0x70
CYBER SECURITY

Key Aspects of Cybersecurity in the Context of Internet of Things

IoT Security Challenges

Who am I

- 28 years of experience working in different sectors and countries
- Including 16 years in the Media (PayTV) industry
  - 14 years in Operations / Project Management
  - Experience in content protection and anti-piracy strategy
- Few years in cybersecurity
  - Incl. Security audit project management

A global experience in

- **Operations / Project Management**
- **Multicultural team leading**
- **Business development**

Curious, interested by innovation

- **IoT**
- **Artificial Intelligence**

● I worked there!

About 0x70 (under construction)

0x70
CYBER SECURITY

- 0x70 (in hexadecimal) = 7x 16 + 0 x 1 = 112

- It’s the emergency number in Europe and globally for 85 countries including countries in Africa, Asia, Latin America.

- What does the 112 does ?
  1. Listen to you
  2. Evaluate the risk
  3. Provide you with the right service

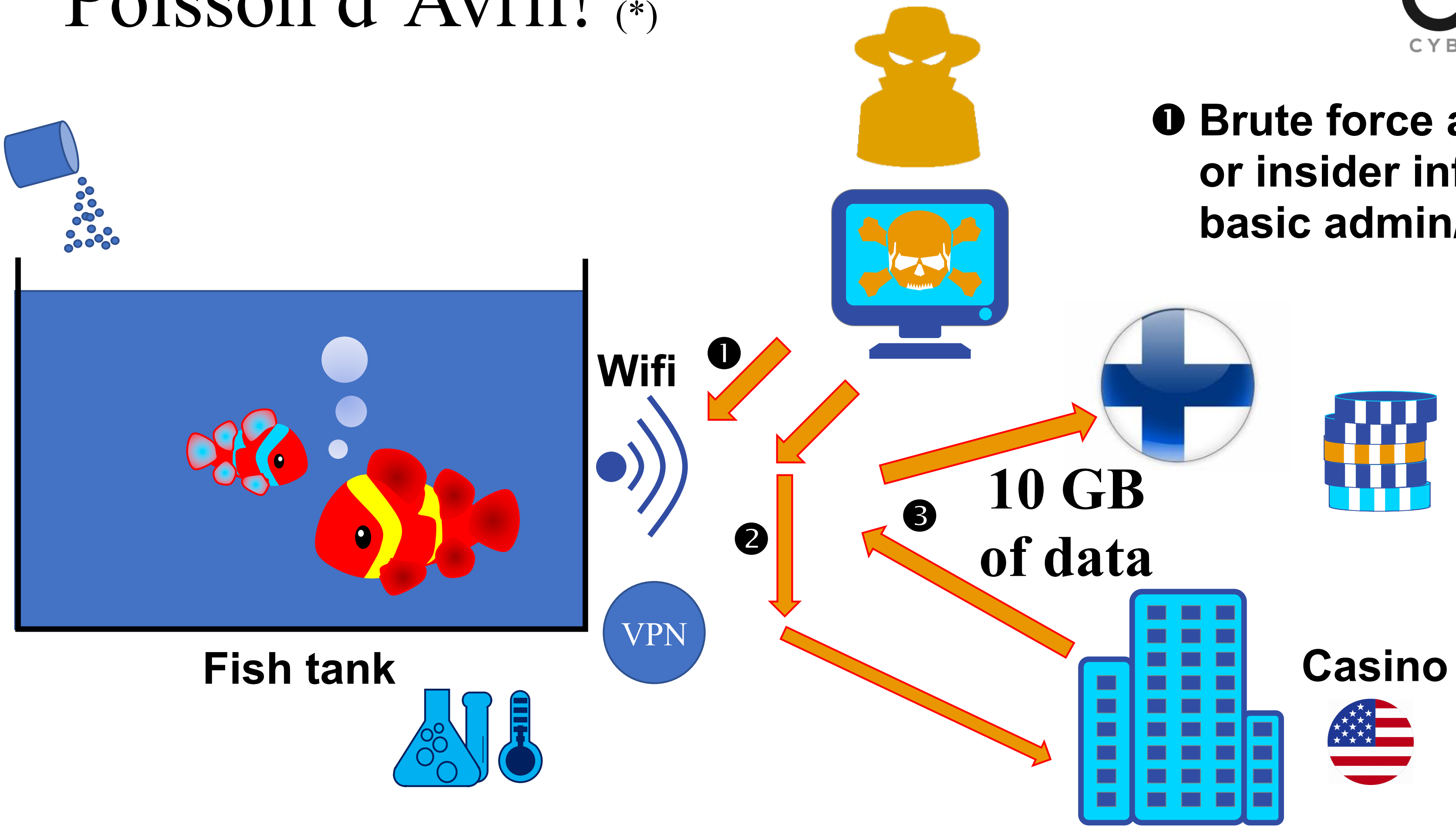
CISO as a Service
DPO as a Service

And no, my name is not James Bond, 007

Key Aspects of Cybersecurity in the Context of Internet of Things

IoT Security Challenges

Poisson d’Avril! (*)



❶ Brute force attack or insider info or basic admin/pwd

Wifi

❶

❷

❸

VPN

Fish tank

10 GB of data

Casino

(*) April Fools' Day

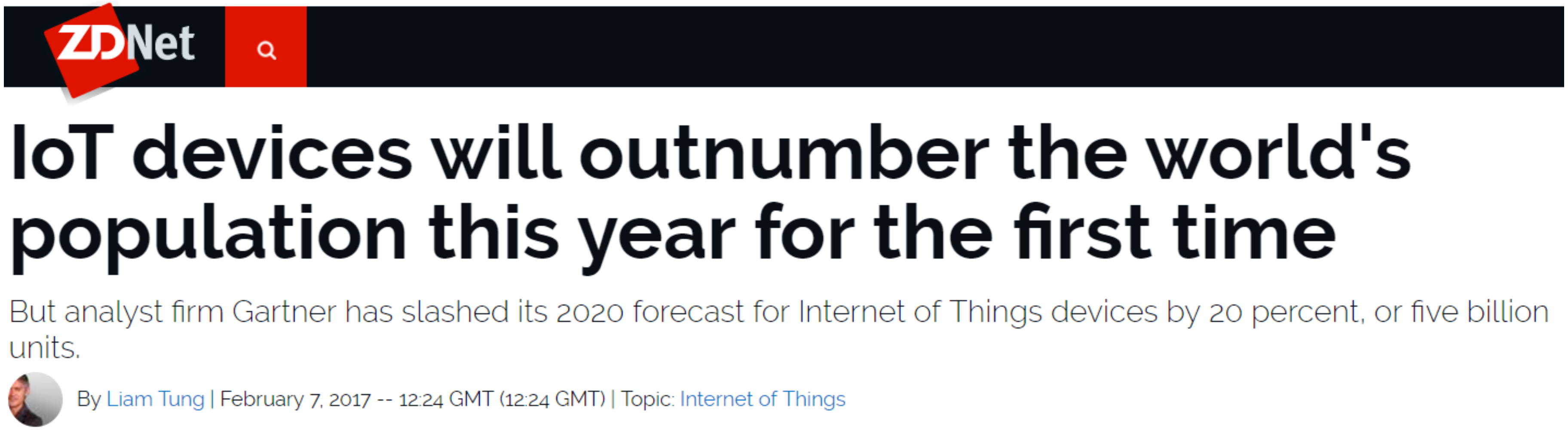
http://www.securityweek.com/hacked-smart-fish-tank-exfiltrated-data-rare-external-destination

Innovation versus Operations

As an enabler….

… if secured

IoT Market Development



IoT devices will outnumber the world's population this year for the first time

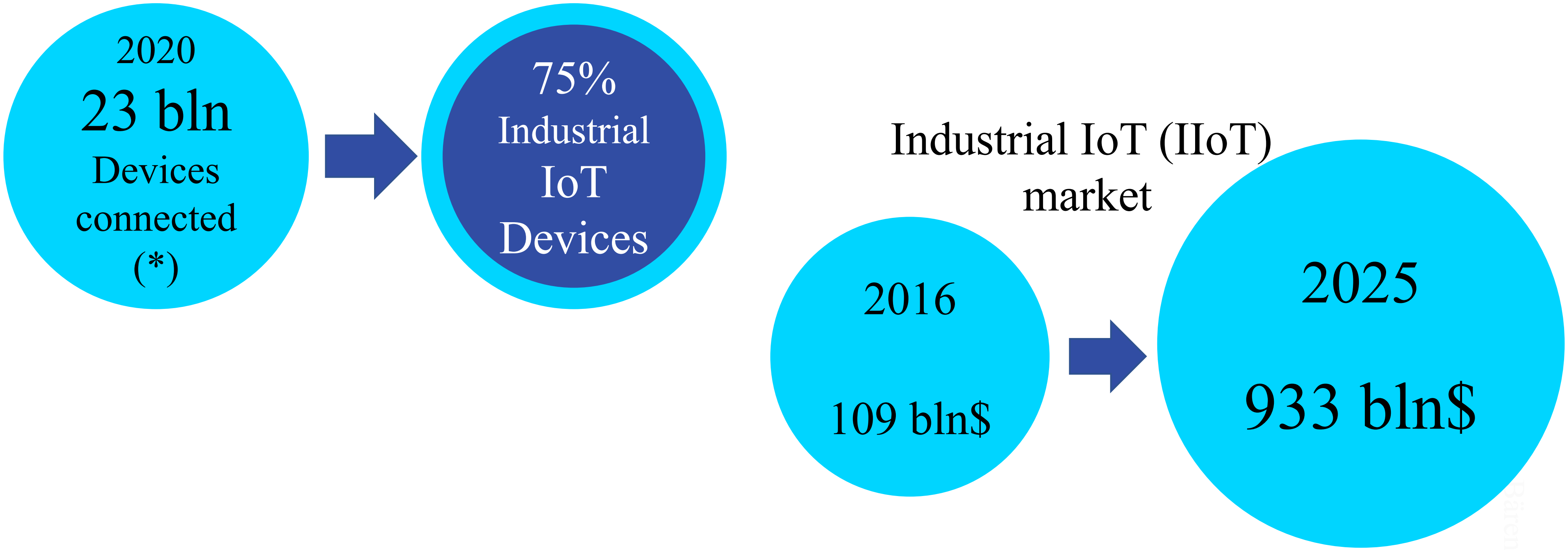
But analyst firm Gartner has slashed its 2020 forecast for Internet of Things devices by 20 percent, or five billion units.

