IoT Security

MO809 - Tópicos em Computação Distribuída

Luísa Madeira Cardoso

Topics

Today's scenario

- Why IoT Security is critical?
- Attacks examples

Securing the Internet of Things

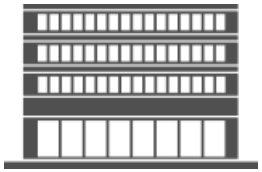
- IoT Attack Surface areas
- Guides

Why IoT Security is Critical?

Connecting **physical** things – can cause direct injury

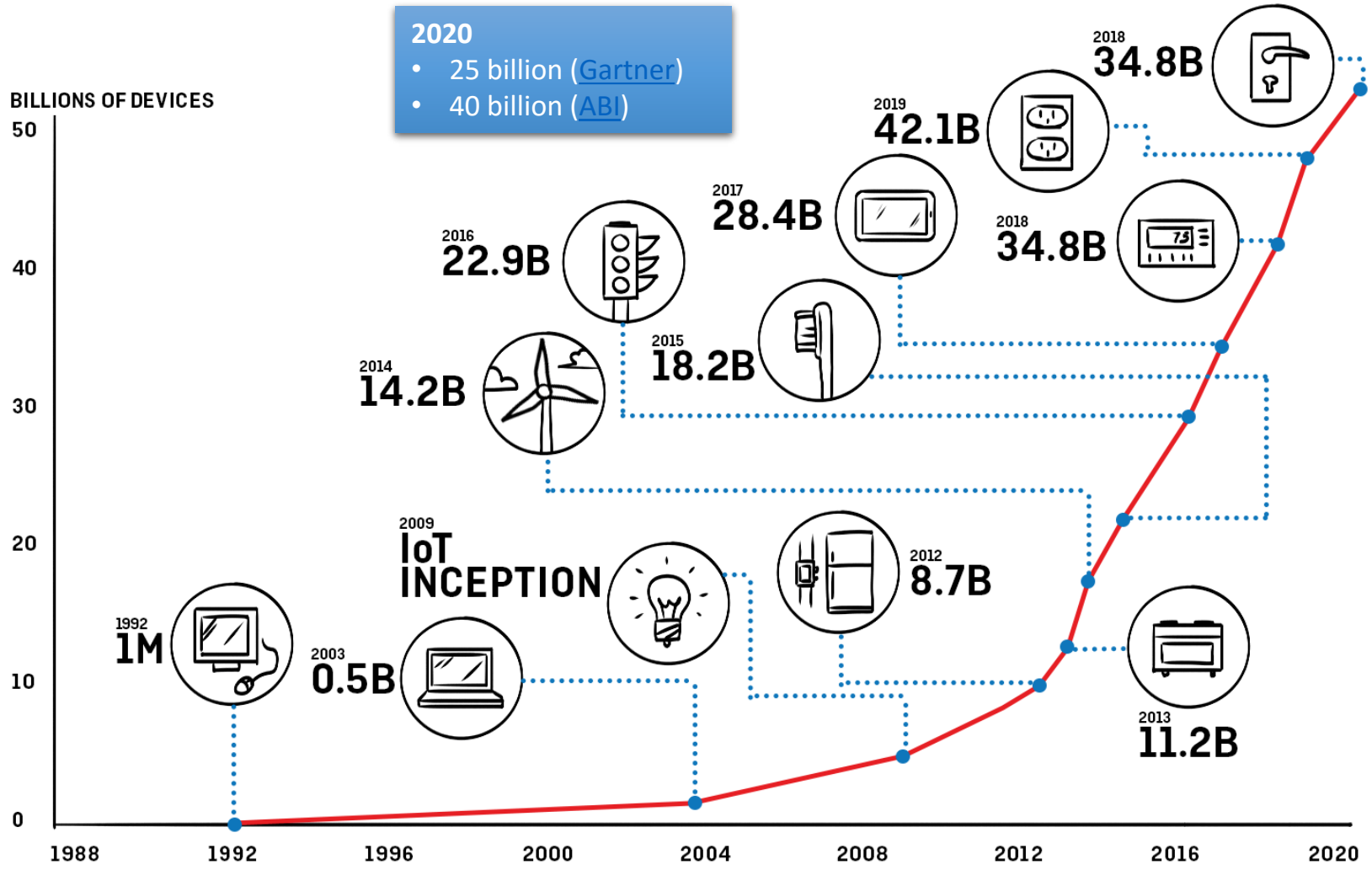
Privacy Issues

Automated houses



Companies

Governments



Source: National Cable & Telecommunications Association, Behind The Numbers: Growth In The Internet Of Things, 2015

Science fiction?

