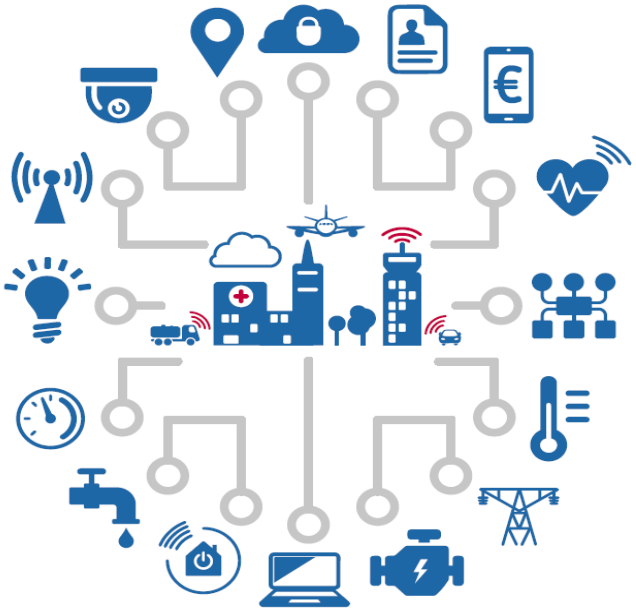
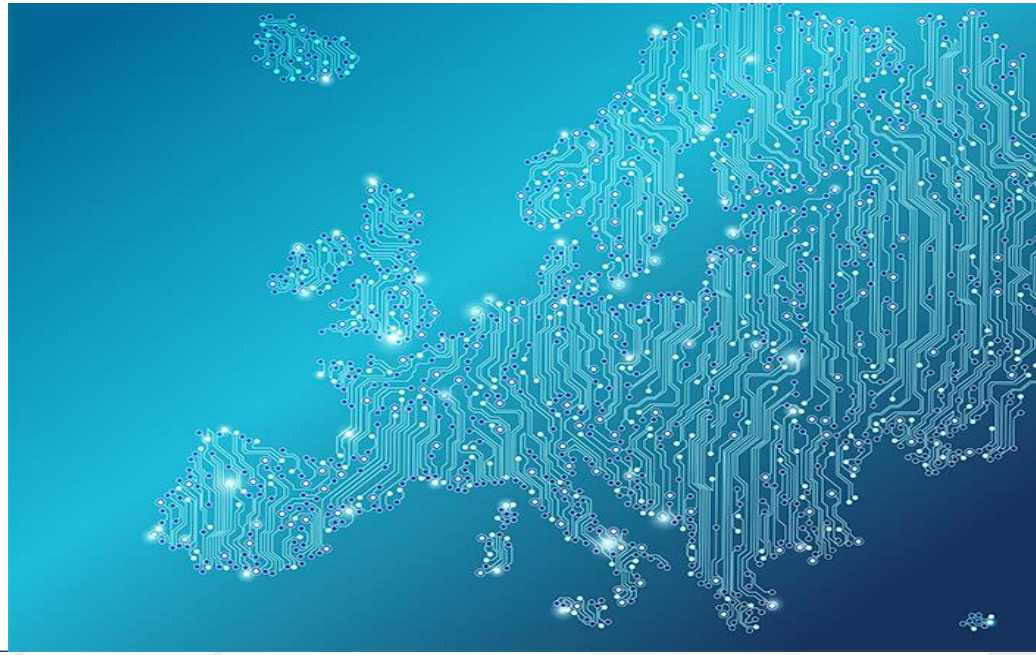


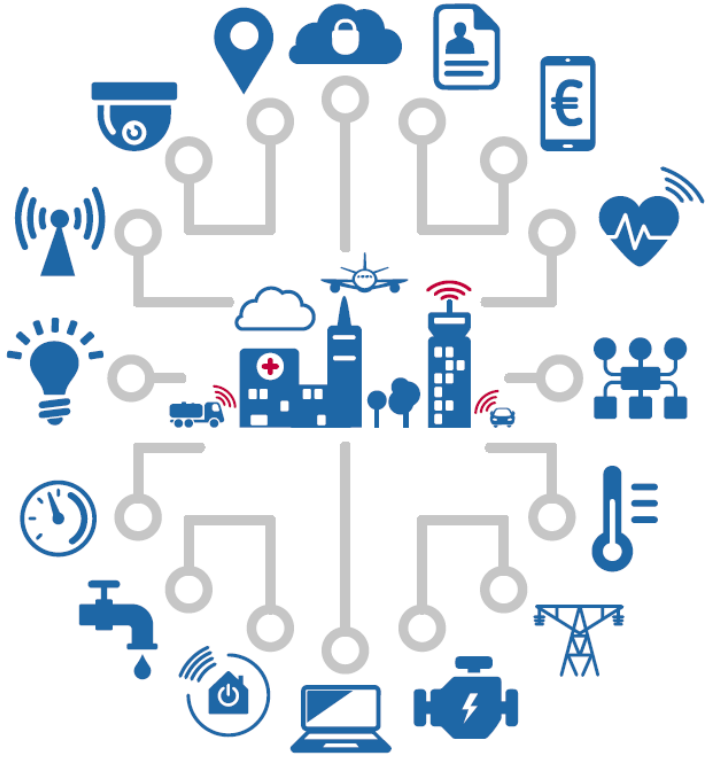


Introduction to IoT security

Christina Skouloudi, Apostolos Malatras | ENISA IoT Security team

ENISA-FORTH NIS Summer School| 26.09.2018

Structure of Day 1



Day 1

- Round table
- Intro & ENISA's efforts on IoT
- IoT 101
  - Intro and definition
  - Ecosystem (including assets and components)
  - IoT platforms
  - IoT protocols
- IoT Security
  - Challenges
  - Threats
  - Attack scenarios
- Case-study: BLE Security
- LAB

Positioning ENISA activities

CAPACITY

- ✓ Hands on activities

POLICY

- ✓ Support MS & COM in Policy implementation
- ✓ Harmonisation across EU

COMMUNITY

Mobilizing EU communities

EXPERTISE

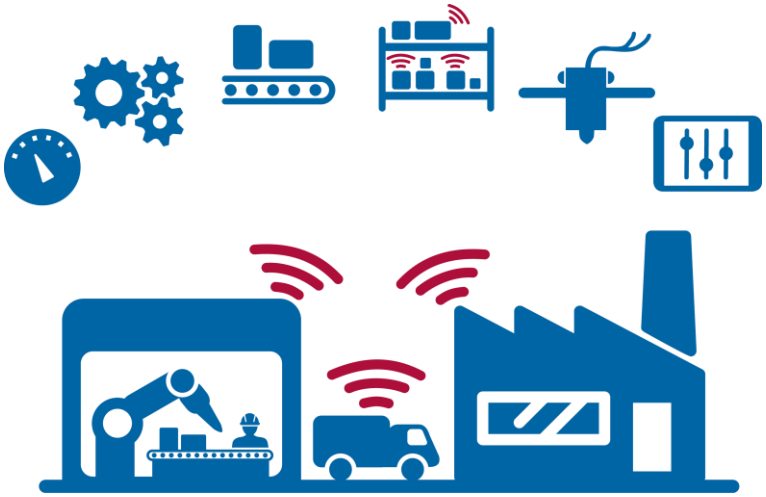
- ✓ Recommendations
- ✓ Independent Advice

ENISA's efforts on IoT Security

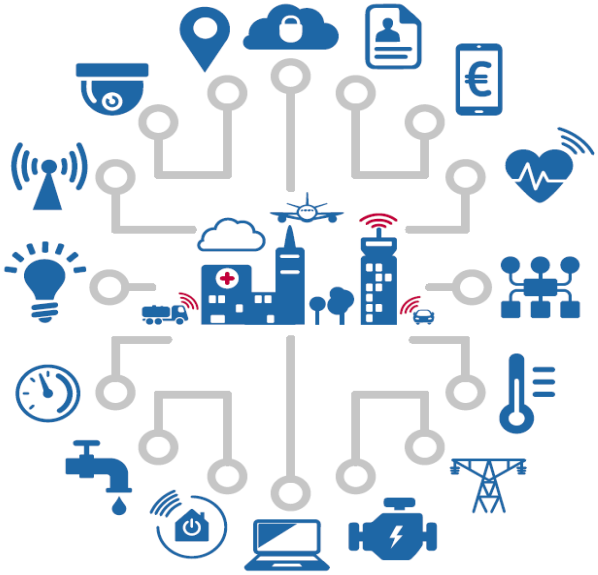
- ✓ Horizontal and vertical Studies
- ✓ Expert Groups
- ✓ Validation Workshops
- ✓ Conferences
- ✓ Summer School

ENISA's efforts on IoT Security

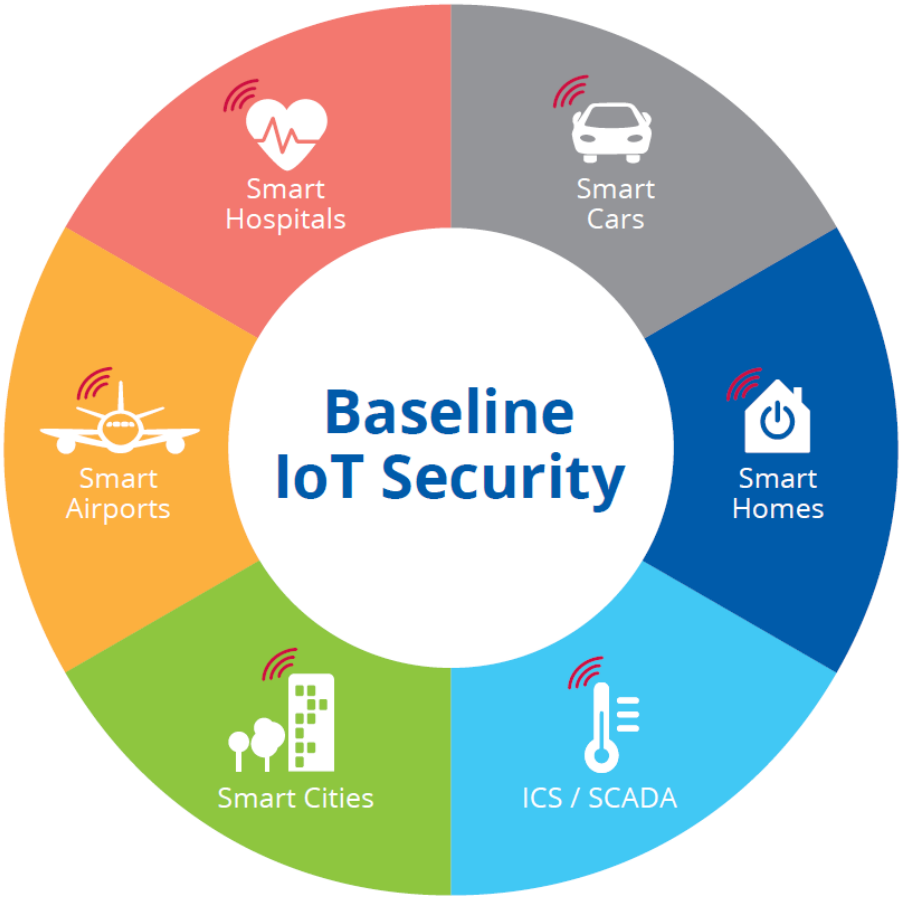
Industry 4.0



Baseline IoT Security



IoT security in sectors



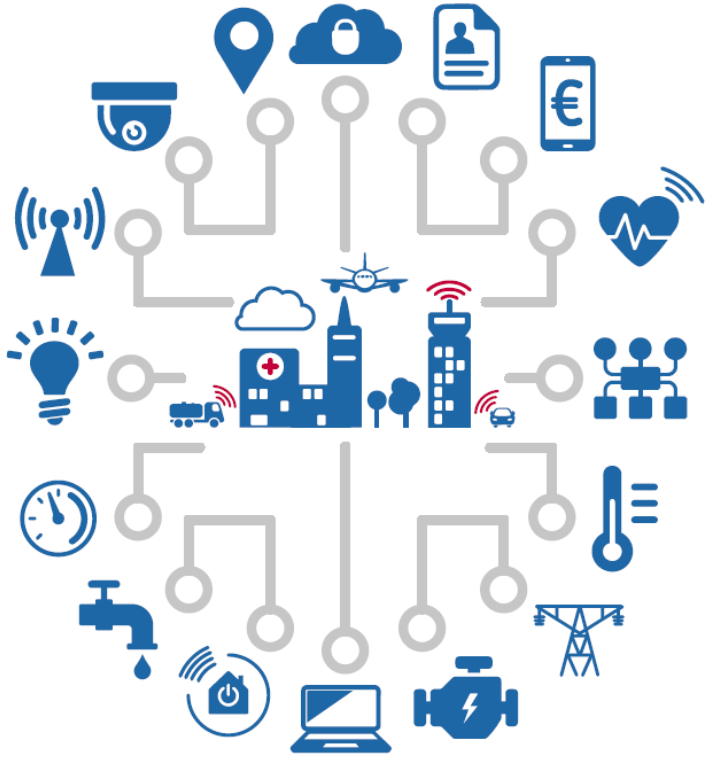
- Understand threats & assets
- Consider context of use
- Highlight security good practices in specific sectors
- Provide recommendations to enhance cyber security
- Expert groups

