ERP extension for EAP Early-authentication Protocol (EEP)
draft-ietf-hokey-erp-aak-02

Zhen Cao, Hui Deng
Glen Zorn
Qin Wu, Yungui Wang
KOKEY WG @ IETF78
July 29, 2010
Maastricht, NL
Status

- Adopted as a WG item at IETF 77
- Revised to 02 version WG draft based on feedbacks from the group.
- Some open issues to be discussed in the mailing list
Issue1#: TLV allocation

- Why some of the TLVs are being allocated by IANA
- List of crypto suites" & NAS-Identifier TLVs are defined in RFC 5296, Why not reuse them?

- Yes, we can reuse them
Issue2#: Incomplete security consideration section

- Security Considerations section needs to be filled
Issue3#: CAP determination logic

- ERP/AAK server should not be involved in this decision
- Is it the AAA server’s job to decide whether the peer could be attached to?
- AAA server lacks capability to distribute the keys for multiple CA
  - Suggest to leave the issue of multiple CAPs for future resolution
  - Focus on distributing the key for a single CAP
Is it possible to parse Flag E correctly without different Code between the two messages

EAP-Initiate/Re-auth-Start messages can be distinguished from the other two message types using the 'Type' field, as in RFC5296

- Re-auth-start : type = 1
- Re-auth: type = 2
**Issue5# : Inter-domain-handover support**

- NAS-Identifier TLV for CA is unsuitable for inter-domain authentication, an additional way is required to support inter-domain authentication.
- Separate draft to address inter-domain-handover?
  - Need to address inter technology handover as well?
  - Need to introduce some new functional box (e.g., 802.21 IS)
    - Consider Multiple CA determination
- Fill this existing draft to support inter-domain-handover?
  - Need to introduce new feature or capability
    - AAA routing across domain?
Moving Forward

- Expect to issue new version based on feedback from group and comments from mailing list
- Encourage more review of draft and early feedback