Tunnel Method Requirements Open Issues

Joseph Salowey
Steve Hanna
Katrin Hoeper
Hao Zhou

Major Changes in -01

- Credential provisioning moved to use case of extensibility
- Channel Binding support now refers to channel binding draft
- EAP Header protection changed to protection of sensitive data outside tunnel (if necessary)
- Added requirement that tunnel must be able to carry inner method without modifying it

Resource Constrained Environments

- Not Well Defined

- Discuss
  - Define better or remove

Authentication Support

- Provide support for other than basic password and EAP

- Proposed resolution
  - Include as a case for extensibility in section 3.9

Tunnel Man-in-the-Middle Protection

- The tunnel cannot fix inner method MitM protection if method is used outside tunnel

- Proposal
  - Change text to

  “The tunnel itself MUST provide MitM protection for the client (via server authentication and data integrity protection) and MUST not weaken any MitM protection provided by an inner method.”

Bypass of Server Authentication

- Emergency service access may require bypass of server authentication, but section 4.5.1.2 forbids this
- Proposed Resolution
  - Leave as is, text requires authentication before password is sent. This is a good requirement.
  - Add text indicating that for emergency services credentials should not be disclosed

Certificate Revocation

- Certificate revocation too onerous a requirement
- Proposed resolution
  - Leave as is, revocation is required so the client can be sure of authenticity of server before sending password
  - Current doc does not require a specific mechanism

Session Resumption

- Currently MUST, should it be?
- Proposal
  - Leave as is

Other Open Issues?