IoT Security Toolkit

Dipl-Ing. Franjo Majstor MSc
TECHNOLOGY EVANGELIST

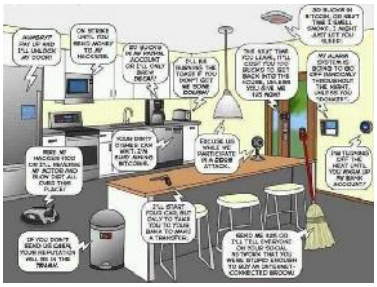
Vienna, Oct 2017

Intro & Disclaimer

- All opinions and suggestions are personal and not endorsed by any vendor
- All vendor names are mentioned only for illustration purposes

Table of Contents

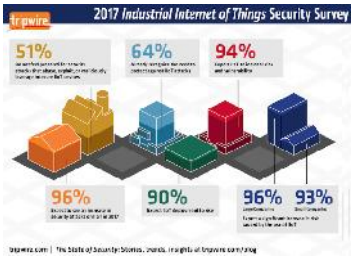
Ready?



Safety vs. Security

- Definition of Security…
  - C-I-A of your DATA
  - You can loose your €$£, reputation,…
- Definition of Safety…
  - A-I of your Controls
  - If your pacemaker stops working, you can use your life…

Really Ready?

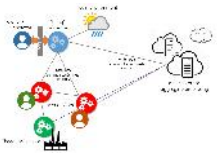


Psssst…

7

Definition(s) of IoT …

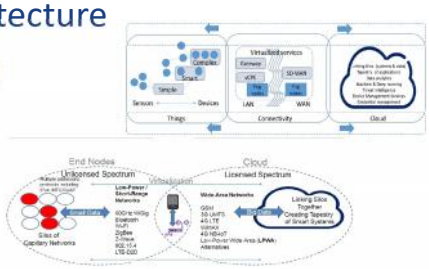
- *New business model*
- *Big Data Analytics*
- *M2M Communication*
- *Machine Learning & Sensors*
- *Predictive Maintenance*
- *Industry v4.0 / IIoT*
- *…or simple to disappear?*



8

IoT Architecture

- GW based
- GW less
- Fog based
- Hybrid
- …



9

IoT Risks

Source	Transport	Network Infrastructure	Data Connections	Host Systems	Recipient
Sensors	Short-range ZigBee, Wi-Fi, etc.	Identity Management	Internet	Servers	Humans
Smart Devices	Medium-range Cellular Low-power RF	Provisioning	VPN	Corporate Network	Processes
Hybrid Tech	Long-range Satellite	Authentication	Point-to-Point	Access Control	Automation
Gateways	Non-wireless	Authorization	Other		
		Access Control			
		Information Control Messages Data Transport			

10

IoT Attack Vectors

- Default Values
- Insecure Protocols (by default)
- Initialization Phases
- Sensor Saturation/Signal Jamming
- IoT devices are available 24/7 for Botnet
- No users behind IoT device
- Weak CPUs (no AV, no FW, no NAC/IPS…)
- Limited memory
- Stripped down OS
- Manufacturing chain (of insecurity)
- Drop down devices (like Pineapple?)

11

Already Known…

- Mirai (scale)
- GRE (attack on CPE CPU)
- Hajime, New Aidra, Bashlight…
- 3rd Party dependencies - service dependencies: DNS, certs, SSO pyramid, micro-services,…
- $19.99 to rent a BotNet?
- ZigBee Worm
- …

12

IoT security Solutions

- **Legacy but adjusted**
  - AI/Machine Learning
  - Pent testing (DDoS pentesting?)
  - 20/80 rule (20% investment solves 85% of issues?)
- **New approaches**
  - Blockchain
  - Industrial FW, AV, IDS…
  - New Architecture?
- **Standards/Frameworks**
  - IEC 62443
  - IEC 13849-1
  - EN/IEC 62061

