Onboarding and Portals

DRAFT-RICHARDSON-EMU-EAP-ONBOARDING-04

MICHAEL RICHARDSON <MCR+IETF@SANDELMAN.CA

ALAN DEKOK

IETF124 - MONTREAL

DEVICE ONBOARDING

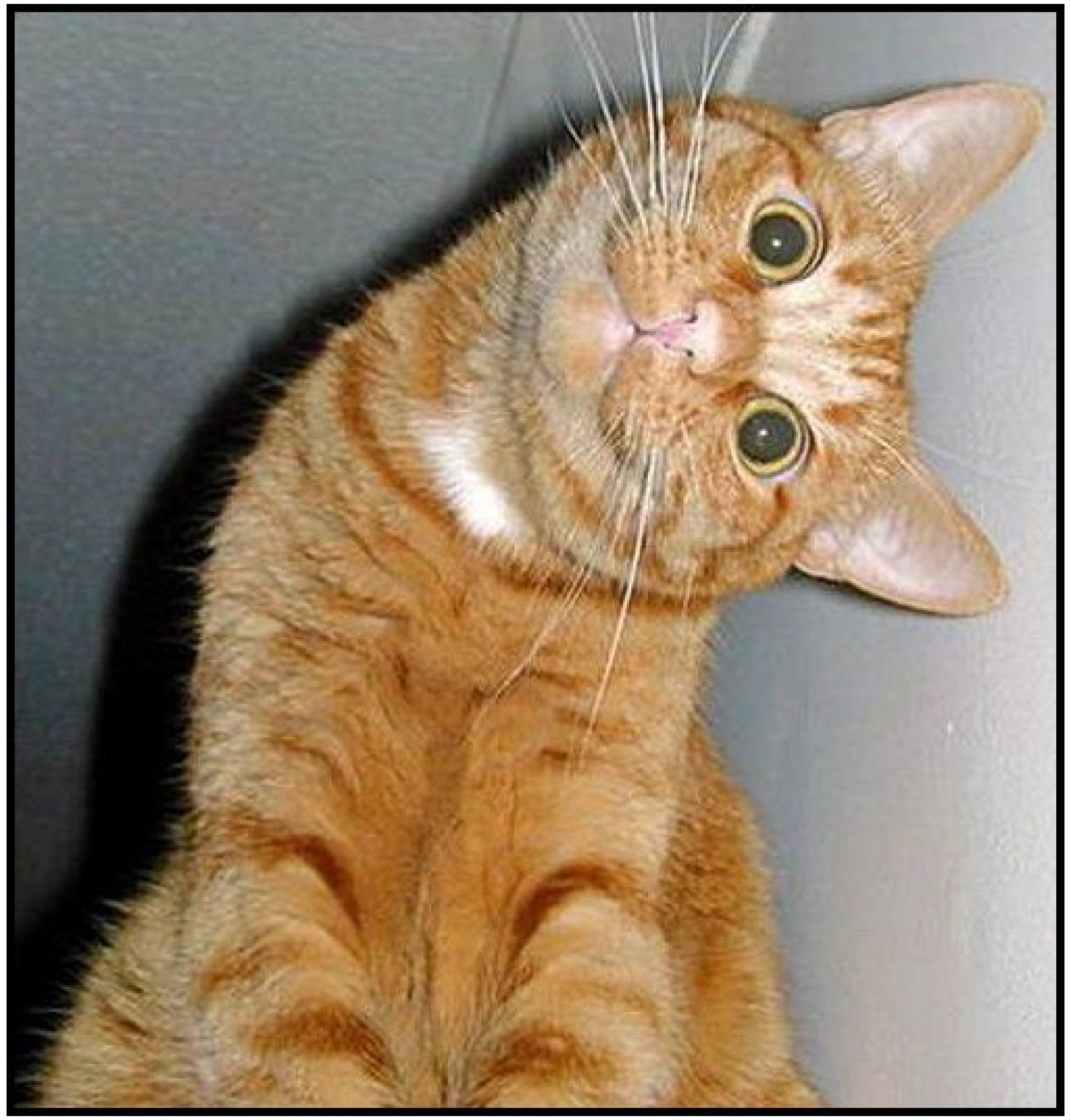
- Unconfigured device needs to be onboarded, but has no credentials
- Solution: use **unauthenticated** EAP-TLS, and join a captive portal network
- RFC 5216 allows for unauthenticated EAP-TLS, but offers no further details
  - This document is the small amount of details required
- Solution: use explicit signalling via NAI of **onboarding@tls.eap.arpa**
  - Enabled by recent work on eap.arpa, approved, in RFC-editor Q
  - This NAI is local only, and cannot be forwarded / proxied
  - device can access a limited network for onboarding: a quarantee network

QUARANTEED AND/OR CAPTIVE!

- Most enterprises have networks (“SSID”s) onto which devices that fail their security posture are placed.
  - Access to limited DNS and operating system update servers is provided.
- Many enterprises, hotels, train-stations, etc.. have guest networks with a typical captive portal.
  - This mechanism lets those networks have encryption without needing yet-another WPA mechanism. You can have it today.
- On a captive portal network, an IoT or headless device can use RFC8995(BRSKI) to get credentials
  - Or another system,
  - SZTP,
  - OPC UA Part 21, …
- this avoids trying to stuff BRSKI into EAP, and reuses existing captive portal infrastructure
  - And does not add any additional SSIDs, so takes no more beacon space, etc.

UPDATES SINCE IETF114 AND IETF123

- A chunk of what was in this document is now in draft-ietf-emu-eap-arpa
- Looks like maybe **onboarding@tls.eap.arpa** or **nobody@tls.eap.arpa** might be correct, but not sure which one yet.
- Had planned running code in 2023, but it has yet to happen.
  - Was discussed in Madrid



DISCUSSION

DRAFT-RICHARDSON-EMU-EAP-ONBOARDING-04