Signal channel implementation report

IETF 101

Presenter: Andrew Mortensen

Arbor DOTS status

- Partial implementation of -17 revision of signal channel draft

- DTLS client/server implementation
  - PKI/PSK mutual auth
  - IPv4/IPv6

- Some local interop testing with NTT's go-dots

Challenges

- Several python CoAP frameworks, but only one appears to support DTLS
  - aiocoap uses tinydtls

Challenges

- No good python DTLS implementations
  - tinydtls limited to PSK, will not add PKI

- Wrap mbedTLS with Cython
  - Working with asyncio/aiocoap/uvloop
  - Goal: release as open source

Challenges

- aiocoap limitations
  - server: ping handling unavailable to application
  - NON handling of error responses causes exception
  - TCP support is rudimentary

- Patches to be submitted upstream
  - Also add support for new DTLS module

Interop

- go-dots
  - Ping
  - Mitigation request

- NCCgroup
  - Ping*

Thank you

Questions?