IETF 91 – opsawg meeting
Honolulu, 12 Nov 2014

RESTENA

draft-winter-opsawg-eap-metadata-01

Recap : Background

- IETF has produced a great standard for authentication : **E**xtensible **A**uthentication **P**rotocol
- EAP is a mere container, carries EAP Methods
  - Needs some configuration itself (e.g. max fragment size)
- Each method has its own set of configuration parameters
  - Authenticate EAP server to the EAP peer
  - Authenticate EAP peer to the server
  - Anonymity support
  - … and plentiful more
- Multiple methods can be configured ; priority ?

Recap : Problem Statement

- EAP server setup must match EAP peer's configuration for successful auth
- EAP peers are configured by **end users** (argh!)
  - Lengthy PDF instructions are the norm, especially in BYOD
  - EAP peer UIs typically make it easier to be insecure than secure (« Don't validate server certificate » ; « do you trust this fingerprint ? »)
- **The best auth protocol can't deliver if its users get it wrong.**
- **Security for end users at stake.**

Diff -00 to -01

- Following WG advice : use YANG model as source format
- Consuming devices can use either derived XML Schema
  - because it's popular in OSes and straightforward
  - Pyang makes my day
- Or JSON
  - Alternative to XML if easier in a consuming device implementation
  - E.g. could plug into Google's « Advanced Network Configuration »
- Still does not contain WiFi and IP Configuration specific settings
  - YANG model allows unique namespace / name identitification
  - Can be referenced from overarching network config descriptions

Future Plan

- Hope to adopt draft as WG item in opsawg
  - Solicit expert review from relevant WGs
    - emu – only about methods, and closing down, but high concentration of expert knowledge on ML
    - radext – much of EAP goes over RADIUS
    - dime – extensive use of EAP-SIM / EAP-AKA in Diameter deployments
- If adopted, aiming for STD track

YANG Service Model ?

- « Connectivity Service » YANG model would be kinda cool
- Authentication (EAP Metadata, Captive Portal specifics, ...) one building block
- Layer 3 specifics (IPv(4/6) Configuration) another
- Layer 2 specifics (Wi-Fi/802.3/...) a third one