CAPPORT Architecture

draft-ietf-capport-architecture-00->01

Authors: K. Larose, D. Dolson

Architecture Updates

Presenter: Kyle Larose

Updates

- Missed deadline to upload `-01`
- Uploaded now, though. :)
- Major changes in this update:
  - Discussed Security of API
  - New section: User Equipment Identity
- Issues being discussed on list and on github

Security of the API

- Privacy and Integrity are a MUST
- TLS is a MUST
- Does the architeceture need to discuss this in any more detail? It's fairly vague

User Equipment Identity

Lots of time spent at IETF 100 discussing this topic. The architecture was updated in an attempt to capture the results of this discussion:

- Identifier should be unique
- It should be hard to spoof
- The API needs to know it
- The Enforcement Device needs to know it

User Equipment Identity

To help with understanding the requirements on the identity, some recommendations for evaluating potential identifiers are provided, along with two examples of possible identifiers:

- Physical Interface
- IP Address

Open Issues

- Security of the API (already discussed)
- Identity of the User Equipment (already discussed)
- Deprecate or Update RFC7710?
- Does the PvD give the state, the API, or both?
- Negative Captive Portal indication?
- ICMP?

Deprecate or Update RFC7710?

Some on-list, and on-github discussion of this:

- The chairs proposed a plan to move it forward
- No objections from authors, with some approval
- Some offers to help
- The chair's plan also had this addressing the Negative Captive Portal indication issue

Does PvD give the state, the API, or both?

No discussion about this. Thoughts?

ICMP?

Not much discussion on this since the last meeting. We need to move it forward.

- Simple ICMP mechanism for notifying of captivity?
- More complex mechanism satisfying more use-cases?
- No mechanism at all? (If so, how do we indicate the non-hotspot cases)?