Digiotouch – Sustainable Digital Transformation

Paradise IoT Platform
- Cyber security
- ICT Standards
- Interoperability
- Mobile Apps
- Open Data
- Cloud, Edge

Smart City Infrastructure
- Mobility-as-a-Service (MaaS)
- Paradise IoT Platform

Manufacturing (Industrial IoT)
- Healthcare
Connecting Things

PARENTING in 1984
Did you REALLY brush your teeth or did you just WET THE BRISTLES to make it seem like you did?

PARENTING in 2014
Did you REALLY brush your teeth or did you just HACK YOUR TOOTHBRUSH to make it seem like you did?

Source: http://www.itworld.com/
What is Industrial IoT (IIoT)?

• IIoT is the current trend of automation and data exchange in manufacturing technologies.

• Business cases
  • Improving safety of workers.
  • Monitoring plant environment for presence of gases, excessive noise.
  • Warehouse stock monitoring.
  • Increasing operating efficiency and predictive maintenance.
Recent Past ...

• Multiple DDoS attacks led to inaccessibility of Github, Twitter, and more in October 2016.
  • Attacks carried out by IoT devices including printers, IP cameras, and baby monitors.
• Stuxnet – malicious computer program targeting industrial computer systems around a decade ago.
Yesterday ...

- Norway based
- One of the world’s largest makers of Aluminium
- Hit by a ransomware
We can not just ...
Growing concerns

• Critical infrastructure being targeted
• Legacy systems that do not handle latest security protocols
• Lack of standards for Industrial IoT security
• Scalability
  • 32% of IIoT devices connect directly to the internet, bypassing traditional IT security layers.
  • Almost 40% said identifying, tracking and managing devices represented a significant security challenge.
• Only 40% reported applying and maintaining patches and updates to protect their IIoT devices and systems.
• 56% cited difficulty in patching as one of the greatest security challenges
  • More info - https://www.themanufacturer.com/articles/iiot-security-endpoints-most-vulnerable-aspect/
Lifecycle of Endpoints in IIoT
## Security Challenges

<table>
<thead>
<tr>
<th>Manufacturing</th>
<th>Bootstrapping</th>
<th>Operation &amp; Updating</th>
<th>Decommissioning</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Harmonization of a security certification mechanism.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Provisioning of initial security parameters (statically configured).</td>
<td>• Derive dynamic security credentials.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Handling changes in domain or operation.</td>
<td>• Network monitoring.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Secure firmware updates.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Discovery of a new threat and recertification process.</td>
<td>• Purge sensitive information before a device becomes “inactive”.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Revocation of certification label.</td>
</tr>
</tbody>
</table>
More Challenges

- Heterogeneity of existing schemes
- Standardization of security certification framework
- Dynamicity – fast and easy process of recertification
- Scalability for manufacturing companies
- IIoT business case specific threats
- Trade-off between usability, effort, and Cybersecurity for IIoT
Cybersecurity Risk Assessment – ETSI Framework

- OWASP Application Security Verification Standard Project
- Microsoft's STRIDE
- Common Vulnerability Scoring System
Testing

• Penetration Testing
  • Industrial IoT systems, critical infrastructure must be tested from outside, similar to an actual attack.

• Fuzzing
  • Inject an IIoT system with valid and invalid message sequences to see if the system breaks.
  • If it does, what is it that breaks the system.

• Risk Based Security Testing
  • Improve security testing through security risk analysis.

• More testing guidelines are available

09/12/19

Digiotouch | Cybersecurity in IIoT, Liverpool
Cyber Resilience

• Ability to prepare for, respond to and recover from cyber attacks.
  • It helps an organisation protect against cyber risks, defend against and limit the severity of attacks, and ensure its continued survival despite an attack.

• Emerged over the past few years because traditional cyber security measures are no longer enough.

• It is now commonly accepted that it’s no longer a matter of ‘if’ but ‘when’ an organisation will suffer a cyber attack.
## Four Step Approach

### Manage and Protect
- Malware protection
- Data security
- Identity and access control
- Encryption, network security...

### Identify and detect
- Continuous monitoring of network and information systems to detect anomalies and potential cyber security incidents before they can cause any significant damage.

### Respond and recover
- Incident response management program
- Measures to ensure business continuity
- Restore normalcy as soon as possible

### Govern and assure
- Such program and measures are a part of enterprise organization and built into business.
Going Forward

• Striking a balance between usability and Cybersecurity for IIoT products and services.
• Policies on cyber resilience.
• Incentivize the security guidelines available for manufacturing industries.
• As a customer of IIoT, ask about security and privacy aspects of the products and services.
Acknowledgement

• The work leading to this presentation is a part of CReAT experiment of Fed4FIRE+.

• Fed4FIRE+ project has received funding under grant agreement No 732638 from the Horizon 2020 Research and Innovation Programme, which is co-funded by the European Commission and the Swiss State Secretariat for Education, Research and Innovation.
Contact

soumya@digiottouch.com

@digiottouch

@skdatta2010

https://www.digiottouch.com