Securing the Web of Things
A COMPOSE Perspective

Daniel Schreckling
University of Passau

1st W3C WoT IG F2F
Open Day – April 20, 2015
Main Design Decision

The situation
- Changing use and types of principals and data
- Unpredictable interactions & information flows
- Security is application dependent: Applications require
  - specific security mechanisms at
  - specific “locations”
- Inflexible, resource-centric security frameworks

COMPOSE approach
- Shrink security perimeter to the granularity of data
- Build flexible, data-centric but scalable security framework
Identity Management

■ Attribute-based
  • Entities associated with set of attributes
  • Attributes
    – Describe properties
    – Fixed or user-defined but approved
    – Defined decentralized

■ Lightweight
  • Partial replication of OAuth (access tokens)
  • Use of API tokens for highly frequent interactions

■ Flat entity hierarchies
Security Meta Data for Virtual Things

Weather

- Security Association
- Policies
- Reputation

http://www.servioticy.com
Data and Services

Weather forecast

- Flow Policies
- Security State
- Provenance

- Security Association
- Policies
- Reputation
- Contracts

http://www.gluethings.com
Flow Policies for Data

- Tagged to data (JSON document)
- Defined over *actors* and their attributes
- Flow-to-rule

\[ \text{Lock}_1(a_1, a_2, \ldots, a_q), \text{Lock}_2(b_1, b_2, \ldots, b_r), \ldots, \text{Lock}_i(z_1, z_2, \ldots, z_t) \rightarrow A \]

- Flow-from-rule

\[ A \rightarrow \text{Lock}_1(a_1, a_2, \ldots, a_q), \text{Lock}_2(b_1, b_2, \ldots, b_r), \ldots, \text{Lock}_i(z_1, z_2, \ldots, z_t) \]

- Set of rules form policies

\[ \text{owner}(U), \] validated
\[ \text{atWork}(U), \] authenticated(U)
Flow-Control:

\[ S \rightarrow \text{actsOnBehalf}(S, U) \]

Access Control:

\[ U \rightarrow \text{authenticated}(U), \quad \text{minBalance}(U, 1.5 \text{ Cent}) \]

\[ S \rightarrow \text{minTrustLevel}(S, 5) \]

Flow-Control:

\[ \text{owned}(S, U) \rightarrow S \]
Contracts

- Promises towards the platform
  - Automatically generated
  - Over-approximated service behaviour

- Developer Contracts
  - are user-defined refinements
  - Impact
    - Performance
    - Trust in Developers

Flow description:
\[ \text{length}(\text{in} 2) \leq 8 \rightarrow \text{out 1} \]

Pre-Condition:
- Encrypted

Effect:
- Encrypted("/etc/*")
- hasName("/etc/passwd")

Resource X

Resource Z

Service
User Deployed Services/Applications

Weather

- Weather
- Forecast
- Service

Location

- Places
- Meet your friends
- Service

Weather forecast Service

Places to meet your friends Service
User Deployed Services

Weather

Location

Places to meet your friends

Fun things to do
Security Conflicts

Framework detects flows with conflicting constraints

Resolution using user, instrumentation and/or dynamic monitors
Dynamic Flow Control

Weather

- Weather forecast Service

Location

- Places to meet your friends Service

Fun things to do Service

Service
Static Flow Control

- Composition Analysis
- Node/Service Analysis (enhanced TAJS, Klee)
- Instrumentation (Dynamic Enforcement, Provenance, Reputation)
- Composition Reconfiguration
- Composition Recommendation
- Flow Policies
- Static Flow Control
- glue.things
  - Composition creation
  - Policy Settings
  - User Feedback
Hybrid Flow Control

Weather

Location

Weather forecast Service

Fun things to do Service

Places to meet your friends Service

Declassifier

Reputation

Provenance
Limitations ...

■ Security of physical devices
  • Authentication
  • Tamper-proof
  • Interface/Firmware security

■ Data confidentiality & integrity
  • Effective Perimeter remains at cloud level
  • Privacy vs. Security
  • Use of existing technologies

■ Analysis tools and instrumentation
  • Low language coverage
  • Efficiency vs. false positive rates
Conclusions

The COMPOSE way of WoT ...

- Introduces required control for the open IoT
- Shows that flow control frameworks appear to be a perfect match
- Creates new dimensions for policy enforcement

BUT ...

- Induces storage and processing overhead
- Dynamic security enforcement architectures

→ Does the WoT want to face this fine granularity?