ENISA and IoT cybersecurity

- Baseline Security Recommendations for IoT
  - Map existing IoT security initiatives
  - Address the problem holistically engaging with wider community
  - Utilize sectorial knowhow
  - Provide horizontal cybersecurity recommendations and security measures
  - One stop shop for IoT cybersecurity in Europe

https://enisa.europa.eu/iot

IoT 101

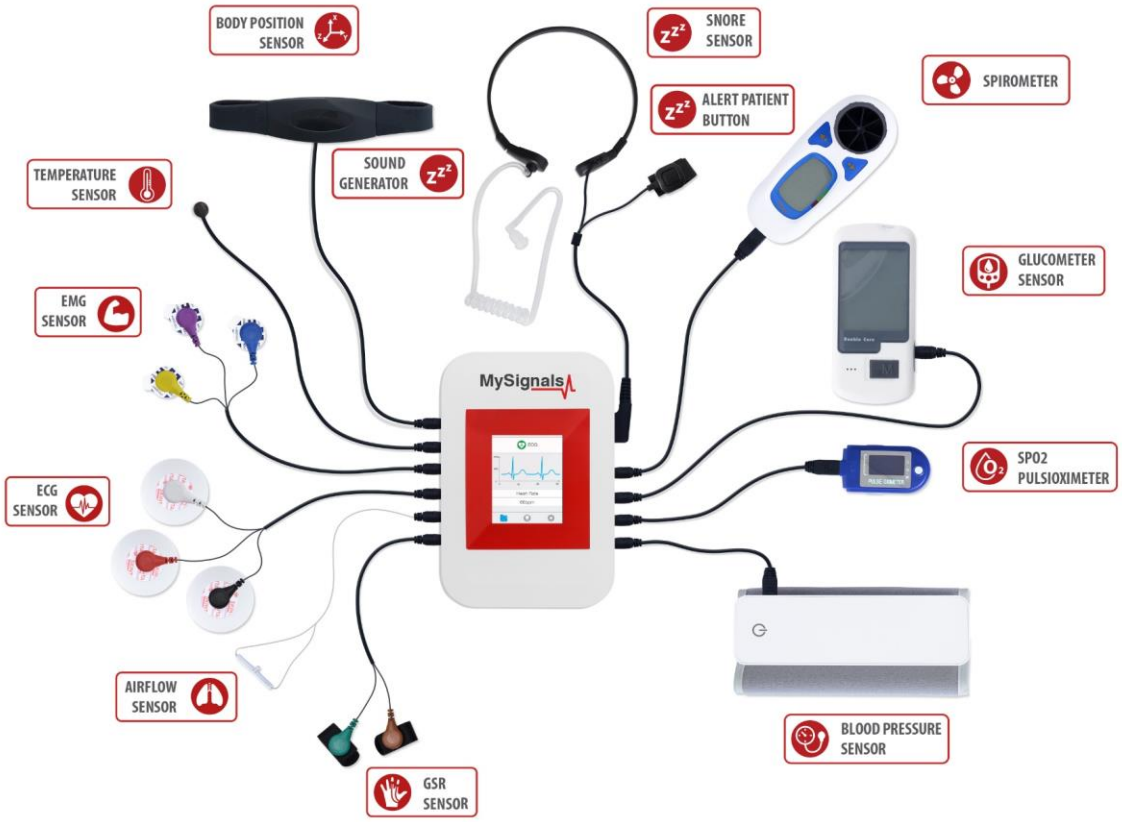


What is IoT to you?

IoT

“ENISA defines IoT as a cyber-physical ecosystem of interconnected sensors and actuators which enable intelligent decision making.”

Sensor


BODY POSITION SENSOR
SNORE SENSOR
SPIROMETER
ALERT PATIENT BUTTON
TEMPERATURE SENSOR
SOUND GENERATOR
GLUCOMETER SENSOR
EMG SENSOR
MySignals
SPO2 PULSIOXIMETER
ECG SENSOR
AIRFLOW SENSOR
BLOOD PRESSURE SENSOR
GSR SENSOR

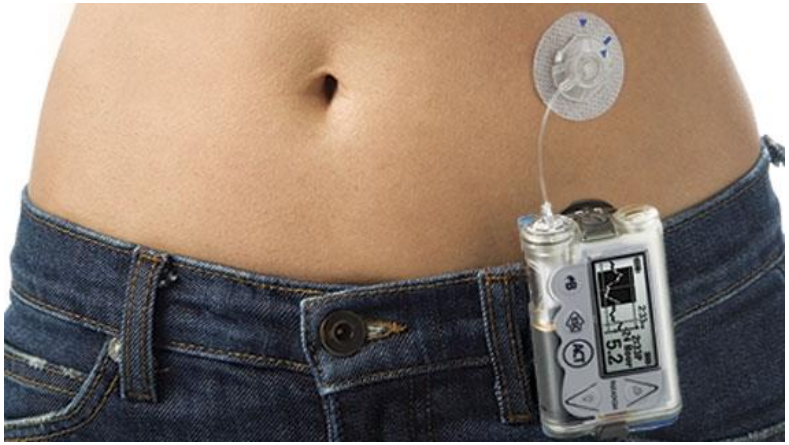
Sensor

element that allows to monitor the environment and the context on which IoT systems operate

sensors can measure defined physical, chemical or biological indicators, and on the digital level, they collect information about the network and applications

- accelerometers
- temperature sensors
- pressure sensors
- light sensors
- acoustic sensors

Actuator



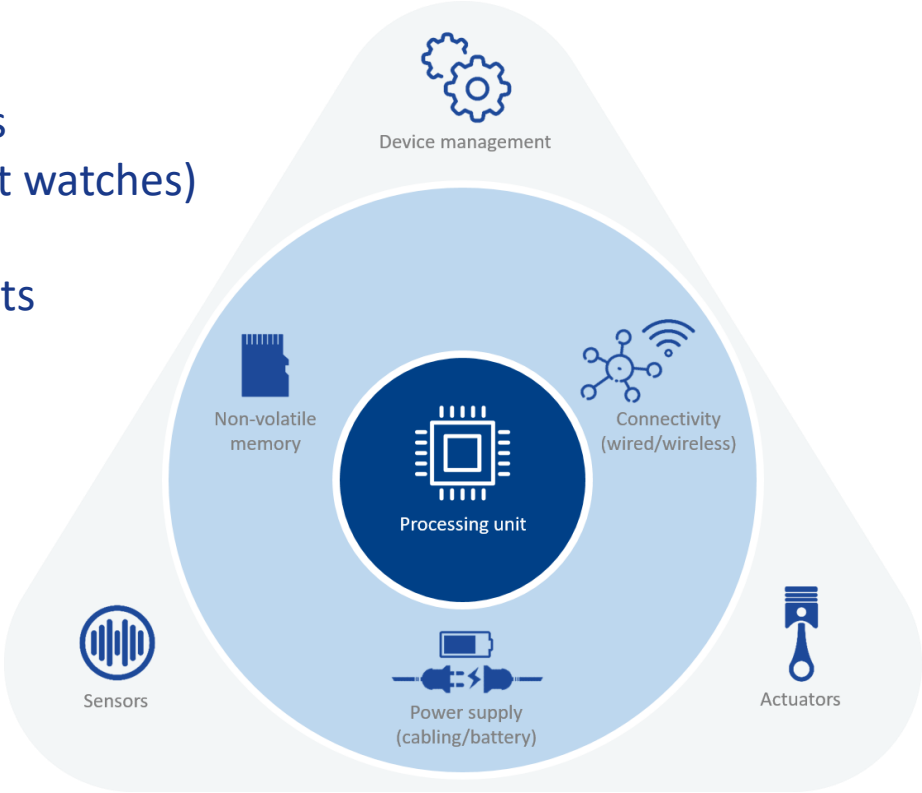
Actuator

the entity responsible for moving or controlling a system or mechanism.

an actuator operates in the reverse direction of a sensor; it takes an electrical input and turns it into physical action.

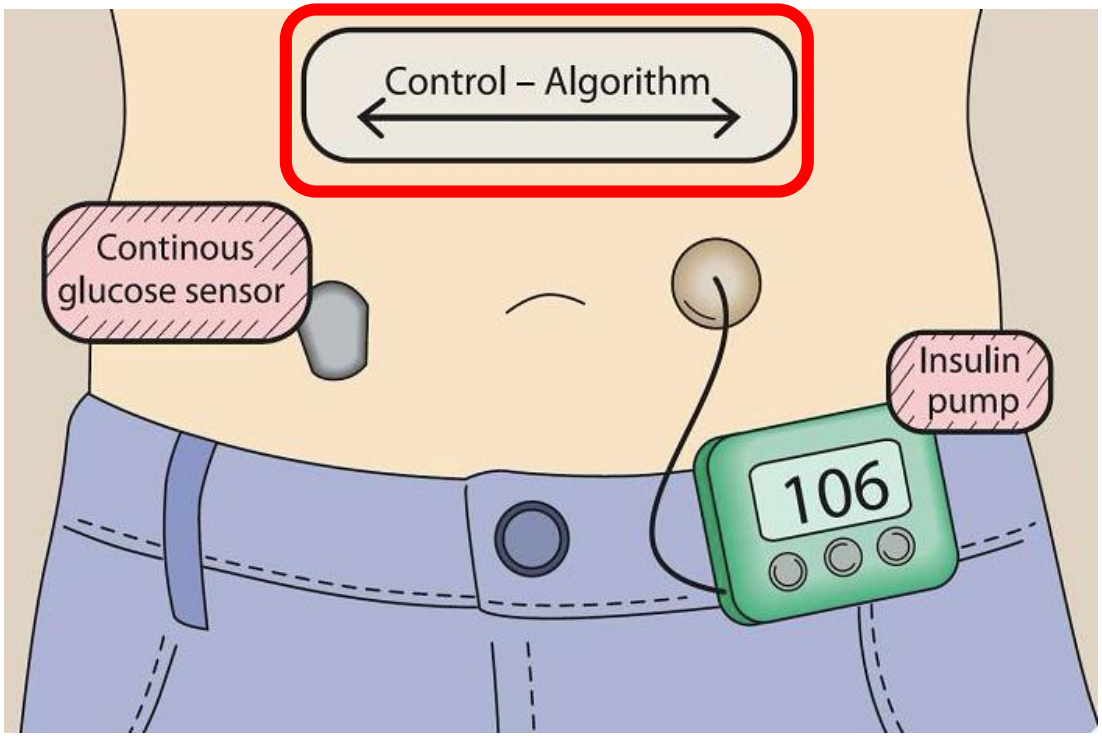
Sensor + Actuator + ..

- medical implants
- wearables (smart watches)
- connected lights
- smart thermostats