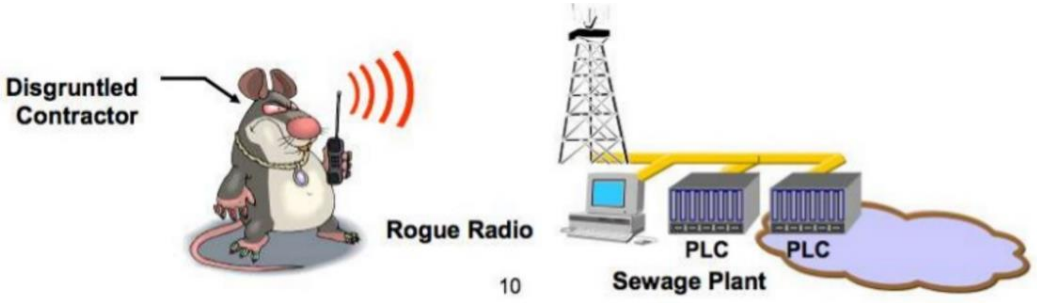
- A man had a NFC chip surgically implanted in his hand, which allowed him to load a malicious Web page into and subsequently control any Android phone he held. [Hackmiami 2015]

- Changing the target of a Linux powered riffle [Black Hat 2015]

- Hackers remotely kill a Jeep on the highway [Wired]

Science fiction?

- In April 2000, a man took revenge of his previous employers: he attacked a Water treatment industry. Using a copy of the control system and a radio transmitter he caused the dump of 250 million tonnes of putrid sludge in the area's rivers and parks. In the factory communications sent by radio links to wastewater pumping stations were being lost, pumps were not working properly, and alarms put in place to alert staff to faults were not going of. [RISI]



Too easy…

"Yes, we get it. Cars, boats, buses, and those singing fish plaques are all hackable and have no security. Most conferences these days have a whole track called '**Junk I found around my house and how I am going to scare you by hacking it.**' That stuff is always going to be hackable whetherornotyouarethecalvalry.org." [Dave Aitel's rant]


Philips Hue personal wireless lighting

Belkin WeMo baby monitor


Belkin WeMo switch


Belkin NetCam

https://www.iamthecavalry.org/domains/automotive/ - Reports in the media about car attacks

Shodan | Developers | Book | View All... | Show API Key

SHODAN | port:554 has_screenshot:true | Explore | Downloads | Reports | Enterprise Access | Contact Us | My Account | Upgrade

Exploits | Maps | Images | Like 77 | Download Results | Create Report

TOP COUNTRIES

Russian Federation	119
Germany	106
Poland	94
United States	91
Brazil	60

TOP ORGANIZATIONS

Deutsche Telekom AG	58
Rostelecom	35
Vodafone DSL	10
Orange Polska	9
Telefonica Germany	6

TOP OPERATING SYSTEMS

Linux 2.6.x	42
Linux 3.x	2

Total results: 892

208.100.175.166

dhcp-208-100-175-166.surelinetelecom.com

Sureline Telecom

Added on 2016-09-07 09:10:09 GMT

United States, Culver

Details

```
RTSP/1.0 200 OK
CSeq: 1
Server: UBNT Streaming Server v1.2
Public: DESCRIBE, SETUP, TEARDOWN, PLAY
```

