Intro to IoT Security

Ivan Marković
Ethical Hacker

MAKER

BUSINESS INCUBATOR
NOVI SAD

Hello, I’m …

- Somebody who like to know how things works
- Somebody who broke into things for fun and profit
- and somebody who like to share knowledge

and from my experience

it’s time to get serious

What is OWASP

OWASP

Open Web Application
Security Project

https://www.owasp.org/index.php/Category:OWASP_Project#tab=Project_Inventory

What is OWASP

https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project

What is KALI Linux

https://www.kali.org/

What we will learn today

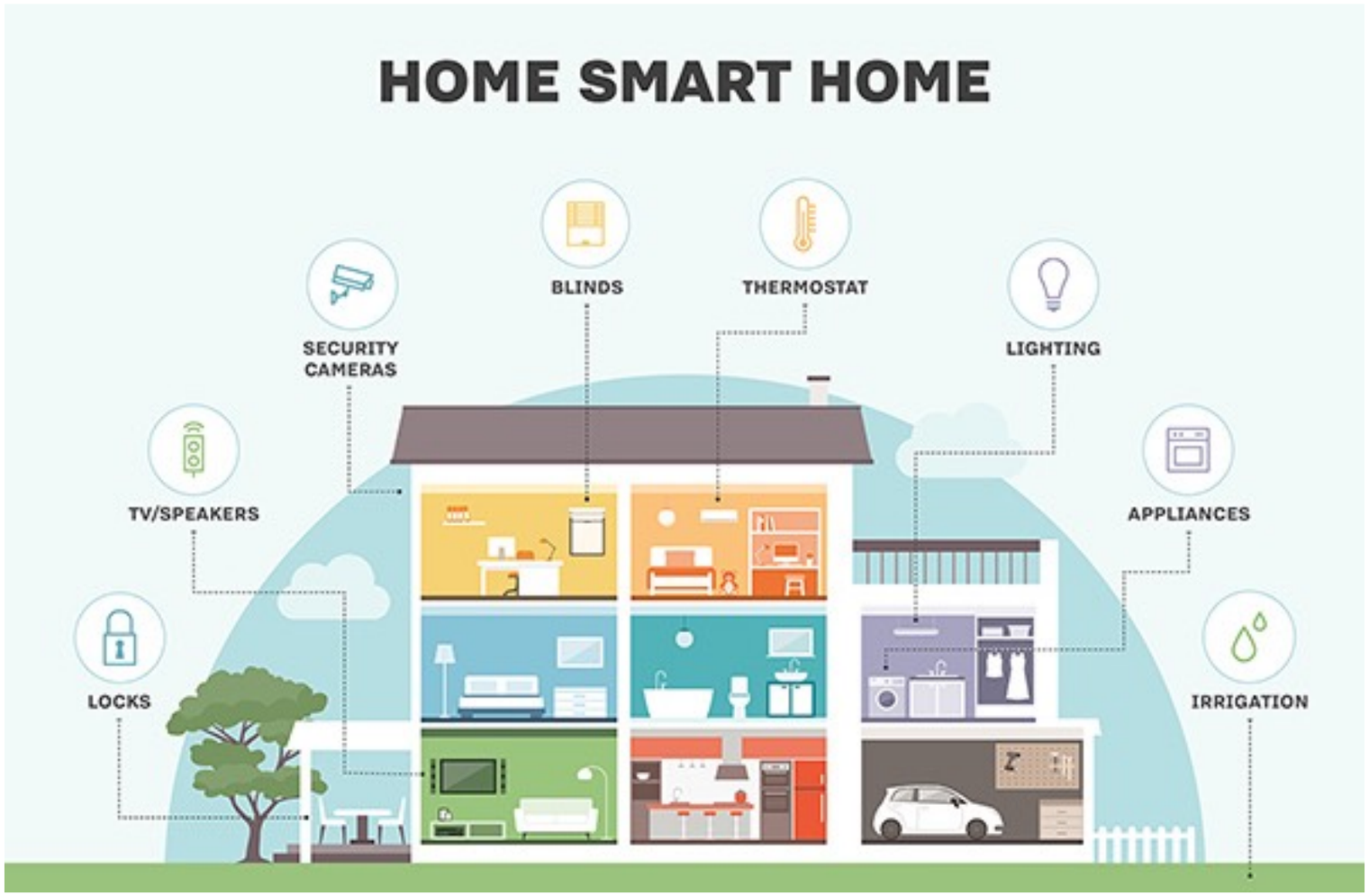
- What is the Internet of Things (IoT)
- Why is so important to take care about security and privacy
- What are the main threats
- How to do basic security overview of your IoT system

What is the Internet of Things (IoT)

- The Internet of Things is the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment.

