Network Security for IoT & IIoT Environments

Bruce Large

OT Security Lead CyberCX

CyberCX

1

1

Agenda

1. IoT and IIoT Definitions
2. IoT and IIoT Architectures
3. Security standards, frameworks and resources
4. Network security considerations by layers
5. Homework
6. Q&A

2

2

/whois

@beLarge

- Operational Technology (OT) Security Lead & Principal OT Cyber Security Architect at CyberCX
- Cyber security specialist who has worked across IT and OT in Network Engineering and Cyber Security roles for just under 15 years
- A Cyber security architecture enthusiast & infrastructure tourist
- Bach Eng (Telecomms) QUT and Master Business (Applied Finance) QUT

SABSA FOUNDATION LEVEL SCF

GRID

Cyber Security Foundation+Practitioner CERTIFIED

CISCO CERTIFIED CCNP ROUTING & SWITCHING *Lapsed 2017*

CISCO CERTIFIED CCDP DESIGN *Lapsed 2017*

CISCO CERTIFIED CCNA SECURITY *Lapsed 2017*

3 v1.2

3

Network Security for IoT & IIoT Environments

IoT and IIoT Definitions

4 v1.2

4

What is the IoT?

- *Things* are devices that can sense, and potentially interact with the world around them whilst communicating with other things and applications to produce valuable information and/or services at low cost and at scale
- Can be for both consumer and enterprise applications
- The combination of the miniaturisation of electronics, improvements in battery technology, ever increasing wireless network performance at lower costs and the emergence of cloud computing have given rise to the Internet of Things

5

5

So what is the Industrial IoT (IIoT)?

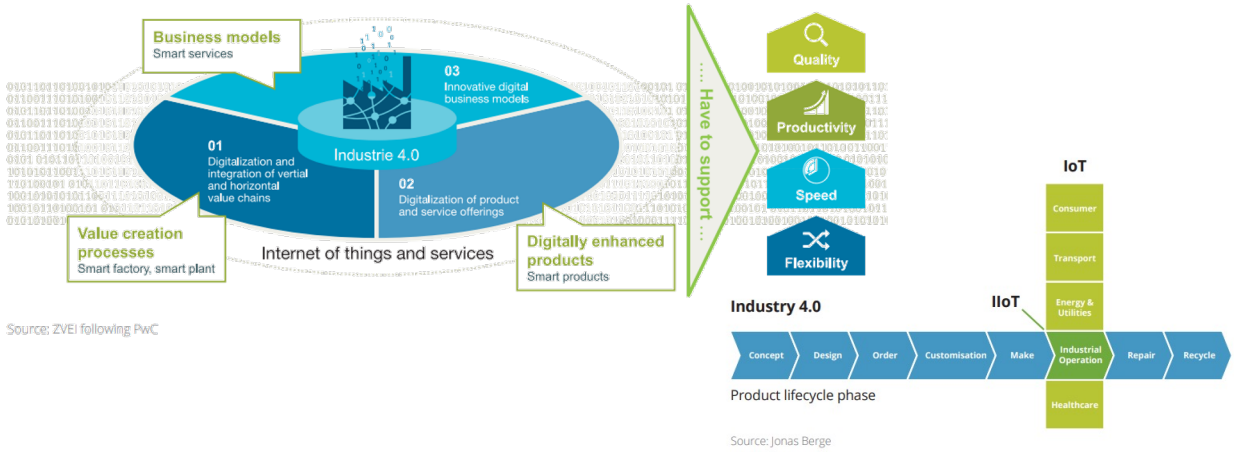
- Using Internet of Things (IoT) systems for Industrial Applications, Think:
  - Utilities
  - Energy and Mining
  - Local Government
- They may interact with existing Operational Technology (OT) systems such as:
  - Industrial Control Systems (ICS) including SCADA
  - Condition Based Asset Management Systems
  - Data Historians and Business Intelligence solutions

6

6

and what is Industry 4.0 then?

Extends from the technology viewpoint into the business viewpoint



Source - https://www.industry.gov.au/sites/default/files/July%202018/document/pdf/industry-4.0-testlabs-report.pdf?acsf_files_redirect

7

7

Network Security for IoT & IIoT Environments

IoT and IIoT Architectures

8

8

Architectural Frameworks

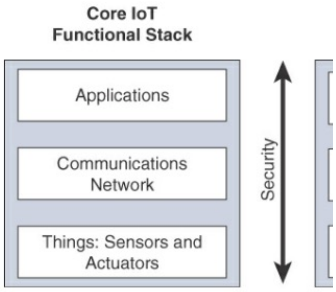
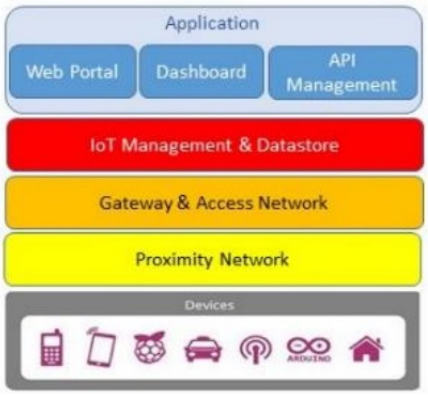


