INTERMEDIATE Exchange Update

draft-smyslov-ipsecme-ikev2-aux-02

Valery Smyslov
svan@elvis.ru

IETF 104
Exchange Overview

One or more **INTERMEDIATE** (ex IKE_AUX) Exchanges may take place between IKE_SA_INIT and IKE_AUTH. Their use is negotiated via exchange of **INTERMEDIATE_EXCHANGE_SUPPORTED** notifications:

**Initiator**

**IKE_SA_INIT**
HDR(MID=0),SAi1,KEi,Ni,
N(INTERMEDIATE_EXCHANGE_SUPPORTED)

**INTERMEDIATE**
HDR(MID=1),SK{…}

**IKE_AUTH**
HDR(MID=2),SK{IDi,AUTH,SAi2,TSi,TSr}

**Responder**

**IKE_SA_INIT**
HDR(MID=0),SAr1,KEr,Nr
N(INTERMEDIATE_EXCHANGE_SUPPORTED)

**INTERMEDIATE**
HDR(MID=1),SK{…}

**IKE_AUTH**
HDR(MID=2),SK{AUTH,SAr2,TSi,TSr}

The exchanges can be used to transfer large amount of data prior IKE_AUTH (e.g. QSKE public keys), since standard IKE Fragmentation works for them.
Changes from -01 version

- Exchange renamed from IKE_AUX to INTERMEDIATE
  - IANA Considerations are updated
- Exchange authentication is changed so, that all INTERMEDIATE exchanges messages are included (via PRF) in AUTH payload calculation
  - thanks to Scott Fluhrer for this suggestion
Old INTERMEDIATE Exchange Authentication

- Previously each party included only her own INTERMEDIATE messages into the AUTH payload computation

\[
\begin{align*}
\text{InitiatorSignedOctets} &= \text{RealMessage1} \mid \text{AUX}_I \mid \text{NonceRData} \mid \text{MACedIDForI} \\
\text{ResponderSignedOctets} &= \text{RealMessage2} \mid \text{AUX}_R \mid \text{NonceIData} \mid \text{MACedIDForR}
\end{align*}
\]

\[
\begin{align*}
\text{AUX}_I &= [\text{AUX}_\text{PRF}_I_1 \mid \text{AUX}_\text{PRF}_I_2 \mid \text{AUX}_\text{PRF}_I_3] \ldots \\
\text{AUX}_R &= [\text{AUX}_\text{PRF}_R_1 \mid \text{AUX}_\text{PRF}_R_2 \mid \text{AUX}_\text{PRF}_R_3] \ldots
\end{align*}
\]

\[
\begin{align*}
\text{AUX}_\text{PRF}_I_n &= \text{prf}(\text{SK}_{\text{pi}_n}, \text{IKE}_\text{AUX}_I_n_H \mid \text{IKE}_\text{AUX}_I_n_E) \\
\text{AUX}_\text{PRF}_R_n &= \text{prf}(\text{SK}_{\text{pr}_n}, \text{IKE}_\text{AUX}_R_n_H \mid \text{IKE}_\text{AUX}_R_n_E)
\end{align*}
\]

\[
\begin{align*}
\text{IKE}_\text{AUX}_{[I/r]}_n_H &= \text{part of the message from the beginning of IKE header till the end of Encrypted payload header} \\
\text{IKE}_\text{AUX}_{[I/r]}_n_E &= \text{content of Encrypted payload before encryption and possible fragmentation (not including payload header, IV, ICV, Pad Length and Padding)}
\end{align*}
\]
New INTERMEDIATE Exchange Authentication

- Authentication is changed so that all INTERMEDIATE messages are included into the AUTH payload calculation by each party

\[
\begin{align*}
\text{InitiatorSignedOctets} &= \text{RealMessage}_1 \mid \text{NonceRDdata} \mid \text{MACedIDForI} \mid \text{IntAuth} \\
\text{ResponderSignedOctets} &= \text{RealMessage}_2 \mid \text{NonceIData} \mid \text{MACedIDForR} \mid \text{IntAuth}
\end{align*}
\]

\[
\text{IntAuth} = \text{IntAuth}_1 \mid [\mid \text{IntAuth}_2 \mid \text{IntAuth}_3] \ldots
\]

\[
\begin{align*}
\text{IntAuth}_n &= \text{IntAuth}_n_I \mid \text{IntAuth}_n_R \\
\text{IntAuth}_n_I &= \text{prf}(SK_{pi_n}, [\text{IntMessage}_n_I_P \mid \text{IntMessage}_n_I_A]) \\
\text{IntAuth}_n_R &= \text{prf}(SK_{pr_n}, [\text{IntMessage}_n_R_P \mid \text{IntMessage}_n_R_A])
\end{align*}
\]

\[
\text{IntMessage}_n_{[I/R]}_P \text{ – content of Encrypted payload before encryption and possible fragmentation (not including payload header, IV, ICV, Pad Length and Padding)}
\]

\[
\text{IntMessage}_n_{[I/R]}_A \text{ – part of the message from the beginning of IKE header till the end of Encrypted payload header}
\]
Impact of New INTERMEDIATE Exchange Authentication

- Strengthens authentication of INTERMEDIATE exchanges, preventing any kind of replay attacks
- Changing the order of authentication inputs to signature calculation simplifies implementations
- Swapping the order of authentication inputs to calculation of \texttt{IntAuth_n_[I/R]} simplifies implementations
Thank you!

- Comments?
- Questions?
- Way forward?