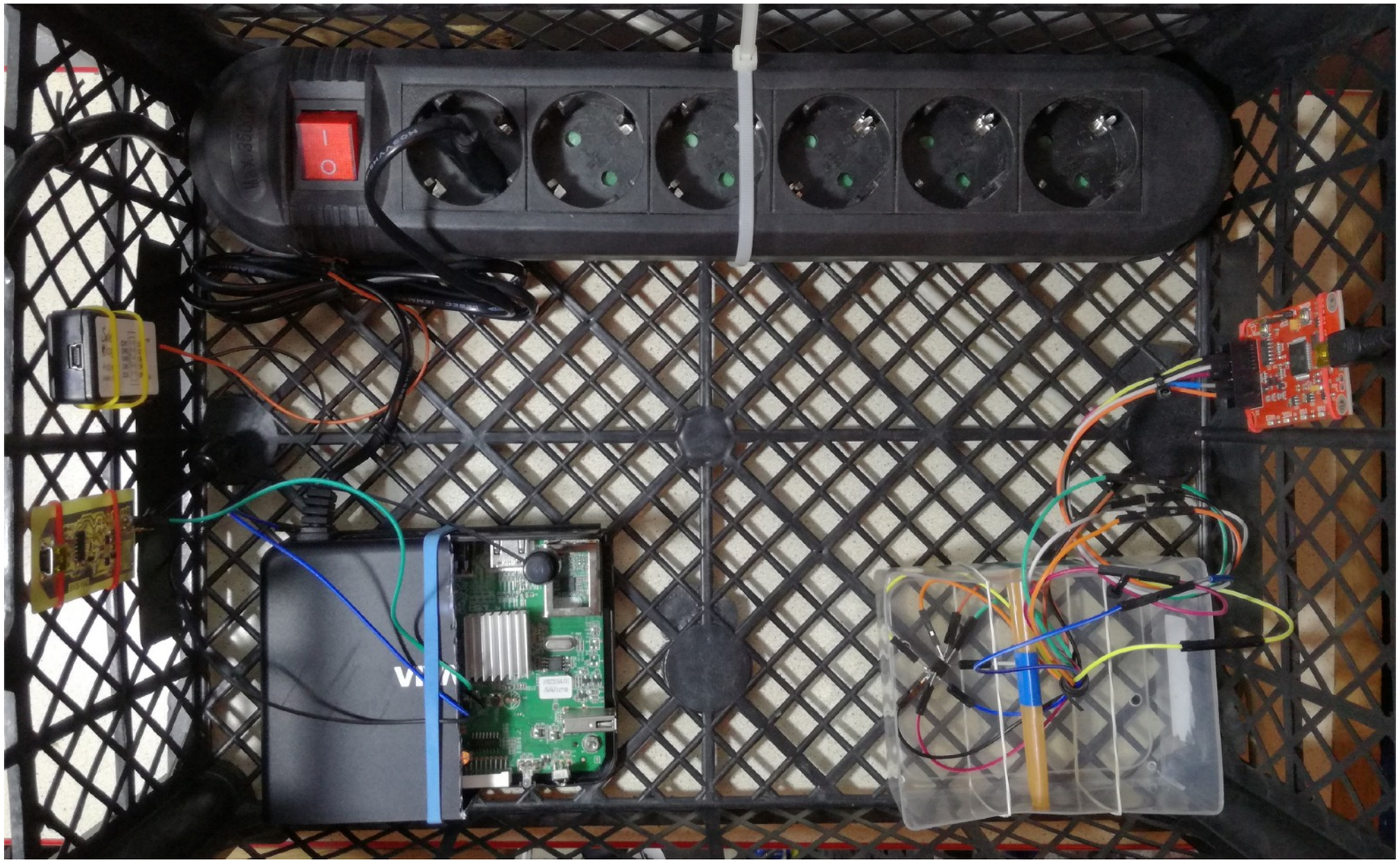
- Things having identities and virtual personalities operating in smart spaces using intelligent interfaces to connect and communicate within social, environmental and user contexts.

What is the Internet of Things (IoT)



What is the Internet of Things (IoT)

Our Laboratory for today (1)

