Threat Analysis of Industrial Internet of Things Devices

Simon Liebl*, Leah Lathrop*, Ulrich Raithel†, Matthias Söllner*, Andreas Aßmuth*

*Technical University of Applied Sciences OTH Amberg-Weiden, Amberg, Germany
†SIPOS Aktorik GmbH, Altdorf, Germany

Presented by Simon Liebl <s.liebl@oth-aw.de>

October 2020
About the Presenter

Simon Liebl, M.Eng.:

- Research Assistant at OTH Amberg-Weiden, Germany
- PhD Student at Abertay University, Dundee, Scotland
- Fields of Research:
  - Industrial IoT Security
  - Hardware Security
  - Lightweight Cryptography
Industrial Internet of Things

Plant Cloud

Device Manufacturer Cloud

Company Cloud

Other Clouds

SCADA

PLC

Large Setup

Middle Setup

Small Setup
Information Technology vs. Operational Technology

Confidentiality  Integrity  Availability  Privacy  Authenticity

+Safety  +Impact on environment and society
Critical Infrastructures

Federal Office for Civil Protection and Disaster Assistance, "Critical Infrastructures", URL: https://www.kritis.bund.de/SubSites/Kritis/EN/introduction/introduction_node.html.
Common IIoT Threats

- Abuse
- Denial of Service (DoS)
- Destruction
- Espionage
- Intellectual property theft
- Maloperation
- Man in the Middle (MitM)
- Ransomware
- Repudiation
- Spoofing
Common IIoT Vulnerabilities

- Code execution
- Communication manipulation
- Design flaws and bugs
- Insecure and outdated components
- Memory manipulation
- Misconfiguration
- Physical manipulation
- Privilege escalation
- Repudiation
- Web-based vulnerabilities
Attack vectors:  

- Device attacks

- Hardware
- Zone 0
- Monitor & Analyze
- Zone 4
- Process & Control
- Zone 3
- Local & Internal Communication
- Zone 2
- Software
- Zone 1
- Hardware
- Zone 0

- Firmware/RTOS
- Application
- Web server

- Sensors
- Device
- Actuators
- MCU
- Memory
- Components

- USB
- JTAG
- RS232
- SPI
- Display
- USB stick
- SD card
- Microcontroller
- PC
- USB stick
- SD card
- Display
- Microcontroller

Simon Liebl: Threat Analysis of Industrial Internet of Things Devices
### Attack Vectors

**Attack vectors:**
- Device attacks
- Application attacks
- Network attacks

#### Zones

**Zone 0**
- Hardware

**Zone 1**
- Software

**Zone 2**
- Local & Internal Communication

**Zone 3**
- Process & Control
  - PROFINET
  - EtherNet/IP
  - Modbus
  - CAN
  - HART
  - PROFIBUS

**Zone 4**
- Monitor & Analyze
  - WiFi
  - Ethernet
  - Bluetooth
  - 5G

**Communication Channels**
- Cloud
- SCADA
- Workstation
- Smartphone
- PLC
- Sensor
- Actuator
- HMI
Recommended Procedure

1. Know your device
2. Creation of a network diagram
3. Identification and ranking of assets
4. Identification of threat sources
5. Identification of threats and vulnerabilities
6. Vulnerability and risk assessment
Conclusion

- Usage in critical infrastructures increases risks
- Additional threats through physical processes
- Additional vulnerabilities through insecure old technology
The project iSEC is funded by the Bavarian State Ministry for Economic Affairs, Regional Development and Energy within the framework of the Bavarian funding program for research and development “Information and Communication Technology”.