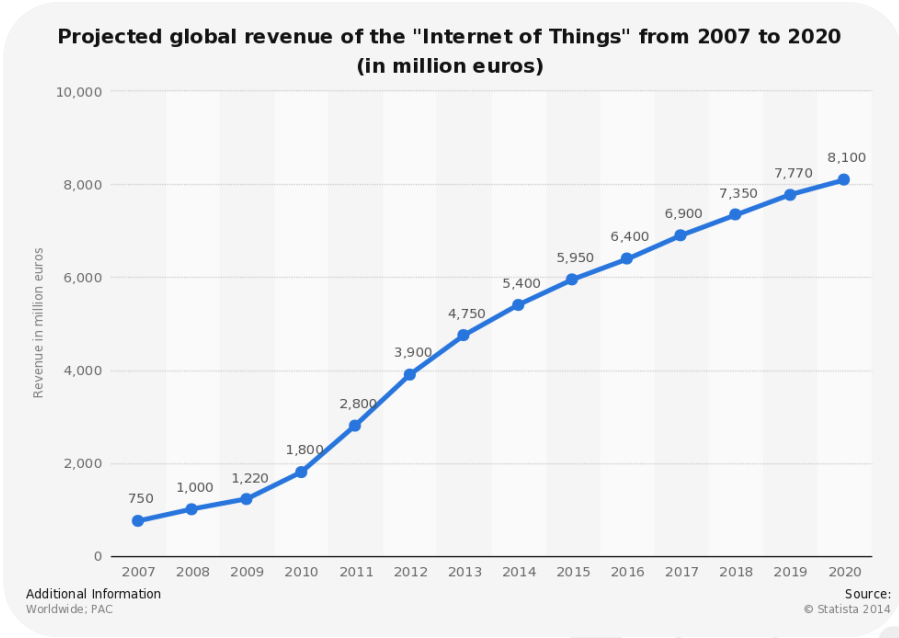


Structure of an IoT embedded system

Intelligent Decision Making



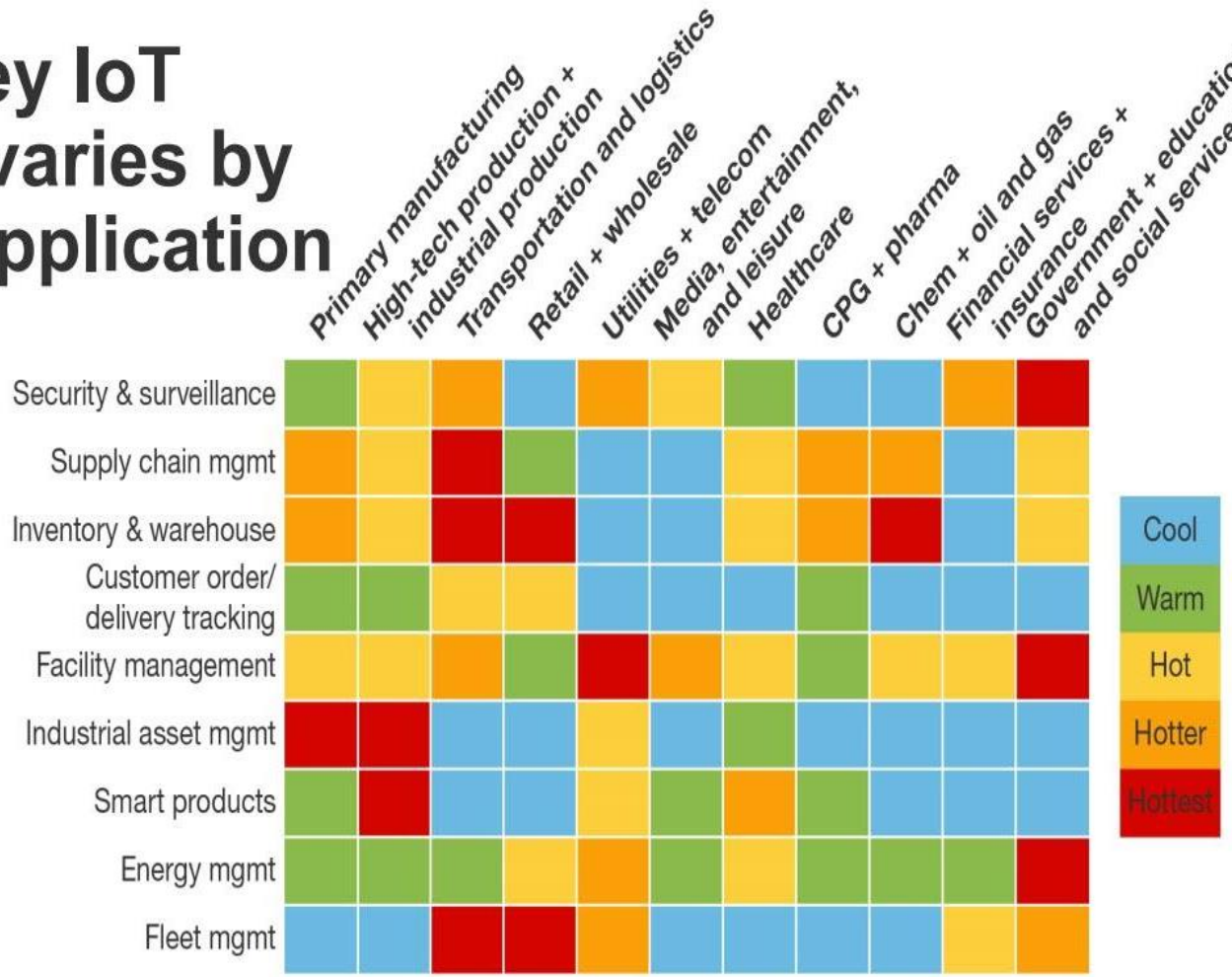
Everything becomes connected



Business side

- "Everything connected" hype
  - Competitors do IoT, hence we must do IoT
  - Competitors don't do IoT, let's be the first one!
- Financial gains
- New business models and opportunities
- Advanced data collection and processing

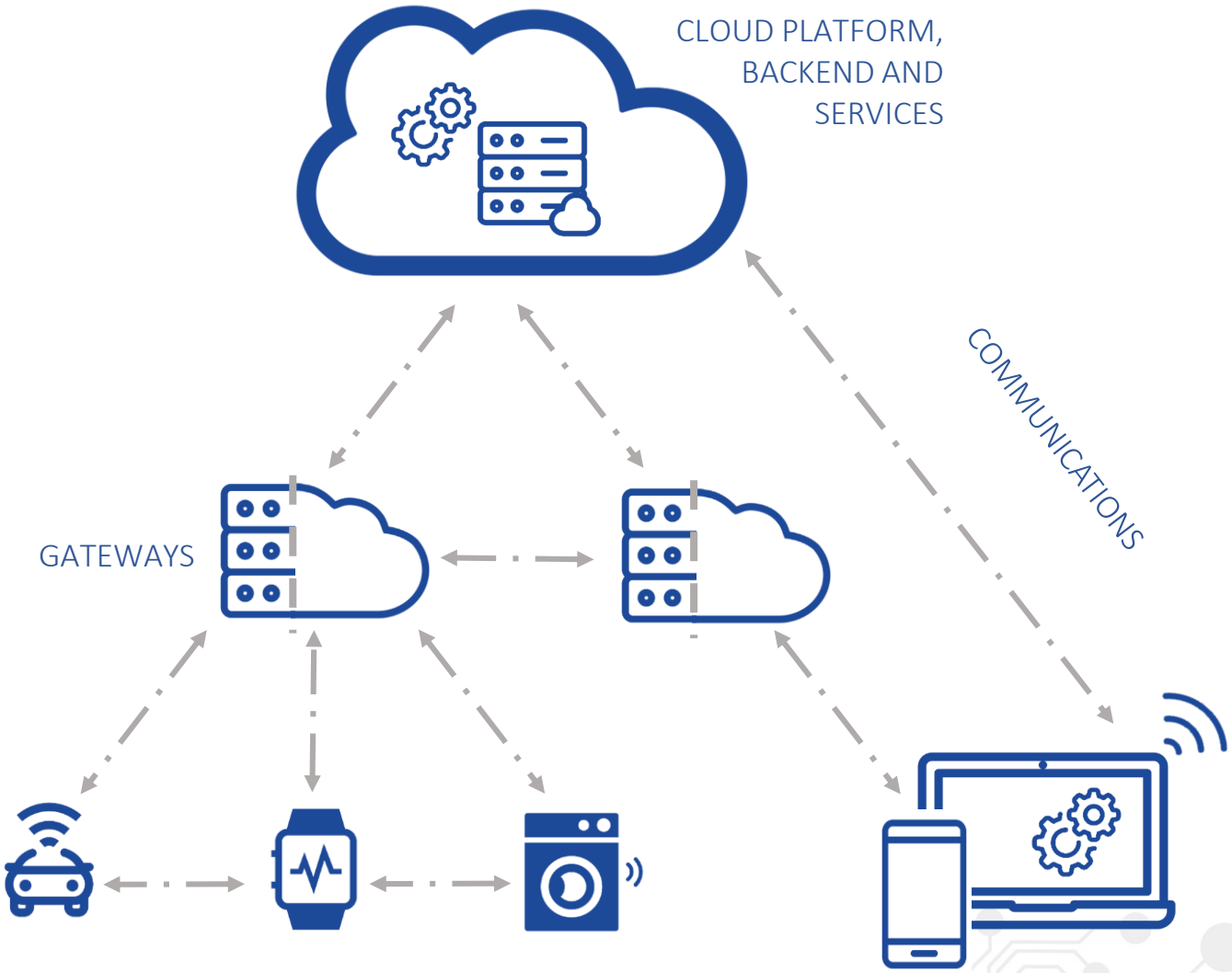
Heat map of key IoT opportunities varies by industry and application



Source: "The Internet Of Things Heat Map, 2017" Forrester report

Components of IoT?

IoT Ecosystem



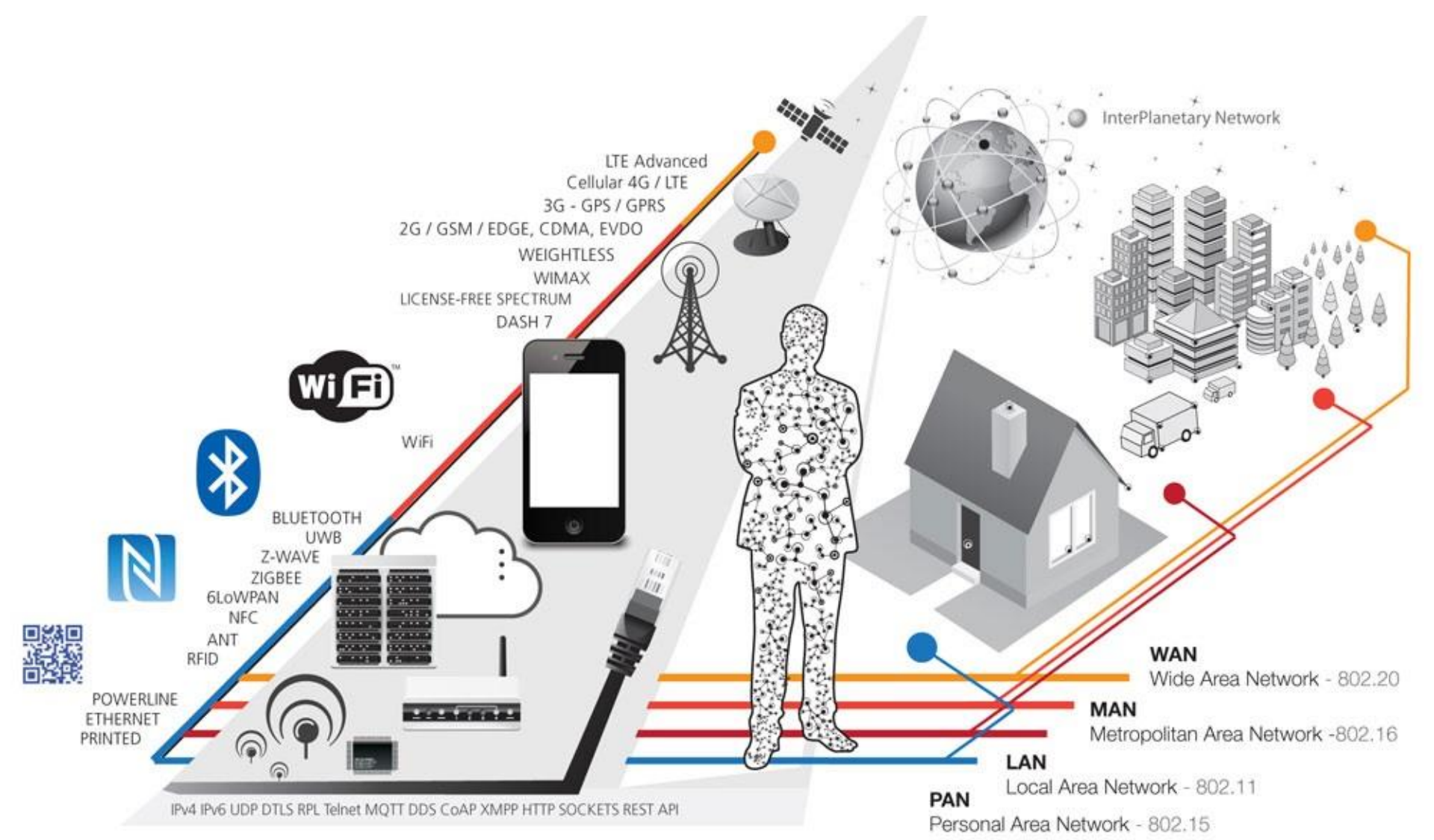
IoT Components – Endpoint Devices

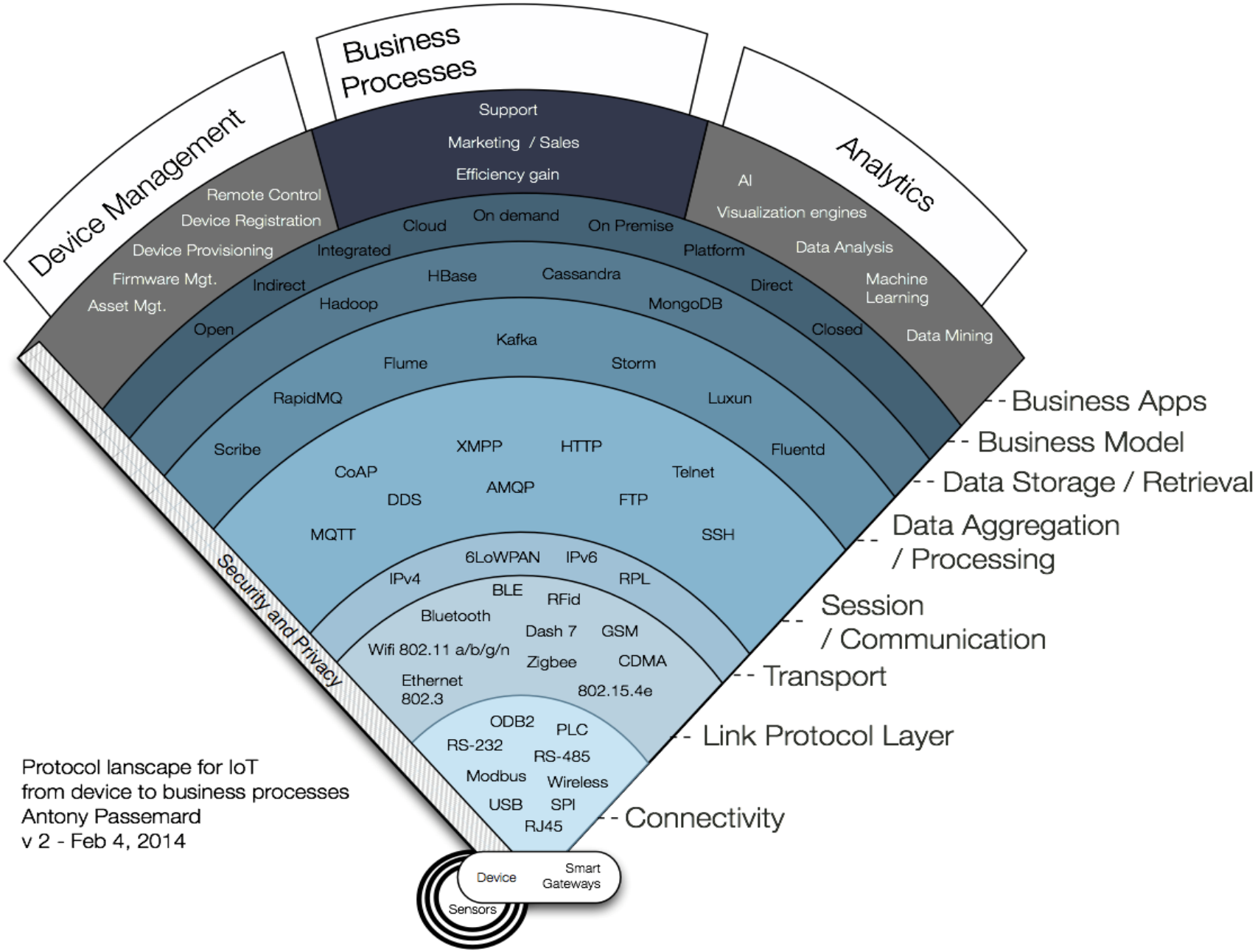
- Smart appliances
- Smartphones
- Smart ‘things’

