networkRADIUS

TLS 1.3

AND TLS-BASED EAP TYPES

ALAN DEKOK IETF 105

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 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”
- It’s not clear what to do for TEAP and FAST
  - Review from implementors / authors is requested

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?

- Who will review key derivation for FAST and TEAP.
- Do we have TEAP errata fixes here for TLS 1.2, or in another document?
  - Leaving them as errata seems wrong
  - As does putting them into this document