



# Internet of



What should be done  
to secure IoT

# IoT Trends

# Internet of everything



# Recent regional IoT news



## Sheikh Mohammed launches Internet of Things Strategy in Dubai

The initiative will also award Dubai Digital Certificates for outstanding government and private entities

<https://www.thenational.ae/uae/government/sheikh-mohammed-launches-internet-of-things-strategy-in-dubai-1.669413>

## Maroc Telecom met les bouchées doubles sur l'IOT

<https://www.tekiano.com/2017/11/01/maroc-telecom-met-les-bouchees-doubles-sur-liot/>

## MCIT and UNDP Launch the 'Internet of Things' to Support Persons with Disabilities



EGYPTIAN STREETS  
SEPTEMBER 7, 2017

## Vodacom- Tackling Nigeria's Healthcare Problems With IoT

July 27, 2017 • Healthcare, Internet of Things, Mobile and Telecoms, Top Stories, West Africa

<http://www.itnewsafrika.com/2017/07/vodacom-tackling-nigeiras-healthcare-problems-with-iot/>

## How IoT will change the future of waste management in Africa

BY: NICK MANNIE

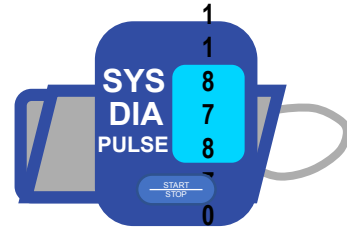
28 AUG 2017

<http://www.bizcommunity.com/Article/196/703/166615.html>

# Major Trends in the region (apart smart cities « showcase »)



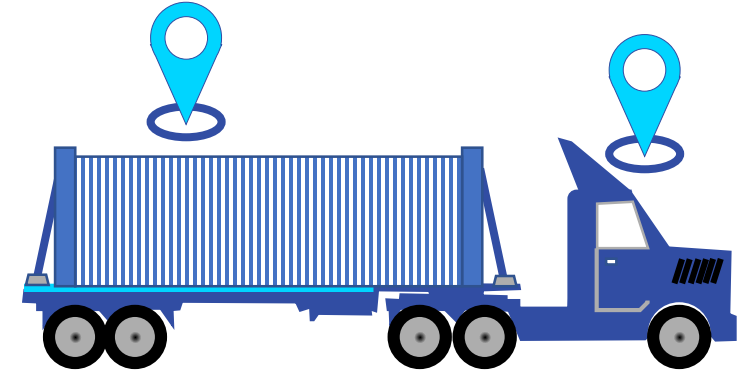
**Smart Meters**



**E-Health**



**E-Farming**



**Logistics**

- Not forgetting that IoT (like ICT) development will require

- IT infrastructure

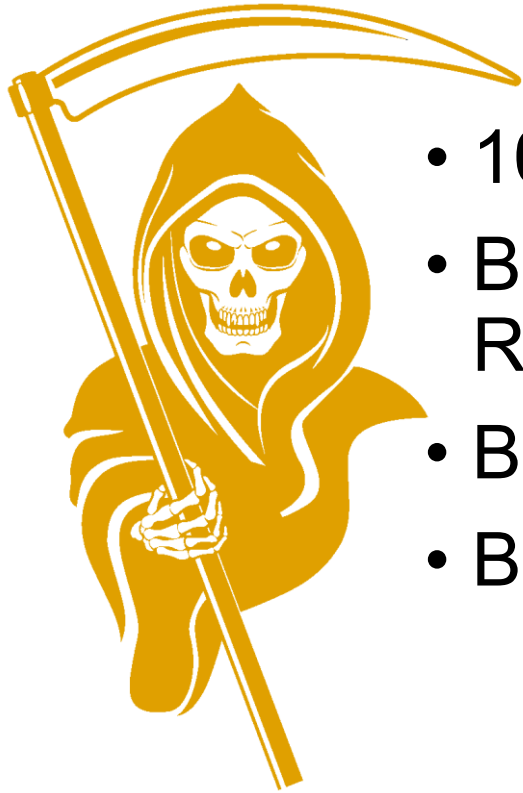


- Skills



# The Internet of Threats

# The Reaper, a « Mirai+ »?



- 10'000 to 20'000 devices botnet
- But additional 2 million hosts identified as potential Reaper nodes
- Build for «intra-China DDoS-for-hire market »
- Based on 9 known vulnerabilities
  - Ex. CVE-2017-8225 - Pre-Auth Info Leak (credentials) within the custom http server



