networkRADIUS

TLS 1.3

IMPLEMENTATION REPORT

ALAN DEKOK IETF 110

PARTICIPANTS

- Apple, Cisco, FreeRADIUS, hostap / wpa_supplicant, Microsoft
- Testing based on -13
  - due to pre-existing implementations, and a desire to not confuse the issue for new participants
- Implementations tested
  - client (Microsoft and wpa_supplicant)
  - server (FreeRADIUS and hostap)

METHODS TESTED

- EAP-TLS, PEAPv0, TTLSv0
- Any implementation should be able to add basic TLS 1.3 support with minimal code changes
  - Presuming that the TLS layer is already abstracted out.
- EAP-TLS is simple, PEAP, TTLS have more issues.
  - Many corner cases with interactions between TLS and EAP state machines
  - TLS libraries APIs can be opaque and difficult to control from an application

OPAQUE TLS LIBRARIES

- In many cases, API calls are *configuration*, not *state change*
  - i.e. “allow X” versus “do X now”
  - SSL_CTX_num_tickets() - allow tickets
  - SSL_new_session_ticket() - send ticket now
    - But only in OpenSSL 3.0.0, which is not yet released
- As a result, inter-operability for PEAP and TTLS is still in flux

OPAQUE TLS LIBRARIES

- It is impossible in current OpenSSL releases to control when session tickets are sent
- For PEAP / TTLS, we see session tickets sent from the server, all alone
  - not merged application data, despite application data being ready
  - This confuses the clients, who expect something more useful

EXTRA NOTES

- All implementations will send (server) or store (peer) only one session ticket
  - Consensus that more than one is not necessary, it’s not clear what more than one can be used for, and RFC 8446 suggests only one for EAP use-case
- Minimal feedback from Apple
  - silence means agreement, or disinterest, or not enough time?
- Cisco is looking into it in more detail in the coming weeks
  - and will have more feedback

SUMMARY

- Both close_notify and 1 octet application data tested for EAP-TLS
  - tested on client / server via configurable flags (to be removed on finalization)
  - Application data is preferred by implementors
  - It can be difficult to convince the TLS layer to send close_notify.
- Key exporters are -13
  - no strong opinions on changes in -14, simple enough to change the code
- Still much spelunking to do in TLS / application interaction for PEAP / TTLS