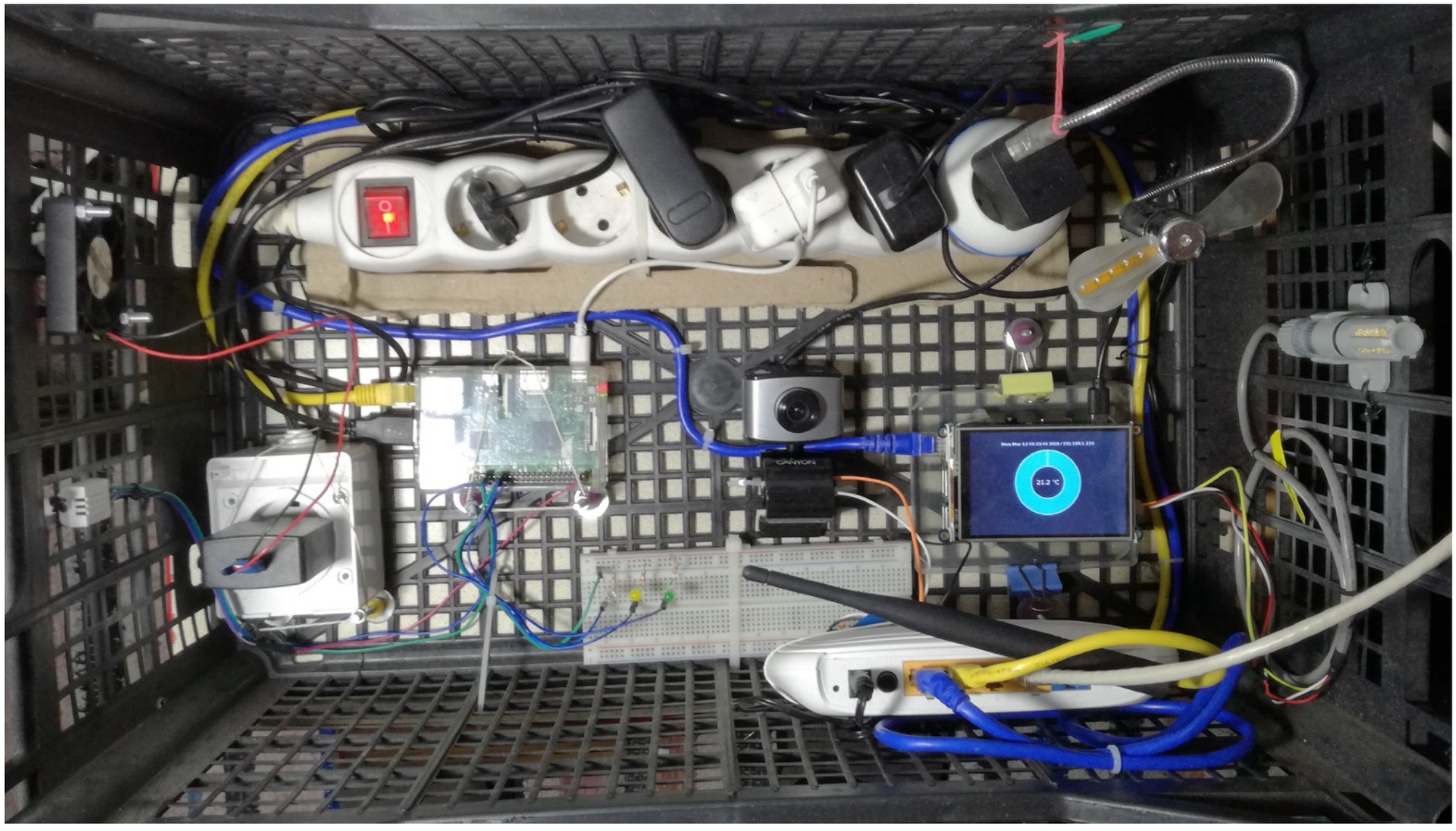


Logic Analyzer, Serial/UART interface, Bus Pirate v4, Set-Top Box

Our Laboratory for today (1)

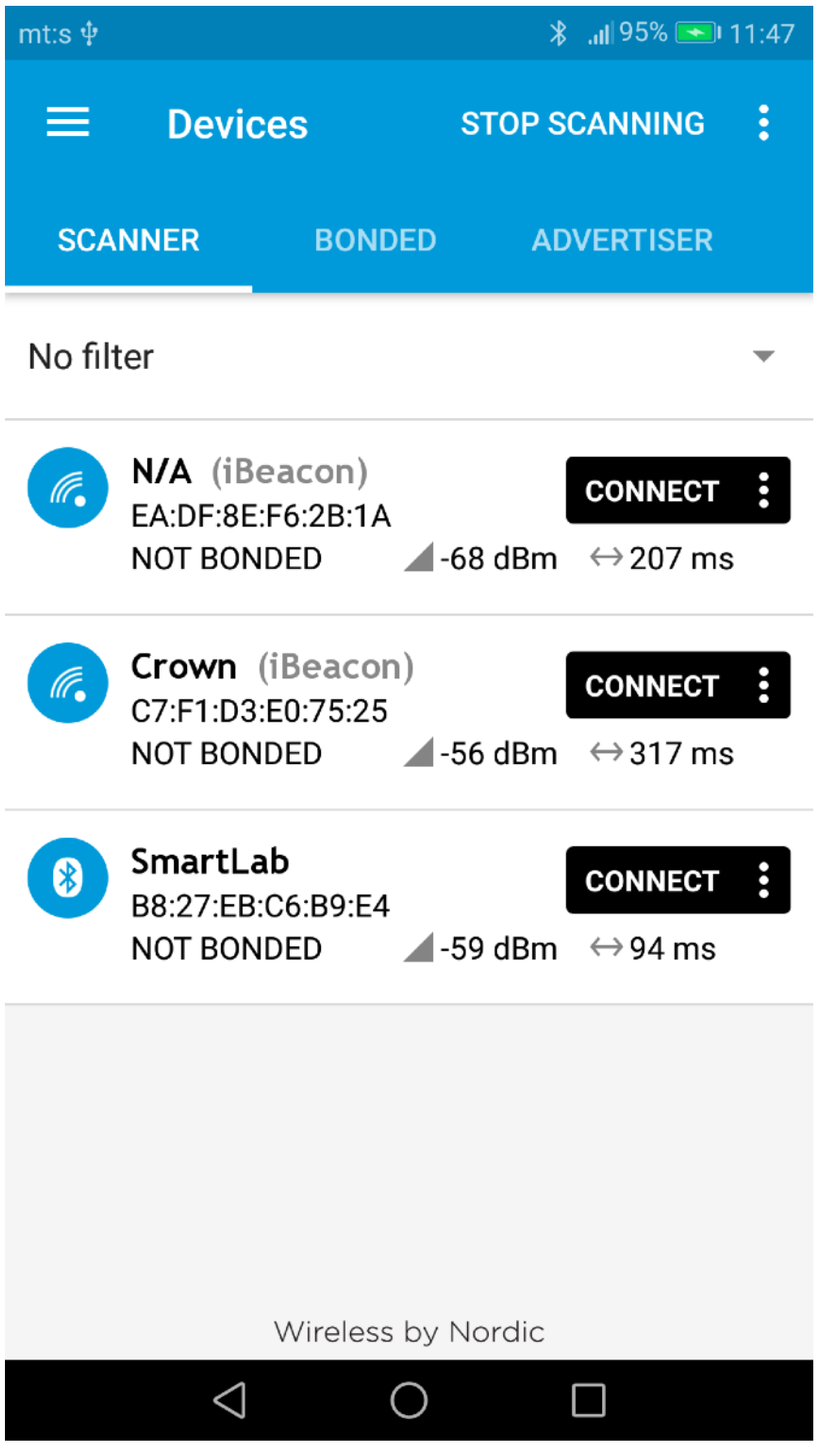
```
BOOTSPI
BIST0_OK
_OK!decomp
_done
done

Hello U-Boot

U-Boot 1.1.6 (Aug 22 2016 - 16:45:10)

Board: MSTAR KRITI (CPU Speed 576 MHz)
DRAM:  64 X 0 MBytes
U-Boot is running at DRAM 0x87610000
Module: USB FAT FLASH SPI LOGO OSD ENV=SERIAL
Flash is detected (0x0C02, 0xC8, 0x40, 0x16)
In:    serial
Out:   serial
Err:   serial
MSVC00B000100100208768TH0000000T
MDrv_PNL_Init u32PnlRiuBaseAddr = BF200000
MDrv_PNL_Init u32PMRiuBaseAddr = BF000000
DAC eTiming =6
HDMITx eTiming =7
HDMITx eTiming =7
Create Dolby single part name task failed!!
[Hal_VE_EnableDI][1430] bEnable = 0, bIsDNR2VE = 0
u32ReadBuffVirAddr = A0000000, u32IntBuffVirAddr = A0100000, u32OutBuffVirAddr = A0730000
verJPD_SetStatus >>>>>>>>>>> w:720,  h:576,  p:720

[GOP3, PID 0, TID 0x-1][Driver Version]: 0089, BuildNum: 0002, ChangeList: 00524916
 keypad_pressed is [0]
 ir_pressed is [0]
<< MStar >>#
```