# Privacy Intruders



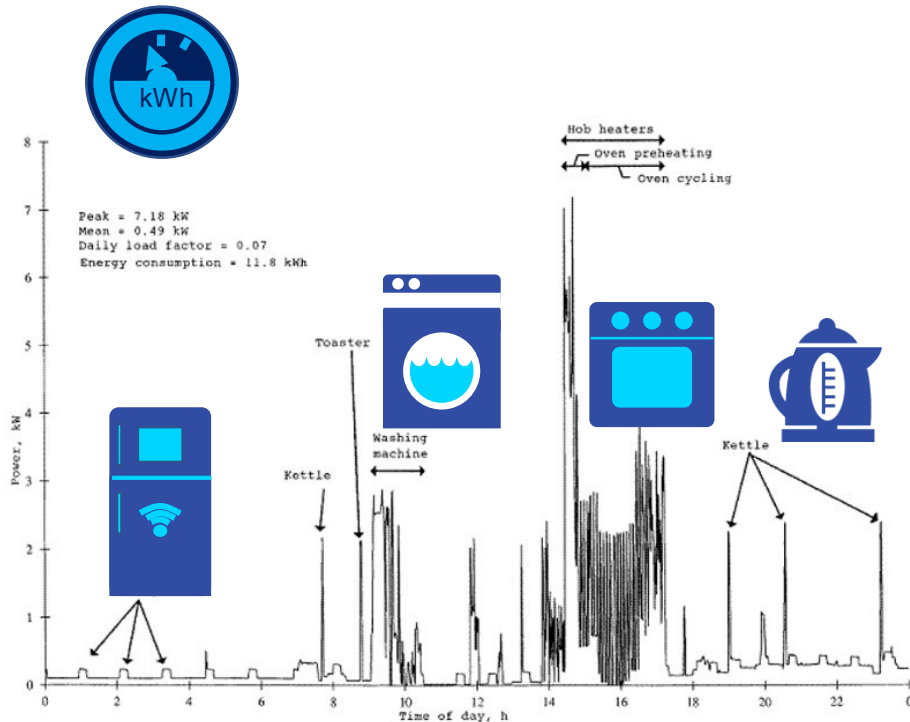
General  
Data Protection  
Regulation  
GDPR

2018  
May, 25th

138  
working days

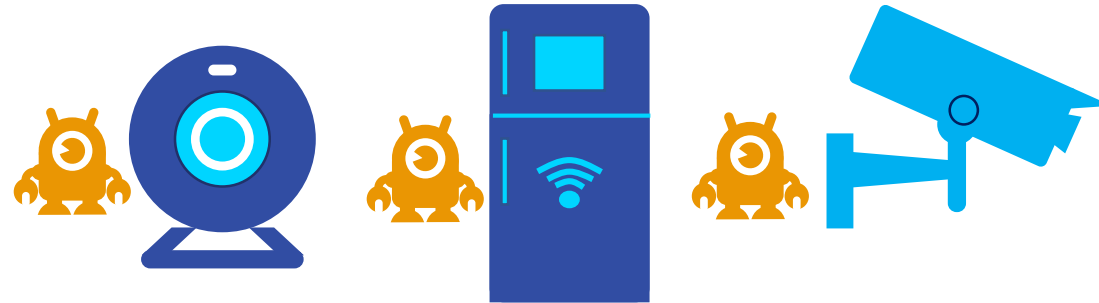
HEAVY NON-COMPLIANCE FEES

GLOBAL IMPACT !

