Security classes, relevance for cloud services

Josef Noll, (on behalf of the SCOTT team)
Secure CONNECTED Trustable Things key message

IoT is the game changer and driver for digitalisation, and SCOTT contributes through:

- **Answer the IoT need for a new and more advanced security paradigm through security classes**
- **Create a Convincing privacy assessment through privacy labelling**
- **Establish a clear link between security and safety**
The challenge from automation

USA work force time spent [%]

- Predictable physical work: 7%
- Data processing: 18%
- Data collection: 16%
- Unpredictable physical work: 14%
- Stakeholder interactions: 12%
- Applying Expertise: 17%
- Managing others: 16%

Technical automation potential 2016 [%]

- Predictable physical work: 78%
- Data processing: 69%
- Data collection: 64%
- Unpredictable physical work: 25%
- Stakeholder interaction: 20%
- Applying Expertise: 18%
- Managing others: 9%

[Source: McKinsey, 2016]
IoT concerns regarding advanced security paradigm

- **Traditional threat-based modelling is not appropriate**
  - Handles only *known threats*
  - Does not address life-time of an IoT system (typical 10-15 years)

Steps

1. Harmonise
2. Apply in domains
Traditional: Threat-based approach

Security attribute
Organisation
Control/Configuration

System of Systems
Vulnerability

Threat

Scalability?
Future Threats?

[Source: http://securityontology.sba-research.org/]

Security Classes
Josef Noll, Apr 2018
IoT threats

- First massive attack from IoT devices
  - 16Oct2016 IoT botnet attack on Dyn
  - Camera (CCTV), video recorder, TV,...
  - 1.2 Gbps Denial-of-Service attack

- How?
- All using Linux BusyBox for authentication
  - admin - admin, root - root, admin - 1111...
  - simple “test” was enough to convert IoTs into botnet

[Source: https://krebsonsecurity.com/2016]
IoT concerns regarding advanced security paradigm

- **Answer the IoT need for a new and more advanced security paradigm**
  - How to measure security of (complex) IoT systems, how to incorporate security into designs, how to have a clear (understandable to end-users) security level assessment
  - Address cybersecurity through proactive safeguard

- **Main outcomes**
  - Measurable security of (complex) IoT systems,
  - Security classes, defined through
  - Goal: Design paradigm for IoT systems

- **Today: Impact of IoT/autonomous processes/CPS/... on Cloud Certification - discussion**
Measurable Security in IoT systems
- applicable for the cloud?
Example: Measurable Security

- From people defined security classes
- To automated security decisions
  - through metrics assessment

- based on
  - security, privacy and dependability (SPD) functionalities
**SPD\textsubscript{Goal} versus System-SPD\textsubscript{Level}**

- Application-based security goals
- Automated assessment

- Visualisation of “operating envelopes”
  - Security good enough?
  - Too high Security

- Critical component/sub-system assessment

---

Table 1: SPD\textsubscript{Goal} of e:

<table>
<thead>
<tr>
<th>Use Case</th>
<th>Security</th>
<th>Privacy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Billing</td>
<td>90</td>
<td>80</td>
</tr>
<tr>
<td>Home Control</td>
<td>90</td>
<td>80</td>
</tr>
<tr>
<td>Alarm</td>
<td>60</td>
<td>40</td>
</tr>
</tbody>
</table>

Table 9: Selected configuration SPD level for each use case

<table>
<thead>
<tr>
<th>Use case</th>
<th>SPD\textsubscript{Goal}</th>
<th>Configuration</th>
<th>SPD level</th>
<th>SPD vs SPD\textsubscript{Goal}</th>
</tr>
</thead>
<tbody>
<tr>
<td>Billing</td>
<td>(90,80,40)</td>
<td>10</td>
<td>(67,61,47)</td>
<td>(○,○,○)</td>
</tr>
<tr>
<td>Home Control</td>
<td>(90,80,60)</td>
<td>10</td>
<td>(67,61,47)</td>
<td>(○,○,○)</td>
</tr>
<tr>
<td>Alarm</td>
<td>(60,40,80)</td>
<td>6</td>
<td>(31,33,63)</td>
<td>(○,○,○)</td>
</tr>
</tbody>
</table>
Security in IoT
- postulation of Security Classes, based on "exposure" and "impact"
Security Classes and System design

- **Security Classes in IoT**
  - Consequence
  - Exposure
- **Consequence**
  - *as in risk map*
- **Exposure**
  - *Physical exposure*
    - people, building, physical ports,...
  - *IT exposure*
    - ports, firewall, connectivity
- Used to assess the security class of Systems, sub-systems and components

New postulate of security class

<table>
<thead>
<tr>
<th>Consequence</th>
<th>Security Class</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Class 5</td>
</tr>
<tr>
<td>4</td>
<td>Class 5</td>
</tr>
<tr>
<td>3</td>
<td>Class 4</td>
</tr>
<tr>
<td>2</td>
<td>Class 3</td>
</tr>
<tr>
<td>1</td>
<td>Class 1</td>
</tr>
</tbody>
</table>

Impact/Exposure: 1, 2, 3, 4+

- Increase weak security:
  - watchdog
  - Attribute based access control (S-ABAC)
Semantic attribute based access control (S-ABAC)

- Lifting the **security class** through S-ABAC
- Access to information
  - *who* (sensor, person, service)
  - *what kind of information*
  - *from where*
- **Attribute**-based access
  - *role* (in organisation, home)
  - *device, network*
  - *security tokens*
- Rules inferring access rights

Attributes: roles, access, device, reputation, behaviour, ...
Conclusions & Discussion

- Things (IoT) are driving the digital societies
- Common challenges
  - Internet + Semantics + Things = IoT
  - Insecure devices
  - Measurable Security and Privacy
  - Autonomous Decisions

- IoT Security and privacy
  - automated privacy/security through Multi-Metrics
  - Security classes for design

Other Topics

Privacy labelling

IoT trust /IOTA.org

Global perspective
UNO SDG 2030