By Liam Tung | February 7, 2017 -- 12:24 GMT (12:24 GMT) | Topic: Internet of Things

http://www.zdnet.com/article/iot-devices-will-outnumber-the-worlds-population-this-year-for-the-first-time/

Internet of Things in few numbers

0x70 CYBER SECURITY



2020
23 bln
Devices
connected
(*)

75%
Industrial
IoT
Devices

Industrial IoT (IIoT)
market

2016

109 bln$

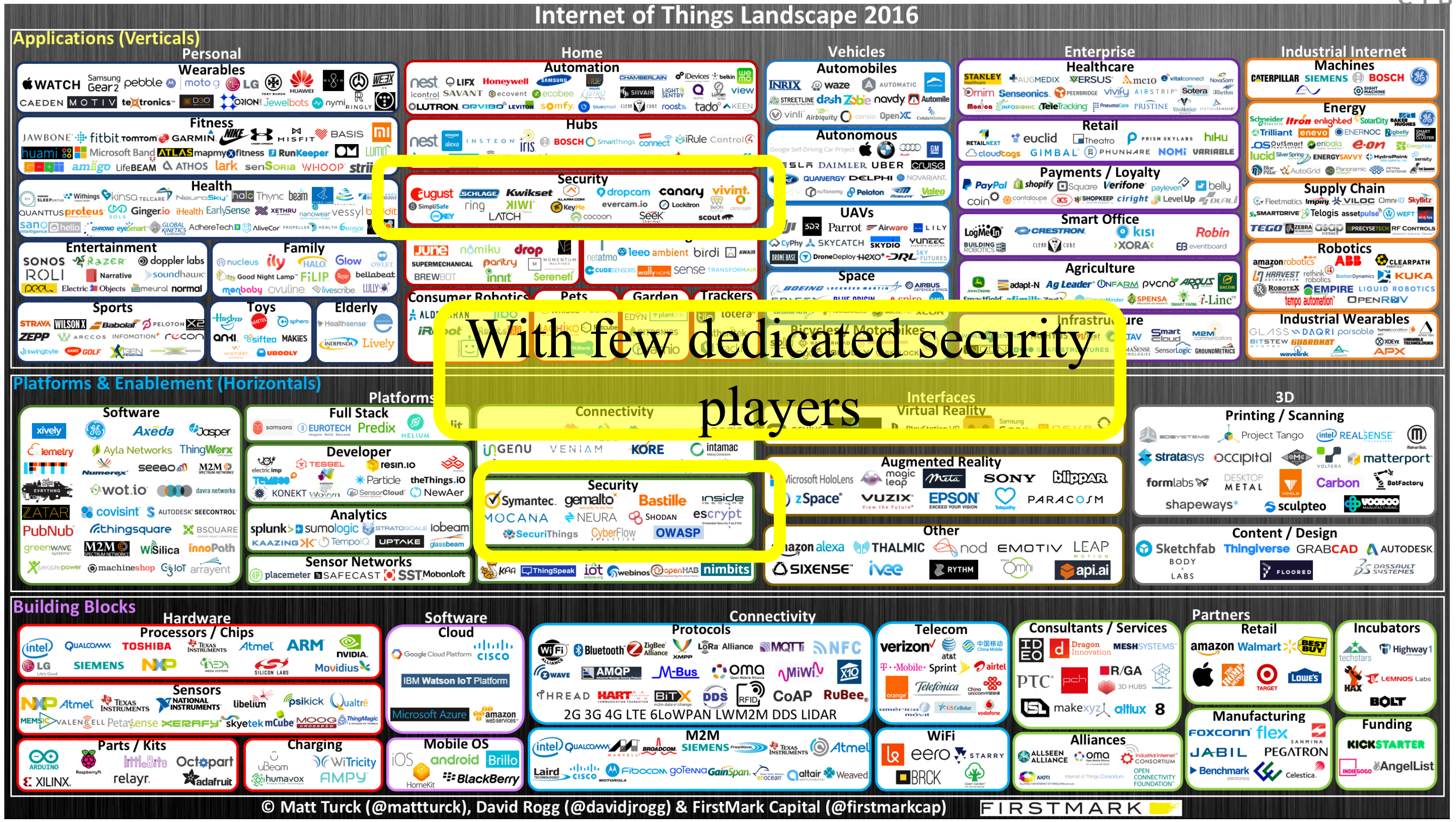
2025

933 bln$

(*): https://ww2.frost.com/news/press-releases/generating-business-revenue-growth-through-use-internet-things-and-big-data-analytics/
Note: Gartner, Dec. 2013 http://www.gartner.com/newsroom/id/2636073 26 bln devices by 2020

(**) http://www.techrepublic.com/article/industrial-iots-global-market-to-reach-934b-by-2025/
http://www.grandviewresearch.com/industry-analysis/industrial-internet-of-things-iiot-market

IoT – A heterogeneous landscape



With few dedicated security players

Source: http://mattturck.com/iot-landscape-2016-clean/

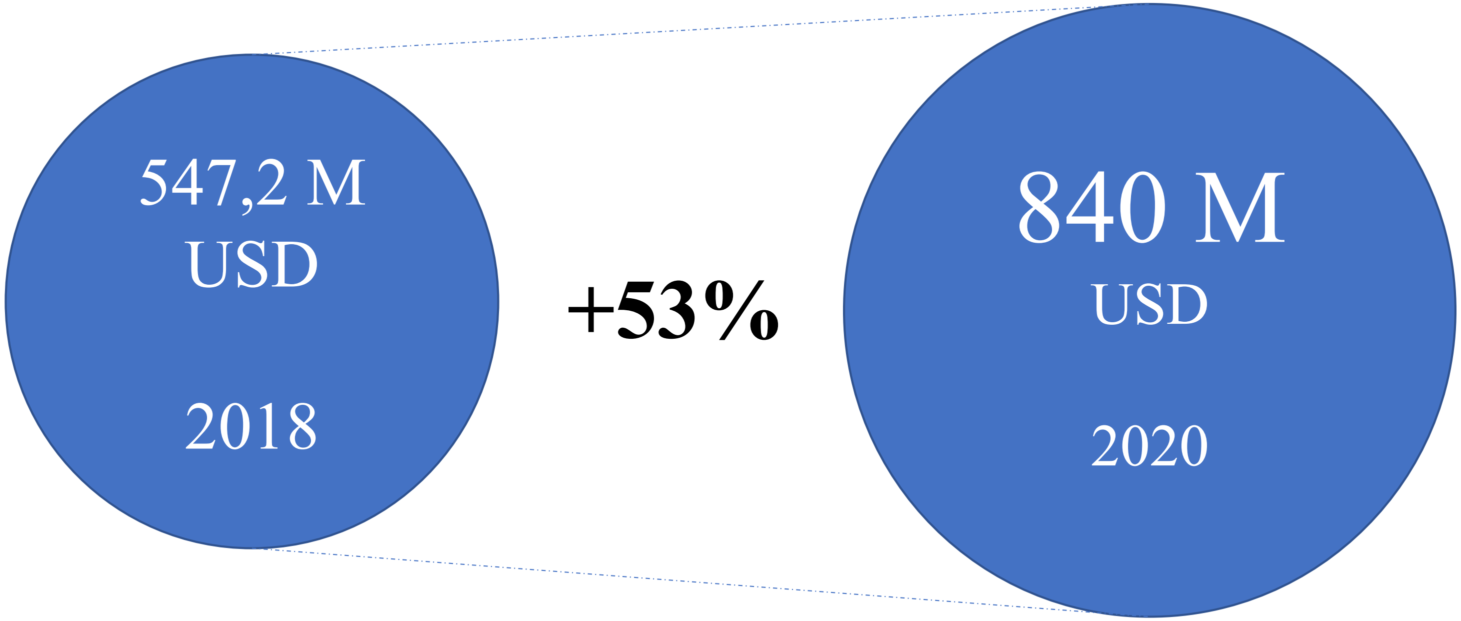
© D.Fletcher for CloudTweaks.com

0x70
CYBER SECURITY

IoT Security

The big picture

The IoT Security market



547,2 M
USD

2018

+53%

840 M
USD

2020

http://internetofthingsagenda.techtarget.com/blog/IoT-Agenda/IoT-Another-opportunity-to-build-in-security-from-the-start

IoT Security goes beyond €

- IoT security failures can cause both
  - Financial loss
  - and physical harm

http://eftm.com.au/2015/02/robots-helping-out-not-taking-over-on-the-audi-production-line-19389

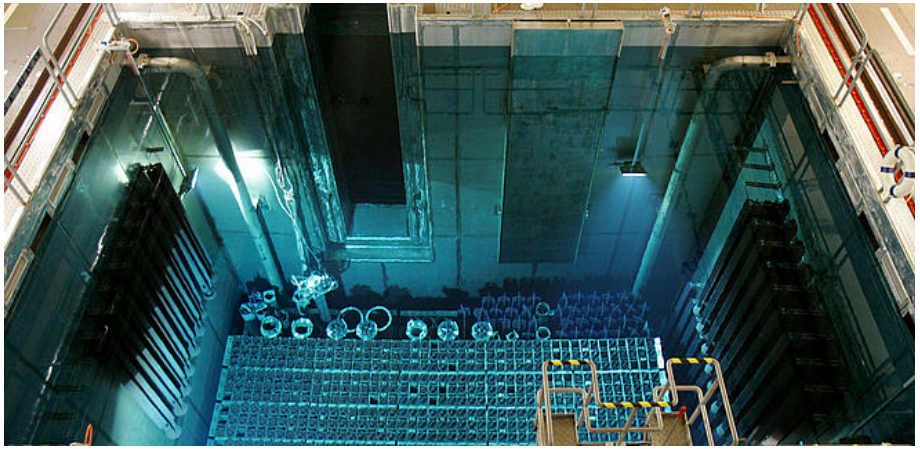


Image source: https://www.allianz.com/en/about_us/open-knowledge/topics/environment/articles/110317-nuclear-power-a-beginners-guide.html/

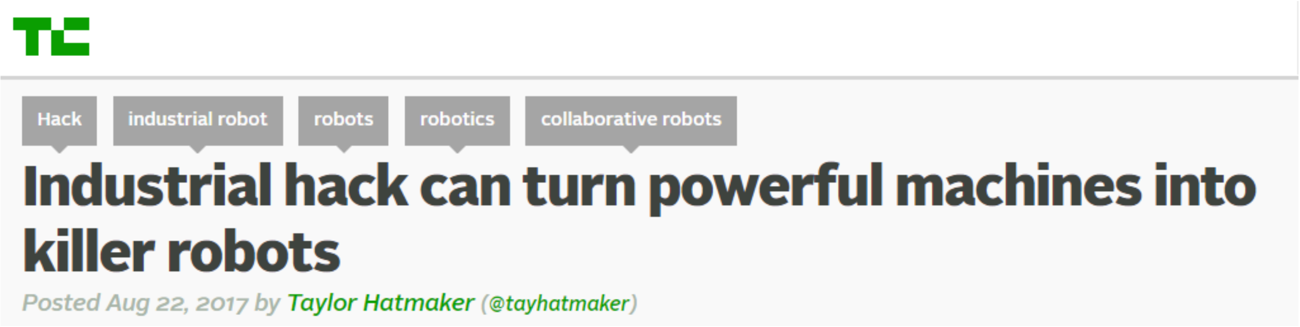
Source: https://www.sjm.com

IoT Security – Two risks

- Devices do something there are not supposed to do
  - Example: fridges / webcams used as part of a DDoS attack (Cf. Mirai botnet)

