Internet of secure things: issues and perspectives

Pasquale Pace
Dimes - UNICAL
ppace@dimes.unical.it
Table of Contents:

• Inter-IoT European Project
  » http://www.inter-iot-project.eu/

• IoT Security
  – IoT Authentication
  – IoT & Blockchain
**INTER-IoT Vision and Mission**

**INTER-IoT** vision is to provide all the building blocks needed to achieve interoperability between IoT Platforms, including a framework, methodology, associated APIs and tools.

By building and demonstrating:

- Seamless inclusion of novel IoT devices
- Seamless support for smart objects mobility
- Service discovery and management
- Reuse and exchange of services between IoT platforms
- Common semantic interpretation of data
- Rapid prototyping of cross-platform IoT applications
- Overcome market barriers

• [http://www.inter-iot-project.eu/](http://www.inter-iot-project.eu/)
INTER-IoT Consortium

TU/e

NEWAYS

rinicom

AFT

develop

UNIVERSITAT POLITÈCNICA DE VALÈNCIA

FUNDACIÓN VALENCIAPORT

Sabien

noatum

TELECOM ITALIA

UNIVERSITÀ DELL’CALABRIA

A.S.L. TOS
INTER-IoT architecture

- The INTER-LAYER tools will provide techniques and technology allowing interoperability and integration between the layers of heterogeneous IoT platforms.
IoT Security

The Internet of Insecure Things
IoT System Model

**APPLICATION LAYER**

- **IoT Applications**
  - Smart Healthcare
  - Smart Home
  - Smart City
  - Smart Factory

- **Application Support Sub-Layer**
  - Cloud Platform
  - Middleware

**TRANSPORTATION LAYER**

- **Core Network**
  - INTERNET

- **Access Network**
  - 3G/4G
  - Wi-Fi
  - Ad Hoc Network

**PERCEPTION LAYER**

- **Wireless Sensor Network (WSN)**
- **RFID Technology**
- **RFID Sensor Network (RSN)**
- **GPS Technology**
Application Layer
- Large users Accessibility
- Some Critical Applications
- Tested security methods

Transportation Layer
- Heterogeneous networks
- Intensive research about vulnerabilities

Perception Layer
- Physical Exposure
- Resource-constrained devices
- Technological heterogeneity
# Traditional IT Security vs IoT Security

<table>
<thead>
<tr>
<th>Traditional IT Security</th>
<th>IoT Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add-on Security</td>
<td>Built-in Security</td>
</tr>
<tr>
<td>Complex algorithms</td>
<td>Lightweight algorithms for resource-constrained devices</td>
</tr>
<tr>
<td>User Control</td>
<td>Privacy issue: IoT devices often automatically collect user information</td>
</tr>
<tr>
<td>Small technological heterogeneity</td>
<td>Large technological heterogeneity (thus also large attack surface)</td>
</tr>
<tr>
<td>Many security guards</td>
<td>Few security guards</td>
</tr>
<tr>
<td>Devices are placed in closed environments</td>
<td>IoT devices are placed in both open and closed environments</td>
</tr>
</tbody>
</table>
IoT Security as a «chain»

- IoT system as a whole system and security can be thought of as a *chain* that is robust as much as its weakest link.

*Multi & Cross Layer Security*
IoT Communication Protocols

- To design IoT security solutions for cross layers usage you have to overcome *heterogeneous* integration issues.

**Interoperability** become one of the enabling factors for IoT security.
Critical Security Issues evaluation

• Common Vulnerability Scoring System (CVSS) is a free and open industry standard for assessing the severity of computer system security vulnerabilities.

