IETF-85
EMU TEAP Updates

Nancy Cam-Winget	ncamwing@cisco.com
Joseph Salowey	jsalowey@cisco.com
Hao Zhou	hzhou@cisco.com
Steve Hanna	shanna@juniper.net

draft-ietf-emu-eap-tunnel-method-04

- New version (04) submitted in October
- Several comments received on -03
  - Thanks Jim Schaad, Jouni Malinen, Simon Josefsson for your comments
- Comments have been resolved
  - One issue remaining on certificate provisioning

Changes from -03

Section	Updates
3.4	All peer and server authenticated identities and identity types need to be exported
3.6.1	Error handling of outer EAP packet layer defined (ignore invalid outer TLVs, else ignore TEAP pkt)
3.6.2	If TEAP server disallows restarts, it MUST terminate with EAP-Failure packet
3.6.3	After Result TLV failures, server now MUST (vs SHOULD) send clear-text EAP-Failure
3.8	Tightened PAC provisioning process flow language
3.9	Clarified cert provisioning happens only after successful client identity proof
3.10	Clarified unauthenticated provisioning conditions (e.g. no validation of server by peer or no authentication during cipher negotiation)
4.1	Added Outer TLV length and flag bit to signal its presence
4.2	Changed to NAK or Result TLV to be optionally sent if none of the TLVs are understood

Changes from -03

Section	Updates
4.2.3	Clarified that peer send the requested Identity Type TLV if it does have it.
4.2.9	Added Request Action TLV processing rules
4.2.13	Introduced EMSK Compound MAC and MSK Compound MAC fields to the Crypto-binding TLV
4.3.1	Added Outer TLV processing rules
5.1	Changed TLS Keying Material Exporter label to "EXPORTER: teap session key seed".
5.2	Changed IMCK generation from MSK based to either EMSK or MSK with corresponding rules.

Certificate Provisioning

- Current Draft uses “PKCS#7” and “PKCS#10”
- Jim Schaad comments that we should use CMS as defined by the IETF instead of PCKS
- Questions:
  - Any issues with using CMS?
  - Can we align closely with draft-ietf-pkix-est?

Next Steps

- Call for review and WGLC after IETF-85

Questions?