Thwarting a Cyberphysical Attack in the IoT Era

William J. Malik, CISA
VP, Infrastructure Strategies
What is IoT?

- Networked sensors, analytical engines, actuators
- Connected non-traditional computing platforms
- Industrial Control Systems ICS
  - Distributed Control Systems DCS
  - Supervisory Control And Data Acquisition SCADA
  - Programmable Logic Controllers PLC
  - Remote Terminal Units RTU
  - Intelligent Electronic Devices IED
  - [https://blog.trendmicro.com/securing-three-families-iot/](https://blog.trendmicro.com/securing-three-families-iot/)
Typical DCS Configuration

- Process Historical Archives
- Engineering and Operator Workstations
- Ethernet TCP/IP
- Field Control Unit
- Field Devices
- Micro FCU
- PLC I/O
- Field Devices
- LAN/WAN Hub
- SCADA Data Server
- PLCs, RTUs, Other 3rd Party
- Field Devices

--- Protocol: TCP/IP, Modbus, OPC, DDE, or Proprietary ---
--- Connection: VSAT, LAN, WAN, Radio, Microwave ---
What is Information Security?

• Information shall not be Lost, Altered, or Inadvertently Disclosed
  – I.e., Availability, Integrity, Confidentiality

• ISO 7498-2, Security across the ISO/OSI Reference Model
  – Identification, Authentication, Data Confidentiality, Data Integrity, Non-repudiation
Integrating Information Security

- Information Security Integrated with SDLC (DevSecOps)
- Security Management Integrated with IT/OT Management (Operations)
- Actuators (ICS) are out of scope for information security
  - Industrial processes are not “information”
The Evolution of IoT

**IoT 0.9 and 1.0 Limitations**
- Hard-coded credentials
- Plain-text communication
- Flat system architecture
- Simple or no software/firmware update
- Minimal logging or alerting
- Proprietary networking
- Very low power
- Sometimes physically inaccessible
- Lightweight systems management infrastructure

**Securing IoT 1.0**
- Restrict to segmented network
- Reduce attack surface
- Monitor network traffic
- Detect unwanted signals
- Monitor processor utilization
- Detect unwanted processes
- Deploy out-of-band sensors
- Logging, analysis, reporting
- Freeze servers and infrastructure
- No updates, no upgrades, no installs

**IoT 2.0 Additional Security Capabilities**
- Secure kernel
- Certificate-based communication
- Trusted over-the-air updates
- Monitoring interface
- Management APIs
- Vendor liability
- Field-replaceable units
- Forensically durable logging
ARM Platform Security Architecture

Non-secure processing environment

Application

Secure IPC

RTOS

Secure partition API

Trusted Functions

Secure partition manager

Secure hardware requirements

Platform hardware

Boot firmware

Root of Trust keys
A new device has been found
Device: Airbus A310
Run Auto-configuration?

Start
Cancel
Case Study: Medical Instruments

- Initially little technology in operating rooms
- Technological improvements – patient monitors, blood-gas analysis, EKG, EEG, but independent
- Introduce networked OR suite, link to hospital IT network ...
- Wannacry ransomware
Wannacry – Taiwan (happened)
Medical Implants (could happen)

“... adversaries could change the settings of the neurostimulator to increase the voltage of the signals that are continuously delivered to the patient’s brain. This could prevent the patient from speaking or moving, cause irreversible damage to his brain, or even worse, be life-threatening.”
Case Study: Maritime and Port

- Extreme supply chain implementation
- Fully automated port loading and unloading
- Multiple risks to shipping:
  - Unbalanced load
  - GPS spoofing “Meaconing”
  - Supply chain disruption – NotPetya
Automated Port Risks
Cargo Ship Risks

Green line = Displayed hacked load
Red line = Actual load
Blue dashed line = Allowable load limits
Case Study: Power Generation

• Initially hard-wired on site
• Technological improvements – sensors, safety systems, but still local
• Introduce networked remotely managed operation and oversight
• Link to utility corporate network ...
• Aurora attack: open breaker, close breaker
IT/OT Reference Architecture

Operational Technology

- Servers
- VDI
- ICS Management

Supervisory

- RTU

Conduit

- Sensor/ Telemetry

Information Technology

- Users
- Email
- Servers

WWW

Copyright 2018 Trend Micro Inc.
Conclusions and Future Work

• “History doesn’t repeat itself, but it rhymes.”

• Inventory IoT landscape
  – Asset management, discovery, categorization

• Upgrade weak IoT devices, networks

• Support secure IoT architecture

• Plan for regulatory mandates
References

Typical DCS Architecture from “Protecting Industrial Control Systems from Electronic Threats,” Joseph Weiss, Momentum Press, 2010
Taiwan ransomware attack http://www.cbc.ca/news/technology/ransomware-cybersecurity-hack-conditions-1.4114349
ARM https://developer.arm.com/products/architecture/platform-security-architecture
Sayano Shushenskaya Dam Accident https://www.youtube.com/watch?v=yfZoq68x7lY
ANSI/ISA 62443: Security for Industrial Automation and Control Systems
Thank you!

william_malik@trendmicro.com
@WilliamMalikTM