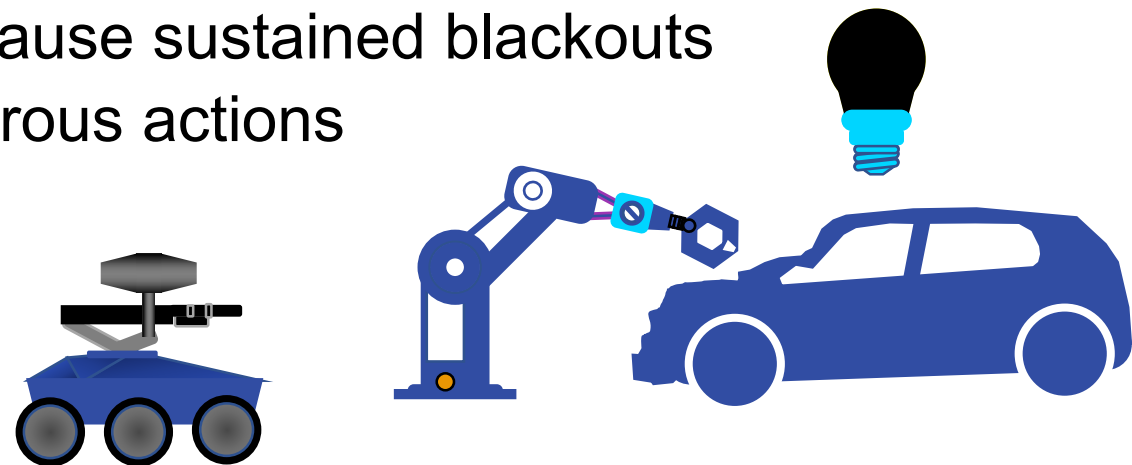


# Two risks

- Devices do something there are not supposed to do
  - Example: IoT devices used to perform a DDoS attack