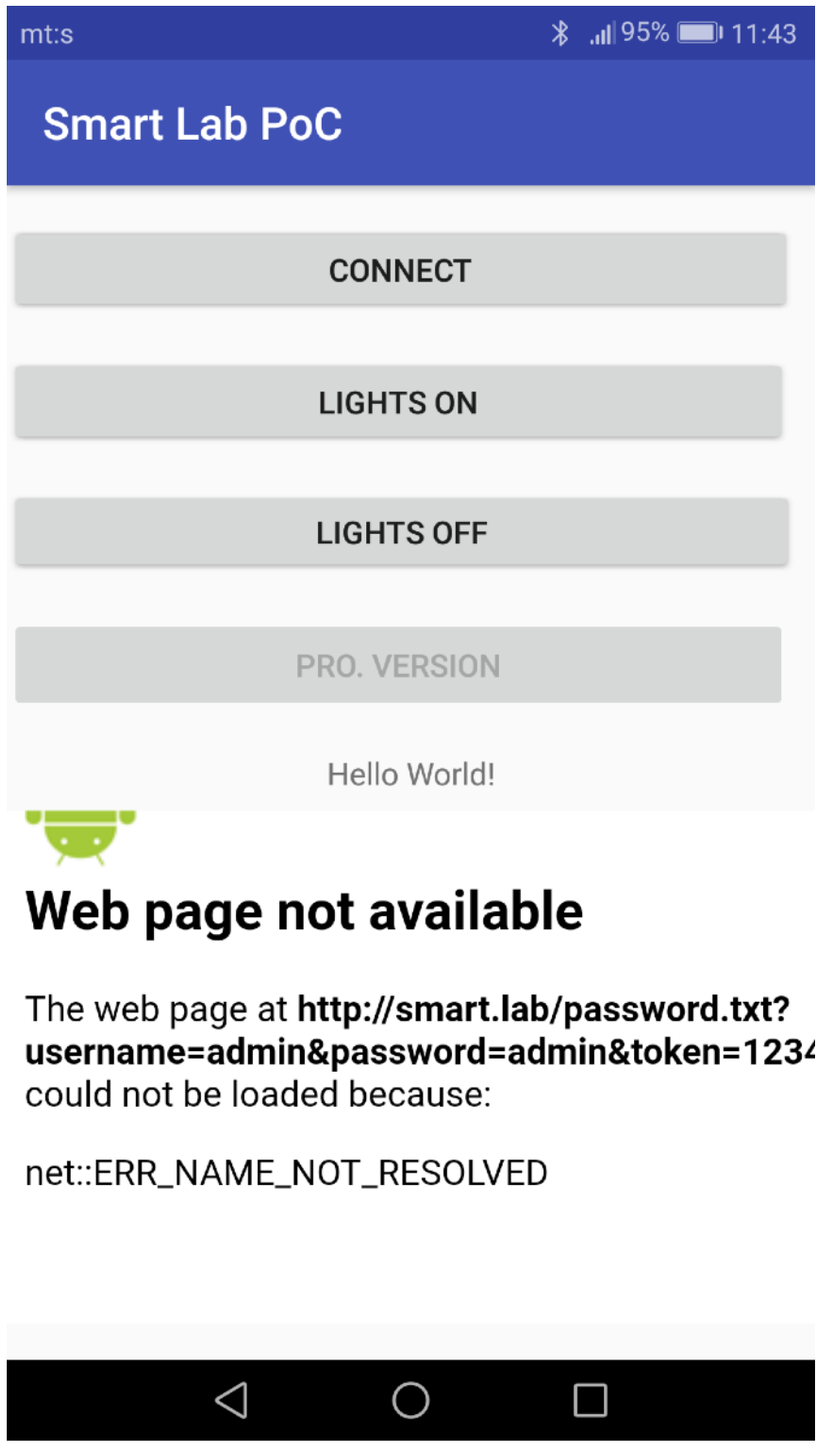
Our Laboratory for today (2)