Figure 2-6 *Simplified Io*

Src - Cisco Press – IoT F
David Hanes e

Figure 1: Reference Architecture for IoT



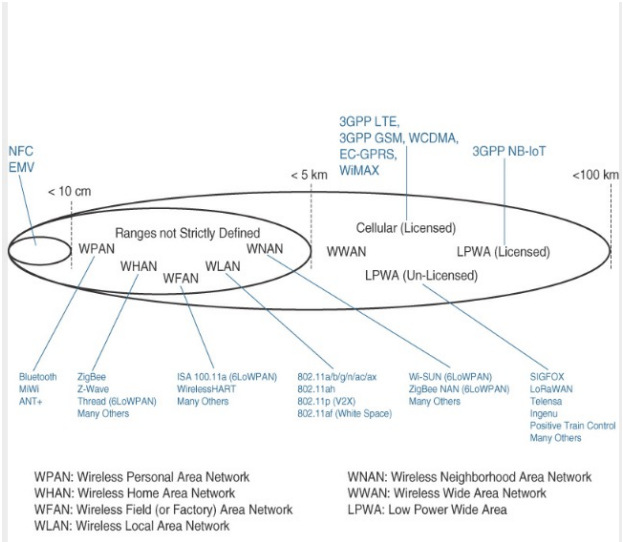
Src – IoTAA Security Guidelines v1.2

Src - https://blogs.cisco.com/digital/the-internet-of-things-capturing-the-accelerated-opportunity

9

9

Different Backhaul Networks

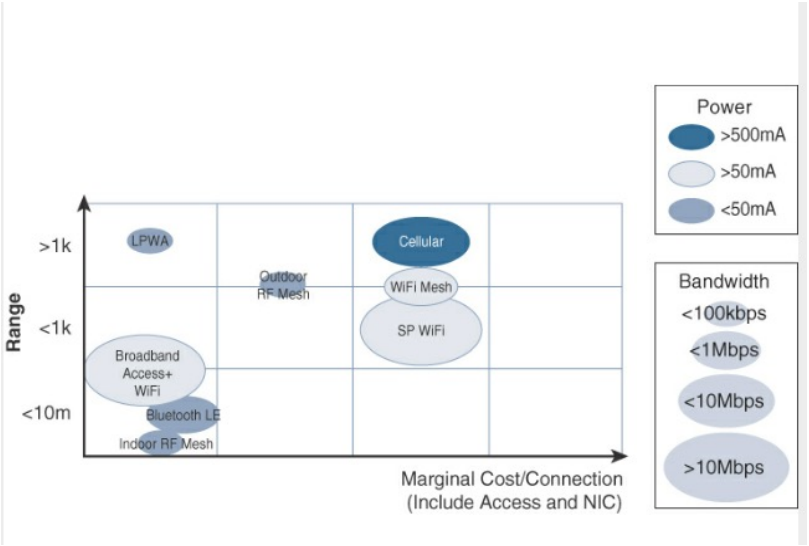


Src - Cisco Press – IoT Fundamentals David Hanes et al

10

10

Different Backhaul Networks (cont.)



Src - Cisco Press – IoT Fundamentals David Hanes et al

11

11

IoT 'Thing' Protocols

- HTTP
  - The Classic
- Constraint Applications Protocol (CoAP)
  - A constrained version of http to account for low power devices
- Message Queuing Telemetry Transport (MQTT) –
  - Originally developed by a team at IBM for satellite communications links, has been made an open standard in
- Secure M2M

Note, due to the scale of things, App protocols may be transported over IPv6

12

12

IoT RF Protocols

- Bluetooth
- Zigbee
- WiFi
- LoRaWAN
- SIGFox
- CAT M-1 & NB-IoT

13

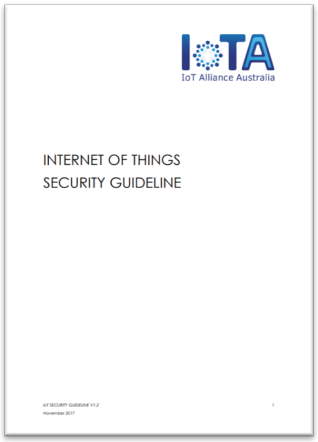
Network Security for IoT & IIoT Environments

Security standards, frameworks and resources

14

IoT Alliance Australia (IoTAA)

- IoTAA – Security Guideline v1.2 (Nov 2017)
  - Background and Architecture, Privacy, Security, Domain Viewpoints, Product & Service Development advice and some legal review.
  - Also includes appendices regarding OWASP principals and security testing advice



Source - https://iot.org.au/

15

15

IoT Security Foundation

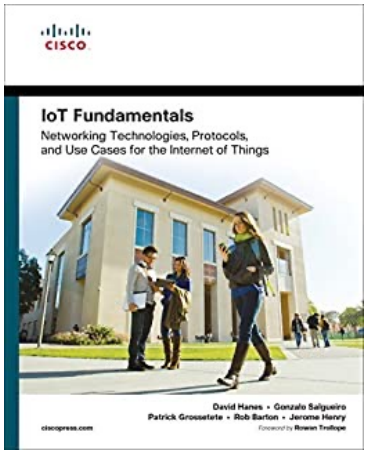
- The Best Practice is technically perspective and also introduces a Compliance class
- The Hub Based document is an architectural reference document for what a hub should do for security services.