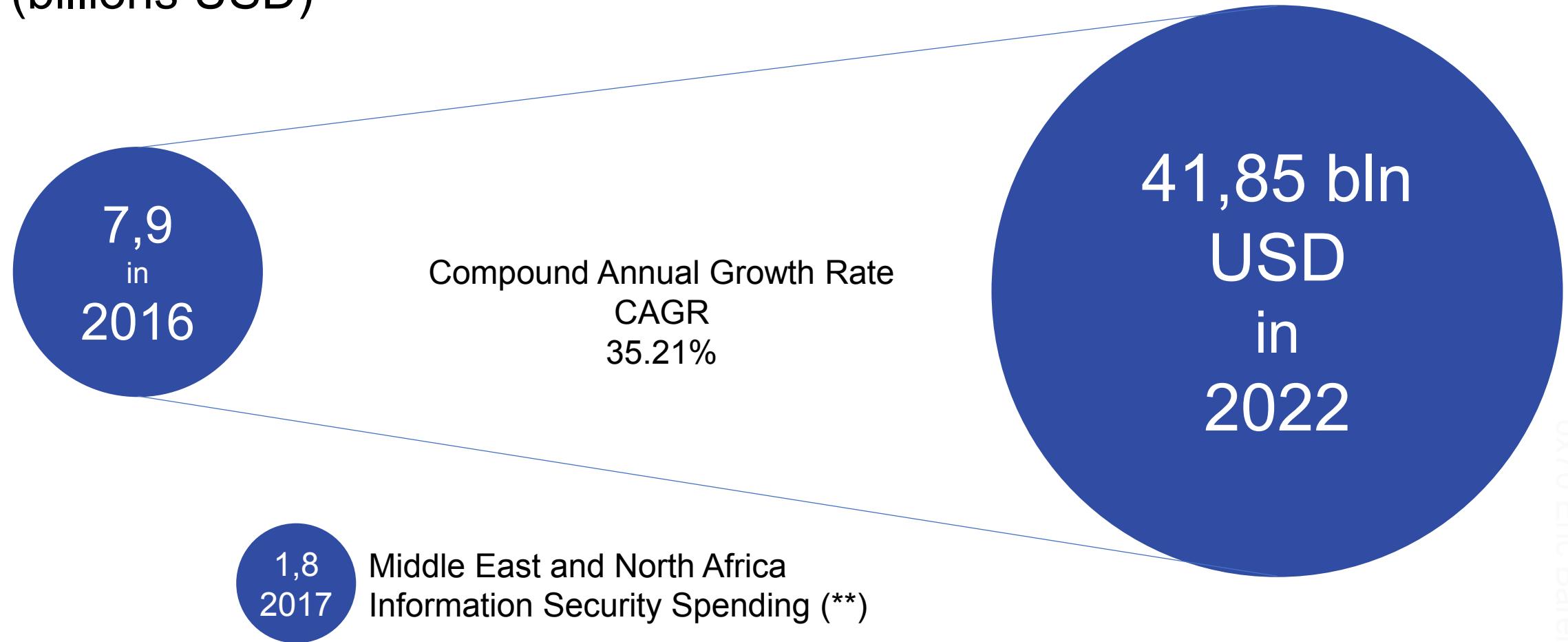


- Devices do exactly what they are intended to do but in a devious way
  - Hacking wireless lightbulbs to cause sustained blackouts
  - Robots doing unsolicited dangerous actions
  - Future autonomous weapons?



# The IoT Security market

(billions USD)



(\*) <http://www.digitaljournal.com/pr/3553821>

(\*\*) Gartner - <https://www.webwire.com/ViewPressRel.asp?ald=215252>

# IoT Domino effect

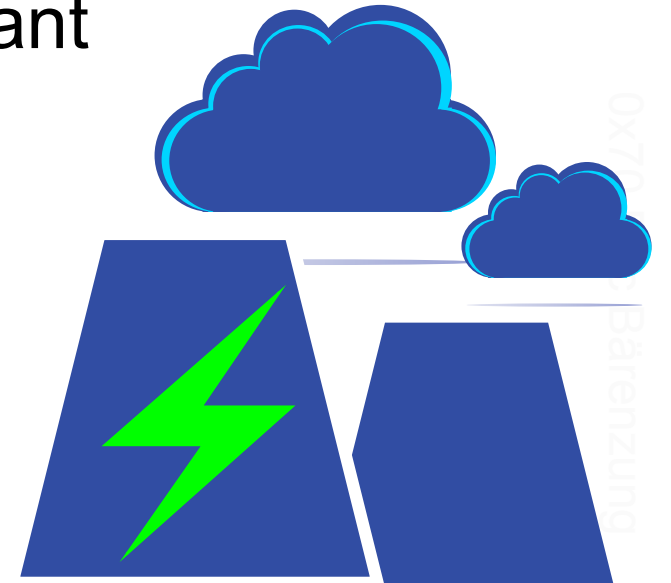




# Think big, start small...



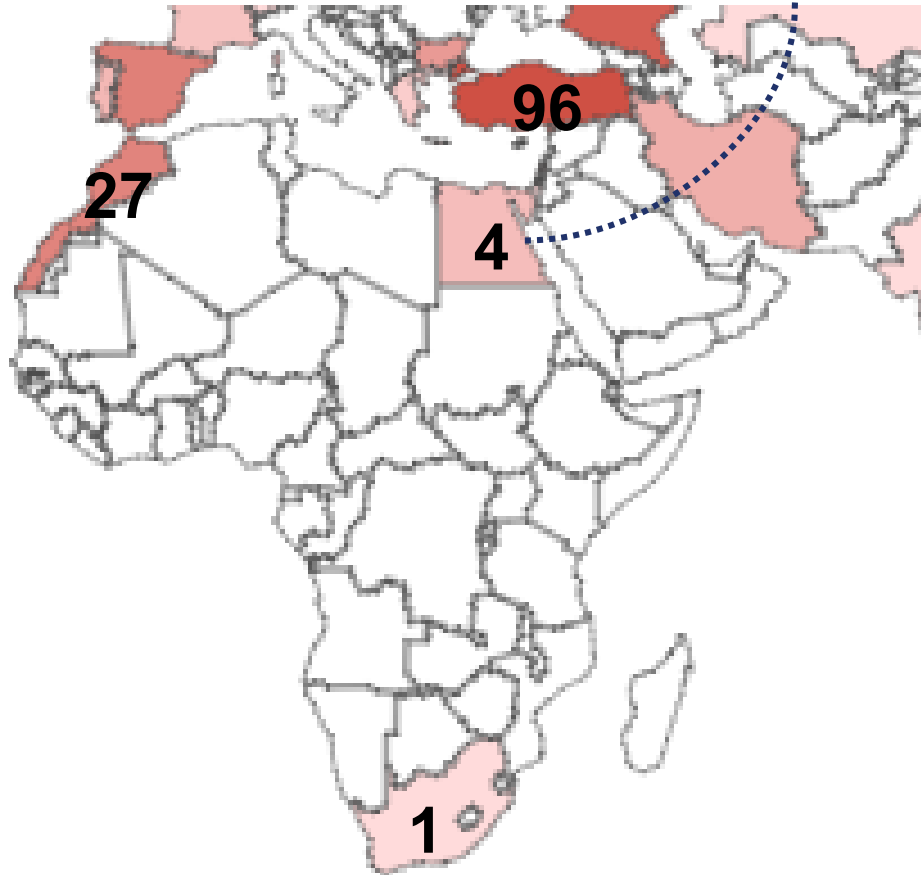
- Identify connected and vulnerable devices, using like 3-7W
- Take control of them
- Get 14-20M of these devices starting at the same time
- You potentially put down a 70/100 MW power plant
- As a note
  - Webcam <10W
  - Baby Monitor: 5-30W