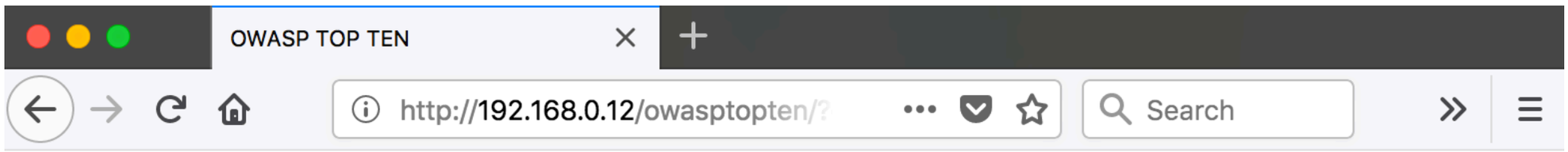
WiFi/LAN Router, 2 x Raspberry Pi 3, 2 x Temperature/Humidity Sensors, 2 x BLE Plugs + Fan’s, USB WebCam, 3 x LEDs

Our Laboratory for today (2)





Our Laboratory for today (3)



Username:

Password:

Open Sesame

Groups () for this user!

Select image to upload: Browse... No file selected. Upload Image

---

DEBUG SQL: SELECT * FROM users WHERE username = '' AND password = '' LIMIT 1
ERROR DESCRIPTION: You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near '' AND password = '' LIMIT 1' at line 1
Content here!