IoT Components - Communications

- WiFi
- Zigbee
- Z-Wave
- NFC
- RFID
- BLE
- LoRAWAN
- MQTT/SIP/CoAP

SESSION		AMQP, CoAP, DDS, MQTT, XMPP
NETWORK	ENCAPSULATION	6LowPAN, Thread
	ROUTING	CARP, RPL
DATALINK		Bluetooth / BLE, Wi-Fi / Wi-Fi HaLow, LoRaWAN, Neul, SigFox, Z-Wave, ZigBee, USB


InterPlanetary Network
LTE Advanced
Cellular 4G / LTE
3G - GPS / GPRS
2G / GSM / EDGE, CDMA, EVDO
WEIGHTLESS
WIMAX
LICENSE-FREE SPECTRUM
DASH 7
WiFi
BLUETOOTH
UWB
Z-WAVE
ZIGBEE
6LoWPAN
NFC
ANT
RFID
POWERLINE
ETHERNET
PRINTED
IPv4 IPv6 UDP DTLS RPL Telnet MQTT DDS CoAP XMPP HTTP SOCKETS REST API
WAN
Wide Area Network - 802.20
MAN
Metropolitan Area Network -802.16
LAN
Local Area Network - 802.11
PAN
Personal Area Network - 802.15

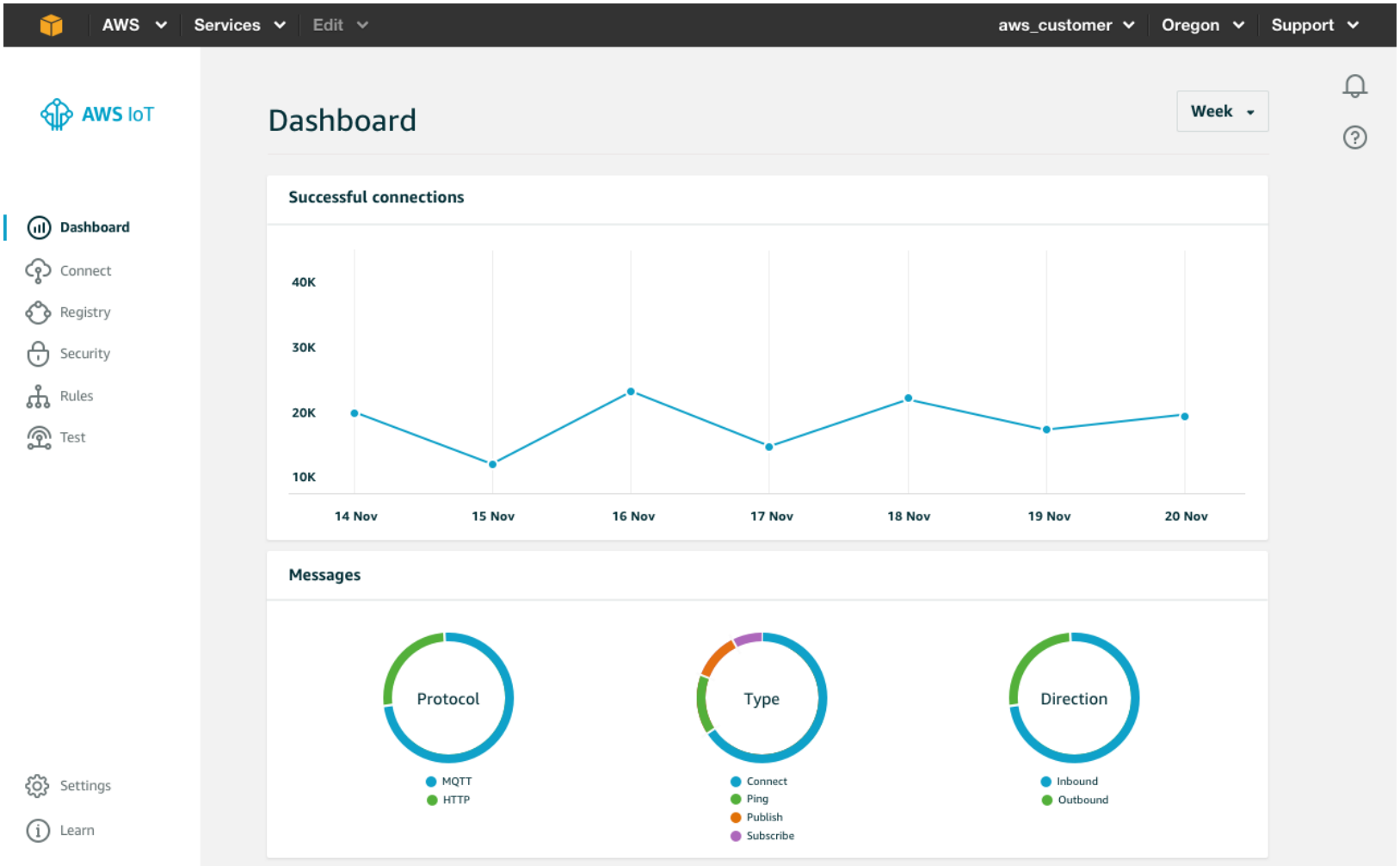


Protocol lanscape for IoT
from device to business processes
Antony Passemard
v 2 - Feb 4, 2014

IoT Components - Cloud

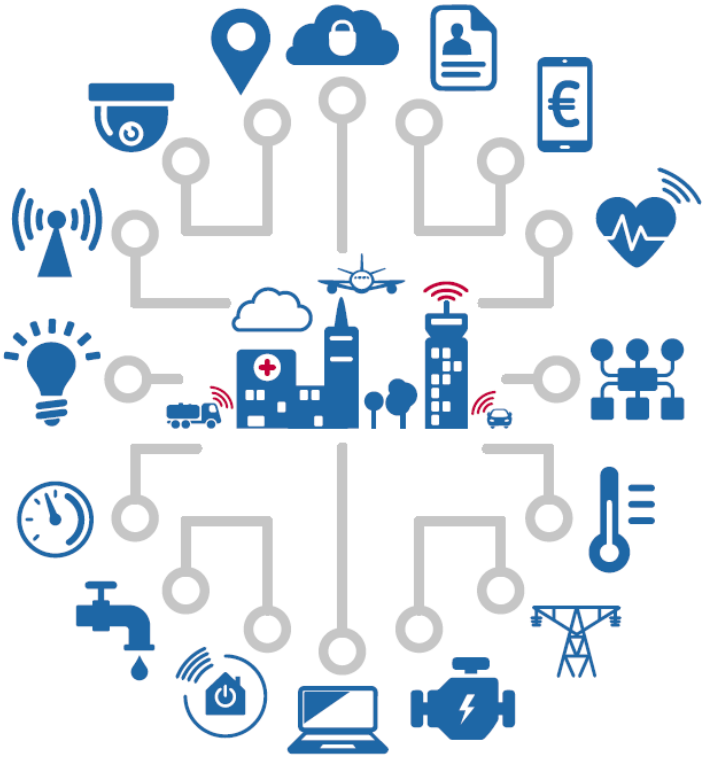
- Data and storage
- Web-based services
- Device management (config, etc)

IoT Cloud platform



IoT Components - Use case / context

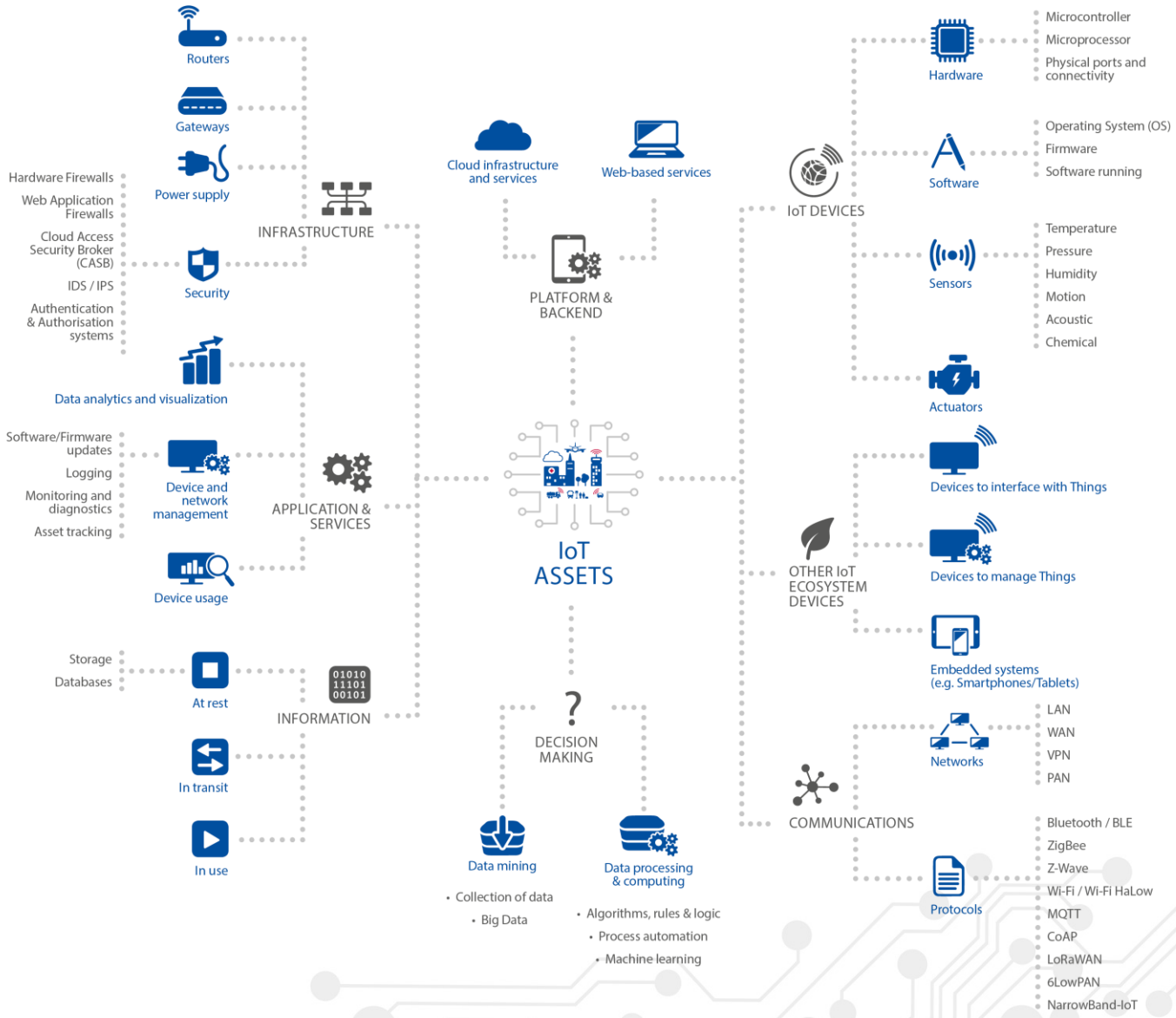
- Consumer Electronics
- Automotive
- Healthcare
- Industrial IoT
- Wearables
- Logistics
- Sport & Fitness



What are the assets of IoT?

Group of 4 – 5’

IoT Assets


Routers
Gateways
Power supply
Hardware Firewalls
Web Application Firewalls
Cloud Access Security Broker (CASB)
IDS / IPS
Authentication & Authorisation systems
Security
INFRASTRUCTURE
Data analytics and visualization
Software/Firmware updates
Logging
Monitoring and diagnostics
Asset tracking
Device and network management
Device usage
APPLICATION & SERVICES
Storage
Databases
At rest
In transit
In use
INFORMATION
Cloud infrastructure and services
Web-based services
PLATFORM & BACKEND
IoT ASSETS
DECISION MAKING
Data mining
• Collection of data
• Big Data
Data processing & computing
• Algorithms, rules & logic
• Process automation
• Machine learning
IoT DEVICES
Hardware
Microcontroller
Microprocessor
Physical ports and connectivity
Software
Operating System (OS)
Firmware
Software running
Sensors
Temperature
Pressure
Humidity
Motion
Acoustic
Chemical
Actuators
OTHER IoT ECOSYSTEM DEVICES
Devices to interface with Things
Devices to manage Things
Embedded systems (e.g. Smartphones/Tablets)
COMMUNICATIONS
Networks
LAN
WAN
VPN
PAN
Protocols
Bluetooth / BLE
ZigBee
Z-Wave
Wi-Fi / Wi-Fi HaLow
MQTT
CoAP
LoRaWAN
6LowPAN
NarrowBand-IoT

Development for IoT

IoT development platforms

- **ThingBox**
- **Node-RED**
- **M2MLabs Mainspring**
- **Kinoma**
- **Eclipse IoT Project**
- **Arduino**

IoT hardware platforms

- Apio
- Arduino Nano
- Arduino Pro Mini
- Arduino Uno
- Arduino Yún
- Arietta G25
- BeagleBoard
- Flutter
- Flutter
- IMUduino BTLE
- Intel Edison
- Intel Galileo
- Libelium Waspmote
- LightBlue Bean
- Local Motors Connected Car
- Microduino
- Nanode
- OpenKontrol Gateway
- OpenPicus
- panStamps
- PicAxe
- Pinoccio
- Raspberry Pi 2
- RasWIK
- SAM R21 Xplained Pro
- SmartEverything
- SODAQ
- SparkFun RedBoard
- Tessel
- Tessel 2
- The AirBoard
- The Rascal
- TinyDuino
- UDOO
- WIOT
- XinoRF

IoT software platforms

Home Automation

- Eclipse SmartHome
- Home Gateway Initiative (HGI)
- Ninja Blocks
- openHAB
- PrivateEyePi
- RaZberry
- The Thing System