• Using CVSS to evaluate some IoT critical security issues.
  • CVSSv2, https://www.first.org/cvss/v2/guide
IoT Authentication

Authentication in IoT

Industry 4.0
Smart Home
Smart Grid
Brand Protection
TPM

15

4° Crati Valley Workshop on Blockchain – 18/07/2017
Top 10 IoT Vulnerabilities (OWASP) – Open Web Application Security Project

<table>
<thead>
<tr>
<th>Rank</th>
<th>Title</th>
<th>Issues</th>
</tr>
</thead>
<tbody>
<tr>
<td>I1</td>
<td><strong>Insecure Web Interface</strong></td>
<td>• 10/10 security systems accept ‘123456’</td>
</tr>
<tr>
<td>I2</td>
<td><strong>Insufficient Authentication/Authorization</strong></td>
<td>• 10/10 security systems with no lockout</td>
</tr>
<tr>
<td>I3</td>
<td><strong>Insecure Network Services</strong></td>
<td>• 10/10 security systems with enumeration</td>
</tr>
<tr>
<td>I4</td>
<td><strong>Lack of Transport Encryption/Integrity Verification</strong></td>
<td>• SSH listeners with root/&quot;&quot; access</td>
</tr>
<tr>
<td>I5</td>
<td><strong>Privacy Concerns</strong></td>
<td>• 6/10 web interfaces with XSS/SQLi</td>
</tr>
<tr>
<td>I6</td>
<td><strong>Insecure Cloud Interface</strong></td>
<td>• 70% of devices not using encryption</td>
</tr>
<tr>
<td>I7</td>
<td><strong>Insecure Mobile Interface</strong></td>
<td>• 8/10 collected personal information</td>
</tr>
<tr>
<td>I8</td>
<td><strong>Insufficient Security Configurability</strong></td>
<td>• 9/10 had no two-factor options</td>
</tr>
<tr>
<td>I9</td>
<td><strong>Insecure Software/Firmware</strong></td>
<td>• Unauthenticated video streaming</td>
</tr>
<tr>
<td>I10</td>
<td><strong>Poor Physical Security</strong></td>
<td>• Completely flawed software update systems</td>
</tr>
</tbody>
</table>
WIRELESS IMPLANTABLE MEDICAL DEVICES

Deep Brain Neurostimulators

Cochlear Implants

Cardiac Defibrillators/Pacemakers

Gastric Stimulators

Insulin Pumps

Foot Drop Implants

HACKED
### IoT Device Authentication

<table>
<thead>
<tr>
<th>Authentication Factors</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Something the device <em>knows</em></td>
<td>credential (device key, e.g., a secret key or a private key)</td>
</tr>
<tr>
<td>Something the device <em>has</em></td>
<td>integrated authentication IC, authentication dongle</td>
</tr>
<tr>
<td>Something the device <em>is</em></td>
<td>logical properties (e.g. the device type); physical properties: device fingerprint</td>
</tr>
</tbody>
</table>

“Advanced Device Authentication: Bringing Multi-Factor Authentication and Continuous Authentication to the Internet of Things” (Rainer Falk and Steffen Fries). CYBER 2016
# IoT Device Authentication

<table>
<thead>
<tr>
<th>Unconventional Authentication Factors</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Something the device <em>knows about its environment</em></td>
<td>Sensing informations</td>
</tr>
<tr>
<td>Something the device <em>does</em></td>
<td>behavior, functionality, e.g., automation control protocol</td>
</tr>
<tr>
<td>The <em>context</em> of the device</td>
<td>neighbors, location, connected periphery</td>
</tr>
</tbody>
</table>

“Advanced Device Authentication: Bringing Multi-Factor Authentication and Continuous Authentication to the Internet of Things” *(Rainer Falk and Steffen Fries)*. CYBER 2016
IoT & Blockchain
Advantages of Blockchain:

- **It is public**: everyone participating can see the blocks and the transactions stored
- **It is decentralized**: there is no single authority that can approve the transactions
  - (the participants in the network have to reach a consensus to accept transactions)
- **It is secure**: it uses public-key cryptography and it is tamper-proof
  - the ledger cannot be manipulated by malicious actors because it doesn’t exist in any single location, and man in the middle attacks cannot be staged because there is no single thread of communication that can be intercepted
To enable message exchanges, devices will leverage **smart contracts** which then model the agreement between the two parties.

**True autonomous smart device** without also the need of human intervention

- smart devices in a manufacturing plant that can place orders for repairing some of its parts without the need of human or centralized intervention
- smart vehicles in a truck fleet will be able to provide a complete report of the most important parts needing replacement after arriving at a workshop
Main challenges

- Resource-constrained devices
- Large technological heterogeneity

The utility of an *IoT Gateway*
“A Mobile Multi-Technology Gateway to Enable IoT Interoperability”