Considering security for descriptions of Things

T2TRG work meeting 2023-11-03

Ari Keränen
ari.keranen@ericsson.com

Questions

- What are relevant security considerations for data and interaction model description formats?
  - Focusing here on considerations for Semantic Definition Format (SDF) but same considerations should apply broadly
- What can we learn from other description formats?
  - Where to look? Taking a look at W3C Web of Things (WoT) here
- What may be different here?
  - E.g., SDF does not itself contain protocol bindings or instance IDs like WoT TD does (but may eventually do…)

W3C WoT Thing Description Security Considerations

- Section 10 in TD spec (and WoT Security and Privacy Guidelines spec)
- MitM attacks through URL-rewriting
  - Only relevant for protocol bindings
- Context definition file tampering (when retrieved externally) can modify interpretation of vocabulary
  - SDF provides “context” via namespaces; content may be retrieved dynamically
    - sdfRef, sdfRelations, ...?
- Limiting duration for access to affordances
  - Only relevant with protocol bindings

WoT TD continue'd

- Attacker with access to TDs may use them to identify vulnerable devices and plan attacks on them
  - Partially applicable (not directly for protocols and security mechanisms), but descriptions can help identify other vulnerabilities
- Script injection
  - Qualities intended for human consumption (e.g., "description") can be used in UI components; need to be sanitized for code (HTML, JS, SQL, etc.) to avoid script injection attacks
- JSON parsing
  - "JSON should not be parsed as JavaScript using eval(); intended to be a pure data exchange format "
  - Yes

WoT TD continue’d

- JSON-LD Expansion
  - Short terms expanded with longer IRIs. Memory consumption may expand considerably and result in e.g., buffer overflow
  - Applicable to SDF due namespaces and CURIEs; high dependency on how implemented

WoT TD privacy considerations

- Context fetching
  - If namespaces and sdfRefs are dereferenced origin host can gather privacy sensitive data based on requests
  - See also draft-bormann-t2trg-deref-id
- Immutable identifiers / fingerprinting / ID metadata / globally unique IDs
  - WoT TDs have identifier (due to instance nature) that could potentially be used for tracking devices and persons attached with them
  - Relevant for SDF instance discussion
- Inferencing of Personally Identifiable Information (PII)
  - Metadata (description) could contain PII; need to handle descriptions accordingly