Middleware

- IoTSyS
- Kaa
- OpenIoT
- OpenRemote

Operating Systems

- AllJoyn
- Contiki
- Raspbian
- RIOT
- Spark

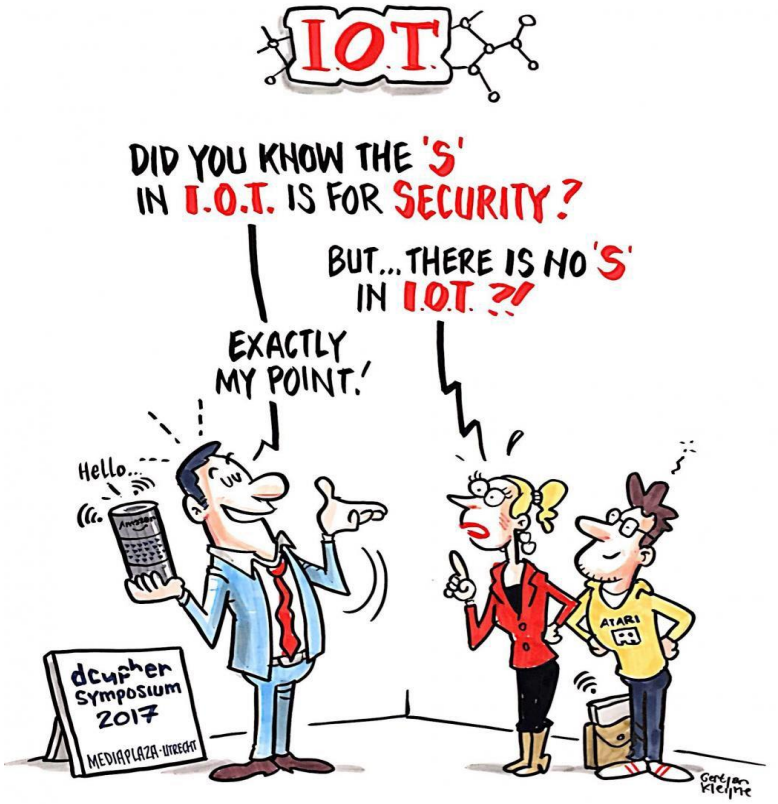
IoT lintegration platforms

- **Canopy**
- **Chimera IoT**
- **DeviceHive(IoT Integration Tools and Horizontal Platforms)**
- **net**
- **Distributed Services Architecture (DSA)**
- **IoT Toolkit**
- **M2MLabs Mainspring**
- **Mango**
- **Nimbits**
- **Open Source Internet of Things (OSIOT)**
- **OpenRemote**
- **Pico Labs (Kynetx open source assigned to Pico Labs)**
- **prpl Foundation**
- **RabbitMQ**
- **SiteWhere**
- **ThingSpeak**
- **webinos**
- **Yaler**

Node-Red

https://nodered.org/

IoT Security



What could possibly go wrong?

What could possibly go wrong?

by Tom Spring August 11, 2016 , 11:27 am

by Tom Spring August 26, 2016 , 2:55 pm

ANDY GREENBERG SECURITY 07.21.15 6:00 AM

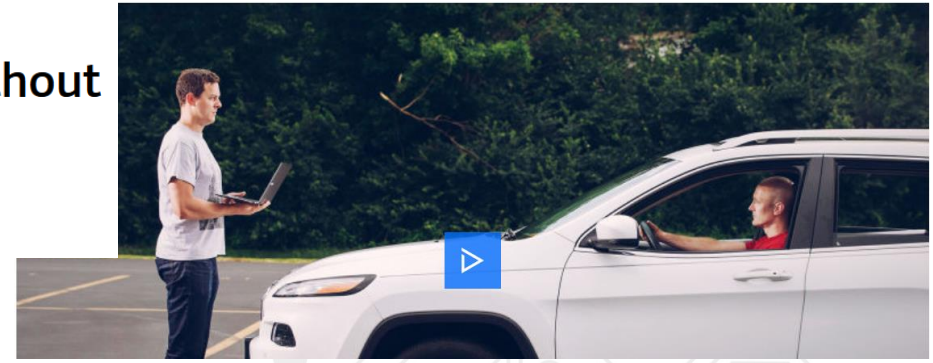
HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT

circuit breaker

This doll recorded kids' conversations without parental consent

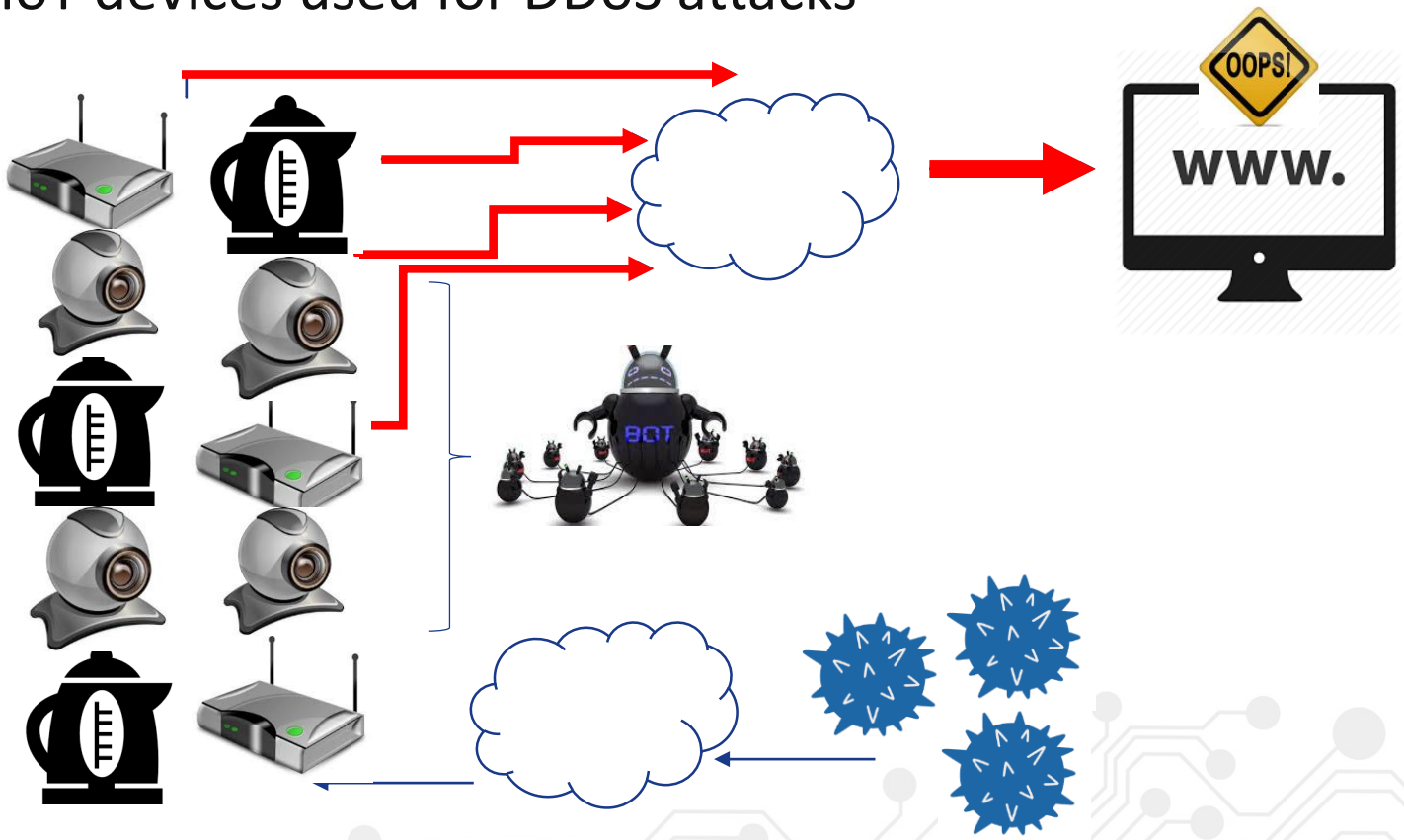
Security experts found ways to listen in

by Ashley Carman | @ashleyrcarman | Dec 8, 2016, 11:36am EST



Based on a real life example

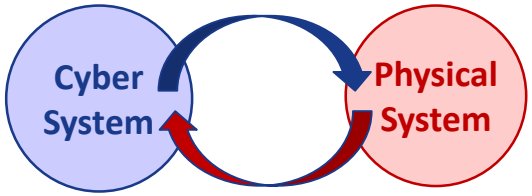
- IoT botnet
  - IoT devices used for DDoS attacks



Why IoT security matters?

No device is fully secured

- Reliance on third-party components, hardware and software
- Dependency on networks and external services
- Design of IoT/connected devices
- Vulnerabilities in protocols
- Security by design NOT the norm.

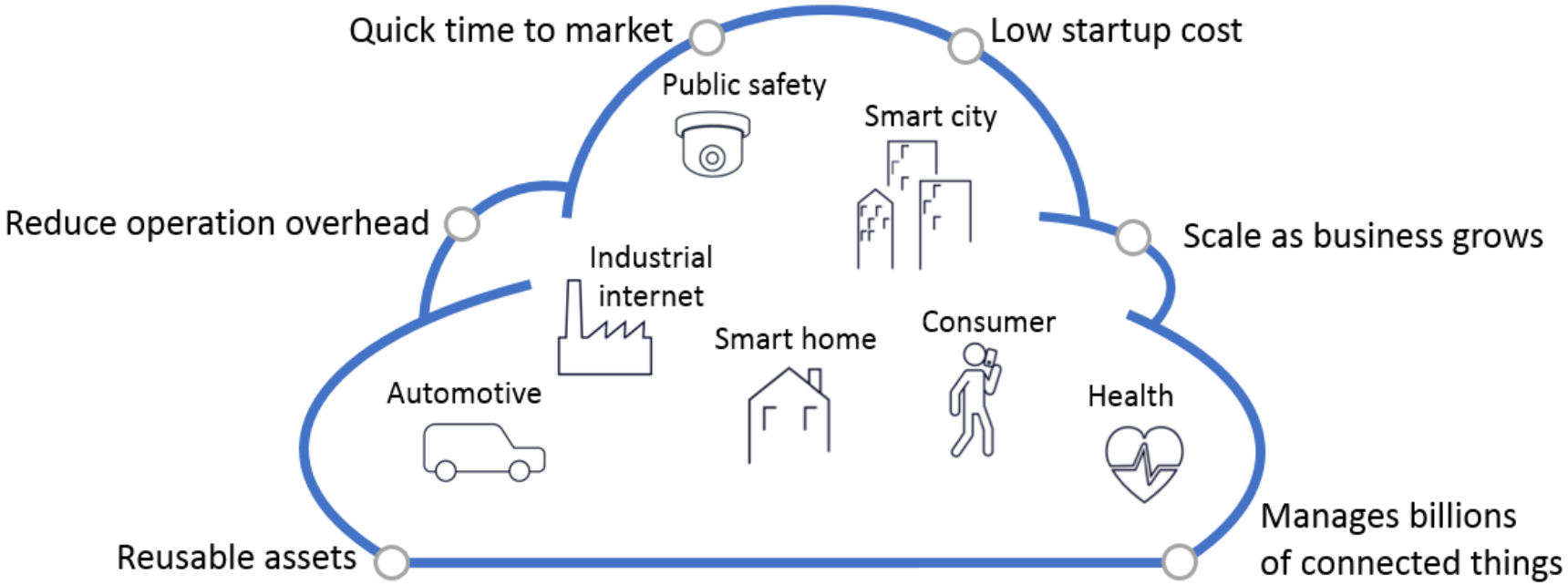


IoT security is currently limited

- Investments on security are limited
- Functionalities before security
- Real physical threats with risks on health and safety
- No legal framework for liabilities

IoT Security – Main challenges

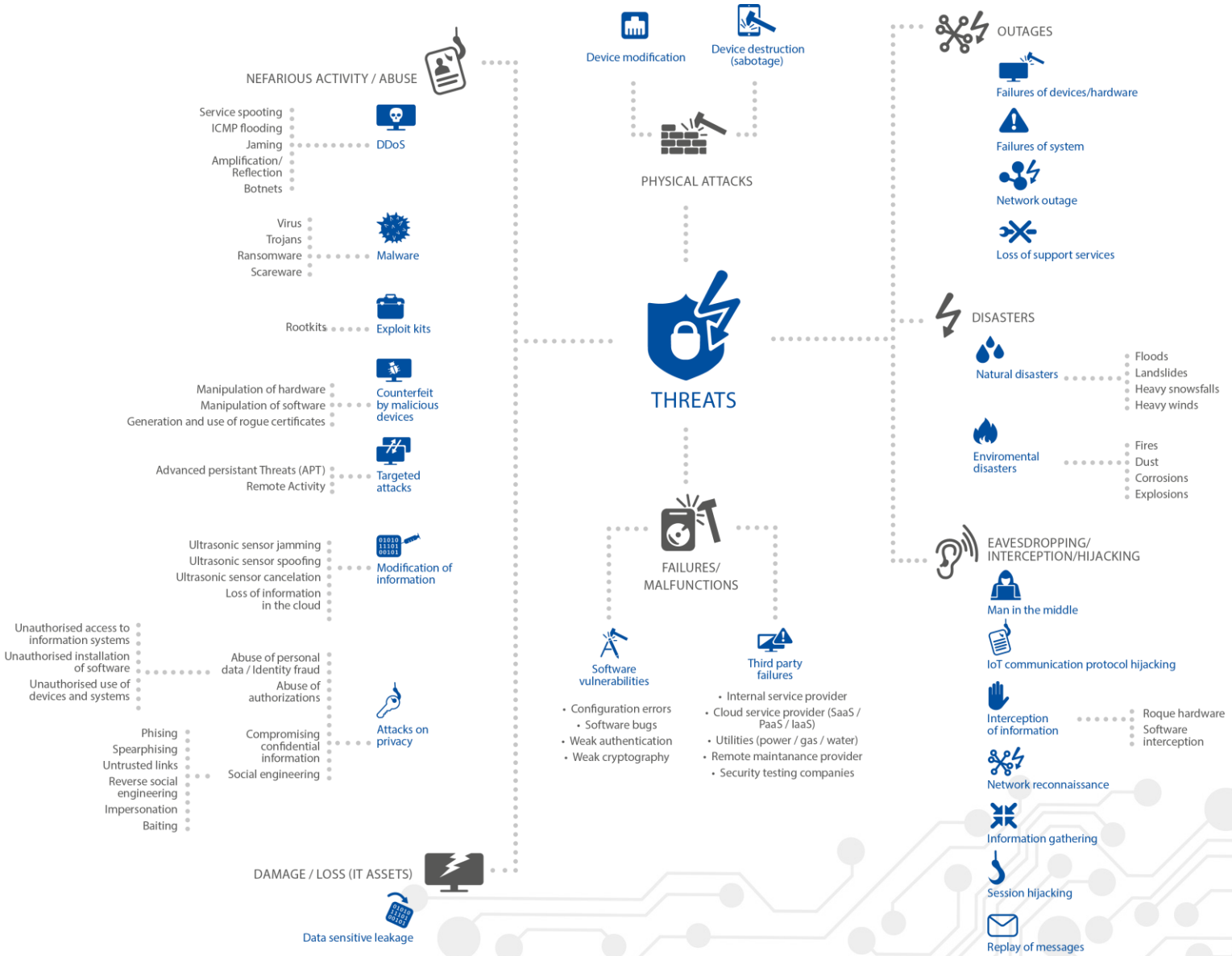
- Very large attack surface and widespread deployment
- Limited device resources
- Lack of standards and regulations
- Safety and security process integration
- Security by design not a top priority
- Lack of expertise
- Applying security updates
- Insecure development
- Unclear liabilities