Why is so important to take care about security and privacy

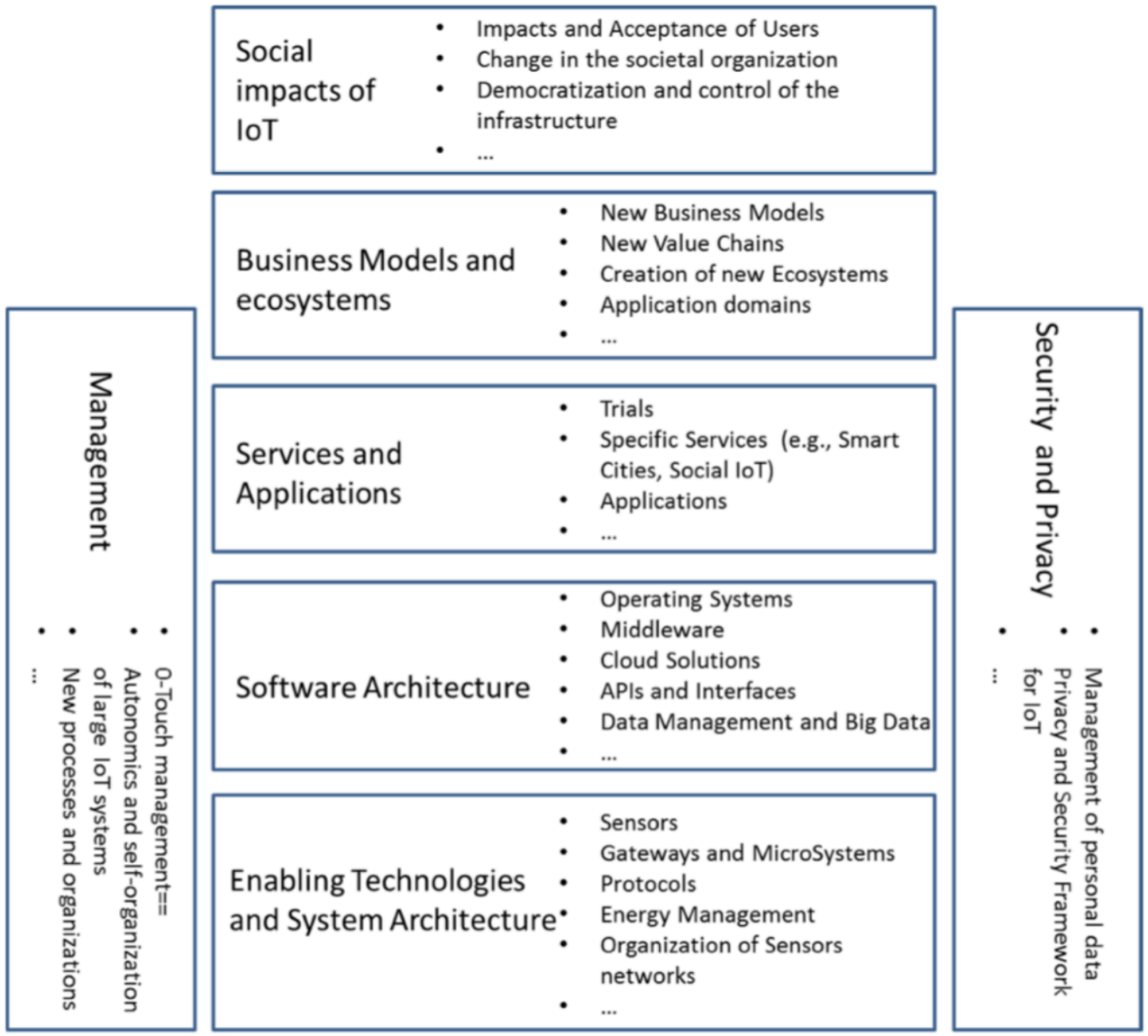


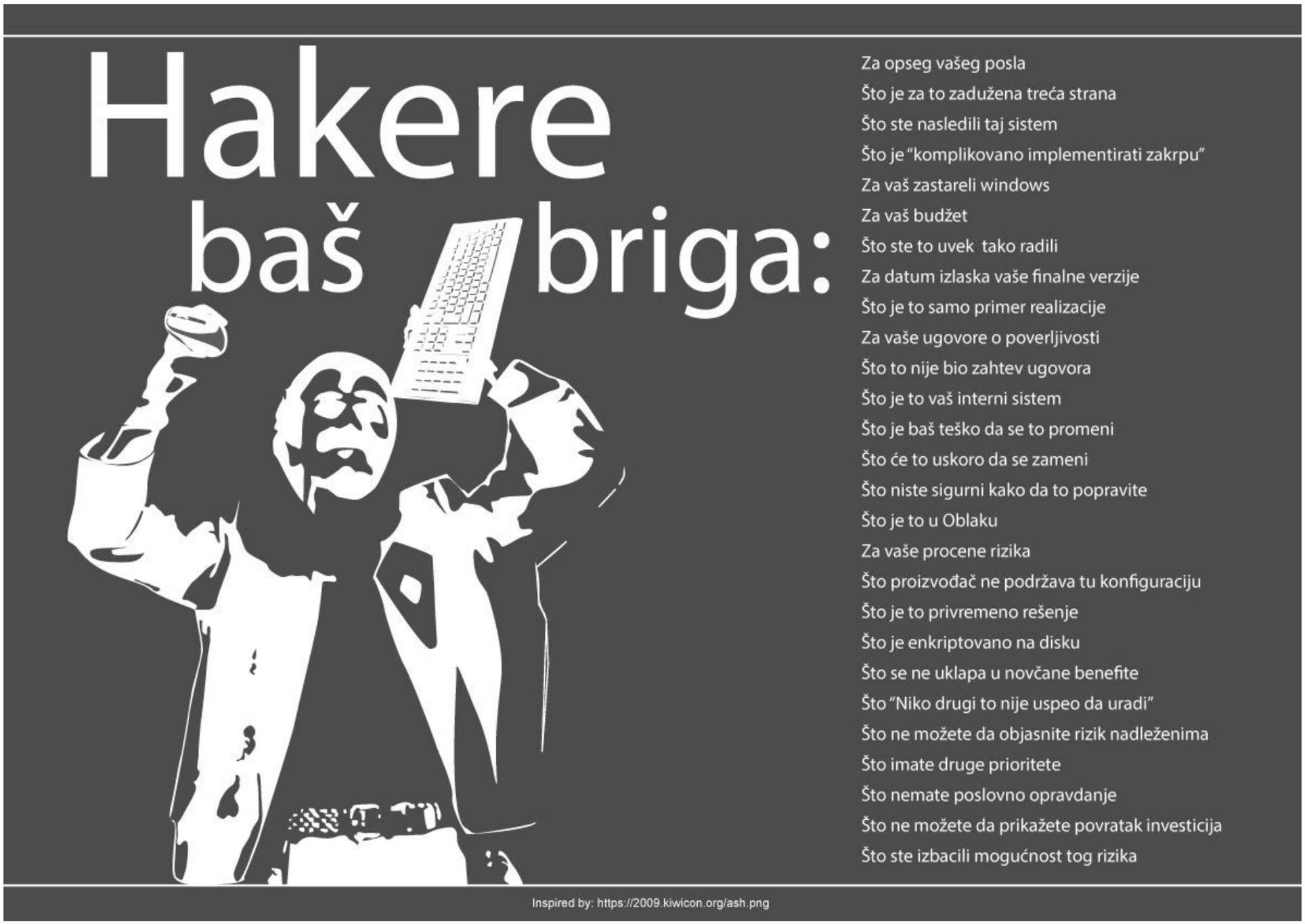
Figure 1. Technological and social aspects related to IoT

Why is so important to take care about security and privacy

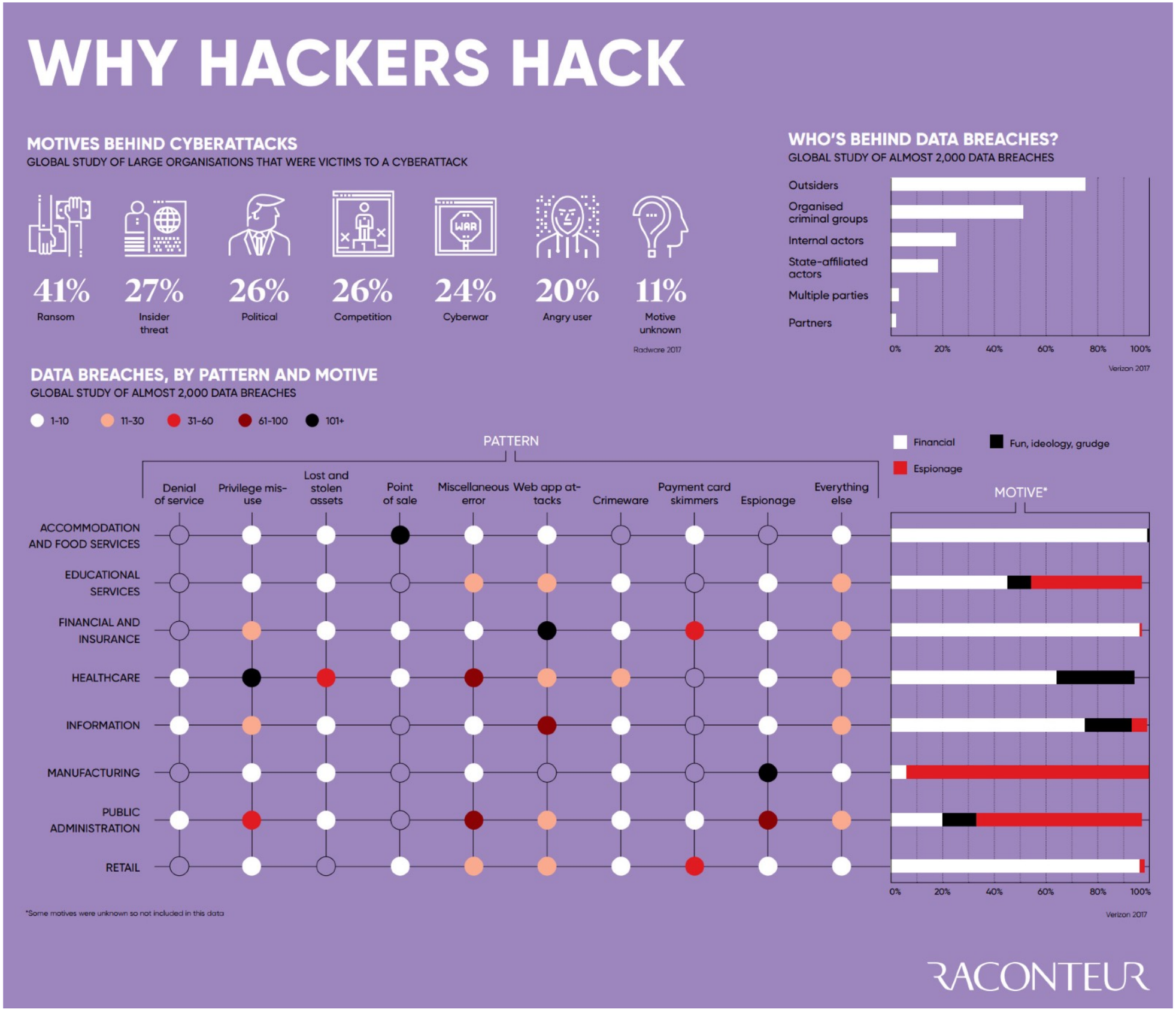
- IoT is all about data and control
- No One's Telling You Your Data Is Valuable
- Limit on Power / Control / Manipulation
- Regulatory compliance