# Taking control of SCADA systems

 SHODAN <https://www.shodan.io>

IEC 60870-5-104 -> port:2404 asdu address



 41.155.243.79

Industrial Control System

Country	Egypt
Organization	Mobinil 3G
ISP	MOBINIL
Last Update	2017-11-08T12:22:32.979758
ASN	AS37069



??

Good news...

# A growing awareness from the industry

## Mocana, Xilinx, Avnet, Infineon and Microsoft Join Forces to Secure Industrial Control and IoT Devices

Industry Leaders to Introduce an Integrated, High-Assurance Industrial Edge-to-Cloud System

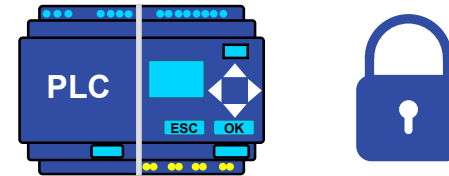
<https://globenewswire.com/news-release/2017/11/07/1176335/0/en/Mocana-Xilinx-Avnet-Infineon-and-Microsoft-Join-Forces-to-Secure-Industrial-Control-and-IoT-Devices.html>



## Tenable and Siemens form partnership to secure critical infrastructure

November 9, 2017 [Paul Dvorak](#) : [0 Comments](#)

<http://www.windpowerengineering.com/dw-sync/tenable-siemens-form-partnership-secure-critical-infrastructure/>



# Regional IoT / security players should cooperate too!



# A growing awareness from Regulators / Governments



## Two New Cyber Acts in the USA Address IoT Security

2017/11/08

<https://www.allaboutcircuits.com/news/two-new-cyber-acts-in-the-usa-address-iot-security/>



## Dutch parliament supports 'hack tests' for IoT devices

Monday 16 October 2017 | 15:28 CET | News

The Dutch parliament has adopted a motion supporting government 'hack tests' to ensure the security of connected devices. The motion was presented by Socialist Party member Maarten Hijink, who called on the government to work with businesses and industry to make IoT devices  
2017/10/16

<https://www.telecompaper.com/news/dutch-parliament-supports-hack-tests-for-iot-devices--1216144>

# What about your country?

# A growing awareness from Customers?

- Who ask security questions when purchasing a webcam or other consumer connected device?

