EAP Tunnel Method

draft-ietf-emu-eap-tunnel-method-05

Hao Zhou, Nancy Winget, Joe Salowey, Steve Hanna

EMU WG group

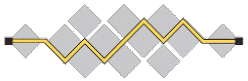
IETF 86

Status

- Draft -05 submitted on Feb 7, 2013
- WGLC completed Feb 26, 2013
- Received a few review comments
  - Thanks Jim Schaad and Sam Hartman for your comments
  - Authors have responded and addressed all comments
- Working on submitting a new revision

Major Changes

- Section 3.3.3, clarified that Intermediate Result TLV and Crypto-Binding TLV MUST be exchanged after each EAP method, even with a single inner EAP method.
- Section 3.5, clarified that tls_unique is from Phase outer TLS tunnel before beginning of the Phase 2.
- Section 3.8, added a section talking about mutual authentication before peer provisioning services.
- Section 3.11, added a section describing channel binding flows.
- Section 7.6, changed SHOULD to MUST for matching server certificate realm portion.
- Updated reference from I-D to RFCs.



Open Issues for Discussion

1. Do we expect that the client certificates would only be used for this purpose and not for general purpose TLS client authentication? Should we should define an EKU for the purpose of doing EAP Tunnel Method (allow it to be used for all of the previous and future versions thus being generic)?

2. Do we want to try and solve the question Sam has raised about naming of entities in certificates. This would mean defining a new OtherName extension to PKIX for the purpose of placing NAIs into certificates. This would allow for an NAI of the form “@realm” to be placed in a server certificate to define that it is the EAP server for the realm. This does assume that there will not be two different servers which are disjoint servicing the same realm but that would be a very unusual case.

Proposal – Create an RFC on EAP server identity representation and verification

Next step

- Submit new revision of draft addressing review comments and issues discussed.
- Submit to IESG for IETF LC?

Thank You !