Security Summary

Michael McCool
Intel

Osaka, W3C Web of Things F2F, 17 May 2017

Summary Summary

- Plenary
  - Review of security process
- Breakout
  - Review of Threat Model
    - Stakeholders, *Roles*, Assets, Adversaries, Attack Surfaces, Threats, Use Cases, Objectives
  - External references and standards for security and privacy
    - Selection
    - Discussion of summarization and evaluation process

Process

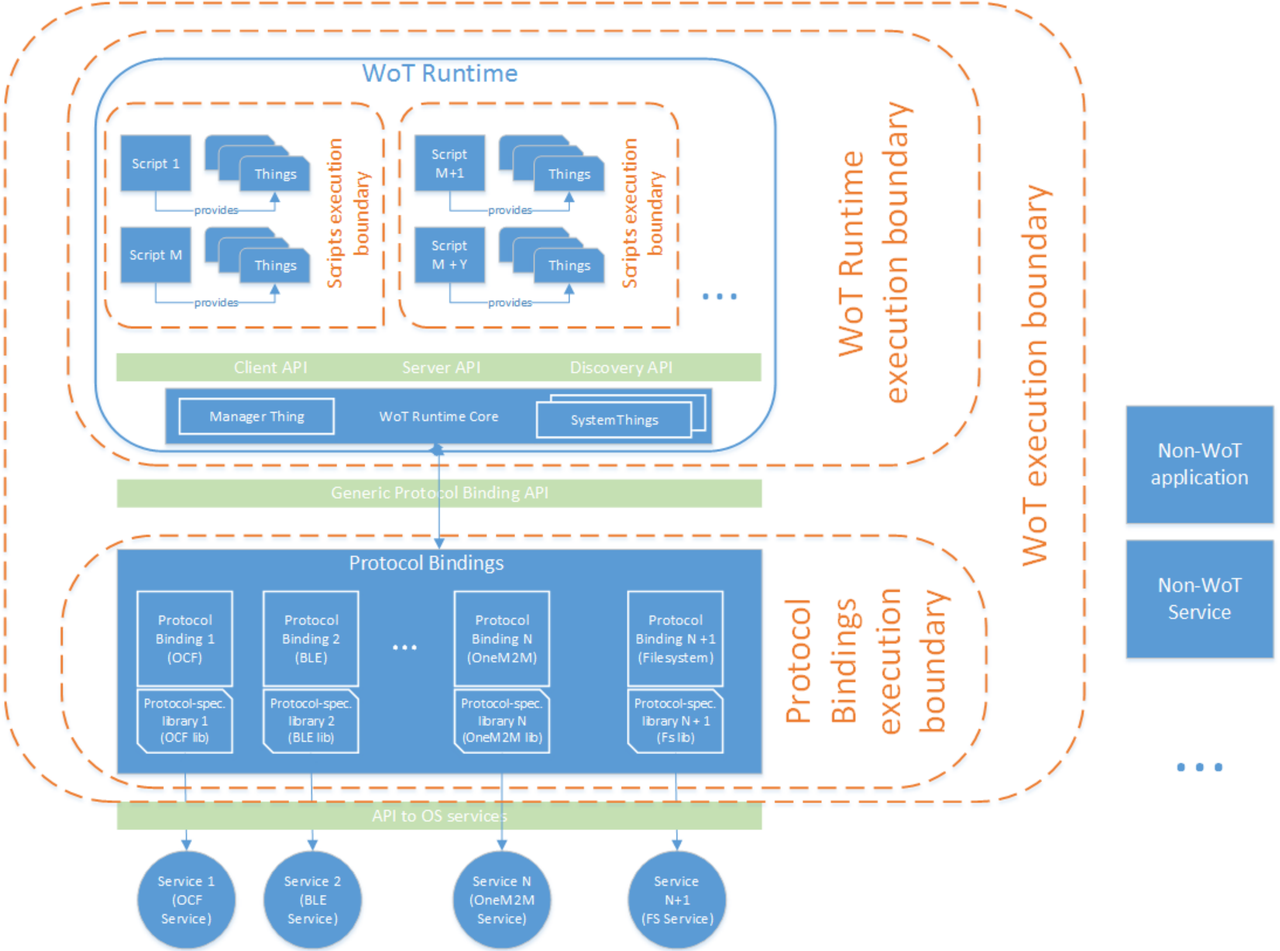
1. **Threat model** – Understand what you need to protect and why
2. **Scoping** – Organize and prioritize threats, define security objectives
3. **State of Art** – Study related areas and their approaches to security
4. **Solutions** – Find a suitable mitigation for each in-scope threat
5. **Implementation and Evaluation** – Implement and Test each solution

Threat Model

See Pull Request #318

- Stakeholders
  - Description, Role, Business-driven security goals, Interesting edge cases
- ***Roles***
- Assets
  - Description, Who should have access (Trust Model), Attack Points
- Adversaries
  - Persona, Motivation, Attacker type
- Attack surfaces
  - System Element, Compromise Type(s), Assets exposed, Attack Method
- Threats
  - Name, Adversary, Asset, Attack method and pre-conditions, priority
- ***Use Cases***
- Security Objectives and Non-Objectives
  - Threats, Mitigation (if an objective), Reasoning (if not)

Attack Surfaces



- Boundaries depends on assets and architecture
- Boundaries between domains provide attack surfaces
- Hierarchy of trust

External References and Standards

See Pull Request #319

- External References:
  - Industrial Internet Consortium Security Framework: http://www.iiconsortium.org/IISF.htm
  - IETF ACE (Authentication and Authorization for Constrained Environments): https://tools.ietf.org/wg/ace/
  - IETF RFC 7252 (CoAP) Security model: https://tools.ietf.org/html/rfc7252
  - IETF (IAB) RFC 3552 – Guidelines for Writing RFC Text on Security Considerations: https://tools.ietf.org/html/rfc3552
  - IETF (IAB) RFC 6973 – Privacy Considerations for Internet protocols: https://tools.ietf.org/html/rfc6973
  - STRIDE Threat Model: https://docs.microsoft.com/en-us/azure/iot-suite/iot-security-architecture
  - OWASP IoT Attack Vectors: https://www.owasp.org/index.php/Threat_Risk_Modeling
  - IoT Security Foundation: https://iotsecurityfoundation.org/
  - FIPS and other national standards

- Liaison References (Systems are built on top of these):
  - OCF 1.0 Security Specification (Draft): https://openconnectivity.org/draftspecs/OCF_Security_Specification_v1.0.0.pdf
  - oneM2M Security Solutions, TS-0003: http://www.onem2m.org/images/files/deliverables/Release2/TS-0003_Security_Solutions-v2_4_1.pdf
  - OPC(-UA)?
  - Echonet (but… no security?), BACnet (but… no security?)