## Raise awareness!



# Think security from day 1!

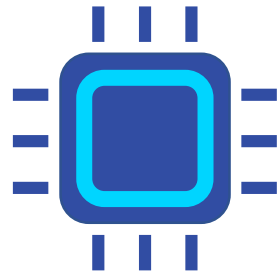
Security by design



# Embedded security



## CHIPSET



Hardware  
Root-Of-Trust

## SOFTWARE



Secure Debug

Serial Bus

Secure Flashing

RAM Scrambling

Secure Boot

Secure Dowload

Secure Execution

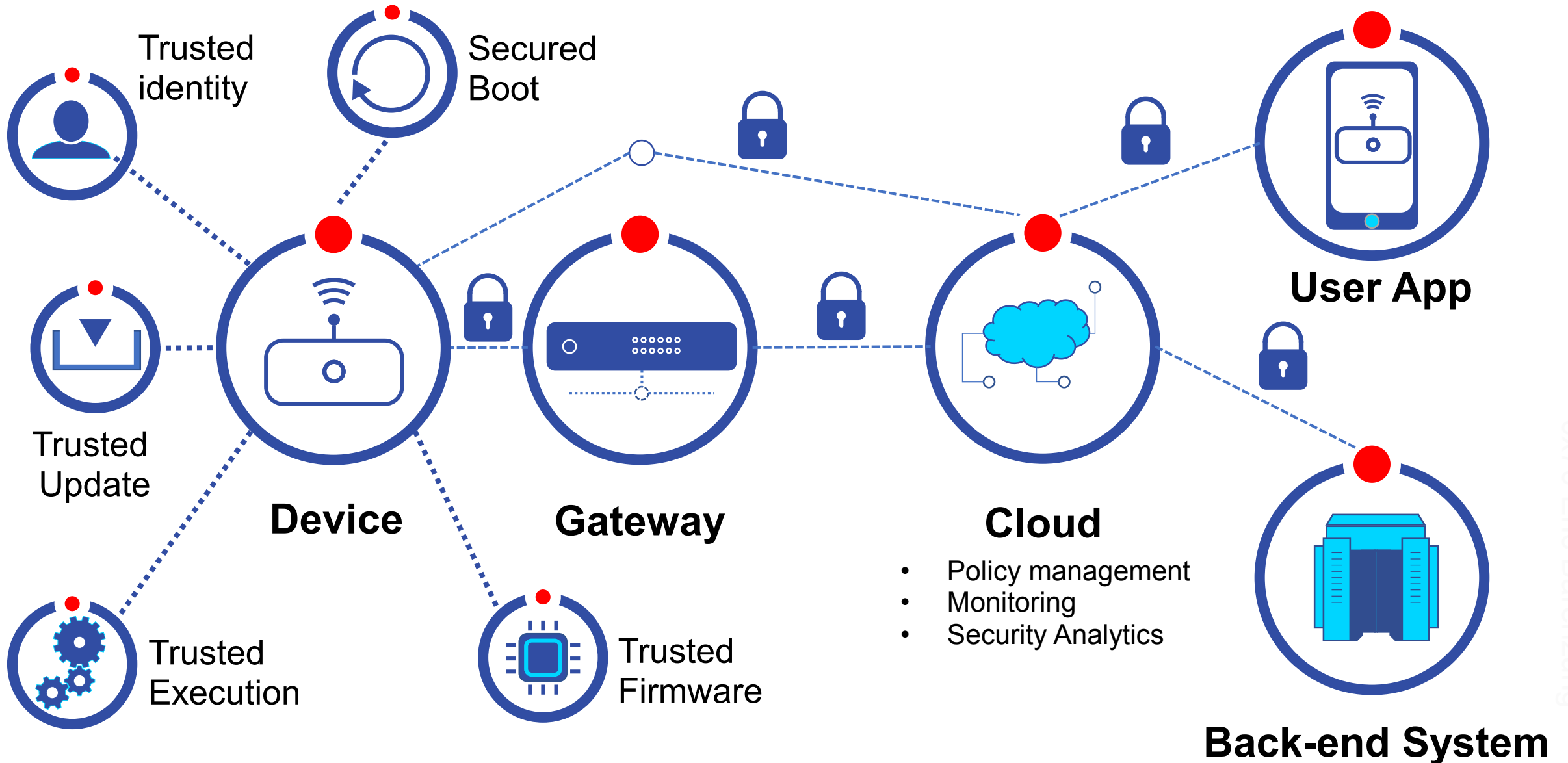
JTAG

SPI

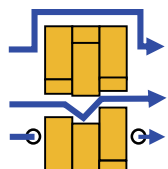
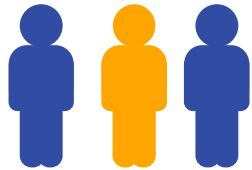
I2C

