

TEAPv2

EMU - IETF 125

WHAT'S WRONG WITH TEAPv1?

- ▶ Key derivation is complex. Start with

$$\text{key}_0 = \text{TLS-Exporter}(\dots)$$

- ▶ Then, for each round:

$$\text{MSK-key}_n = \text{mash}(\text{MSK}_n, \text{key}_{n-1}) \quad \text{EMSK-key}_n = \text{mash}(\text{EMSK}_n, \text{key}_{n-1})$$
$$\text{key}_n = \text{choose}(\text{MSK-key}_n \text{ or } \text{EMSK-key}_n)$$

- ▶ MSK and/or EMSK might not exist, and MSK is sometimes set to zero.
- ▶ Everyone did something different for the key derivation.

FIXING IT

- ▶ We create a new TEAPv2 with greatly simplified key derivations.
- ▶ use hostap / eapol_test for implementation
- ▶ Test code before new specification is finished.
 - ▶ Everyone can test against it
- ▶ Eliot has rough draft working

FIXING IT EVEN MORE

- ▶ Mandate all allowed flows, including PKCS#7, PKCS#10, etc.
 - ▶ Which means implementing all of them in hostap / eapol_test
- ▶ Fix MTU issues by mandating maximum fragment size = 1280
 - ▶ We can't add negotiation to 802.1X / EAPoL, so we just fix TEAP

QUESTIONS

- ▶ Comments?
- ▶