Report: Joint F2F of W3C IG on Web-of-Things and IRTF Thing-to-Thing RG Meeting Prague, July 28/29 – **Security and Privacy**

Oliver Pfaff
(oliver.pfaff@siemens.com)

Preface

- Starting points for this joint workshop:
  - W3C page
  - IRTF page
- Security and privacy breakouts were moderated by Carsten Bormann
- W3C WoT IG participants (in the security and privacy breakout): Edoardo Pignotti, Oliver Pfaff
- Report to IRTF by Carsten Bormann (note: I offered input text to Carsten, the following re-uses his resulting report)

Saturday Breakout (B)

- Ca. 4 hour mainly discussing the state-of-the-art
- Workshop contributions:
  - B1: Security & Privacy Features in Current IoT Projects (discussion with the breakout participants based on some questions prepared beforehand, see below for findings)
  - B2: Existing Infrastructure vs. New Challenges (Oliver Pfaff, Siemens AG)
  - B3: Access Control on Multiprotocol Networks (Pablo Puñal Pereira, LTU)
  - B3: WiFi Alliance Device Provisioning (ad-hoc talk by Mohit)
  - B4: Highlights from the ACE WG (Olaf Bergmann, TZI/Uni Bremen)
  - B4: Interaction of ”Things” with the ”big” Internet: Authentication and Authorization (Stefanie Gerdes, TZI/Uni Bremen)
  - B5: no time left, skipped

Sunday Breakout (B)

- Ca. 2 hours mainly discussing possible next steps
  - The T2TWG wants to consider the use cases “Home Automation” and “Building Automation” (plus some others too) in order to
    - 1st frame them from a SP perspective (requirements)
    - 2nd ask each interested party to throw their preferred SP mechanisms at this and
    - 3rd see what sticks in order to derive patterns, identify white-spots and follow-up on this later on (how exactly will depend on the outcome)
  - The W3C WoT IG should track this work item and contribute to it as it is a good complement to what [IG-SP] is doing

Main Takeaways

1. More **capital goods** projects than consumer goods (in W3C WoT the impression is inverse)
2. Actual thing usually is of **low value** but controls (parts of) a **high value** asset
3. Focus in on **cross-domain scenarios** (not all things/components from the same provider)
4. Most projects already implement some authz. In absence (as of now) of a standard authz solution for things the current solutions are **ad-hoc** resp. **DIY**. That's an apparent contradiction: DIY solutions are a valid same-domain approach (one vendor/provider controls all components) but not cross-domain
5. Preference is on **symmetric cryptography** (here: schemes that hit devices). If asymmetric schemes are used then in the 'raw' form factor. Public key cryptography with public key certificates is avoided

Note: this reflects the projects that were present in the breakout and should not be assumed to be representative for an industry

Recommendation

- *The same vs cross-domain question is fundamental and should be tracked:*
  - If same-domain is/stays a valid proposition for (most) IoT/WoT projects then a standards-based SP solution gives reuse. Stuff could also be done without
  - If cross-domain is aimed at (by a relevant subset of the projects) then a standard solution gives interop AND reuse. Things cannot be done without
- *Beware of the potholes on your road:*
  - If you aim at cross-domain then many current SP proposals will not really help as they consider a same-domain solution