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

# Ensuring End-To-End Security



# Security evaluation techniques



Open Source Intelligence

Documentation Review

Face-to-face Interviews

Random Sampling

Data Flow Analysis

Architectural Risk Analysis

Threat & Attack scenarios

Log Analysis

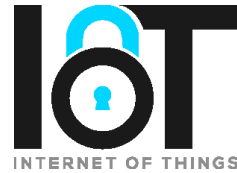
Vulnerabilities Analysis

Penetration testing

Forensic Investigation



OWASP



Testing Guidance



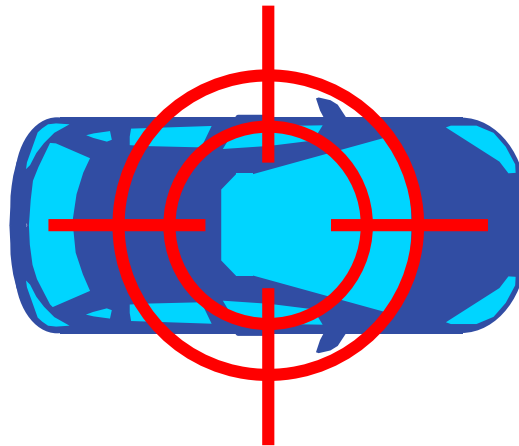
11: Insecure Web Interface

12: Insufficient  
Authentication/Authorization

13: Insecure Network Services

14: Lack of Transport  
Encryption

15: Privacy Concerns



16: Insecure Cloud Interface

17: Insecure Mobile Interface

18: Insufficient Security  
Configurability

19: Insecure  
Software/Firmware

110: Poor Physical Security

# Start with basics

- Password policies

- No default password, nothing hardcoded, etc.

- Reminder Mirai: quick dictionary attack

- `root admin admin admin root 888888 root default root 123456`
- `root 54321 support support Root (none) admin password`

- ΕΥΚΛΗΒΕΤΗ COMMUNICATION

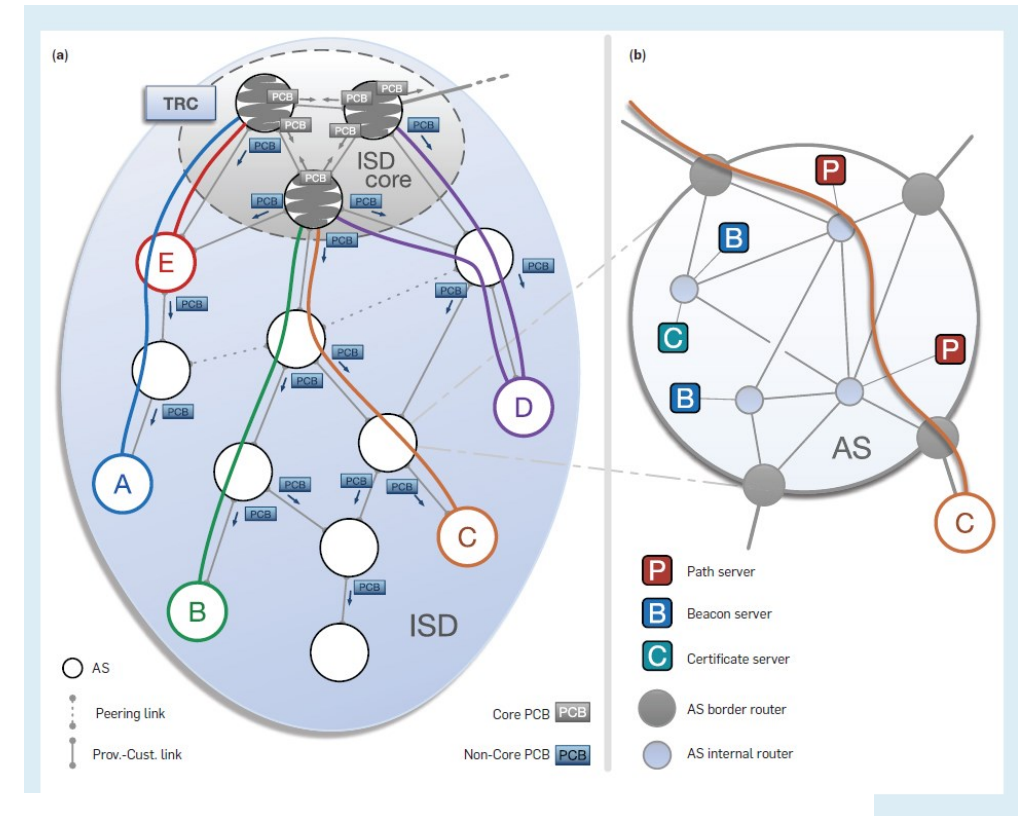
- Secured authentication and trusted communication

