W3C Web of Things Plugfest Security Review

Michael McCool

W3C WoT WG Security and Privacy TF

Bundang, July 2018

Outline

- Who tried what
  - Intel, Panasonic, Smart Things, Siemens, EURECOM, others?
  - HTTPS (direct and via proxy), Auth (basic, digest, bearer tokens, psk)
- Issues Arising
  - Security Metadata Structure
    - Definitions, multiple levels (2? 3?)
  - Security Metadata Content
    - Schemes, scheme parameters, vocabulary
  - Interactions with Architecture
    - Proxies
- TO DO
  - Online and plugfest
  - Security testing and validation

Intel

- Auth
  - HTTP Basic
  - HTTP Digest
- Encryption
  - HTTPS Proxy endpoint, Let's Encrypt certs
    - Running in cloud service
    - Transparent proxy (endpoint wrapper)
    - Both cloud and reverse tunneled HTTP services
  - Direct HTTPS with Let's Encrypt certs
    - Running on local device; reverse tunneled out and exposed on cloud endpoint
    - Certificate valid for cloud endpoint; but TLS managed by device (end-to-end security)
  - Direct HTTPS with self-signed certs
    - For local devices
    - Client must accept self-signed cert
- Secured services
  - Thing Directories (cloud and gateway)
  - Thing Playground (cloud)
  - OCF-WoT metadata bridge (gateway)
  - CoAP/HTTP bridge (gateway)
  - OCF devices (via CoAP/HTTP bridge)
  - Simple-webcam (native web service)
- Other notes
  - Two cloud servers
  - Two separate local networks behind NATs
  - TDs with multiple forms (different endpoints) with different security for the same physical device
  - Challenges with port 22 being blocked…

Siemens

- Auth
  - HTTP basic
  - JWT bearer tokens
- Encryption
  - HTTPS
- Other
  - HTTP proxy support:
    - Both forward proxies and reverse proxies (things only reachable through proxies)
  - Used with Oracle instance
  - Bearer tokens with Fujitsu beacon light

Panasonic: Implementation 1

- Bearer authentication using `"bearer"` security scheme
  - Indicated authorization Url…
  - But actually formed a bearer token manually
- Specified security in TD by default
- Indicated no authentication is required using `"security": []` override.

At top level, used this:

```
"security": [{
        "scheme": "bearer",
        "format": "jwt",
        "alg": "ES256",
        "authorizationUrl": "…"
}],
```

In forms for interactions that did not use security, used this:

```
"forms": [
    {"href": "operationStatus",
     "mediaType": "application/json"},
    {"href": "https://…/operationStatus",
     "mediaType": "application/json",
     "subProtocol": "LongPoll",
     "rel": "observeProperty",
     "security": []
    },
    {"href": "wss://…./operationStatus",
      "mediaType": "application/json",
      "rel": "observeProperty",
      "security": []
     }
]
```

Panasonic: Implementation 2

- Online WoT Server Simulator requires the following HTTP header upon request

```
X-PWOT-TOKEN: <access token>
```

However, the TD is not correct at this moment. Currently we have:

```
"security": [{
        "cat": "token:jwt",
        "alg": "ES256",
        "as": "https://plugfest.thingweb.io:8443"
    }],
```

- It should updated to the new TD specs.
- It should use `"scheme": "apikey"`.

==> plan to update the TD of Online WoT Server Simulator by the next PlugFest.

Smart Things

- Example TDs for CoAP devices using PSK
- Raising need for CoAP-specific security metadata
- MQTT metadata can probably reuse existing vocabulary, eg "basic"
  - An assumption that needs to be tested

Eurecom

- Auth:
  - Bearer tokens
- Encryption
  - HTTPS for both Things and TD service
  - TDs encrypted and decrypted after download using pre-shared key

Issues Arising

- NAT Traversal
  - Can't depend on port 22 being open…
- Pre-shared keys
  - Is `"scheme": "psk"` needed?
- Self-signed certificates
  - Need to validate certificate: Onboarding service? Validation service?
  - Is `"scheme": "cert"` needed?
- Security definitions vs activated security configurations
- Multilevel security configurations
  - Right now can be given at three levels; top, interaction, form
  - Configurations at lower overrides higher
  - All three needed?
- "Add-on" security configurations
  - Would be nice to have way to add configs, not just overrides

Next

- Implementations/use cases for all existing schemes
- New schemes
  - Local TLS/DTLS
  - MQTT, CoAP, OCF
  - Basic auth over HTTPS, Digest over (local) HTTP
- Demonstration of at least one scheme using external vocabulary
  - And maybe move some existing schemes out to external vocabulary…