Industrial IoT (IIoT) Security – A Holistic Approach

Jalal Bouhdada – Founder & Principal ICS Security Consultant
IoT Expo – Connected Industry
Wednesday 27 June 2018, Amsterdam
WHO WE ARE

• Working on a global scale, we provide both Fortune 500 enterprises and small to medium-sized businesses with the cyber security solutions required to effectively manage cyber risks.

• Through robust protection against cyber threats, our services and solutions transform the way our customers’ procure, build, integrate and manage their critical infrastructures.
AREAS OF EXPERTISE

Applied Risk offers industrial cyber security and consultancy services to critical infrastructure globally. Sectors include:

- Oil & Gas
- Power
- Water
- Manufacturing
- Transportation
- Pharmaceutical
TALKING POINTS

B - Background of IIoT

E - Emerging threat landscape and IIoT risk factors

I - IIoT security challenges

B - Best practices for securing IIoT

Applied Risk
A seismic shift is underway within the industrial environment, transforming the way manufacturers and engineers operate. The Industrial Internet of Things (IIoT) has arrived and is here to stay.

This is enabling faster production, but also optimising processes, driving down costs and generating energy efficiencies.
Ubiquitous computing – sensors, processors and actuators that are connected to each other can cause and control actions. Everyday objects that are equipped with this connection are able to include environmental information and act on this basis.

Dr. Johann Bizer, ULD (2006)
Mechanization, water power, steam power
Mass production, assembly line, electricity
Computer and automation
Cyber Physical Systems
IIoT DEVICES ECOSYSTEM

Field network

Field equipment

Factory Automation Edge

Local Area Ethernet Network

Industrial IoT gateway

Wide Area Access Network

IoT Head End
INTERNET OF THINGS IN THE FUTURE

2020

- 4 billion connected people
- 4$ trillion in revenue opportunity
- 25 million apps
- 25 billion embedded and intelligent systems
- 50 trillion GBs of data

Source: Marlo Morales
The Industrial IoT is projected to be worth $151bn.

25% of identified attacks in enterprise will involve IoT.

However, businesses will only spend 10% of their cyber security budgets protecting themselves.

This means we face an industry that grows faster than we can secure it.
EARLY SIGNS ONLINE: SHODAN, ZOOMEYE

https://icsmap.shodan.io/

Map of Industrial IoT on the Internet
The impact of a cyber event can cascade across an organization, reinforcing its magnitude.
The market can't fix this. The buyer and seller don't care.

Bruce Schneier, November 2016, House Energy and Commerce Committee hearing (USA)
ARE OUR DEVICES TRUSTWORTHY?

- Does the board understand the risk of IIoT security?
- Do we have a plan and are we ready for IIoT transformation?
- Do we have a security framework and architecture blueprint for our IIoT?
- Have security assessments for IIoT readiness been undertaken?
COMPLEX ECOSYSTEM

Internet of Things (IoT), Industrial environments, various benefits, vulnerabilities, devices, sensors, manufacturing, attack, various benefits.
Quote
Behavior-based safety
IoT SECURITY USE CASE: THE BTC PIPELINE ATTACK

- “On 5 August 2008, a major explosion and fire in Refahiye (eastern Turkey Erzincan Province) closed the pipeline. The Kurdistan Workers Party (PKK) claimed responsibility. The pipeline was restarted on 25 August 2008. There is circumstantial evidence that it was a sophisticated cyber attack on line control and safety systems that led to increased pressure and explosion. The attack might have been related to Russo-Georgian War that started two days later.” (Source: Wikipedia)

- Pipeline capacity: 1 Mbpd
- Lost days: 20
- Oil price then: $125/barrel
- Potential loss: $2.5B
IloT AS BUSINESS ENABLER

1. Close collaboration between suppliers and end-users to enhance security of IloT components
2. Secure by design throughout the device lifecycle
3. Adherence to industry security and compliance standards IEC 62443 4-1, 4-2

This will enable you to benefit from all the advantages that IloT offers, while preventing a cost increase due to unexpected vulnerabilities.
THE IIC’S SECURITY FRAMEWORK: IISF

- Published in September 2016
- 160 pages

Key Contents:
- Key Systems Characteristics Enabling Trustworthiness
- Distinguishing Aspects of Securing the IIoT
- Managing Risk
- Permeation of Trust in the IIoT System Lifecycle
- Functional View
- Protecting Endpoints
- Protecting Communications
- Security Monitoring and Analysis
- Securing Configuration and Management
- Looking Ahead – the Future of IIoT
OWASP IoT ATTACK VECTORS

- Open Web Application Security Project (OWASP): The free and open software security community, Internet of Things Project
  www.owasp.org/index.php/OWASP_Internet_of_Things_Project

- Top 10 list
  - Insecure web interface
  - Insufficient authentication/authorization
  - Insecure network services
  - Lack of transport encryption
  - Privacy concerns
  - Insecure cloud interface
  - Insecure mobile interface
  - Insufficient security configurability
  - Insecure software/firmware
  - Poor physical security
BEST PRACTICES FOR SECURING IIoT

- Secure development lifecycle
- Assessing security from the outset
- Robustness testing
- Hardware and firmware security assessments
- Static code and protocol analysis
No matter how strongly the statistical records emphasize personal faults or how imperatively the need for education activity is shown, no safety procedure is complete or satisfactory that does not provide for the correction or elimination of physical hazards."