, but still possible.
The Problem

• The problem was first encountered when RSA-PSS signature format appeared in IKEv2
  – newer initiators tried to use PSS signatures while older responders didn’t support it, sending back AUTHENTICATION_FAILED
  – if initiators knew responders’ capabilities they would have chosen PKCS#1 and the SA succeeded
Source of the Problem

- Currently there is no way for the peers to explicitly indicate the supported authentication methods
  - it is possible to guess them via indirect means, e.g. CERTREQ content, but this is unreliable
- With new signature formats and authentication methods appearing in the future (including PQ and hybrid ones) the situation of mis-selecting may happen more often
Proposed Solution

• Add new optional status notification `SUPPORTED_AUTH_METHODS` to indicate the supported authentication methods
  – for certificate-based authentication add an ability for the peers to indicate which signing algorithms can be used with each of CA in the `CERTREQ` payload
  – avoid creating new IANA registries
SUPPORTED_AUTH_METHODS

Notification Format

• Notification data consists of a list of supported authentication methods in the following formats:
  1. Two-octet format for the methods that are not linked to CERTREQ payload (PSK, NULL)
  2. Three-octet format that allows optional linking to CERTREQ payload (RSA-SIG etc.)
  3. Multi-octet format that allows optional linking to CERTREQ payload and specifying ASN.1 AlgorithmIdentifier for use with particular CA (SIG)

• The linking to CAs is done by specifying the ordinal number of CA within the CERTREQ payload the method can be used with
SUPPORTED_AUTH_METHODS
Notification Format Illustration

HDR, SAr1, KEr, Nr, CERTREQ, N(SUPPORTED_AUTH_METHODS)

CA1 (RSA)
CA2 (ECDSA)
CA3 (RSA)
CA4 (RSA)

AUTH  LINK  AlgorithmIdentifier
PSK
SIG  1  sha256WithRSAEncryption
SIG  0  RSASSA-PSS
SIG  2  ecdsa-with-sha256
RSA-SIG  1
NULL
Exchanges (Option 1)

Initiator

\[
\text{IKE\_SA\_INIT} \\
\text{HDR,SAi1,KEi,NI}
\]

\[
\text{IKE\_AUTH} \\
\text{HDR,SK\{IDi,\[CERT,\][CERTREQ,]} \\
\text{[IDr,] AUTH, SAi2, TSi, TSr,} \\
\text{[N\(\text{SUPPORTED\_AUTH\_METHODS}\)\(\ldots\)]}}
\]

Responder

\[
\text{IKE\_SA\_INIT} \\
\text{HDR,SAr1,KEr,Nr,[CERTREQ,]} \\
\text{[N\(\text{SUPPORTED\_AUTH\_METHODS}\)\(\ldots\)]}
\]

\[
\text{IKE\_AUTH} \\
\text{HDR,SK\{IDr,\[CERT,\] AUTH, SAi2, TSi, TSr,} \\
\text{[N\(\text{SUPPORTED\_AUTH\_METHODS}\)\(\ldots\)]}}
\]
Exchanges (Option 2)

**Initiator**

**IKE_SA_INIT**
- HDR, SAi, KEi, Ni

**IKE_INTERMEDIATE**
- HDR, SK{...}

**IKE_AUTH**
- HDR, SK{IDi, [CERT, ][CERTREQ,] [IDr,] AUTH, SAi2, TSi, TSr, [N(SUPPORTED_AUTH_METHODS)(...)]}

**Responder**

**IKE_SA_INIT**
- HDR, SAr1, KEr, Nr, [CERTREQ,] [N(SUPPORTED_AUTH_METHODS)]

**IKE_INTERMEDIATE**
- HDR, SK{...,
  N(SUPPORTED_AUTH_METHODS) (...)}

**IKE_AUTH**
- HDR, SK{IDr, [CERT,] AUTH, SAi2, TSi, TSr}


Thanks

- Comments? Questions?
- More details in the draft
- WG adoption?