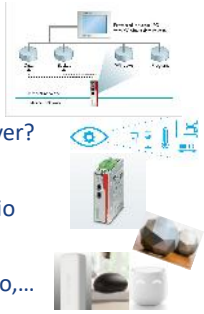
13

IIoT Security Architecture

- Zones:
  - ❑Internet
  - ---------
  - ❑DMZ + Internal
  - -------
  - ❑Control Network

14

IoT Firewall



- Industrial IoT…
  - Specific protocols, starting all over?
- "Legacy FW"
  - re-shaping their existing portfolio
- Home IoT:
  - New Players, RatTrap, CUJO, dojo,…

15

Pentesting/Scanning Tools

- Perytons Eye-O-T Vulnerability Analyzer
- Red Button "DDoS on demand"
- SHODAN.io, GHDB, defpass.com, …
- www.insecam.org/en/bycountry/AT/
- exploit-db.com

16

Machine Learning / A.I.

- Scaling with an amount of messages…
- "Products TALK back to you…"
- *Always on Protection, Inspection, Control…*
- *Examples: LightCyber/PAN, Darktrace, Cybertrap…*

www.iot-now.com/2017/02/09/58275-iot-based-cyberattacks-ai-can-defend-growing-threat

- ***The cyberattack in India used malware that could learn as it was spreading, and altered its methods to stay in the system for as long as possible. Those were "early indicators" of A.I.***

www.nytimes.com/2017/07/02/technology/hackers-find-ideal-testing-ground-for-attacks-developing-countries.html

For the cyber security industry, this has made cyberspace increasingly difficult to defend with existing security methods having remained relatively stagnant in comparison to this rapid evolution. Artificial intelligence is one of the few technologies that is part of this new era of connectivity and therefore may offer *a solution to the underlying problem within the IoT sector.*

17

Blockchain:

Blockchain – the few technologies that is part of this new era of connectivity and therefore may offer a solution to the underlying problem within the IoT sector.

The Watson IoT Platform has a built-in capability that lets you add selected IoT data to a private blockchain. The protected data is shared among only the business partners involved with the transaction.

Decentralized IoT networks are the future of IoT. Blockchain is the missing link that will enable scalability, privacy and reliability of IoT transactions. Blockchain technology can serve as a tool to track and coordinate connected devices, enable processes and ultimately support the billions of transactions that will take place within the Internet of Things, making use of a transparent, impenetrable distributed ledger. Ultimately, decentralized marketplaces will enable a global Economy of Things, where IoT data can be traded and exchanged autonomously.

Sources:

www.ibm.com/internet-of-things/platform/private-blockchain/
www.iotcentral.io/blog/using-blockchain-to-secure-iot
medium.com/@eciotify/key-ways-that-blockchain-can-revolutionize-the-internet-of-things-iot-a00edb50dfb7

18

Challenges & Conclusions

- Standardization vs. proprietary
- Thing-Bots
- Old Tools vs. New Tools

19

References

- **ZigBee 141 Success Secrets**, Dawn Rivas
- **Vision and challenges for realizing the Internet of things**, CERP-IoT book
- **Z-Wave Alliance**: *z-wavealliance.org*
- *www.bsi.bund.de*
- **Abusing the Internet of Things**, Nitesh Dhanjani
- *www.theregister.co.uk/2017/04/27/hajime_iot_botnet/*
- **802.15.4/ZigBee Analysis and Security**, Dartmouth Computer Science Technical Report
  iasaglobal.org/itabok3_0/trends-and-techniques-2/internet-of-things
- www.gsma.com/connectedliving/future-iot-networks/
- **Internet of Things: Challenges and Opportunities**, Subhas Chandra Mukhopadhya
- *www.iotcentral.io/blog/using-blockchain-to-secure-iot*
- *securelist.com/hajime-the-mysterious-evolving-botnet/78160/*

20

Questions?

Thank you!

Dipl-Ing. Franjo Majstor MSc
TECHNOLOGY EVANGELIST

Vienna, Oct 2017