IETF-75 EAP Method Update (EMU)

Joseph Salowey
(jsalowey@cisco.com)
Alan DeKok
(aland@freeradius.org)

Agenda

1. Administrivia

   Blue sheets, note takers, etc (5 min)

2. Tunnel Method requirements (Salowey - 25 min)

   http://tools.ietf.org/html/draft-ietf-emu-eaptunnel-req-03

3. Channel Binding (Hoeper - 20 min)

   http://tools.ietf.org/html/draft-ietf-emu-chbind-03

4. EAP-EKE   (Sheffer - 15 min)

   http://tools.ietf.org/id/draft-sheffer-emu-eap-eke-02.txt

5. Session policy information in EAP tunnelled method. (McCann - 15 min)

6. WAI in EAP (Richard - 20 min)

   http://tools.ietf.org/id/draft-richard-emu-wai-00.txt

Tunnel Method Requirements

- Draft -03
  - Changes to address Glen Zorn’s review
- Review from Bernard Aboba’s review
  - Discussion of issues follow

Method Chaining

- May be useful for supporting both user and device authentication
  - However it may be possible to perform without method chaining
- Is Method Chaining a requirement
  - If so MUST or SHOULD?
- Is meta-data required for differentiating user vs. device auth?

Internationalization

" The payload MAY provide a standard attribute format that supports international strings. This attribute format MUST support encoding strings in UTF-8 [RFC3629] format. Any strings sent by the server intended for display to the user MUST be sent in UTF-8 format and SHOULD be able to be marked with language information and adapted to the user's language preference.“

What is the purpose of the language information, is UTF-8 sufficient?

What about for username and password?

Data Outside Tunnel

- Some data outside the tunnel may need to be protected
  - Version, method ID
  - Methods have additional data that needs protection
  - Methods may provide protection in different ways
    - Method ID may be implicitly protected by method behavior such as key derivation

Mandatory Attributes

“The payload MUST support marking of mandatory and optional attributes, as well as an attribute used for rejecting mandatory attributes.”

Is this required?

Why not standard vs vendor specific?

Peer Identity Protection

- Peer identity protection is for method specific identifiers
  - – Not for EAP Identity outside the tunnel

Tunnel Authentication and Authentication Requirements

- Need clarification on recommendation to make them “actionable”