84.124.163.37

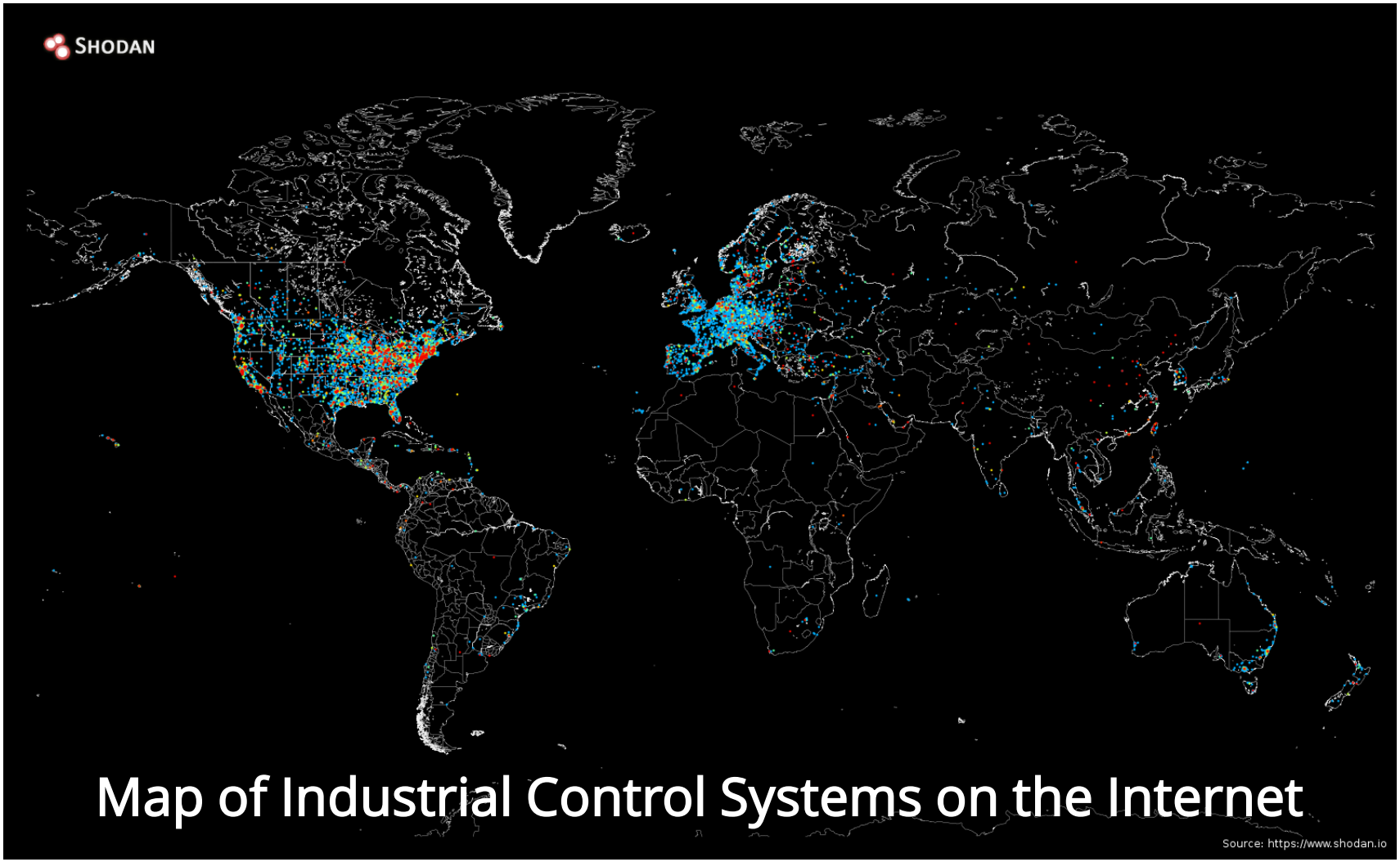
84.124.163.37.dyn.user.ono.com

Vodafone Ono

Added on 2016-09-07 08:30:52 GMT

Spain

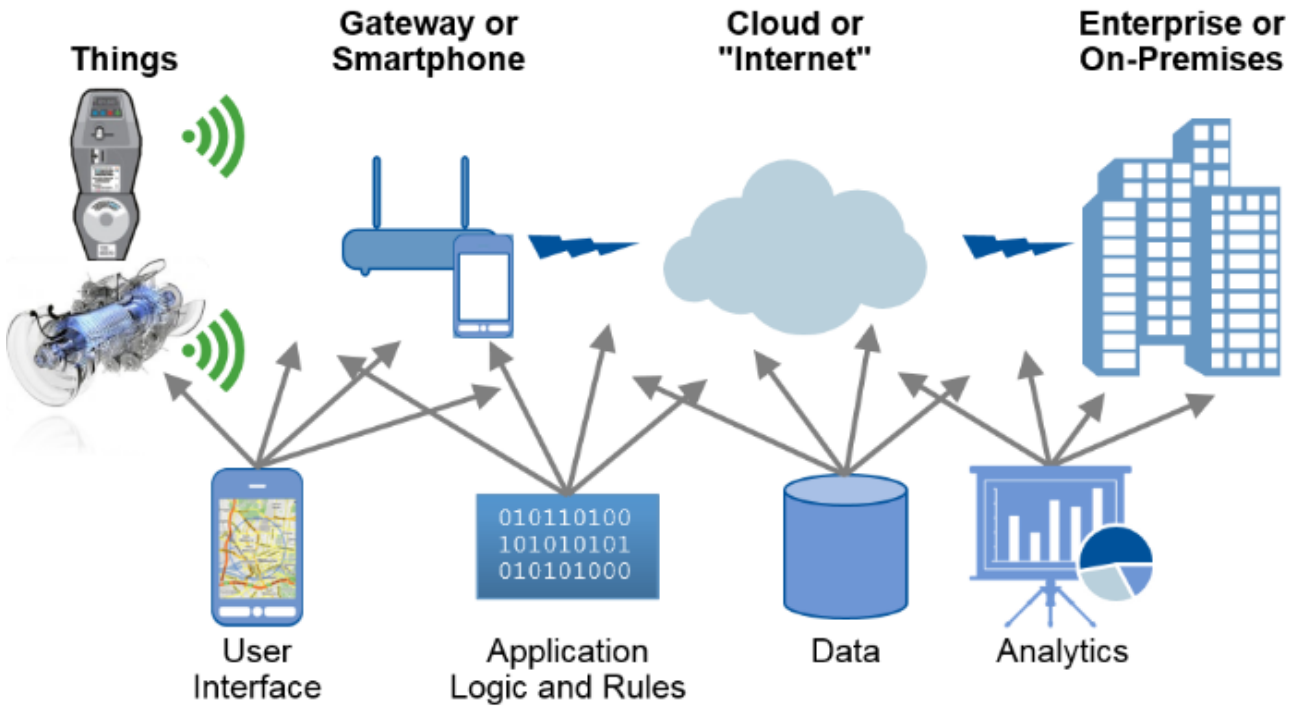
Details


SHODAN
Map of Industrial Control Systems on the Internet
Source: https://www.shodan.io

Securing the Internet of Things

Security Goals

IoT Security != Device Security



GUI, application logic, data and analytics can be placed anywhere

Layers

- Perception
- Network
- Middle-ware
- Application

How to add security to the design

- OWASP Internet of Things Project

  Designed to help manufacturers, developers, and consumers better understand the security issues associated with the Internet of Things, and to enable users in any context to make better security decisions when building, deploying, or assessing IoT technologies

- Builditsecure.ly

- IoT Security Foundation

IoT Attack Surface Areas

- Ecosystem (general)
- Ecosystem Access Control
- Device Memory
- Device Physical Interfaces
- Device Web Interface
- Device Firmware
- Device Network Services
- Administrative Interface
- Local Data Storage
- Cloud Web Interface
- Third-party Backend APIs
- Update Mechanism
- Mobile Application
- Vendor Backend APIs
- Ecosystem Communication
- Network Traffic
- Authentication/Authorization
- Privacy
- Hardware (Sensors)

Device Layer

- Unauthorized Access
- Tag cloning

- Local Data Storage
  - Unencrypted data
  - Data encrypted with discovered keys
  - Lack of data integrity checks

- Device Memory
  - Cleartext usernames/passwords
  - Third-party credentials
  - Encryption keys

- Device Physical Interface
  - Firmware extraction
  - User CLI / Admin CLI
  - Privilege escalation
  - Reset to insecure state
  - Removal of storage media
  - Tamper resistance
  - Debug port
  - Device ID/Serial number exposure

Device Layer

- Device Web Interface
  - SQL injection
  - Cross-site scripting
  - Cross-site Request Forgery
  - Username enumeration
  - Weak passwords
  - Account lockout
  - Known default credentials
- Device Firmware
  - Hardcoded credentials
  - Firmware version display and/or last update date
