Security and Privacy Challenges in Open Source Software IoT Platforms

Arkady Zaslavsky
Outline

- Setting the scene
  - IoT
- Privacy & security
  - Challenges in IoT
- Open IoE
- CAS Demo
- Conclusion
Internet of Things (IoT)

A dynamic, global network infrastructure with self-configuring capabilities are seamlessly integrated into the information network. Based on standard & interoperable communication protocols, virtual personalities, use intelligent interfaces, and where physical & virtual “things” have identities, physical attributes, and

DS Ricardo Bonilla, CSIRO
Why is IoT security challenging?

- Wireless communication
- Physical insecurity
- Constrained devices
- Potentially sensitive data
- Lack of standards
- Heterogeneity: weakest link problem
- A systems, not software problem
- Classic web / internet threats
- Identity management & dynamism
- Inconvenience and cost
Categorisation of topics and technologies in the IoT
7 out of 10 fear security implications of IoT

IoT security & privacy roadmap – EU take

Before 2010
- Security mechanisms and protocols defined
- Security mechanisms and protocols for RFID and WSN devices

2010-2015
- User centric context-aware privacy and privacy policies
- Privacy aware data processing
- Virtualisation and anonymisation

2015-2020
- Security and privacy profiles selection based on security and privacy needs
- Privacy needs automatic evaluation
- Context centric security

Beyond 2020
- Self adaptive security mechanisms and protocols
Privacy Legal Framework

Data Protection Directive 95/46/EC, collecting and processing the personal data of individuals in one of the following (laid down by Article 7):

- ...
- Where the individual concerned, (the 'data subject'), has unambiguously given his or her consent, after being adequately informed; or

Reform Directive for Data Protection, January 2012:

- Whenever consent is required for data processing, it will have to be given explicitly, rather than be assumed.
OpenIoT Factsheet

Contract No.: 287305  
Objective: ICT-2011.1.3 Internet-connected Objects

Coordinator: NUIG-DERI, Galway, Ireland

Contact Person: Dr. Martin Serrano  
DERI NUI Galway  
IDA Business Park Lower Dangan, Galway, Ireland

EC Contribution 2,455,000.00 Euro

Project Start Date: 01 Dec 2011  
Duration: 36 months

Open Source Cloud Solution for the Internet of Things
OpenIoT General Vision

OpenIoT providing a cloud-based middleware infrastructure in order to deliver on-demand access to IoT services, which could be formulated over multiple infrastructure providers. (such as smart cities and smart enterprises)
OpenIoT Open Source Project

<table>
<thead>
<tr>
<th>Open Source</th>
<th>License</th>
<th>Governance</th>
</tr>
</thead>
</table>
| • http://github.com/openiot/OpenIoT
• Open Source Release of OpenIoT software (1 Oct, 2014, release 2.0) | • OpenIoT will be released under LGPL (Business Friendly)
• Ensures compatibility with background libraries/projects | • Master-governed planning
• Masters (OpenIoT partners) defined for major subprojects |
OpenIoT and Standards

W3C
- Use and Enhancement of W3C SSN Ontology
- Standardized Solution for Dynamic Discovery of Sensors and Internet-Connected Objects (ICO)

OGC
- Open Architecture for IoT/Cloud Integration
- Best Practice Paper

RESTful
- RESTful access to sensors and ICO (CoAP)
- Implementation of Driver/Virtual Sensor in GSN
High Level Architecture
Overview of (Supported) OpenIoT Capabilities

**What can I do with OpenIoT?**

- Dynamic Sensor/ICO Discovery
- Visual IoT Service Definition & Deployment
- IoT Service Visualization (via Mashups)
- Sensor/ICO Deployment & Registration
- IoT Platform Architecture & Capabilities
- Resource Management and Optimization
Scenarios – Use Cases

Community sensing for large scale (collaborative) e-Science Experiments
  • Phenonet

Enabling Service Platform for Resilient City Services
  • Smart Campus
  • Silver Angel
  • Crowd Sensing

Intelligent Manufacturing and Logistics
  • Smart Industry
OpenIoT IDE
CAS - Central authorization and authentication service
OpenIoT Security and Privacy

Proper access control by means of “sticky” policies
Accountability on data access through logging of actions
Safe storage by means of encryption and with durability guarantees
Confidentiality through encrypted communication
User-side privacy leakage control through Privacy Enhancing Technologies
  • Automatically configured based on a SLA
OpenIoT Architecture

- WP5-T5.3 Secure, Trustworthy and Privacy Friendly Interactions
Security & Privacy Module

- **OpenIoT CAS**: Centralised Authentication and Authorisation server

- **OpenIoT Security Console**: Web application for Users, roles and Permissions management

- **Security Client API & Tag Libraries**: Enable security and CAS integration in all OpenIoT modules
OpenIoT CAS

- Central authorization and authentication service for all OpenIoT applications
- User credentials checked and maintained only by CAS
- Token-based authorization
- Based on OAuth2.0 framework
OpenIoT Security Management Console

- Registering OpenIoT services
- Managing *permissions* and *roles*
- Assigning/revoking permissions to/from users
OpenIoT Client API & Tag Libraries

- Client API to enable security in all OpenIoT Application and Web Services
- Java classes, provide common authentication and authorization methods
- CAS interaction and forwarding
OpenIoT Client API & Tag Libraries

- Tag Libraries for JSF (Java Server Faces) and JSP
- Ready to use in Web applications
- Simple integration, CAS interaction behind the scenes

```xml
<openiot:hasPermission name="admin:user_mgmt_general">
   <li><a href="roles.jsf">Manage roles</a></li>
   <li><a href="users.jsf">Manage users</a></li>
   <li><a href="perms.jsf">Manage permissions</a></li>
</openiot:hasPermission>

<openiot:lacksRole name="admin">
   <span class="label label-warning">
      <h2>You don't have the required authorization for</h2>
   </span>
</openiot:lacksRole>
```
Thank you!

Dr Arkady Zaslavsky, Professor
Senior Principal Research Scientist
Email: arkady.zaslavsky@csiro.au

www.csiro.au