- Using for ex. Public Key Infrastructure (PKI)



# Innovate!

- For ex. new protocols
- **SCION Protocol** *ETH zürich*
  - **SCALABILITY, CONTROL, AND ISOLATION ON NEXT-GENERATION NETWORKS**
- <https://www.scion-architecture.net/>



ETH zürich

Google

KDDI

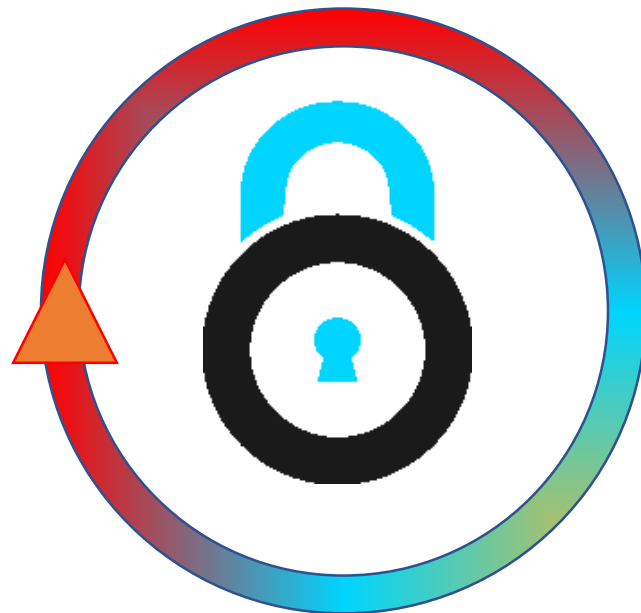


swisscom

SWITCH

# And don't forget!

Security  
is a  
continuous process




# 4 take aways on IoT

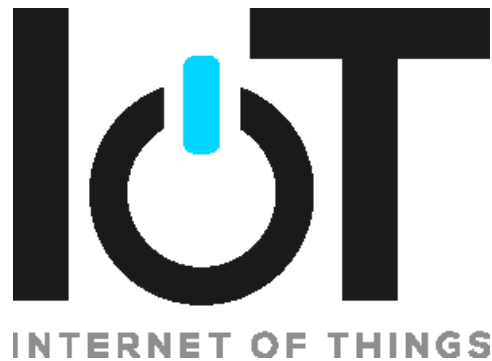
 environment is vulnerable

Security is not e**X**pensive if « by design »

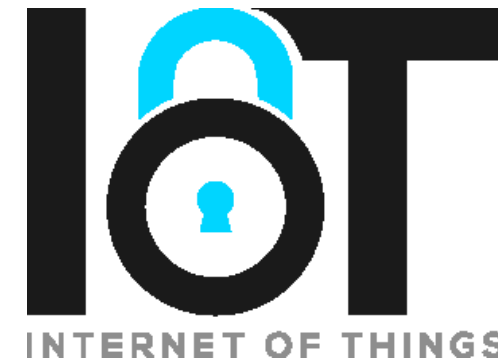
**2017** : 8.4 Billion Connected « Things »

 has to be secured to grow

Asante – شكرا - Thanks - Merci



As an enabler....



... if secured

Eric Bärenzung

ebg@0x70.eu

Twitter: @EricBarenzung

LinkedIn: <https://www.linkedin.com/in/ericbaerenzung/>