  - Backdoor accounts
  - Vulnerable services (web, ssh, tftp, etc.)
  - Security related function API exposure
  - Firmware downgrade
- Device Network Services
  - User CLI / Administrative CLI
  - Injection
  - Denial of Service
  - Unencrypted Services
  - Poorly implemented encryption
  - Test/Development Services
  - Buffer Overflow
  - UPnP
  - Vulnerable UDP Services
  - DoS
  - Device Firmware OTA update block
  - Replay attack
  - Lack of payload verification
  - Lack of message integrity check

Device Layer

Can the software in the device be upgraded?

You can't **secure** it if you can't upgrade it!

If you can upgrade the firmware…

You must secure this channel.
If an attacker reflashes the device…

Low cost sensors, batteries, weak processing power

Lightweight cryptography
Sleep deprivation attacks

Network layer

- Jamming
- Eavesdropping
- Sniffing

Attacks

- Sybil Attack
  - Single node pretends multiples identities. Problems can arise in a reputation system: the attacking node has a disproportionally large influence
- Sinkhole Attack
- Sleep depravation attack
- DoS

Network layer

- Jamming
- Eavesdropping
- Sniffing

Attacks

- Sybil

  Single node pretends multiples identities. Problems can arise in a reputation system: the attacking node has a disproportionally large influence

- Sinkhole

  Attacker makes the compromised node look attractive to the nearby nodes

- Sleep depravation

  Keeps the node awake, resulting in more battery consumption

- DoS

  Network is flooded with useless traffic or requisitions

Application Layer

- Administrative Interface
- Mobile Application
- Web Application

Usual vulnerabilities

- SQL injection
- Cross-site scripting
- Weak passwords
- Account lockout
- Known default credentials
- Security/encryption
- DoS
- **…**

References

- Twenty security considerationsfor cloud-supported Internet of Things
- A Critical Analysis on the Security Concerns of Internet of Things
- A Systemic Approach for IoT Security

- OWASP
- BuildItSecure.ly
- Science Fiction and Ancient Warfare Can Teach Lessons on Security for the IoT
- Securing the Internet of Things