Quick time to market
Low startup cost
Public safety
Smart city
Reduce operation overhead
Scale as business grows
Industrial internet
Smart home
Consumer
Automotive
Health
Reusable assets
Manages billions of connected things

What are the threats to IoT?

Group of 4 – 5’

IoT Threat Landscape

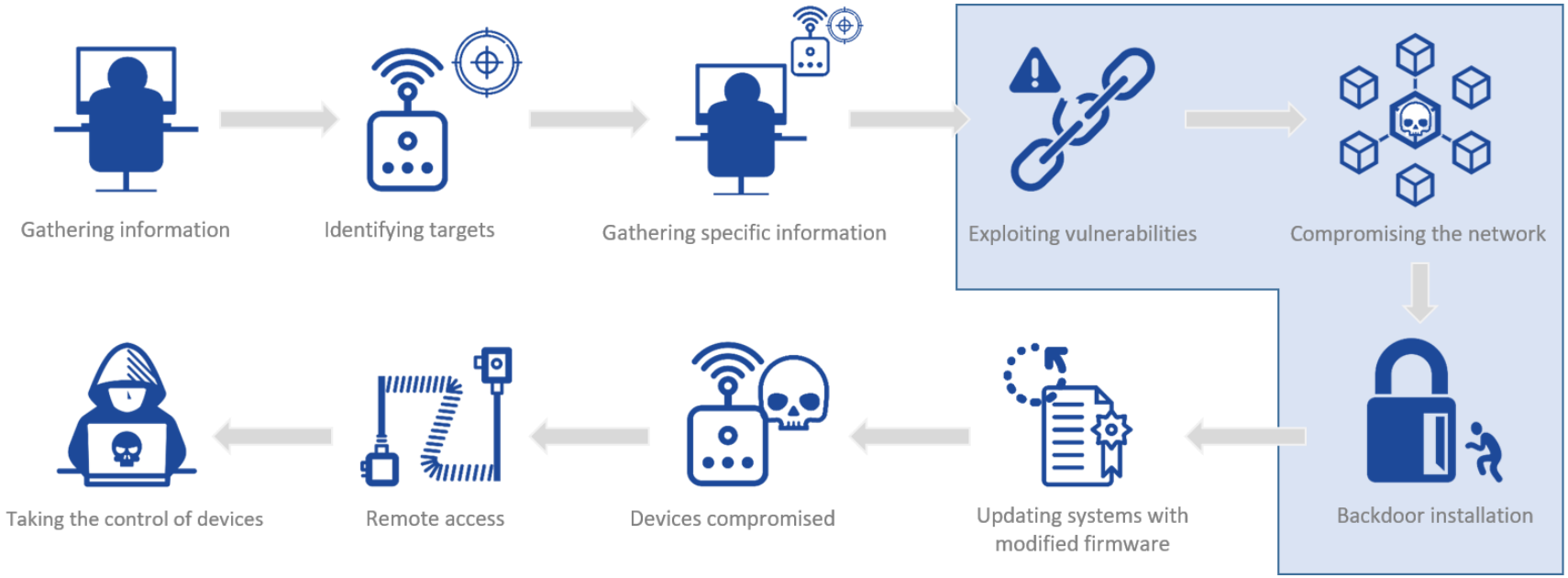


Which way would you attack IoT? Attack scenarios

Many ways to attack IoT

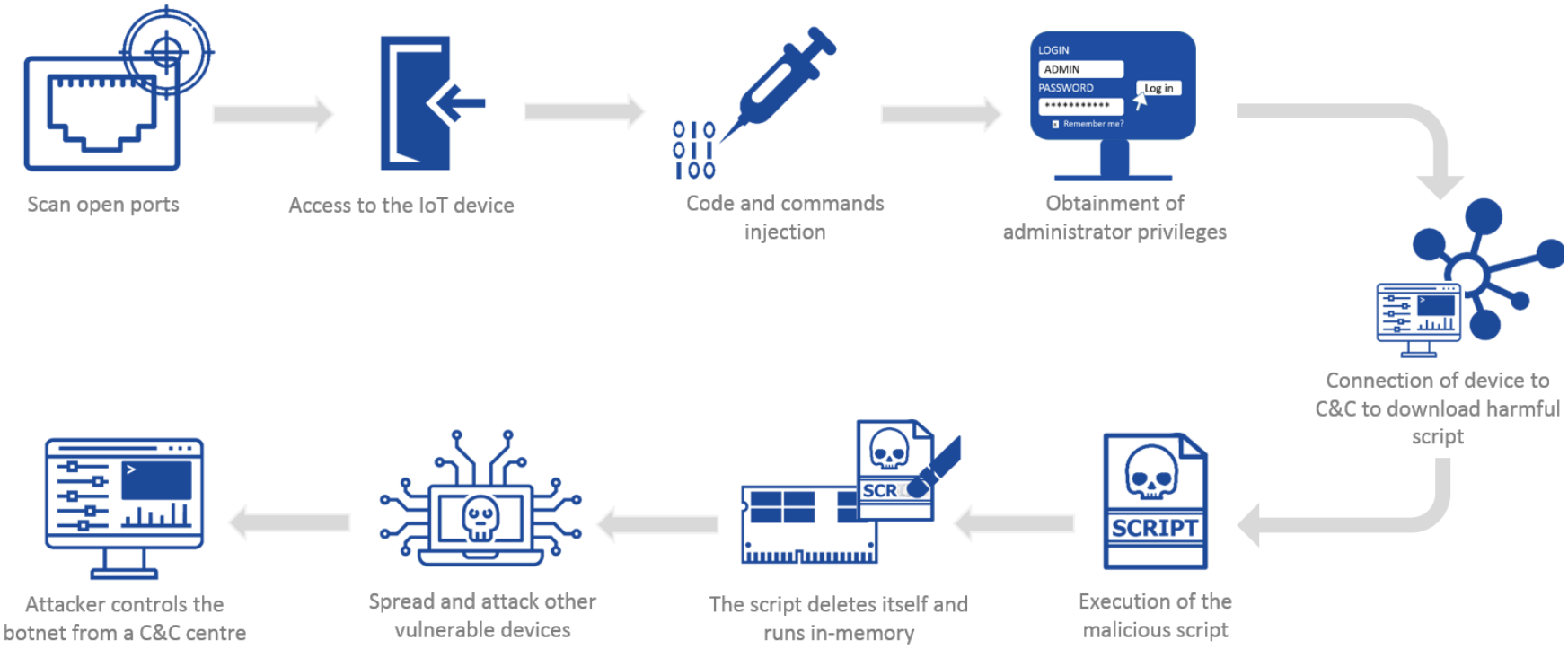
- Attacks over the entire IoT ecosystem
  - Sensors/actuators
    - E.g. draining the battery of pacemakers
  - Communications
    - E.g. intercepting Bluetooth LE communication
  - Decision making (data integrity, etc.)
    - E.g. modification of messages to modify smart car behavior
  - Information privacy
    - E.g. smart toys exploited to eavesdrop on children

IoT Attack Scenarios



IoT administration system compromised

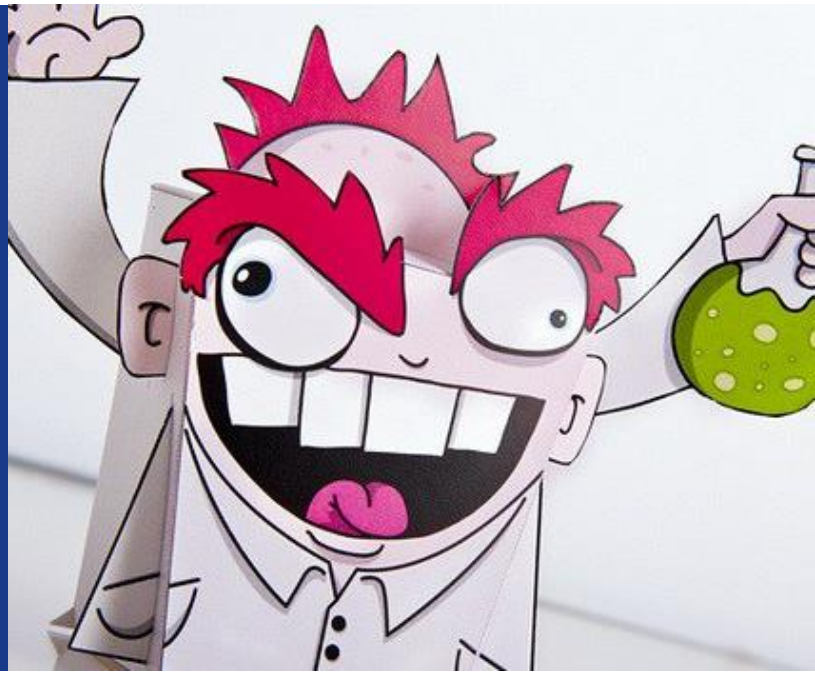
IoT Attack Scenarios



Botnet / Commands injection

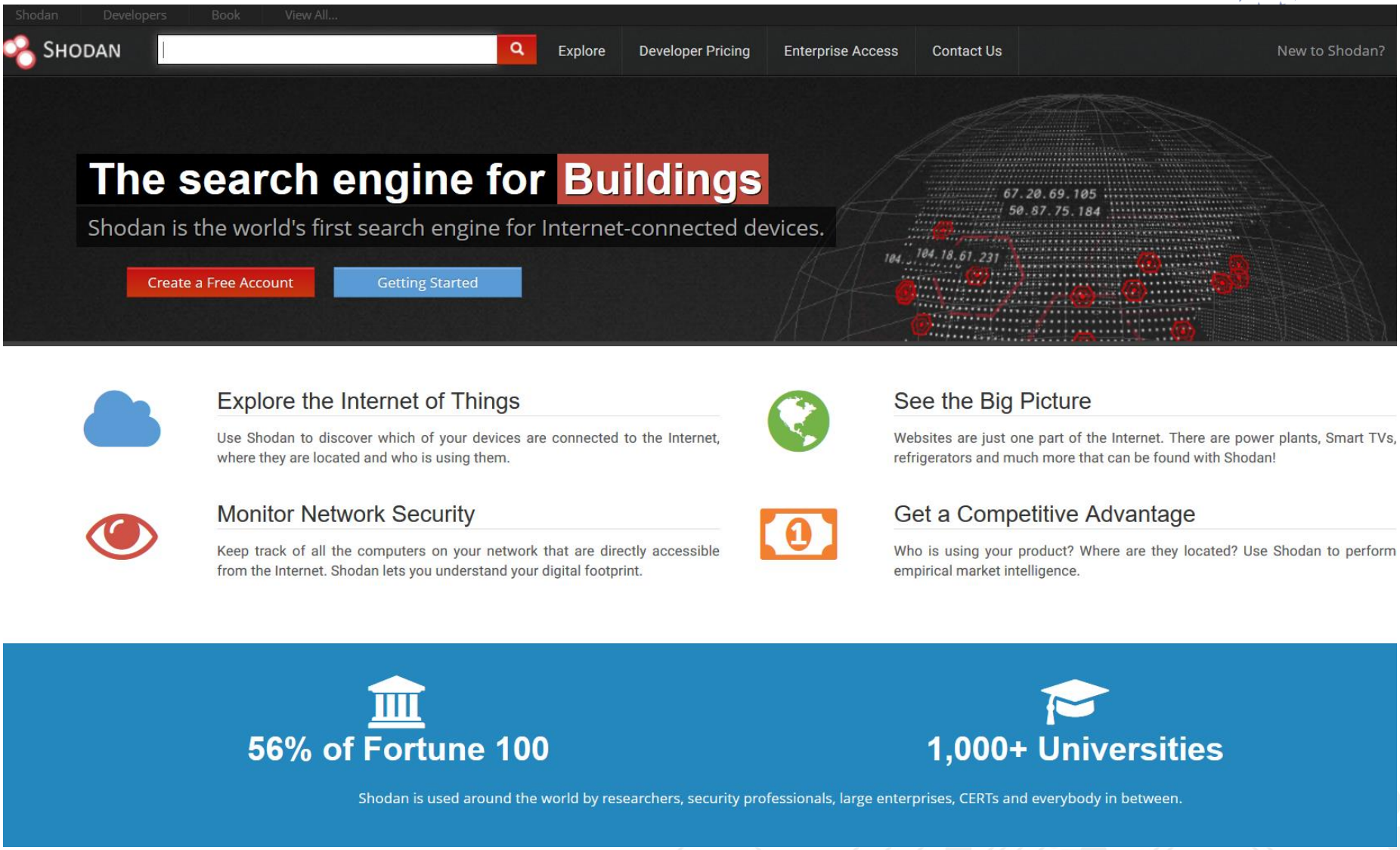
Class Exercise

Botnet (Mirai)




