IETF Hackathon: EAP-TLS with large certs and long chains

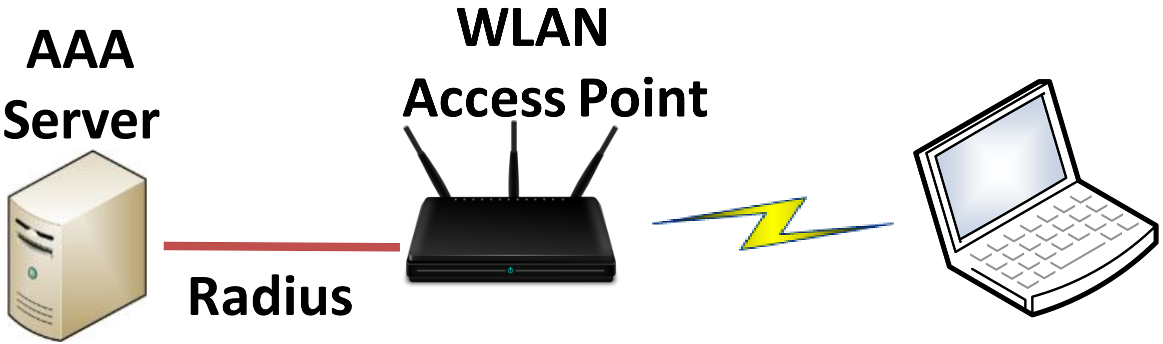
IETF 101

17-18 March, 2018

London

Hackathon Plan

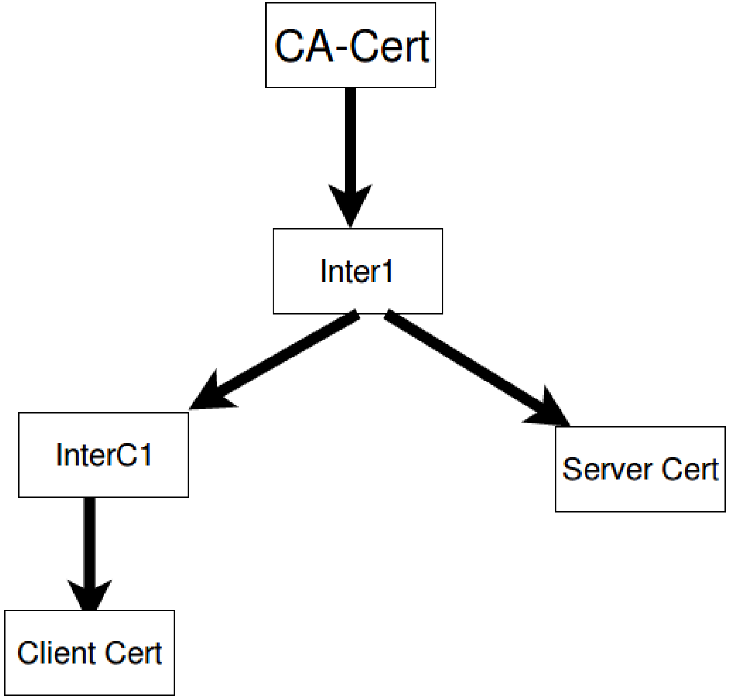
- Extensible Authentication Protocol (EAP)
  - Wireless access authentication