Why is so important to take care about security and privacy

Why is so important to take care about security and privacy



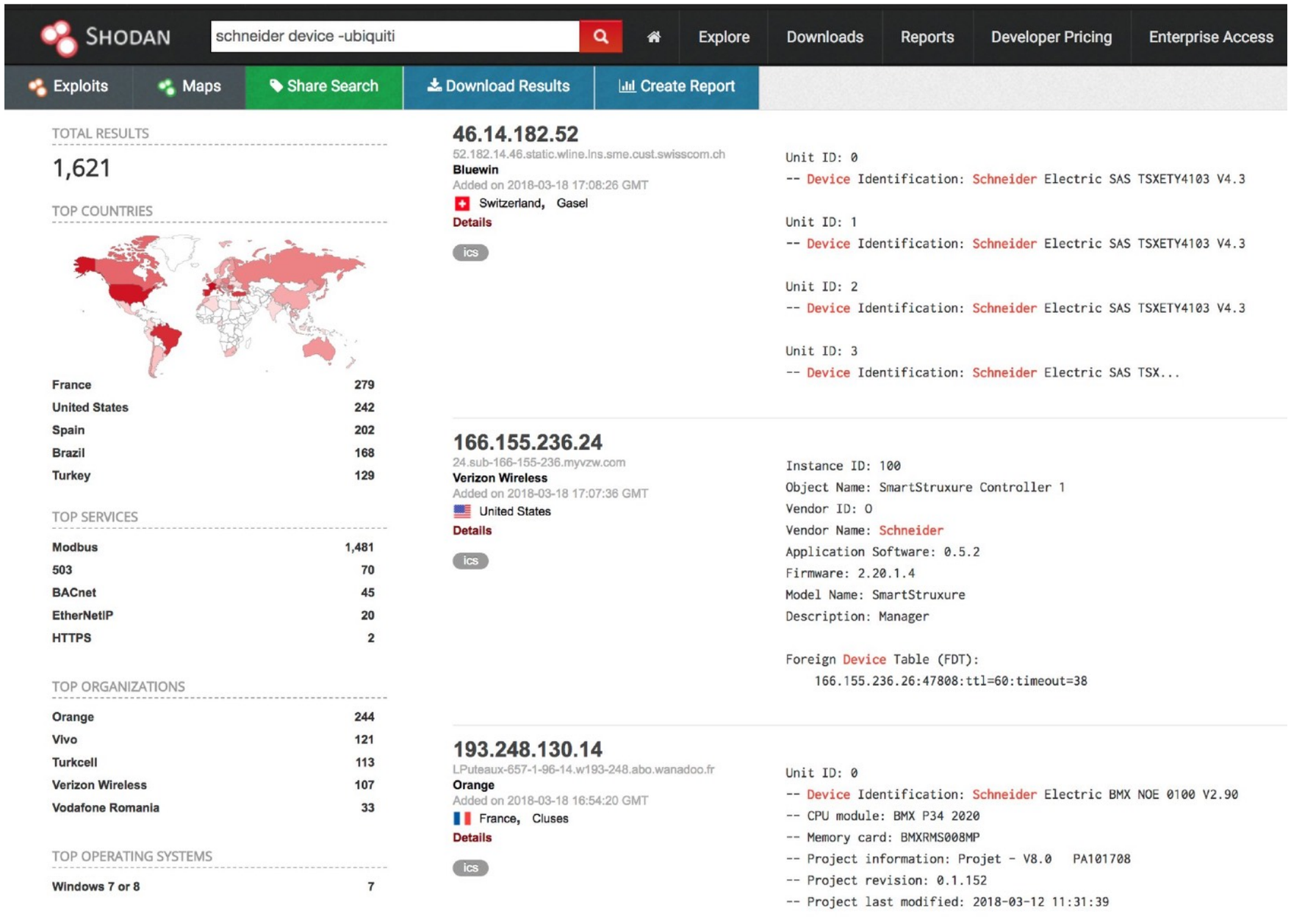
Why is so important to take care about security and privacy



