networkRADIUS

TLS 1.3

AND TLS-BASED EAP TYPES

ALAN DEKOK IETF 104

TLS 1.3 AFFECTS MANY THINGS

- Key derivation has changed in TLS 1.3. This affect many EAP types:
- FAST (RFC 4851)
- TTLS (RFC 5281)
- TEAP (RFC 7170)
- PEAP (MS web site)
- ??? other vendor methods ???

THE SIMPLE SOLUTION

- Update EAP-TLS to include “Method type” in key derivations
- Update other methods to use the same key derivation
- Changing only the value of “Method type”
- This seems better than the existing mish-mash of type-specific key derivations and type-specific labels

THE HARDER SOLUTION

- FAST and TEAP both have much more complex key derivations
  - The document makes proposals
  - These need external review. It's not clear if the draft is in any way sane
- PEAP is vendor-defined
  - But in wide use. Can we update a vendor spec?
  - In discussions with MS about this

SECURITY CONSIDERATIONS

- Not a lot of issues with the new key derivation
- Many, many, issues related to EAP and TLS
- Some discussed in EAP-TLS draft, others many need discussing here

QUESTIONS?

- Please review key derivation for FAST and TEAP.