EAP Extensions for EAP Re-authentication Protocol

draft-ietf-hokey-rfc5296bis-02

Qin Wu
Zhen Cao
Yang Shi
Baohong He

Outline

- History
- Changes
- Issues
- Moving Forwarding

History

- “Submit a revision of RFC 5296 ” is an Hokey goal for July 2010
- Glen Zorn wrote the initial draft for this document and provided useful reviews.
- The version 02 is submitted before this meeting.
  - Address some remaining issues discussed in the last meeting

Changes since previous versions

- Change using MAY in section 5.3.1.1 to using SHOULD.
- Mandate sending the EAP-Initiate/Re-auth-Start message instead of optional
- Update obsolete reference RFC4306 into RFC5996
- Allow local server respond to the peer directly without forwarding the ERP message to the home domain

Issue – simplify bootstrapping

- Deprecate the flag ‘B’
  - Pro:

    In implicit bootstrapping, ‘B’ flag is useless since peer will not send out ERP message;

    In Explicit bootstrapping, ‘B’ flag can be used to trigger local ER server go back to home domain.
  - Con:

    In both above cases, local ER server can decide if forward ERP message to the home domain according to if the local server has keying materials for the peer.
- Mandate including both the name of the home domain and one of the local domain in ERP requests
  - Pro:

    the local ER server decide if respond directly to the peer by comparing the domain name in the request with its own domain name
  - Con:

    Need to assign two new TLVs to carry both home domain and local domain.

    the local ER server decide if respond directly to the peer by comparing the realm part of keyName-NAI with its own domain name.

Issue-May vs Should in RFC5296bis

- RFC 5296 uses "SHOULD" several times in section 5.2 (2nd, 3rd paragraph) but uses "MAY" in section 5.3.1.1 about if the authenticator MAY/SHOULD send a EAP-Initiate/Re-Auth-Start message when a new peer appears.
- Suggestions
  - Mandate sending EAP-Initiate/Re-Auth-Start from authenticator
  - But allow the peer send EAP-Initiate without waiting for Re-Auth-Start.

Issue-Remove local and home distinction

- Pro
  - In EAP, there is no concept of domain involved
  - In ERP, we add one entity: the ER server. This entity is inserted "between" the authenticator and the backend authentication server. Also add a new capability to derive key hierarchies called as ERKS

    Then we have now the following logical entities:
    peer <--> authenticator <--> ER server <--> ERKS <--> EAP server.
- Con
  - Domain concept comes from AAA infrastructure
  - If we consider roaming or handover across AAA domain, we should differentiate concept between local and home.

    If we limit scenario to handover within one AAA domain, then we do not need to distinct local and home.

    Bootstrapping means each mobile use should download its user profile or other subscriber information from its home domain.

Moving Forward

- Any other issues?
- Encourage more review of draft and early feedback