W3C Web of Things Security Plugfest Postmortem

Michael McCool

W3C WoT WG Security and Privacy TF

Prague, March 2018

Outline

- What we tried
- Issues
- Plans for the next plugfest

What we did…

- Intel: Two exposed Things with
  - local https
  - two global https endpoints (reverse ssh tunnel, Let's Encrypt)
  - Basic auth
  - Unfortunately technical problems disabled them during the plugfest…
  - Not used by anyone else (no node wot connection)
- Siemens
  - https + basic authentication and bearer tokens (jwt)
  - HTTP proxy support: forward proxies and reverse proxies (things only reachable through proxies)
  - Used with Oracle instance: config flag disabling cert check (see wot-servient –h and look for allow-self-signed to allow consume)
  - Tested previously:
    - Bearer tokens with Fujitsu beacon light
- EUROCOM
  - TDs distributed via https from cloud, AES-256, bearer token auth
  - Things themselves did not (yet) have security
- Panasonic
  - https + bearer (jwt) for Air conditioner (global https) – Let's Encrypt; local http only; no node-wot connection
- Fujitsu
  - Proxy supported https; proxy support; external CA for global https; locally http only
  - https supported locally, but turned off for plugfest)

Issues

- Intel: “Protocol error” – worked in hotel, not at Oracle
- Network disconnection/local https/self-signed certificates
  - See wot-servient option to allow self-signed certificates
  - Maybe we should work with HTTPS Local CG in W3C
- Incomplete security metadata
- Cross-site scripting
  - Browser (chrome) preventing access unless use appropriate header option
- Only limited set of authentication schemes
  - Basic auth and bearer tokens (jwt)

Security Test Tooling

- Chrome browser
  - Has cross-site scripting protection (for use of scripting API)
- Curl
- Postman
- ARC
- Node-Red
- Not working:
  - Copper under Firefox
    - But there is a version for Chrome, but not as nice
  - How to do coaps testing?

Scripting API

- Cross-site scripting issue specific to using WoT scripting API inside a browser
  - “Dashboard” app trying to connect to Things that were not based at the URL the script was served

Followup

- Put postmortem in MD on github (security-portmortem.md)
- Create survey
- Ask for edits to above MD
- Determine difference between OCF security model and IETF ACE
  - Discuss in IETF T2TRG
- Want to look at other ecosystems
  - EG OPC-UA, LwM2M
- General security topics (for now: practice first, then generalize)
  - Metadata
  - Lifecycle
  - Gap between current security document and issues raised at plugfest
  - Testing and validation

What we need to do

- By the next plugfest…
  - Consistent security metadata
  - 30 june/1 july plugfest
  - Done by : 1 june
- More authentication schemes (need to prioritize list…)
  - OAuth2
  - API keys over HTTPS
  - Basic auth over HTTPS, Digest over (local) HTTP
  - Wider use of bearer tokens (needs HTTPS)
  - Pop tokens (at least as as a 1-1 prototype)
  - All externally visible endpoints with HTTPS
  - HTTP Proxy support
  - ACE over UDP/DTLS (and TCP/TLS?)
    - OCF is based on ACE: coap/DTLS + AS, CMS, ACL, roles
    - How do we build a test system? Siemens has a Node