- Devices do exactly what they are intended to do but in a devious way
  - Example: Nuclear power plant enrichment centrifuges rapidly speeding up and then suddenly slow down, potentially damaging them (Stuxnet)

IoT's security – some recent news



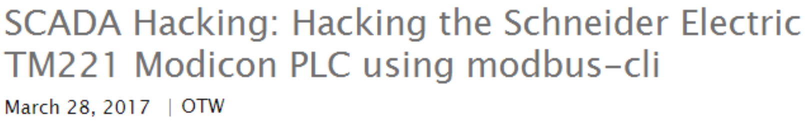
TC

Hack | industrial robot | robots | robotics | collaborative robots

Industrial hack can turn powerful machines into killer robots

Posted Aug 22, 2017 by Taylor Hatmaker (@tayhatmaker)

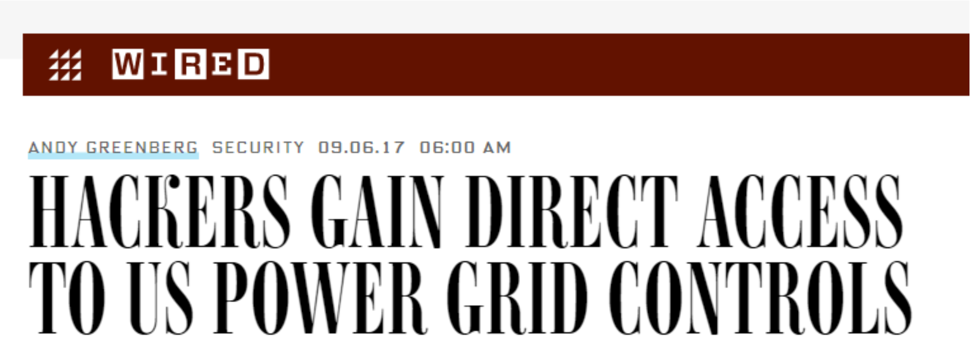
https://techcrunch.com/2017/08/22/universal-robots-exploit-ioactive/



SCADA Hacking: Hacking the Schneider Electric TM221 Modicon PLC using modbus-cli

March 28, 2017 | OTW

https://www.hackers-arise.com/single-post/2017/03/28/SCADA-Hacking-Hacking-the-Schneider-Electric-TM221-Modicon-PLC-using-modbus-cli



WIRED

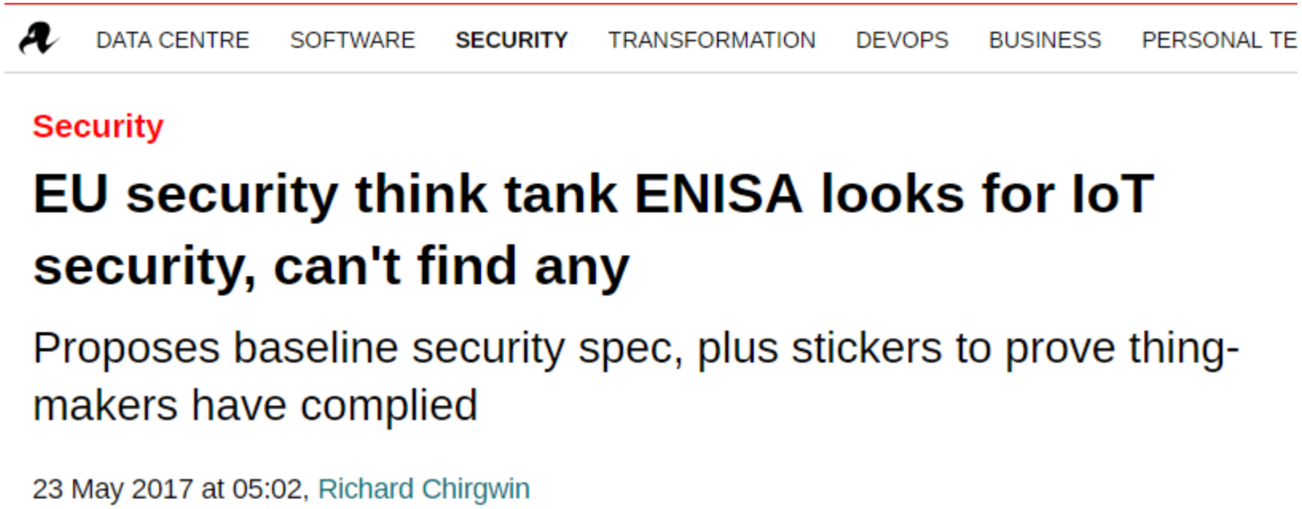
ANDY GREENBERG SECURITY 09.06.17 06:00 AM

HACKERS GAIN DIRECT ACCESS TO US POWER GRID CONTROLS

https://www.wired.com/story/hackers-gain-switch-flipping-access-to-us-power-systems/

SCADA
Supervisory Control And Data Acquisition

A security nightmare…??



Security

EU security think tank ENISA looks for IoT security, can't find any

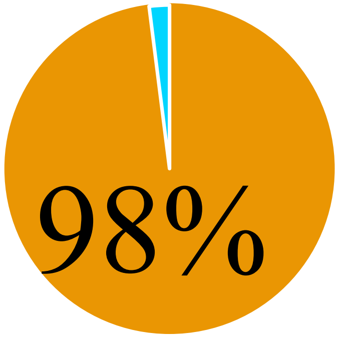
Proposes baseline security spec, plus stickers to prove thing-makers have complied

23 May 2017 at 05:02, Richard Chirgwin

Source: https://www.theregister.co.uk/2017/05/23/enisa_proposes_internet_of_things_security_standards/

More info on https://www.enisa.europa.eu/news/enisa-news/enisa-works-together-with-european-semiconductor-industry-on-key-cybersecurity-areas

Looks like for IoT devices



98%

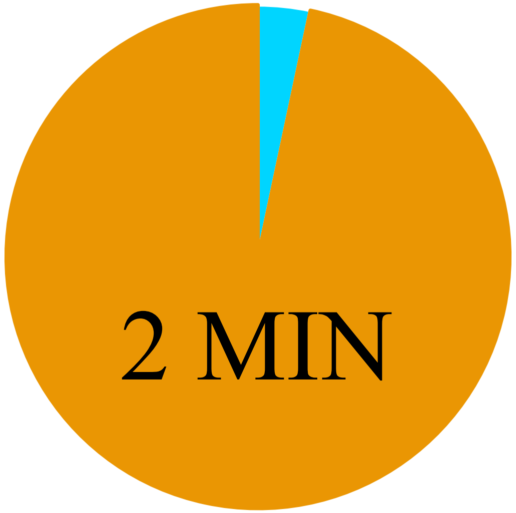
of web interfaces and administrative panels had fundamental security problems.

Such as:

- ❖Hardcoded and unmodifiable admin credentials
- ❖Outdated software (e.g. web server)
- ❖Lack of HTTP traffic encryption,
- ❖Various critical vulnerabilities in the interface

Source: https://www.htbridge.com/news/application-security-trends-report-2017.html

An easy target…



Time it took for an IoT device to be attacked
(peak time during Mirai botnet period)

Source: https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf

IoT Device

You need only one vulnerability in only one part of the device to compromise the whole system

Some of the security challenges

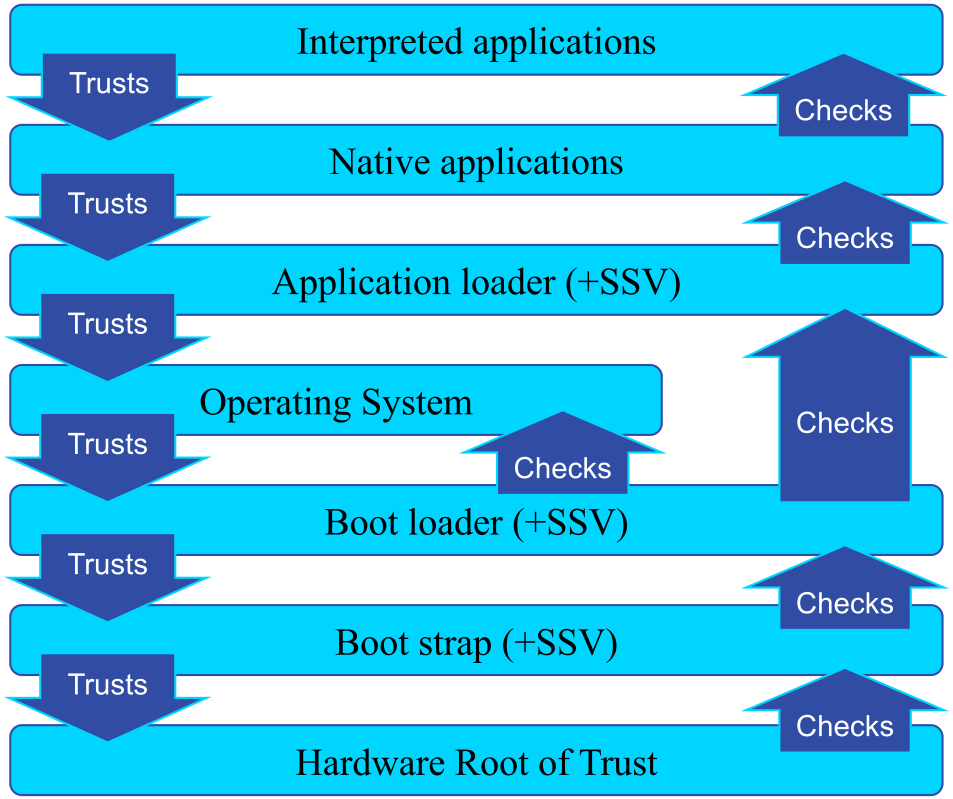
- Trusted Execution Environment (TTE)
- Integration of multiple components (Hardware/Software)
- Secured Over-The-Air (S-OTA) software update

EMBEDDED SECURITY PRINCIPLE

The trusted computing base (TCB) of a computer system is the set of all hardware, firmware, and/or software components that are critical to its security, in the sense that bugs or vulnerabilities occurring inside the TCB might jeopardize the security properties of the entire system. By contrast, parts of a computer system outside the TCB must not be able to misbehave in a way that would leak any more privileges than are granted to them in accordance to the security policy.

https://en.wikipedia.org/wiki/Trusted_computing_base

The full chain must be secured



Interpreted applications

Trusts

Checks

Native applications

Trusts

Checks

Application loader (+SSV)

Trusts

Checks

Operating System

Trusts

Checks

Boot loader (+SSV)

Trusts

Checks

Boot strap (+SSV)

