Security for Hotspot Lite

Darshak Thakore (CableLabs), Thomas Derham (Broadcom)

Capport WG

IETF 101, London

The Problem

- Public Wi-Fi hotspots today: typical security options
  - Semi-public WPA2-Personal
    - No meaningful security (passphrase known to hacker)
  - Open (often combined with captive portal)
    - No security
  - Passpoint, based on WPA2-Enterprise
    - Complex deployment (CA-based PKI security and signup/onboarding); limited to large operators/enterprise
- Lower complexity secure solutions are needed for public Wi-Fi hotspots deployed by smaller operators/entities, for which Passpoint may not be a viable option

Context

- CAPPORT is working on Captive Portal Architecture and API, which is well-suited to many public Wi-Fi hotspots
  - Consider proposing protocols by which the user can trust the network and establish authenticated secure connectivity

Security components

- There are multiple aspects to providing security in these hotspots:
- (1) Trust and authentication of the hotspot network (by the client device)
  - No expectation of pre-provisioning
  - Make “evil-twin AP” attacks HARDER (combine capport API authentication with AP validation)
- (2) Pairwise link encryption
  - Comes for “free” with DPP, OWE(RFC8110)
- (3) Network integrity
  - Nothing to do specifically with capport

Complexity to deploy and maintain needs to be low (for user and operator)

Questions to capport

- Can we leverage capport API to “improve” cryptographic binding with the AP’s (and possibly with the NAS)

- Is this of interest to wg?
- Is this within scope ?

- If NO to (1)
  - Would an individual submission be considered?