Operational Considerations for use of DNS in IoT devices

Michael Richardson
IETF111 OPSAWG meeting
July 30, 2021

`draft-ietf-opsawg-mud-iot-dns-considerations-02`

DNS names in MUD files

- previously (IETF107, IETF110 at DNSOP) explained the situation
  - https://datatracker.ietf.org/meeting/110/materials/slides-110-dnsop-sessa-operational-considerations-for-use-of-dns-in-iot-devices-00
  - watch IETF110 DNSOP presentation https://youtu.be/61Mti_hwLGs?t=6308
- most of advice is about not using IP literals, and using names that a manufacturer controls
- most problems come from outsourcing to “cloud”
  - because cloud provider controls names

DNS, MUD and geofenced

- A common thing today is that DNS servers give different answers depending upon who asks
- for instance A/AAAA returned depends upon where the query comes from, so that geographically (network topology) closest server is used
- for IoT devices, we might see this for cloud server part, and for firmware update sources
- ***IoT devices gets different answer than MUD controller, so ACLs are not correct***

Summary from DNSOP presentation

- it’s more complicated, not predictable
  - “it will never work”
- “it will require special DNS server for MUD”
- suggestion here that we should use SOCKS
-
- my Conclusion: suggest that IoT vendors don’t use geofencing
  -

Discussion

?