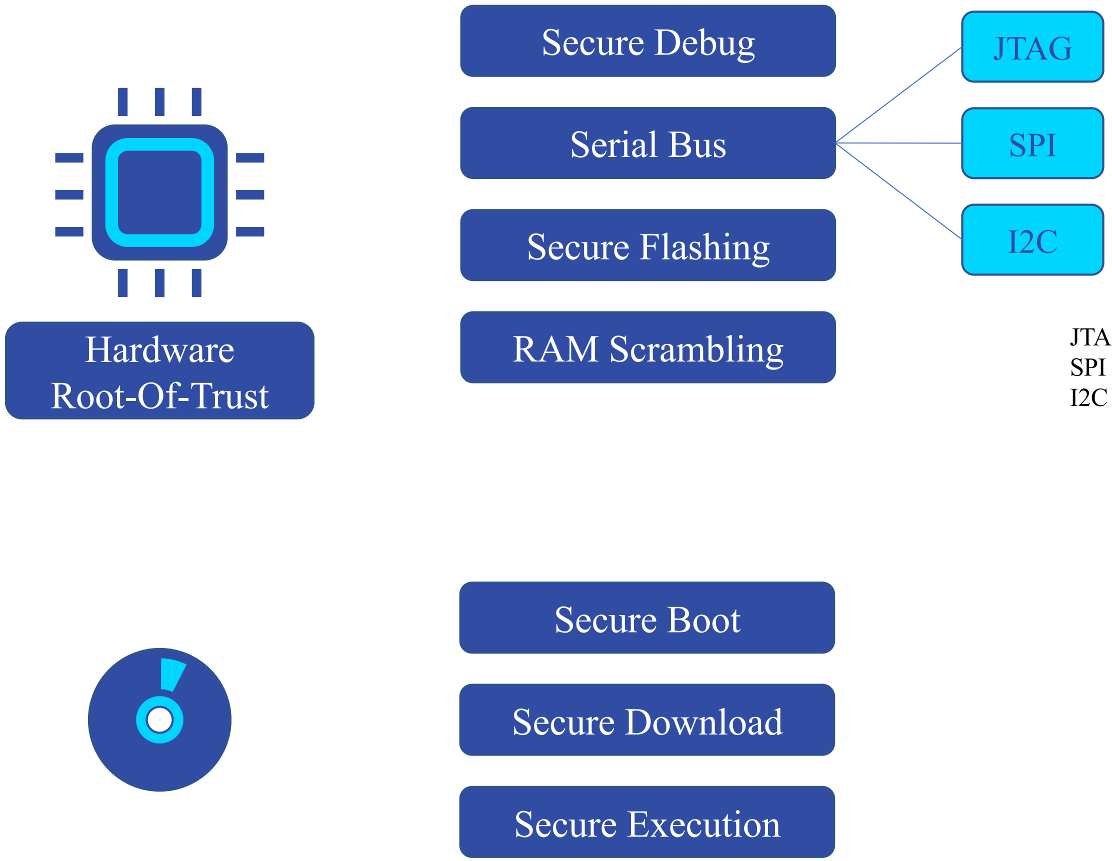
Trusts

Checks

Hardware Root of Trust

SSV: Safe and Secure Virtualization

Embedded security



Hardware Root-Of-Trust

Secure Debug

Serial Bus

Secure Flashing

RAM Scrambling

JTAG

SPI

I2C

Secure Boot

Secure Download

Secure Execution

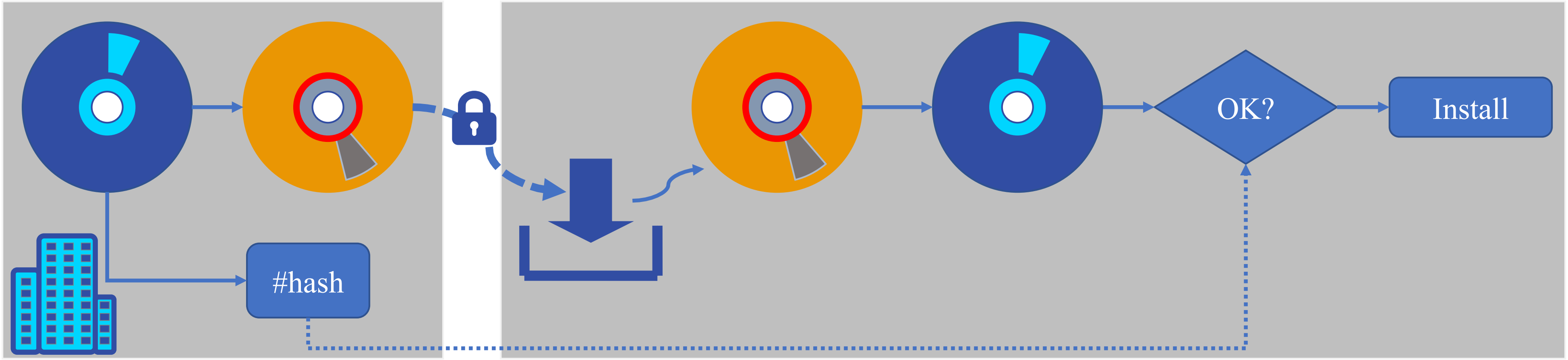
JTAG - Joint Test Action Group
SPI - Serial Peripheral Interface
I2C - Inter-Integrated Circuit

Hardware Root Of Trust

- Some of the components
  - Unique Identifier & Secret Data
  - Secured Chipset start (SCS) – ROM level
  - Debugging ports protection
    - no access to inner-chip functions / data
  - Key ladder - AES keys

Software Secure Download

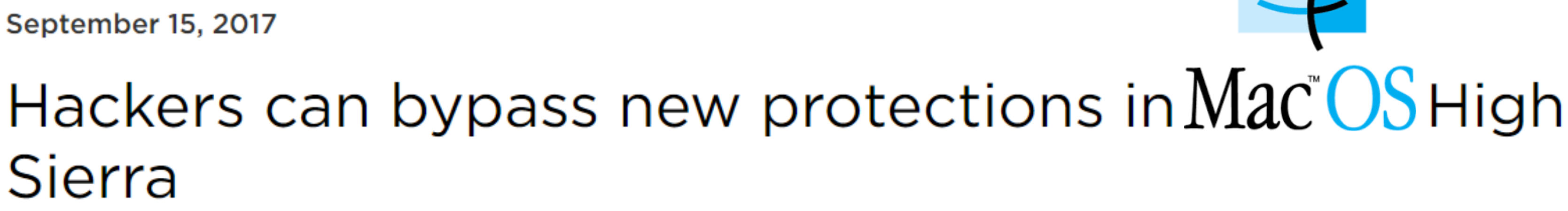
- Software (SW) encrypted and signed (#hash)
- Integrity potentially checked through Cyclic Redundancy Check (CRC)
- IoT Device rebooting after SW download AND CRC check



Secured Execution

- Need OS and application secured
  - Kernel configuration (including Stack protection)
  - Networking security
    - Including protocol restriction
  - Isolation
    - Sandbox
    - Privilege Management
  - Disk / Partition / File management

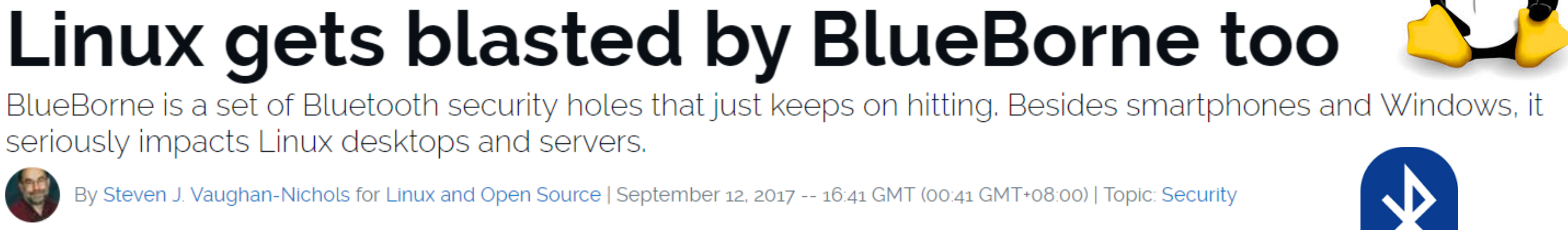
Not an easy game to play…



September 15, 2017

Hackers can bypass new protections in MacOS High Sierra

Source: https://www.scmagazineuk.com/hackers-can-bypass-new-protections-in-macos-high-sierra/article/688998/



Linux gets blasted by BlueBorne too

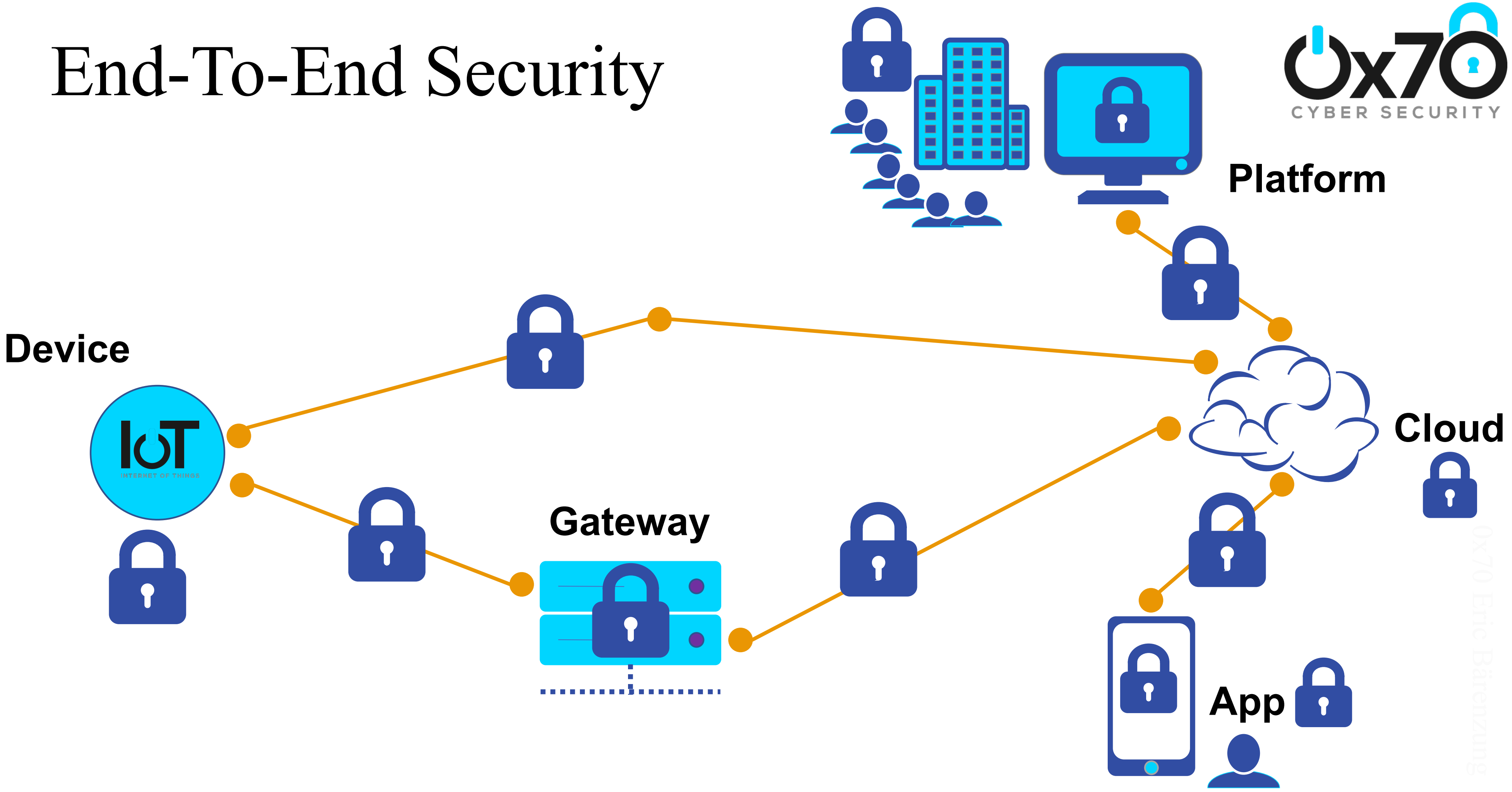
BlueBorne is a set of Bluetooth security holes that just keeps on hitting. Besides smartphones and Windows, it seriously impacts Linux desktops and servers.