Source - https://www.iotsecurityfoundation.org/

16

16

Cisco Resources



https://www.ciscopress.com/store/iot-fundamentals-networking-technologies-protocols-9781587144561

Part 1 - Introduction to IoT

Part 2 - Detailed Information per layer of the architecture including security

Part 3 - Use cases for:

- Manufacturing
- Oil and Gas
- Utilities
- Smart and Connected Cities
- Transportation
- Mining
- Public Safety

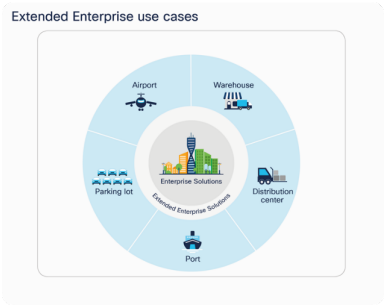
17

17

Cisco Resources (cont.)

Cisco Validated Designs (CVD) for:

- Extended Enterprise
- Connected Communities
- Utilities
- Transportation
- Industrial Automation



https://www.cisco.com/c/en/us/solutions/enterprise/design-zone-industry-solutions/index.html

Image ref - https://www.cisco.com/c/en/us/solutions/collateral/internet-of-things/solution-overview-c22-742351.html & https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CCI/CCI/DG/cci-dg/cci-dg.html

18

18

Engineers Australia – Applied IOT Engineering

- Access for members of EA, ACS, IEEE and the IET
- Webinars
  - Overview of IoT, Architecture, Comms Technologies, Data Analytics, Power Management, Security, Sensors and Embedded Electronics
  - **Industry Applications** – Agriculture, Buildings, Defence, Manufacturing, Mining and Energy, Smart Cities, Utilities
  - **Practices** – Business Planning and Innovation, Design, Intellectual property, Legal, Project Management and Systems
- Forums

Source - https://iot.engineersaustralia.org.au/

19 v1.2

19

Network Security for IoT & IIoT Environments

Network security considerations by layers

20 v1.2

20

So what network security do we need at what layers?

Let's use the IoTAA model as the reference architecture.

5. App Layer
4. Data Aggregation Layer
3. Backhaul Networks
2. Proximity Network
1. "Things"

21 v1.2

21

1. "Things"

1. Need to consider the encryption capabilities of devices in terms of compute and power usage trade offs
2. Need to consider how devices are securely enrolled into the network and how are credentials stored on the device
3. Need to be able to consider low touch network based solutions to device onboarding and support for large device counts

22 v1.2

22

2. Proximity Networks

1. Are you building the proximity network? How much of the network security are you designing/responsible for?
2. What network security capabilities exist in the RF Network and what are their trade offs for enabling them?
3. How do you securely allow devices to join the proximity network?
4. How do you successfully revocate devices from the network if you believe they have been compromised?
5. What network addressing scheme will you use?
6. Can you limit lateral movement in the RF network?
7. How are proximity network events logged?

23

3. Backhaul Networks

1. What Backhaul Network Technologies are you going to use? How do you implement network segmentation
2. How do you securely add devices to the back haul network? Is that centrally managed
3. What networking addressing scheme will you use? Do you need to translate from the Proximity Networks?
4. Is the transport back to the data layer segmented from other networks? Is it on it's own APN or VPN?
5. How do you get logging back to the application layer
6. How do you deal with High Loss and High Latency networks securely

24

4. Data Aggregation Layer

1. How do you maintain system segmentation?
2. How much do you rely on the network services for integrity of transmissions (e.g. transport VPNs)?

25

5. App Layer

1. How do users and services securely access the IoT based Applications? What network security services do you rely on?
2. How do you limit network access to administration interfaces?
3. How do you connect with other applications securely?

26

Network Security for IoT & IIoT Environments

Homework

27

Homework

Next Week	1. Next Month	Next 6 Months
1. Review the relevant IoT Framework materials for you 2. Join community groups such as the Applied IoT Engineering group or the IoTAA	1. Begin to develop your IoT security architecture, including network architecture	1. Aim to have established and approved Network Security Patterns for IoT Services 2. Build a whole of life security management plan for IoT services

28

QUESTIONS?

bruce.large@cybercx.com.au

https://linkedin.com/in/blargeau

29

Thank You!

30