networkRADIUS

EAP Usability

ALAN DEKOK IETF 111

https://datatracker.ietf.org/doc/draft-dekok-emu-eap-usability/

THE PROBLEM

- EAP is hard to configure
- Vendors randomly change UIs, APIs, work flows, etc. for EAP configuration
- MDM vendors sell “add ons” for simplification and ease of use

- *Draft assumes people-oriented devices, may be of interest to IoT.*

THE REQUIREMENTS

- A device has:

1) Network connection (untrusted is fine, slow is fine)
2) root CAs for web PKI
3) user name to authenticate with: **`bob@example.com`**
4) Password* to authenticate with: **`superSecret`**

* Entry of the password can be delayed until much later

THE PROPOSAL

- Get NAI from username: **`bob@example.com ➡ example.com`**
- Look up DNS CERT RR: **`_server._cert._eap.example.com`**
  - get URI: **`https://example.com/.well-known/eap/server.pem`**
- Verify Web cert via web root CAs, download certs
- Similar method for CA cert / server cert / client cert
- Certs can include network identification information (SSID, RCOI, etc)
- Client can now authenticate to network, verify server cert, use name/password

RUNNING CODE

- https://github.com/NetworkRADIUS/automatic-eap/
- Host defines domain name and certificates (generation scripts included)
- Brings up docker images for client and servers (RADIUS, DNS, WWW)
- Client does lookups, downloads certs
- Generates configuration, and runs eapol_test against RADIUS server
- ~~Trust on First Use~~ **End to end trust verified at every step**

QUESTIONS / COMMENTS?