By Steven J. Vaughan-Nichols for Linux and Open Source | September 12, 2017 -- 16:41 GMT (00:41 GMT+08:00) | Topic: Security

Source: http://www.zdnet.com/article/linux-gets-blasted-by-blueborne-too/

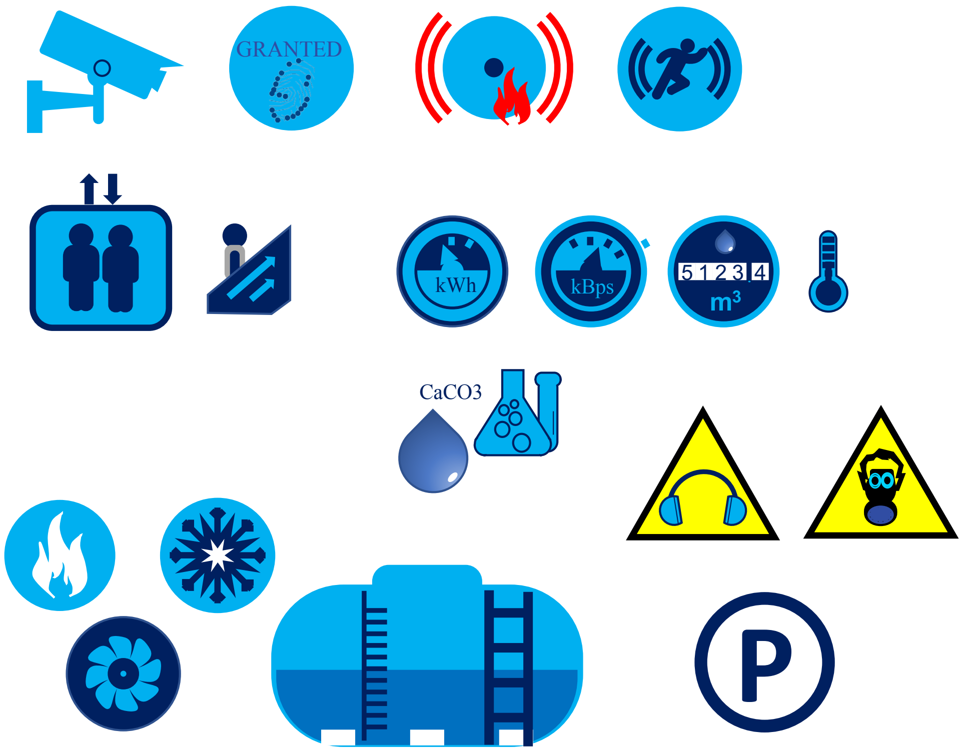
IoT Ecosystem

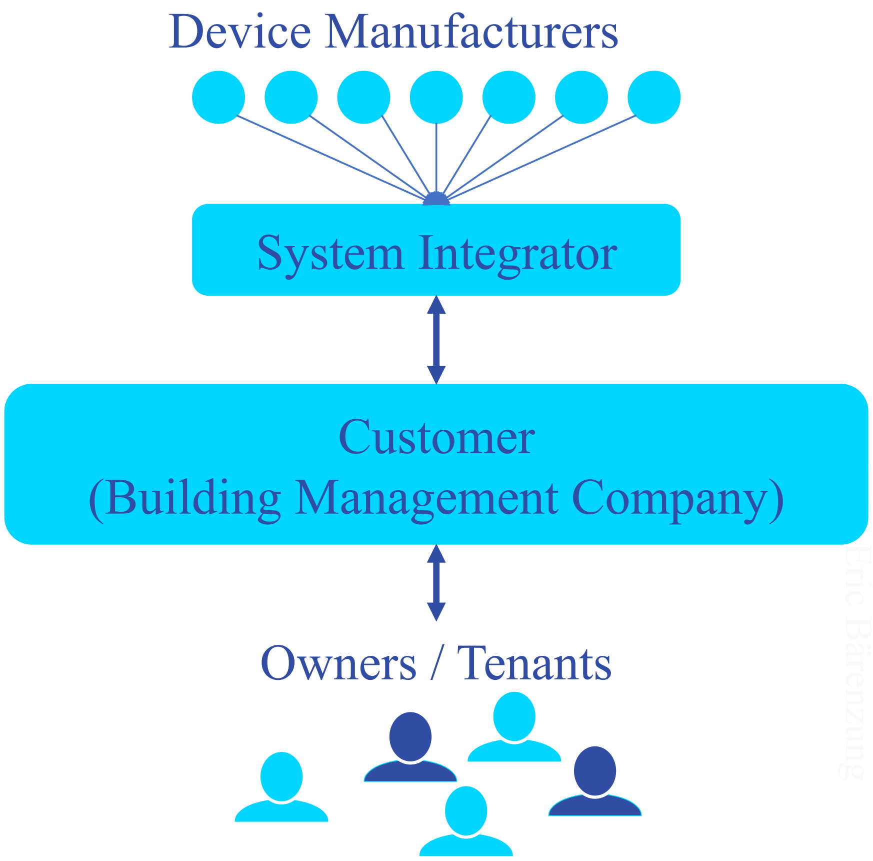
End-To-End Security



0x70
CYBER SECURITY

The companies
(Smart Building case)





Device Manufacturers

System Integrator

Customer
(Building Management Company)

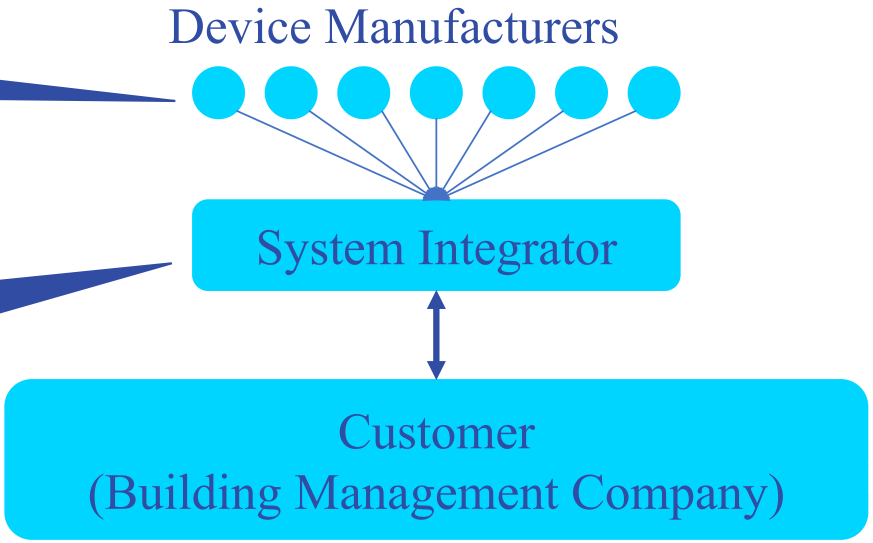
Owners / Tenants

Responsabilities….

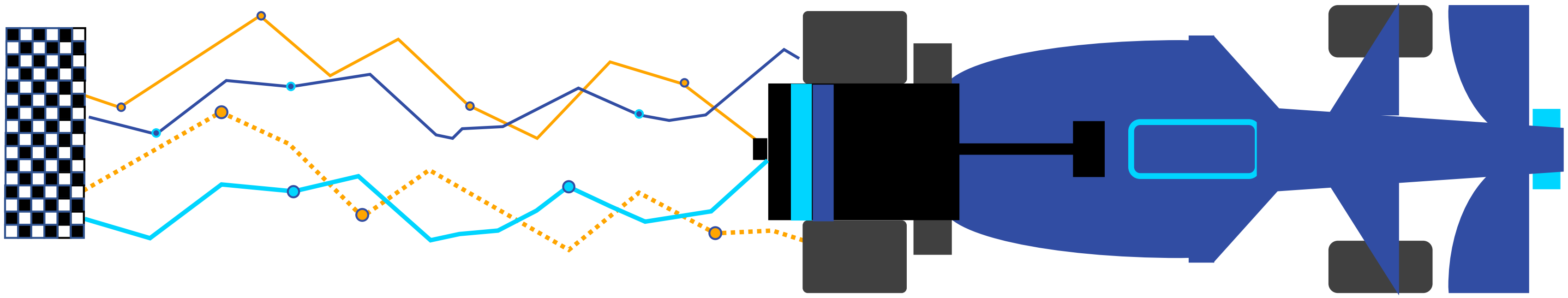
Ensure security / data protection at the device level

Ensure security / data protection of the end-to-end system including management platform and end-user application

Ensure security and data protection of the usage of the platform, typically to avoid a data breach from an internal user