OSINT Landscape v.1 February 2018
Open Source Intelligence (/OSINV – Open Source Investigation)
COVERT SHORES www.hisutton.com
bellingcat
Social Media Platforms
Facebook
Weibo
Twitter
Qzone
Instagram
Odnoklassniki
Linkedin
VK
Snapchat
YouTube
Periscope
stalkscan
Facebook Search Tool
Graph Search Generator
FBDOWN
Signal
peoplefindThor
Tweetbeaver
twXplorer
Twitter List Copy
TweetDeck
WEBSTA
Instagram Downloader
picodash
socilab
PHOTO MAP
savefrom.net
Youtube DataViewer
frame by frame
storyful
Geo Search Tool
Scopedown
Snap Map
Dataminr
INTELTECHNIQUES
Echosec
War Wire
Messaging & closed groups
Sharing & Publishing
flickr
Pinterest
Google+
Blogging, Forums & other communities
STRAVA
tumblr.
LIVEJOURNAL
classmates
WORDPRESS.ORG
Blogger
WiX.com
Medium
ProBoards
SQUARESPACE
Joomla!
ghost
weebly
Internet Search
Google
Yandex
Bing
waybackMachine
DuckDuckGo
NAVER
Baidu 百度
搜狗搜索
goo
Рамблер/
kakao
YAHOO!
archive.today
PimEyes
Geospatial Data
GeoNames
SECRETS OF THE WEST
DualMaps
wikimapia
Free GIS Data
OpenRailwayMap
MAPS.ME
Mapillary
Google Maps
Bing maps
Maps
here
Yandex
Satellite Imagery
Google Earth
Descartes Labs
TERRA server
AIRBUS GeoStore
Zoom Earth
unitar
HARRIS
USGS EarthExplorer
esa opernicus
planet
Radiant.Earth
NOAA
EARTHDATA
esa Earth Online
DigitalGlobe
SENTINEL
Maritime Movements
MarineTraffic
IHS Markit
AISLive
Lloyd's List Intelligence
SHIPSPOTTING.com
Vessel Finder
Shipfinder
AISHub
shipfinder
OpenSeaMap
SHIPAIS
ShippingExplorer
BoatNerd
AISDecoder
Aviation Movements
COAA
AirNav RadarBox
LiveATC.net
ADS-B Exchange
flightradar24
GVA Dictator Alert
FlightAware
PLANESPOTTERS.NET
Radio
RadioReference
Broadcastify
Radio Garden
SDR.hu
ProScan
MilScanners
Commercial Registries
opencorporates
infobel
ICU OFFSHORE LEAKS DATABASE
Investigative Dashboard Search
EUROPEAN JUSTICE
Webcams
pentopia
Insecam
SHODAN
EarthCam
Webcams.travel
PICTIMO
wetter.com
lookr
wisuki
Image / Vid / Doc Forensics
GET-METADATA
Jeffrey's Image Metadata
metapicz
FotoForensics
Forensically Beta
IRFANVIEW
hatlord / Spiderpig
exifdata
ExifTool
InVID
This landscape shows data sources (mostly platforms, tools or apps) that provide publicly available data which may be of use in OSINT. Some tools may charge for data access. It is intended to be extensive, but not exhaustive, and may be updated periodically.
Authors:
H I Sutton, (@CovertShores) Covert Shores and Jane's contributor,
Aliaume Leroy, (@Yeoln) Bellingcat & BBC,
Tony Roper, (@Topol_M5527), planesandstuff, Jane's contributor

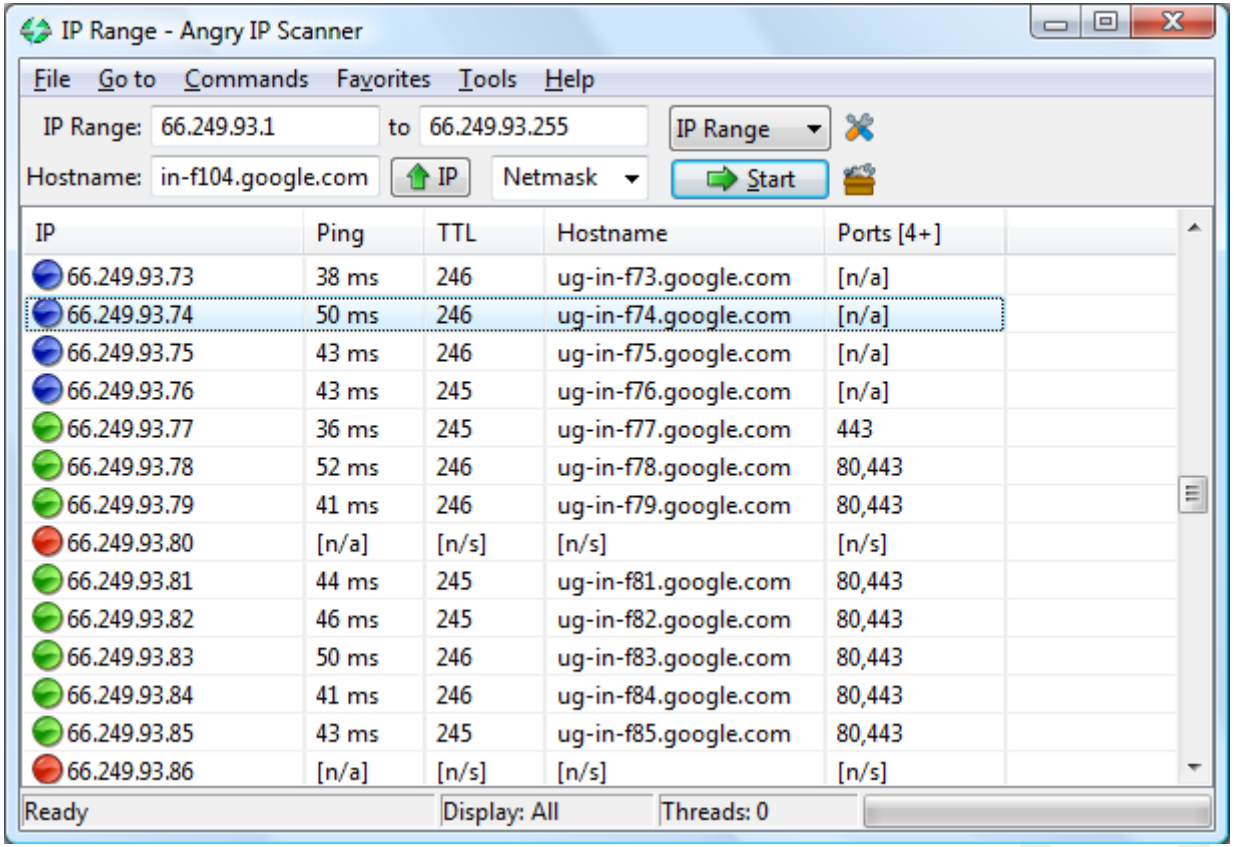
Shodan


Shodan
Developers
Book
View All...
SHODAN
Explore
Developer Pricing
Enterprise Access
Contact Us
New to Shodan?
The search engine for Buildings
Shodan is the world's first search engine for Internet-connected devices.
Create a Free Account
Getting Started
67.20.69.105
50.87.75.184
104.18.61.231
Explore the Internet of Things
Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.
See the Big Picture
Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan!
Monitor Network Security
Keep track of all the computers on your network that are directly accessible from the Internet. Shodan lets you understand your digital footprint.
Get a Competitive Advantage
Who is using your product? Where are they located? Use Shodan to perform empirical market intelligence.
56% of Fortune 100
1,000+ Universities
Shodan is used around the world by researchers, security professionals, large enterprises, CERTs and everybody in between.

What to understand

- What we are exposing on the internet
- Online scanners
- The use of shodan, and the many grey areas.
- Who is a potential target of these kind of scanners?
- Are shodan results an indicator of potential attacks and more sophisticated version of current attacks? (eg. Mirai evolved to target specific ports – why?)

IP Angry


IP Range - Angry IP Scanner
File Go to Commands Favorites Tools Help
IP Range: 66.249.93.1 to 66.249.93.255 IP Range
Hostname: in-f104.google.com IP Netmask Start
IP Ping TTL Hostname Ports [4+]
66.249.93.73 38 ms 246 ug-in-f73.google.com [n/a]
66.249.93.74 50 ms 246 ug-in-f74.google.com [n/a]
66.249.93.75 43 ms 246 ug-in-f75.google.com [n/a]
66.249.93.76 43 ms 245 ug-in-f76.google.com [n/a]
66.249.93.77 36 ms 245 ug-in-f77.google.com 443
66.249.93.78 52 ms 246 ug-in-f78.google.com 80,443
66.249.93.79 41 ms 246 ug-in-f79.google.com 80,443
66.249.93.80 [n/a] [n/s] [n/s] [n/s]
66.249.93.81 44 ms 245 ug-in-f81.google.com 80,443
66.249.93.82 46 ms 245 ug-in-f82.google.com 80,443
66.249.93.83 50 ms 246 ug-in-f83.google.com 80,443
66.249.93.84 41 ms 246 ug-in-f84.google.com 80,443
66.249.93.85 43 ms 245 ug-in-f85.google.com 80,443
66.249.93.86 [n/a] [n/s] [n/s] [n/s]
Ready Display: All Threads: 0

Code of a Botnet

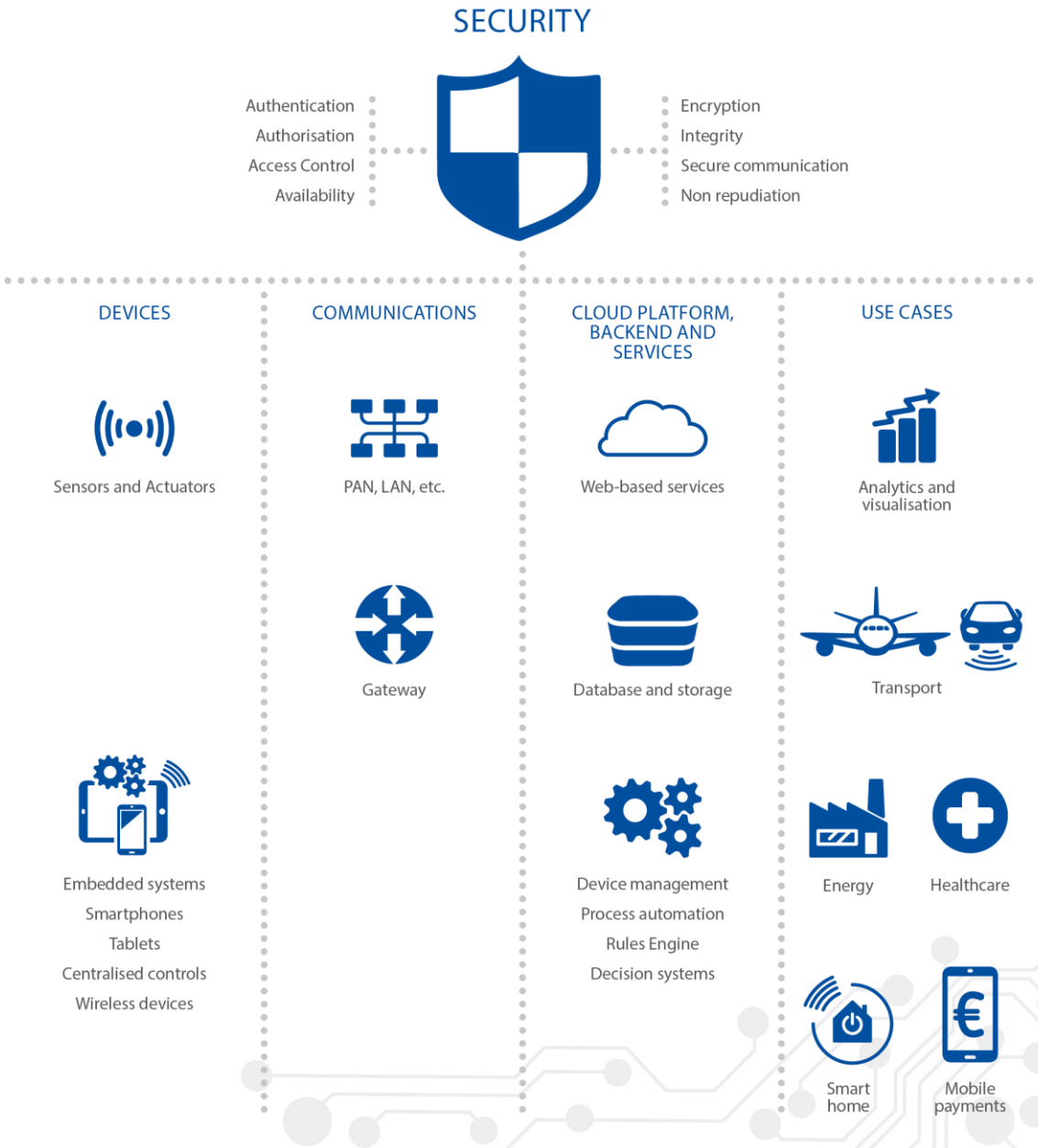
Study Mirai code on github:

https://github.com/jgamblin/Mirai-Source-Code

IoT Security Architectures

- AIOTI High Level Architecture functional model
- FP7-ICT – IoT-A Architectural reference model
- NIST Network of Things (NoT)
- ITU-T IoT reference model39
- ISO/IEC CD 30141 Internet of Things Reference Architecture
- ISACA Conceptual IoT Architecture
- oneM2M Architecture Model
- IEEE P2413 - Standard for an Architectural Framework