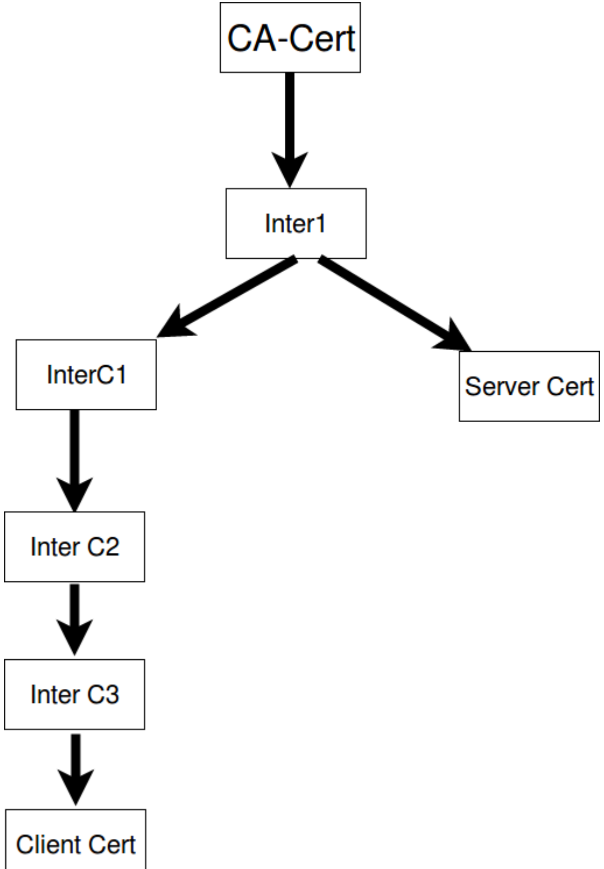


Hackathon Plan

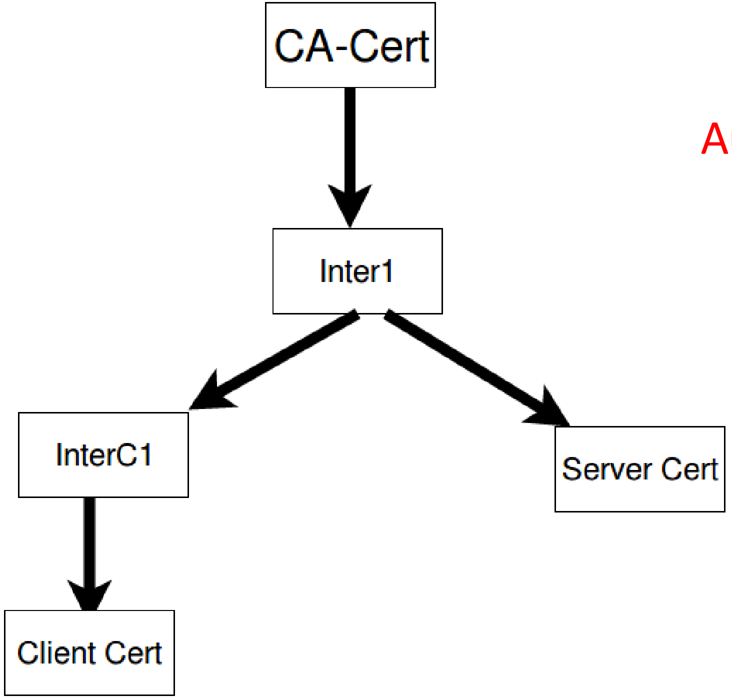
- EAP Method Update (EMU) WG re-started and re-chartered
  - Reported issue on the list with EAP-TLS
    - Certificates are large and chains are long
    - Especially in some enterprise deployments
    - Authentication fails even with valid certs on both sides
    - AP implementations drop EAP session after 40 packets
- GOAL: Reproduce the errors

What we learned

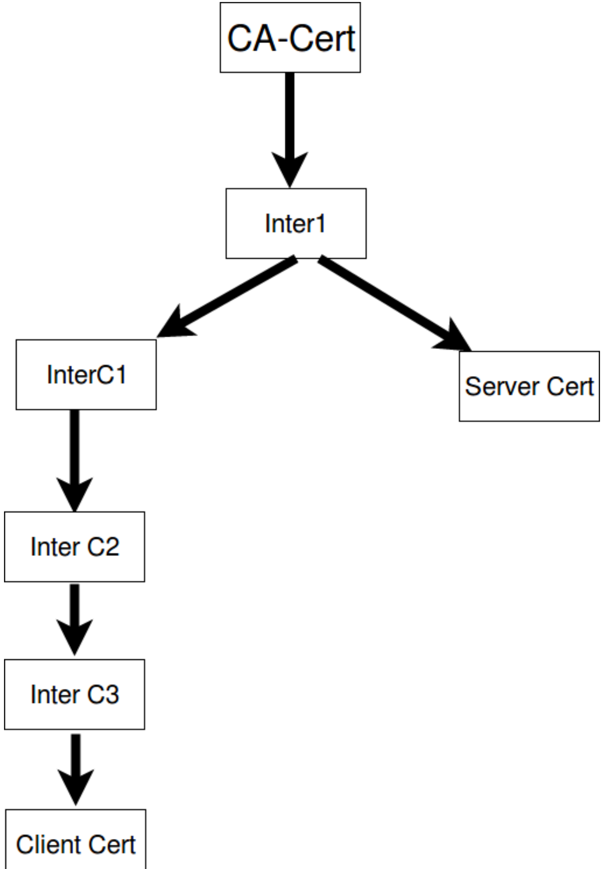




What we learned



Authentication
Successful



What we learned

- Reduce EAP fragment_size: from default of 1396 to 200 bytes
- Voila: We have a failure
  - AP barfs and drops the session
  - Back-of-the-envelope calculations show that cert chains should be 55000 bytes for it to fail in ‘normal’ scenarios
  - Testing continues with ECC based certs
  - Input to EMU on Monday

Wrap Up

Team members:

First timers @ IETF/Hackathon:

Aleksi Peltonen, Aalto University

Claire Delcourt, Nokia

Regulars:

Darshak Thakore, Cablelabs

Mohit Sethi, Ericsson