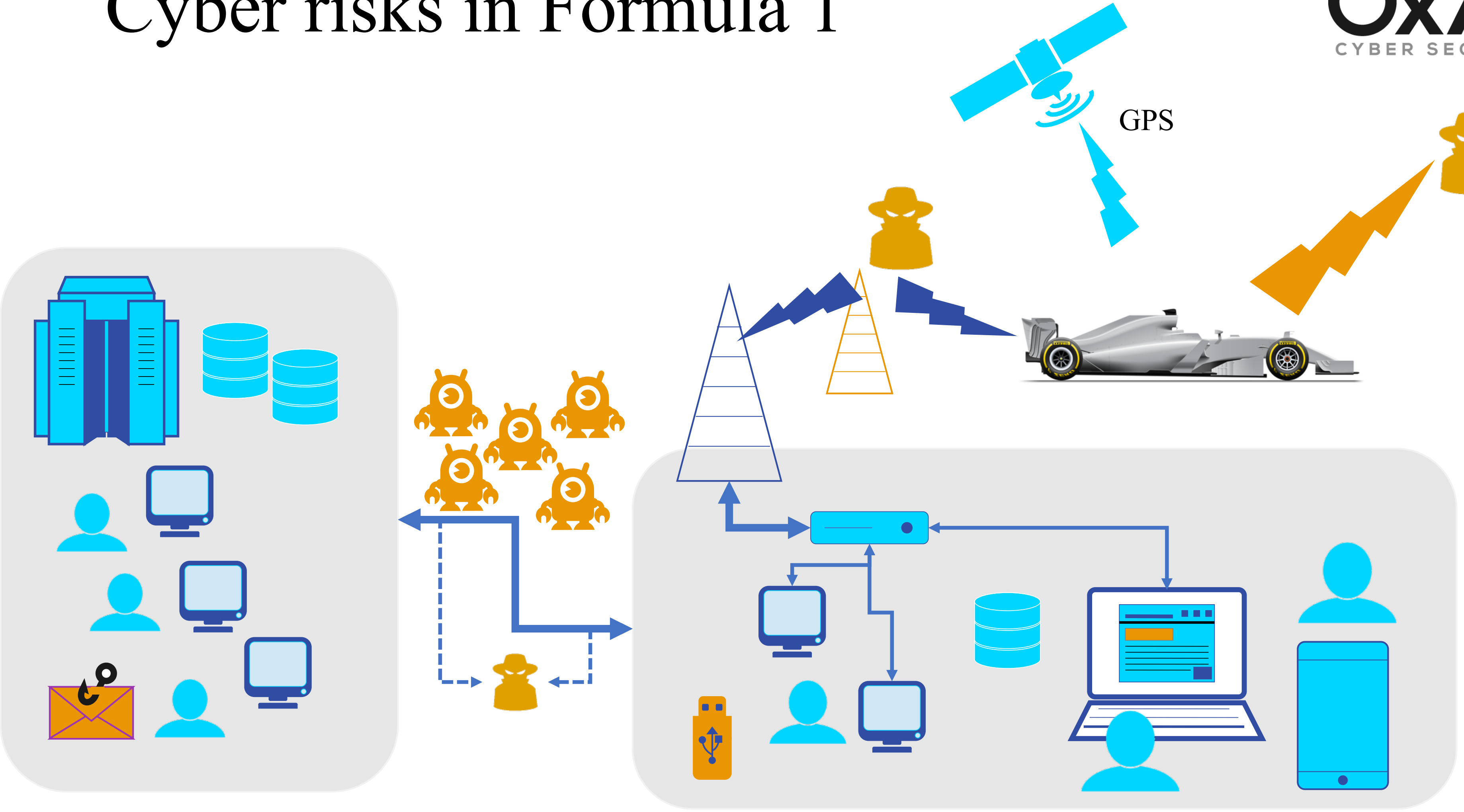
IoT in Formula 1



150
-
300
sensors

Cyber risks in Formula 1

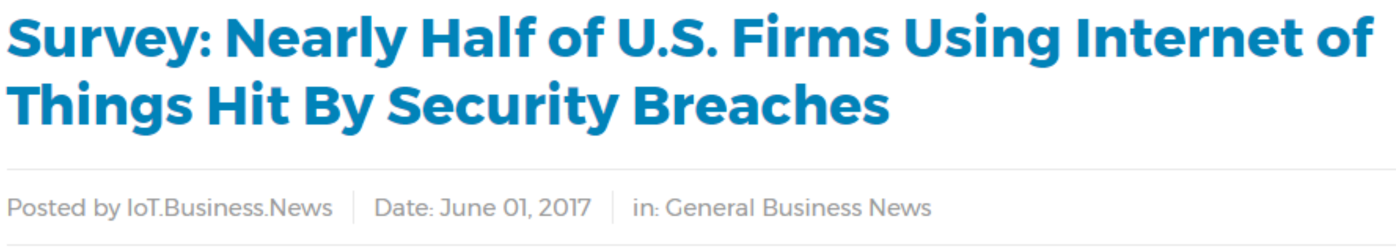
0x70 CYBER SECURITY



$ecurity cost

The Security versus Cost dilemna

Insecurity has a cost



Survey: Nearly Half of U.S. Firms Using Internet of Things Hit By Security Breaches

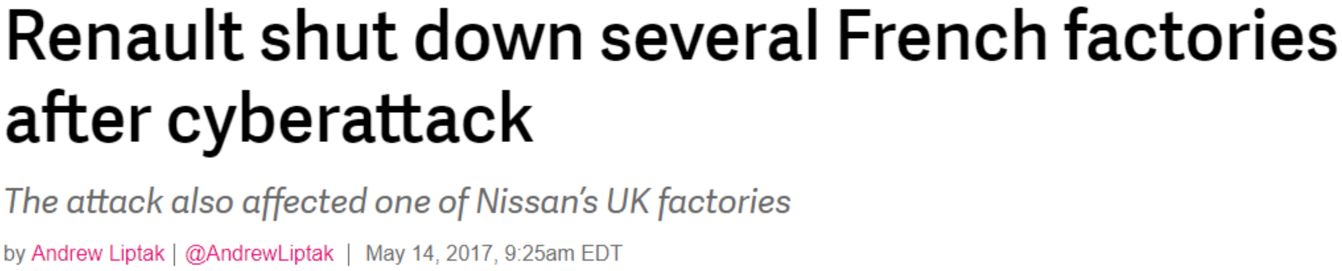
Posted by IoT.Business.News | Date: June 01, 2017 | in: General Business News

https://iotbusinessnews.com/2017/06/01/65662-survey-nearly-half-u-s-firms-using-internet-things-hit-security-breaches/

- Cost of breaches
  - SMEs (revenues <5M$ per year): 13.4% of total revenues
  - Tens of millions for larger ones
    - Nearly half of firms with annual revenues above $2 billion estimated the potential cost of one IoT breach at more than $20 million.

Insecurity has a cost

0x70 CYBER SECURITY



Renault shut down several French factories after cyberattack

The attack also affected one of Nissan's UK factories

by Andrew Liptak | @AndrewLiptak | May 14, 2017, 9:25am EDT

Wannacry

- Several manufacturing plants impacted…
  - Incl. Douai's factory that is producing 800 cars a day

…luckily during the week-end (less impact on production)

Source: https://www.theverge.com/2017/5/14/15637472/renault-nissan-shut-down-french-uk-factories-wannacry-cyberattack

Security too

- More secured chipsets are more expensive

- Encrypted communication potentially requires:
  - more bandwith…
    - But (I)IoT is not a huge bandwith eater (short message) at the device level
    - IoT has specific network (LoRa, Sigfox, 5G/LTE-M, etc.)
  - …and more calculation power
  - But these are « negligeable »

- Performing a security audit is « expensive »
  - But not if done at the beginning through « security by design »
  - And less costly than potential impacts of vulnerabilities

Security Balance with Ease of Use

- An example: two-factor identification process

- Other solutions available such as Public Key Infrastructure

To resume

Take aways

4 take aways

IoT ecosystem is vulnerable

Security is not eXpensive if « by design »

Roma was not built in 7 days, neither secured IoT

IoT has to be secured

Thanks for your attention

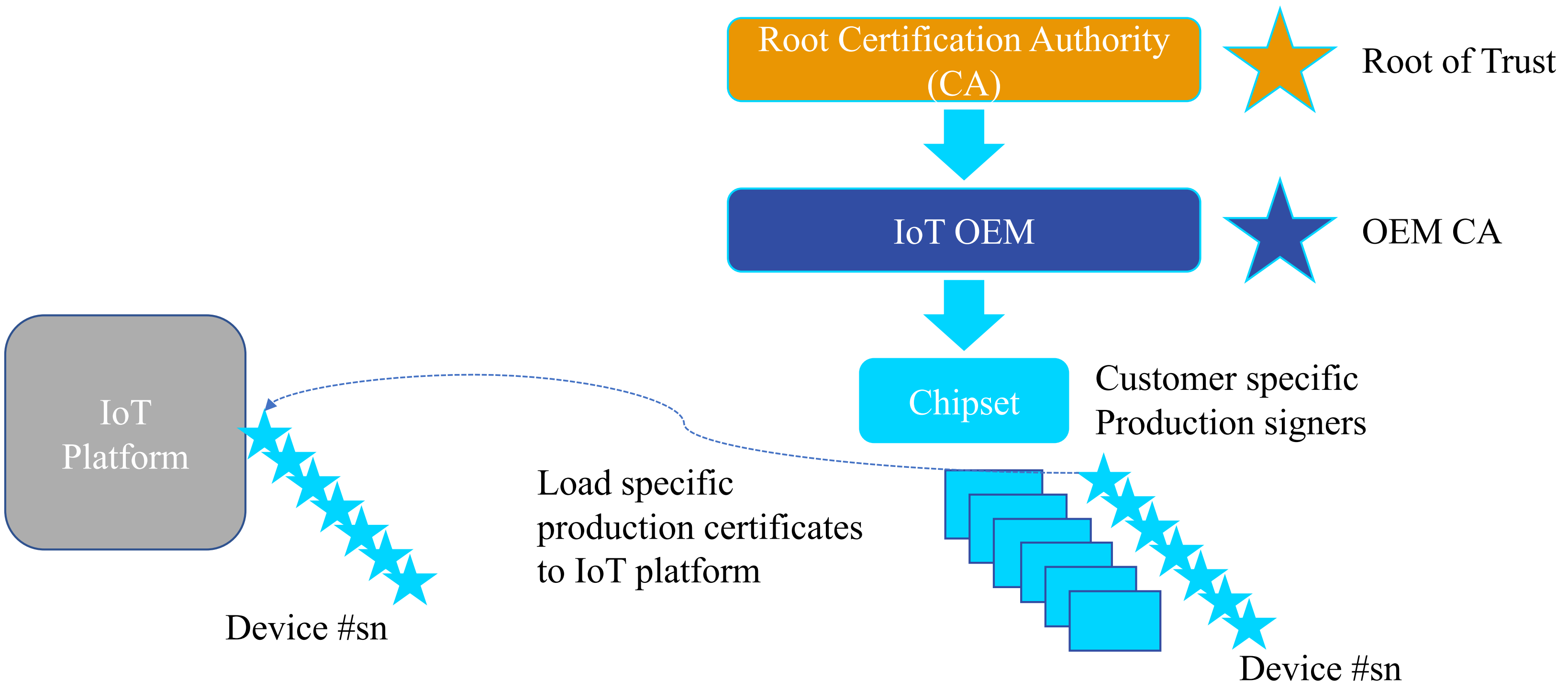
Eric Bärenzung

ebg@0x70.ch

Using Digital Certificates (1/3)

- The ultimate goal: « Just in time »
  - The IoT platform the first time they request service from it. IoT devices can automatically connect to and be recognized by
- How?
  - Unique cryptographic keys generated for each device during production
  - Signed by a Certification Authority (CA) as part of an offline digital certificate verification process
  - Loaded into the IoT platform to await a service request from systems containing the corresponding key pairs.

