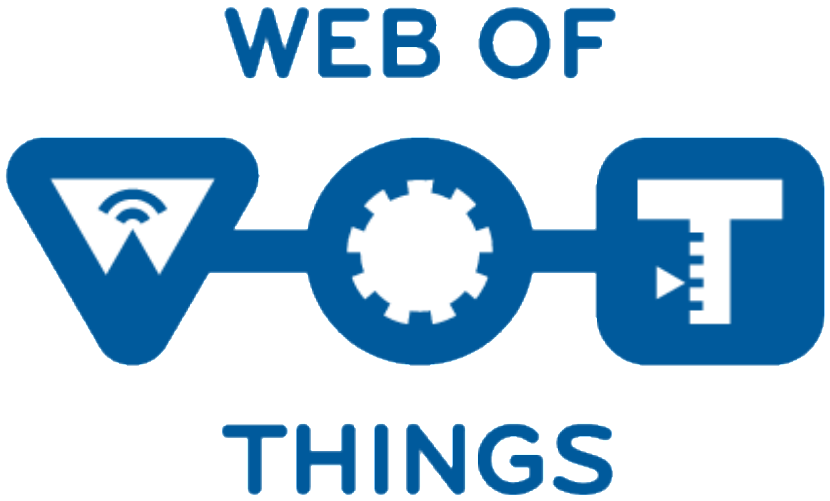

Security and Privacy

Michael McCool

15 September 2023

TPAC 2023

Outline

Agenda (wiki) – 30m (20m presentation, 10m discussion)

1. Threat Model vs. Considerations (7m)
2. Use Cases and Requirements (8m)
3. Work Items and Reorganizations (5m)
4. Discussion (10m)

Threat Model vs. Considerations

- Detailed threat model and stakeholder definitions exist in the WoT Security and Privacy Guidelines (S&PG).
- Detailed security and privacy considerations exist in each deliverable, e.g. the WoT Thing Description 1.1
- S&P Considerations follow a template: risk, then mitigation(s)
- **These are not consistent!**
  - *Risks in considerations should link to Threats in S&PG.*
  - *Names of Threats/Risks (and definitions) should be consistent.*
- A related issue: UC&R lists "stakeholders", as does S&PG, but these are not consistent.
  - S&PG also has actual definitions, not just a list of names.

Use Cases and Requirements

- How to motivate/justify security and privacy features?
  - Submitted use cases often don't do a good job defining their security and privacy requirements
- Need chain: feature → requirement(s) → use case(s)
- Current (documented) justifications are incomplete:
  - https://w3c.github.io/wot-usecases/#security
  - https://w3c.github.io/wot-architecture/#sec-security-guidelines

Proposal:

- Establish set of "use case categories": Manages PII, Safety Critical, Confidential, etc.
- For each category, list use cases in that category
  - Use cases can be in more than one.
  - New use cases would self-identify what categories they fall under.
- List threats in Requirements section of UC&R document.
  - Names only; full definitions in S&PG
- For each threat, list the use case category for which mitigations are required.

Work Items and Reorganization

- Security Planning
- Proposed New Features with an S&P aspect:
  - Signing (also impacts Discovery)
  - Onboarding
    - Do we or don't we?
    - Where would it go?
- Reorganizations:
  - Context Extensions (also related to Bindings)
  - Ease of Use (e.g. inlined security)

Work Items - Discussion

- How do we deal with security and privacy considerations?
  - Should they be normative or not?

- How and when should we define best practices?
  - How does this overlap with existing mechanisms in protocols?
  - Should we define best practices in profiles?
  - Best practices for “new” Things (greenfield) should not constrain our descriptive power for “existing” Things (brownfield)

- Constraints on deployments vs. specification features/design?
  - Is use of TLS, for example, a deployment option?

General Discussion

- Need more people to work on the above…
  - Since security experts are limited, can't do all the work
  - Instead, want to engage experts for guidance and review, with other tasks taken up by other task forces
- Suggested Plan
  - Align considerations and threats/risks in S&PG and UC&R documents (proposed above)
    - Consistent names, categories, cross-references/link, etc.
  - Need to update considerations in each deliverable as well
    - While we are at it, may move considerations to more suitable deliverable or consolidate
  - Need to consider normative nature of S&P mitigations
    - Testability is important, maybe we need a pseudo-assertion “Guideline” or something.