High-level IoT reference model



Case-study

Demo on Smart Health Security

Sensor

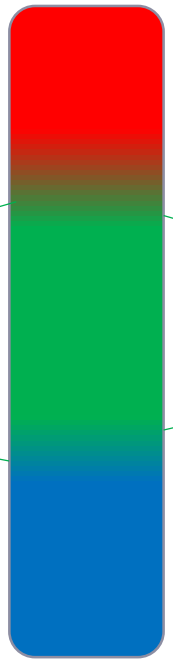
Sensor
(RGB sensor)

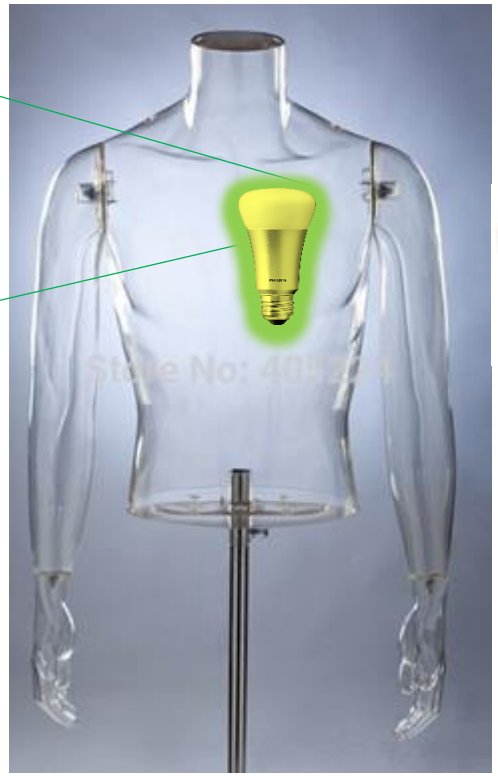
1 = red
0 = green
-1 = blue

1 High

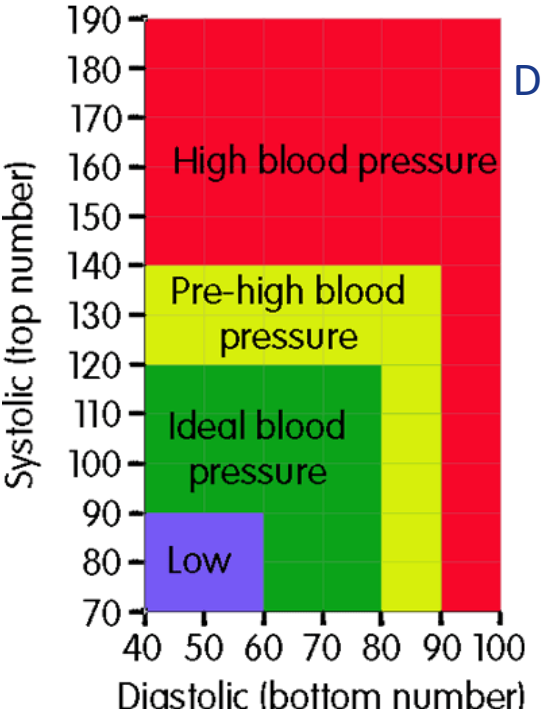
0 Med

-1 Low





Display?/LED



Interconnectivity

1 = red
0 = green
-1 = blue

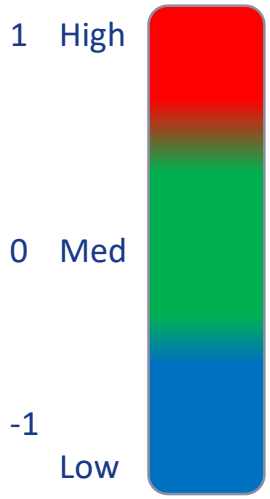
Decision Making

Based on reading, we want to increase or decrease value to get optimal state

If(red)
  add blue

If(green)
  do nothing

If(blue)
  add red



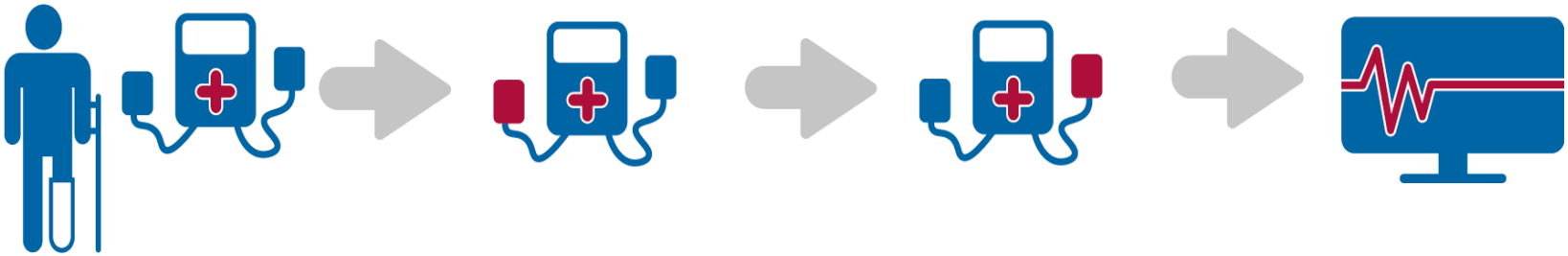
Actuator

If(red)
  add blue

Scenario 1: Sensor tampering

modifying the values read by sensors or their threshold values and settings

ATTACK SCENARIO 1 – TAMPERING



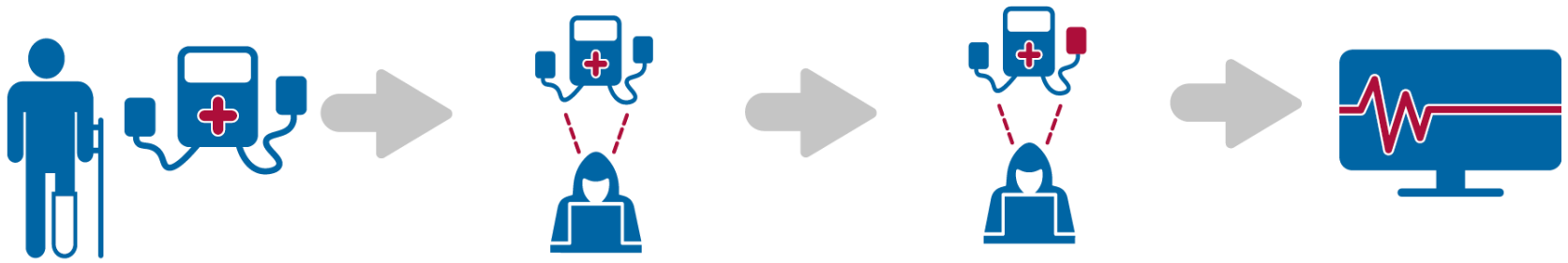
1. Normal operation of device
2. Sensor Tampered
3. False decision making
4. Service Down

Real life practice – Electronic thermometer

Scenario 2: Man-In-the-Middle

modifying the values intercepted from the man in the middle

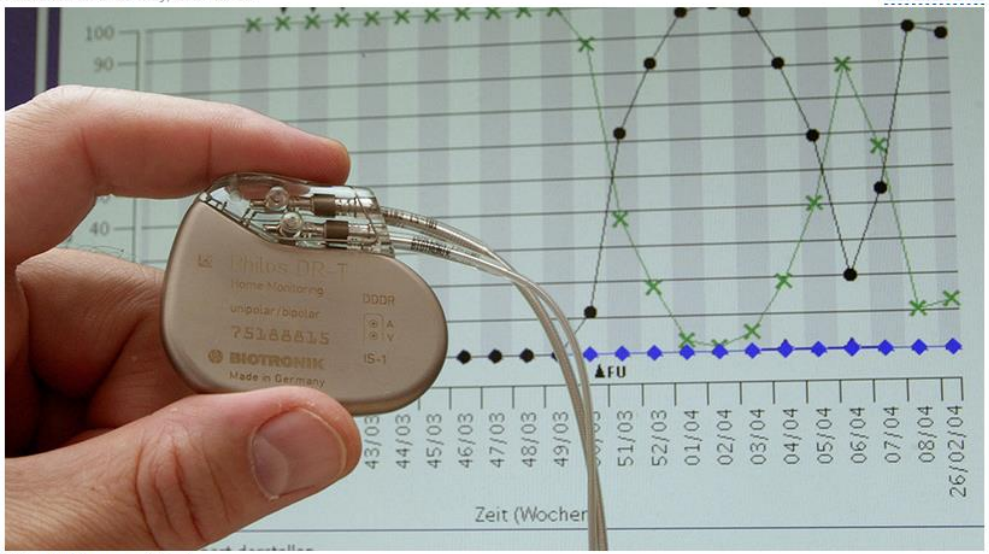
ATTACK SCENARIO 2 – MAN-IN-THE-MIDDLE



Real life practice – Pacemaker

Can the heart be hacked? Experts find 8,000 security flaws in pacemaker software

Published time: 28 May, 2017 18:10 Get short URL



© Arnd Wiegmann / Reuters

A tech security evaluation has found a whopping 8,000 software vulnerabilities in the code of pacemakers.

Security research firm WhiteScope carried out the assessment on implantable cardiac devices, physician programmers and home monitoring devices for four major manufacturers.

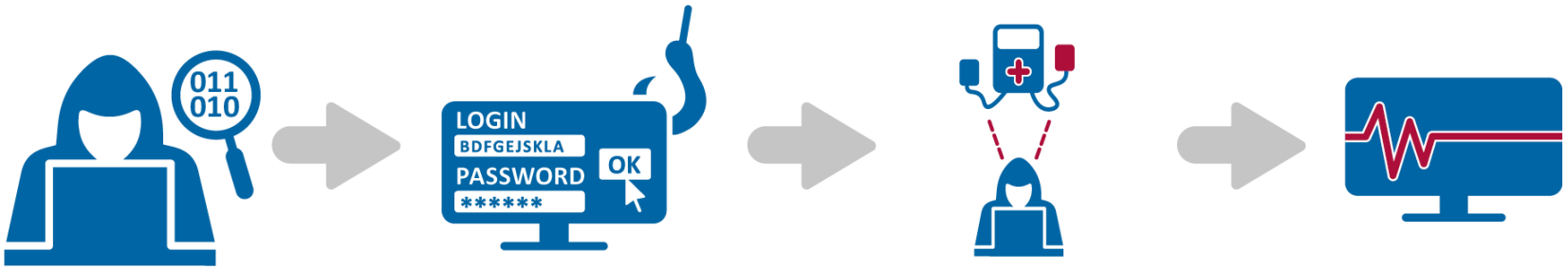
The researchers found a worrying consistency across all vendors, highlighting inherent system weaknesses in file system encryption and storage of unencrypted patient data.

The report notes that pacemaker security faces *"some serious challenges"*.

Scenario 3: Unauthorised access

modifying or sabotaging normal settings of the device

ATTACK SCENARIO 3 – UNAUTHORISED ACCESS USING DEFAULT PASSWORDS



1. Information gathering
2. Logon abuse
3. Establish connection to the actuator
4. System Down

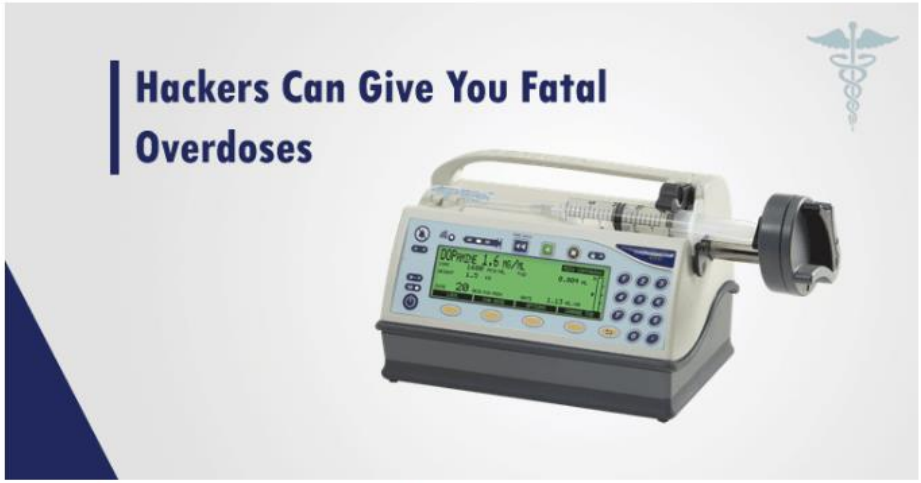
Real life practice – Unauthorised syringe injections

The Hacker News™
Security in a serious way

Hackers Can Remotely Access Syringe Infusion Pumps to Deliver Fatal Overdoses

Saturday, September 09, 2017 Swati Khandelwal

Tweet Share Share 48 Share 890 Share 2.81k Share



Internet-of-things are turning every industry into the computer industry, making customers think that their lives would be much easier with smart devices. However, such devices could potentially be compromised by hackers.

Summary

- IoT 101
- IoT Security
  - Challenges
  - Threats
  - Attack scenarios
- Case-study

Lab exercises on BLE attacks

Time to set up the VMachines!

Thank you

1 Vasilissis Sofias Str, Maroussi 151 24, Attiki, Greece

Tel: +30 28 14 40 9711

info@enisa.europa.eu

www.enisa.europa.eu