Using Digital Certificates (2/3)



Root Certification Authority (CA)

Root of Trust

IoT OEM

OEM CA

Chipset

Customer specific Production signers

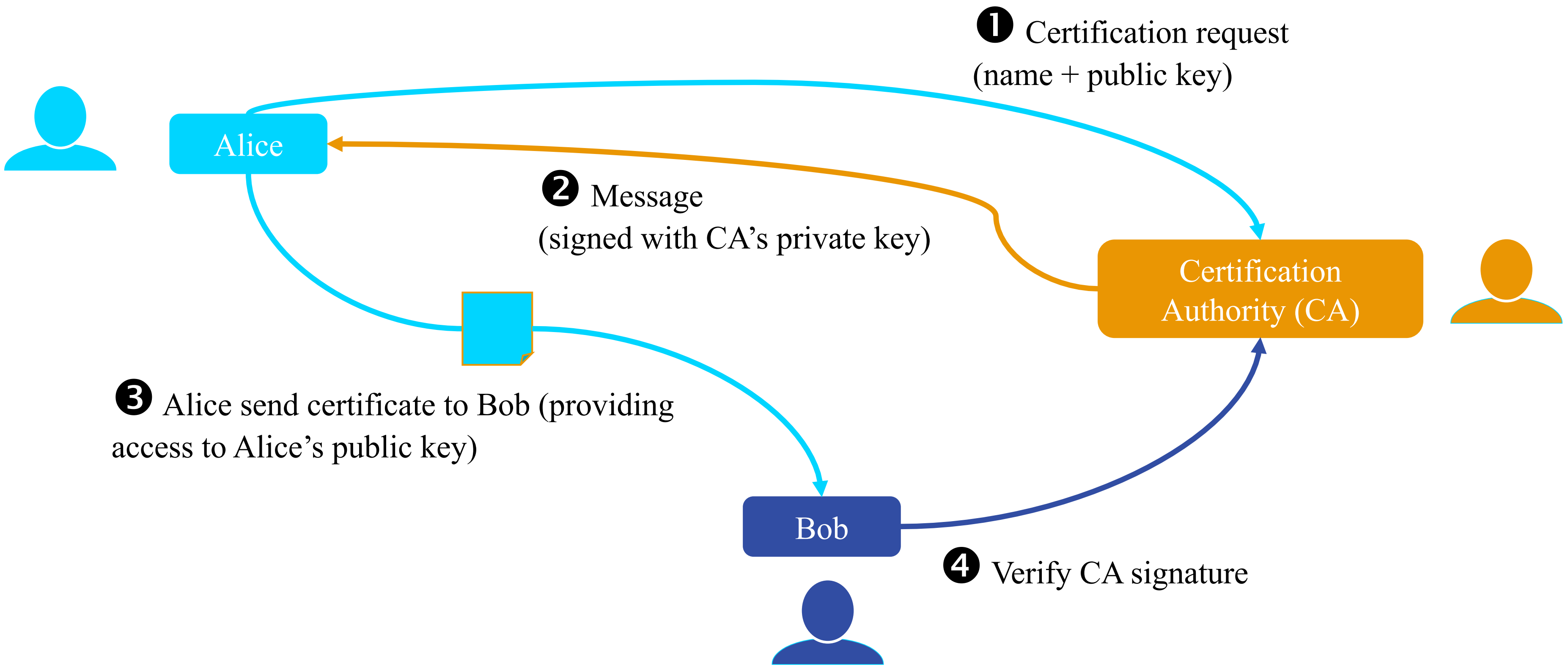
IoT Platform

Load specific production certificates to IoT platform

Device #sn

Device #sn

Using Digital Certificates (3/3)



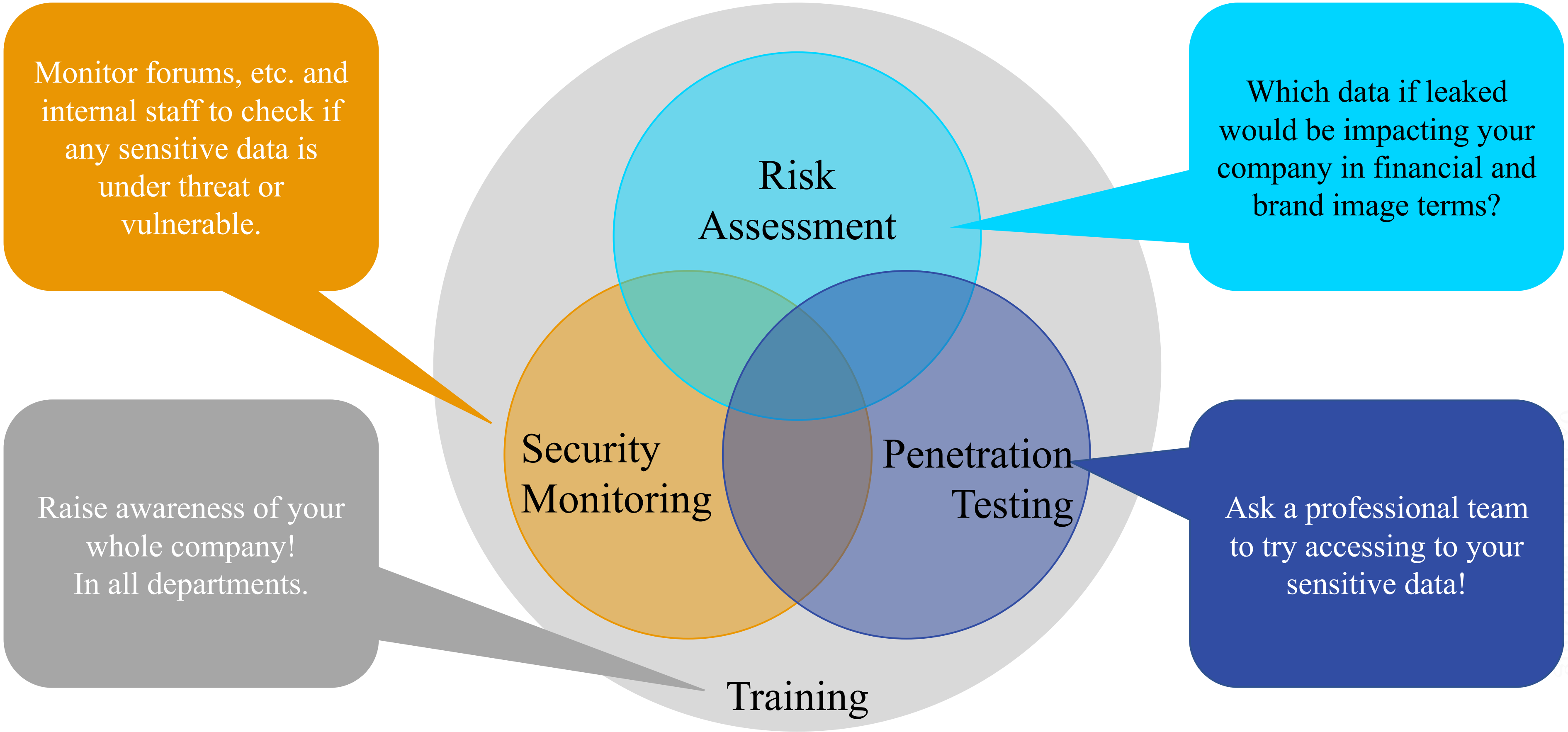
❶ Certification request (name + public key)

❷ Message (signed with CA’s private key)

❸ Alice send certificate to Bob (providing access to Alice’s public key)

❹ Verify CA signature

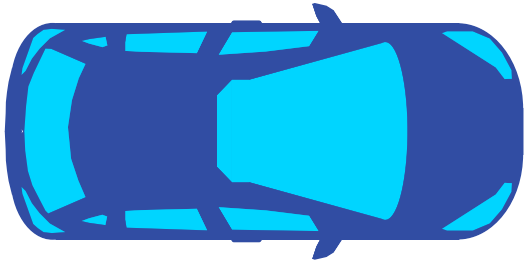
The pillars of (cyber) data security



Monitor forums, etc. and internal staff to check if any sensitive data is under threat or vulnerable.
Risk Assessment
Which data if leaked would be impacting your company in financial and brand image terms?
Security Monitoring
Penetration Testing
Raise awareness of your whole company!
In all departments.
Ask a professional team to try accessing to your sensitive data!
Training

