EAP Key Derivation For Multiple Application

(draft-salowey-eap-key-deriv-00.txt)

Pasi Eronen
(pasi.eronen@nokia.com)
Joe Salowey
(jsalowey@cisco.com)

Motivation

- Key Material needed for multiple applications
- Independent of EAP-Mech
- Independent of Applications
- Cryptographic Separation between apps
- Consistent Key Derivation

Applications

- Link Layer Ciphering (WEP,802.11i,MPPE,…)
- Fast Roaming
- Re-Authentication
- Message Protection
- Things we have not thought of yet!

Requirements

- Reserve/Specify Extended Master Session Key Material (EMSK)

  (draft-aboba-pppext-key-problem-06.txt)

  - Not enough alone, No guarantee that applications will derive independent keys.
  - Cryptographic separation and EMSK security left to chance

- Standard KDF to derive application specific master session keys (AMSK) from EMSK

Key Derivation

- Use labeled key derivation (e.g. TLS PRF)
  - Label = string (“application name and key use”)
  - May include application specific data

- Application
  - Registers key label (with IANA)
  - Defines how keys will be used/derived from (AMSK)
  - Defines where keys are used and how they get there

- Independent Keys are derived for each application

Issues

- How much material should be reserved for EMSK?
- EMSK stays within EAP-Server
- Binding of multiple keys

Questions?

- http://www.ietf.org/internet-drafts/draft-salowey-eap-key-deriv-00.txt

jsalowey@cisco.com

pasi.eronen@nokia.com