ERP for IKEv2

draft-nir-ipsecme-erx-01

Why ERP for IKEv2?

- RFC 5296 and the bis document define a quick re-authentication protocol for EAP.
  - ERP requires fewer round-trips, so it's faster.
  - ERP can be automatic – does not require user interaction.
- Having ERP allows a smooth transition between local networks such as 802.1x to remote access networking, such as with IKEv2. This is especially desirable in mobile devices.
- However, IKEv2 (RFC 5996) is not suited for ERP, hence the need for an extension. As section 1 of RFC 5296-bis says:

```
Specifically, the IEEE802.1x specification
must be revised and RFC 5996 must be updated
to carry ERP messages.
```

ERP in the IKEv2 protocol

- Adding ERP was pretty straightforward. Here’s IKE_AUTH:

```
first request    --> IDi,
                     SA, TSi, TSr,

first response   <-- IDr, [CERT+], AUTH,
                     EAP,

                  / --> EAP
repeat 1..N times |
                  \ <-- EAP

last request     --> AUTH

last response    <-- AUTH,
                     SA, TSi, TSr,
```

ERP in the IKEv2 protocol

- Adding ERP was pretty straightforward. Here’s IKE_AUTH with ERP:

```
first request    --> EAP(EAP_Initiate/Re-auth),
                     SA, TSi, TSr,

first response   <-- IDr, [CERT+], AUTH,
                     EAP(EAP-Finish/Re-auth),





last request     --> AUTH

last response    <-- AUTH,
                     SA, TSi, TSr,
```

ERP in IKEv2 Protocol

- So what's added?
  - An "ERP supported" notification in the IKE_SA_INIT response. This replaces the Re-auth-Start message, and may contain the domain name.
  - ERP in the first IKE_AUTH exchange.
  - Update RFC 5996 to allow ERP codes.
- The domain name is passed in the clear. Probably OK.

Open Issues

Local ER Server for IKEv2?

- RFC 5296 specifies a method-independent re-authentication protocol applicable to two specific deployment scenarios:
  - where the peer's home EAP server also performs re-authentication; and
  - Where a local re-authentication server exists but is collocated with a AAA proxy within the domain.

- We're not convinced that there is a use case for IKE with anything but the first scenario.
  - Although remote-access IKE is a form of network attachment, it works over the Internet, not the local network, so the home attachment point is reachable
  - This is very different from 802.1x or PPP.

Local ER Server for IKEv2?

- We're looking for feedback.
- Is there a use-case for performing IKE with a local as opposed to a home server?
- Yes, I should be asking the IPSECME group, but they're not meeting this week.
  - Not too big on responding to the mailing list either…
- If the answer is no, then the open issue in the next slide probably becomes moot as well.

User Name in ERP?

- IPSec as defined in RFC 4301 defines a very granular policy related to identities. One user may be allowed to send and receive traffic matching a certain traffic selector, while another may not.
- With regular EAP the user is identified by either a username or an RFC-822 formatted NAI.
- With ERP the only identifier is the keyName-NAI TLV that looks like `09c2360fc3a4cd72@example.com`.
- The username part of this NAI is a hexadecimal representation of the EMSKname, which is an ephemeral value.
- A local ERP server which did not perform the original authentication cannot map this to a user name, and consequently cannot map authorizations.

User Name in ERP?

- In the first deployment scenario there's no problem.
- The ERP server is the same that made the full authentication.
- It is able to map the ephemeral EMSKname to real username.
- It can pass the real user name in the AccessAccept message it sends to the VPN gateway.
- The VPN gateway can then make authorization decisions based on policy.

- But what do we do if they ERP servers are not the same?

Questions?
Answers?