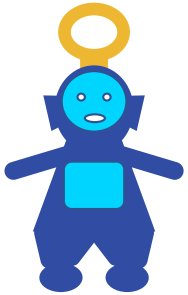
Getting « worse » with IoT

Wearables

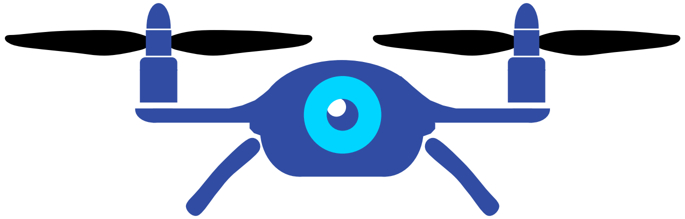


Connected cars

Smart home



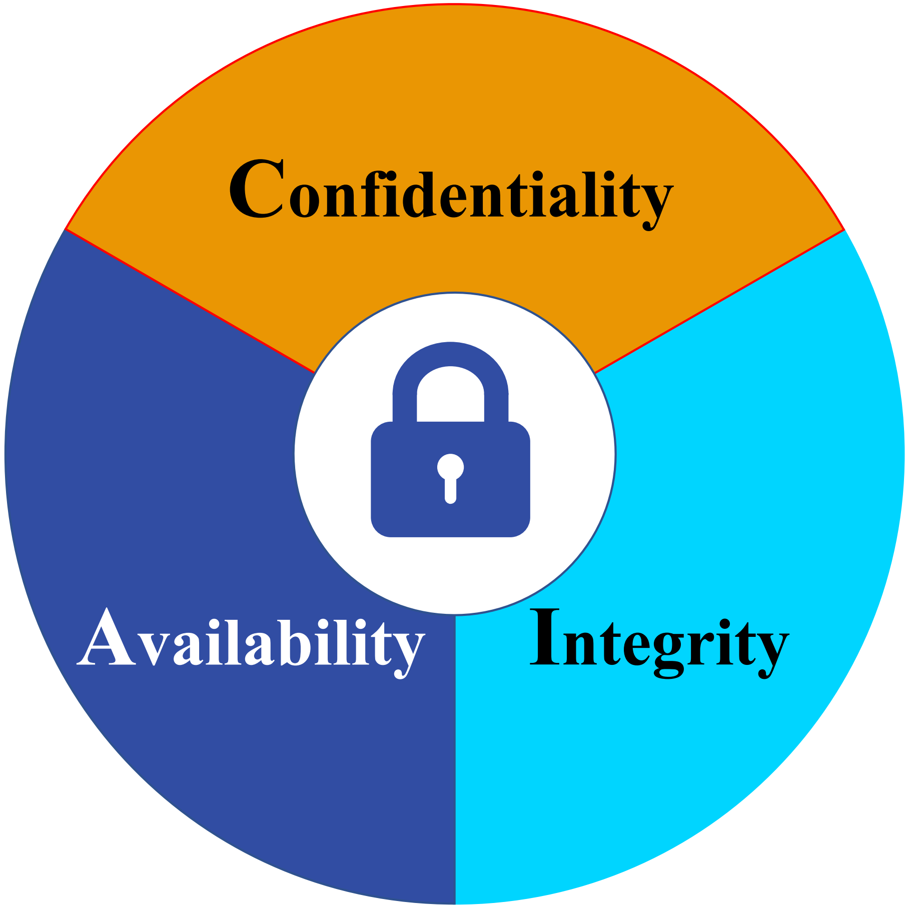
Smart Toys

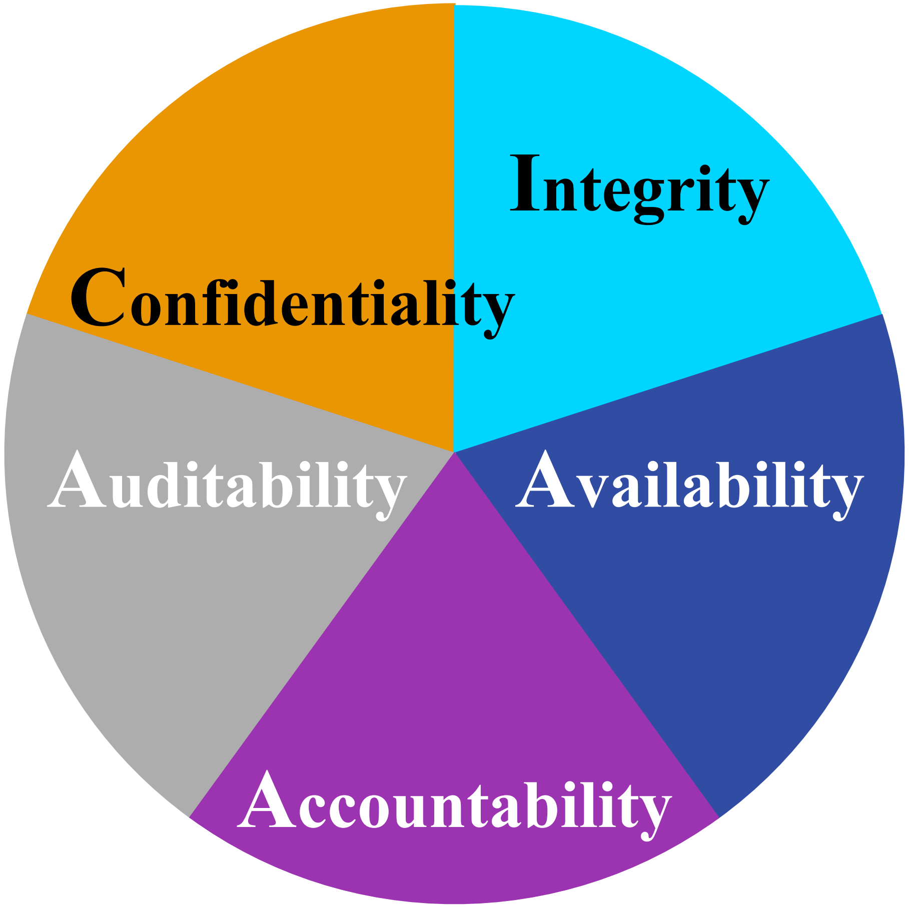


Drones

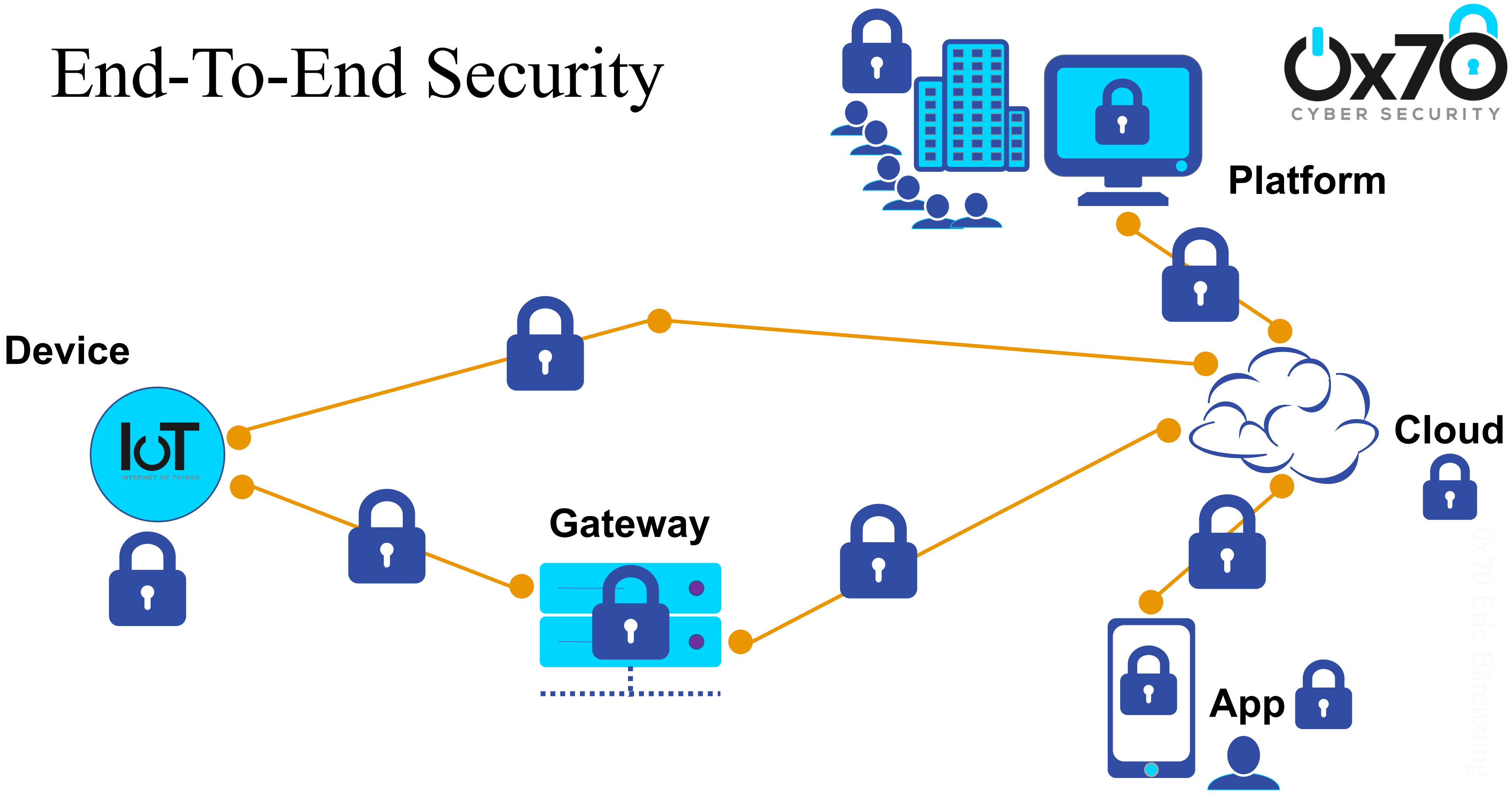
Back to basics

0x70
CYBER SECURITY





End-To-End Security



Platform

Device

Cloud

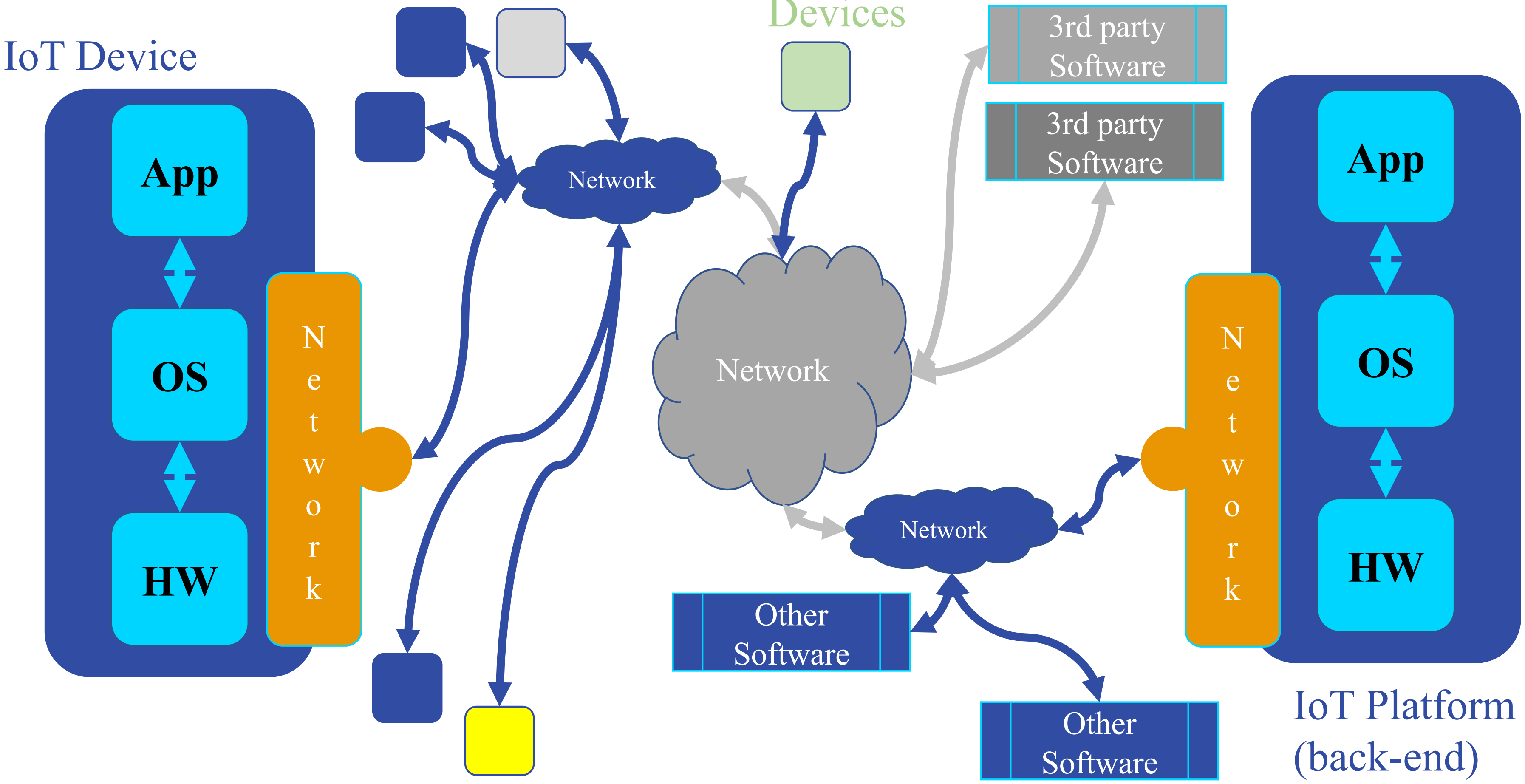
Gateway

App

The Internet of Hackable Things

Source: https://arxiv.org/pdf/1707.08380.pdf

The components


IoT Device
App
OS
HW
Network
Network
Other Devices
3rd party Software
3rd party Software
Network
Network
Other Software
Other Software
App
OS
HW
Network
IoT Platform (back-end)