Towards a Trustworthy Industrial Internet of Things Infrastructure

Arjmand Samuel, Ph.D.
Microsoft Azure - Internet of Things
Internet of Things is a game changer
Organizations are benefiting from IoT today
IoT Challenges

Scale
# devices >> # humans, and growing fast
Volume of data generated (and network traffic)

Pace
Innovation pressure: analysis, command and control
Skill pressure: data science, other (niche) specialties

Environment
Extreme heterogeneity
IT/OT collaboration
Internet security and privacy
Emerging standards & regulations
New competitors
Get started quickly with preconfigured solutions for common IoT scenarios.

Leverage a worldwide ecosystem of experienced IoT partners to tailor IoT solutions to your needs.

Connect millions of devices and integrate your business systems with new insights to transform your business.

Get started quickly with preconfigured solutions for common IoT scenarios.

Leverage a worldwide ecosystem of experienced IoT partners to tailor IoT solutions to your needs.

Benefit from a comprehensive solution

Connect and scale with efficiency

Analyze and act on new data

Integrate and transform business processes

- Real-time operating systems
- Analytics
- Device Registry
- Rules and Actions
- Dashboards & Visualization
- SAP
- Salesforce
- Dynamics
- Oracle
- DB2
- WebSphere
- Informix
- Twitter
- Office 365
Azure IoT Suite security

**Defense in depth**

- Securely connect millions of devices...
- Over a secure internet connection...
- To Microsoft Azure – built with security from the ground up

**Device Security**
Device Provisioning and Authorization

**Connection Security**
X.509/TLS-Based Handshake and Encryption

**Cloud Security**
- Azure Security Center
- Azure Active Directory
- Key Vault
- Policy-Based Access Control
Why is IoT vulnerable?

- Low resources and low power devices
- Unattended devices
- User managed devices
- Changing environment – mobility
Moving towards IoT you can trust

- Secure deployments start with secure design, development and deployment
  - Secure development Lifecycle (SDL)
  - Secure design by threat modeling
  - Secure ecosystem
Secure development lifecycle

http://microsoft.com/sdl

Development process for creating (and running) secure software as practiced at Microsoft
IoT Threats

The STRIDE model

Spoofing Identity:
A person or device using another person’s or device’s credentials

Tampering with Data:
Altering the data related to a device or traversing the network

Repudiation:
Denial that a person or device was involved in a particular transaction or event

Information Disclosure:
Exposure of information to individuals who are not supposed to have access to it

Denial of Service:
A particular service unavailable

Elevation of Privilege:
An unprivileged user gains privileged access and thereby has sufficient access to compromise or destroy the entire system
Threat Modeling for IoT – Data Flow
Threats – Denial of Service (DoS)

- **Threat:** Data Flow Binary Is Potentially Interrupted
  - **Description:** An external agent interrupts data flowing across a trust boundary in either direction.
  - **Category:** Denial Of Service

- **Threat:** Potential Process Crash or Stop for Field Gateway
  - **Description:** Field Gateway crashes, halts, stops or runs slowly; in all cases violating an availability metric.
  - **Category:** Denial Of Service

- **Threat:** Potential Process Crash or Stop for IoT Hub
  - **Description:** IoT Hub crashes, halts, stops or runs slowly; in all cases violating an availability metric.
  - **Category:** Denial Of Service
Threats – Elevation of Privileges

- **Threat: Field Gateway May be Subject to Elevation of Privilege Using Remote Code Execution**
  - **Description:** Device(s) may be able to remotely execute code for Field Gateway.
  - **Category:** Elevation Of Privilege

- **Threat: Elevation Using Impersonation**
  - **Description:** Field Gateway may be able to impersonate the context of Device(s) in order to gain additional privilege.
  - **Category:** Elevation Of Privilege

- **Threat: Elevation by Changing the Execution Flow in Field Gateway**
  - **Description:** An attacker may pass data into Field Gateway in order to change the flow of program execution within Field Gateway to the attacker's choosing.
  - **Category:** Elevation Of Privilege
### Example threats and mitigations

<table>
<thead>
<tr>
<th>Component</th>
<th>Threat</th>
<th>Mitigation</th>
<th>Risk</th>
<th>Implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device</td>
<td>S</td>
<td>Assigning identity to the device and authenticating the device</td>
<td>Replacing device or part of the device with some other device. How do we know we are talking to the right device?</td>
<td>Authenticating the device, using Transport Layer Security (TLS) or IPSec. Infrastructure should support using pre-shared key (PSK) on those devices that cannot handle full asymmetric cryptography.</td>
</tr>
<tr>
<td>Field Gateway</td>
<td>S</td>
<td>Authenticating the Field gateway to Cloud Gateway</td>
<td>If someone can spoof Field Gateway, then it can present itself as any device</td>
<td>TLS RSA/PSK, IPSe, RFC 4279. All the same key storage and attestation concerns of devices in general</td>
</tr>
<tr>
<td>Device</td>
<td>TID</td>
<td>TLS (PSK/RSA) to encrypt the traffic.</td>
<td>Reading data in transit between devices. Tampering with the data. Overloading the device with new connections</td>
<td>Security on the protocol level (HTTP(S)/AMQP/MQTT/CoAP).</td>
</tr>
</tbody>
</table>
Securing IoT is an ecosystem play

- IoT hardware manufacturer and integrator
- IoT solution developer
- IoT solution deployer
- IoT solution operator

aka.ms/iotbestpractices
Microsoft Azure

Security from the ground up

Microsoft Cloud
Largest online services in the world

Centers of excellence
Microsoft Digital Crimes Unit
Microsoft Security Response Center
Microsoft Malware Protection Center.

Operational Security Assurance (OSA) process

Security Development Lifecycle (SDL)

[Link to documentation page]

azure.microsoft.com/documentation/articles/securing-iot-ground-up/
Best practices – Hardware manufacturer/integrator

- Scope hardware to minimum requirements
- Make hardware tamper proof
- Build around secure hardware
- Make upgrades secure
Best practices - Solution developer

- Follow secure software development methodology
- Choose open source software with care
- Integrate with care
Best practices - Solution deployer

- Deploy hardware securely
- Keep authentication keys safe
Best practices - Solution operator

- Keep system up to date
- Protect against malicious activity
- Audit frequently
- Physically protect the IoT infrastructure
In closing

Internet of Things is the next big thing

For IoT hacks it is not about if, but when and how

Security in IoT

- Secure design
- Secure development
- Secure ecosystem
Thank you

Give us your feedback for this session: aka.ms/iotsecurity