Why is so important to take care about security and privacy

HACKING TOOLS & SERVICES	
Account Hacking Program	**$12.99** (See more details on page 10)
Hacked Instagram Accounts in Bulk	1,000 - 10,000 accounts **$15 - $60**
Botnet: Blow-Bot Banking Botnet	Monthly Basic Rental **$750** | Monthly Full Rental **$1,200** | Monthly Support **$150**
Disdain Exploit Kit	Day **$80**, Week **$500**, Month **$1,400**
Stegano Exploit Kit: Chrome , FireFox, Internet Explorer, Opera, Edge	Unlimited Traffic, Day **$2,000** Unlimited Traffic, Month **$15,000**
Microsoft Office Exploit Builder	Lite exploit builder **$650** Full Version **$1,000**
WordPress Exploit	**$100**
Password Stealer	**$50**
Android Malware Loader	**$1,500**
Western Union Hacking Bug For World Wide Transfer	**$300**
DDoS Attacks	Week long attack **$500 - $1,200**
ATM Skimmers: Wincor, Slimm, NCR, Diebold	**$700 - $1,500**
Hacking Tutorials	Multiple Tutorials **$5 - $50**

Why is so important to take care about security and privacy



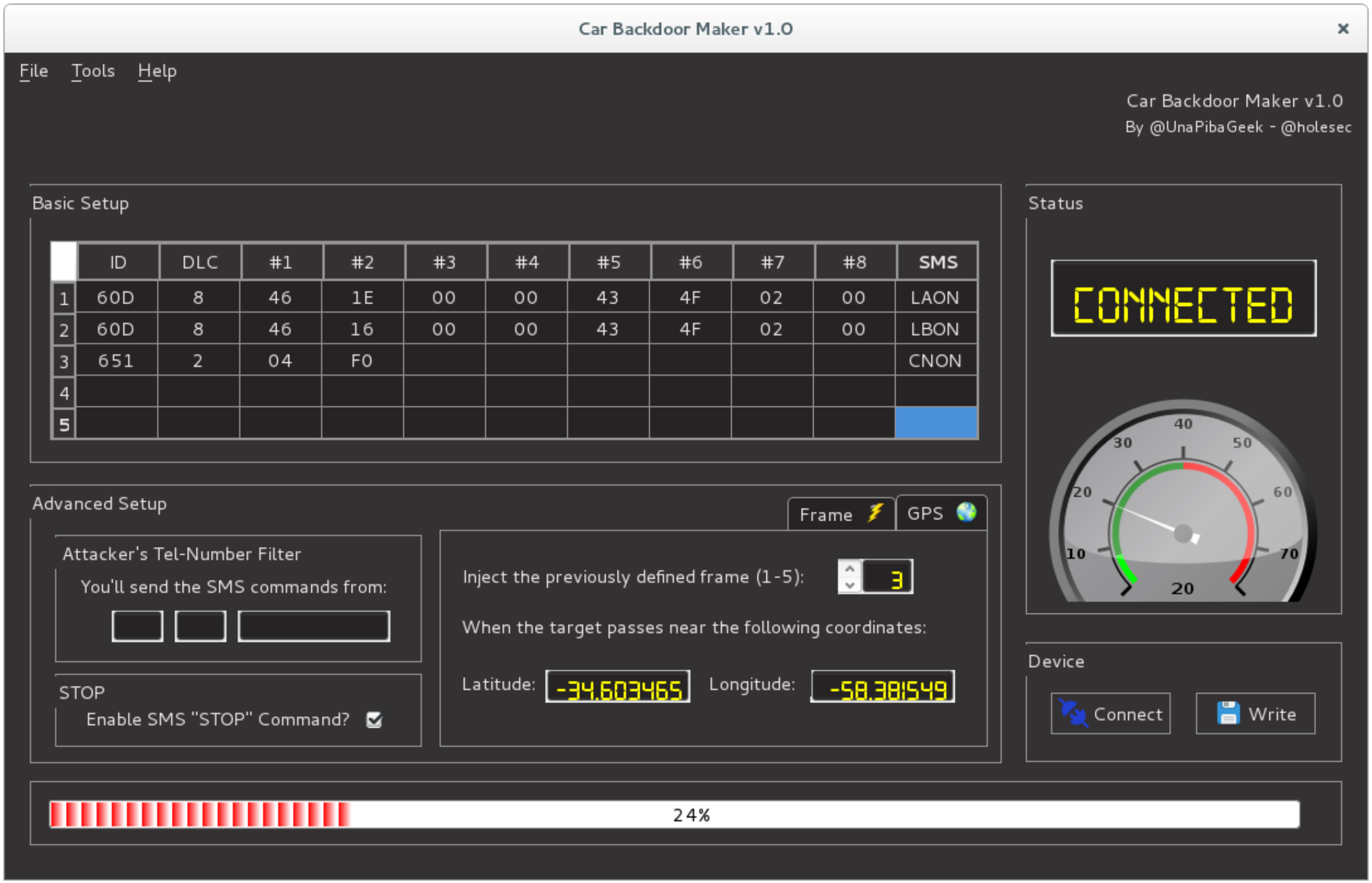
Why is so important to take care about security and privacy

Autosploit marries Shodan, Metasploit, puts IoT devices at risk

Autosploit marries Shodan, Metasploit, puts IoT devices at risk

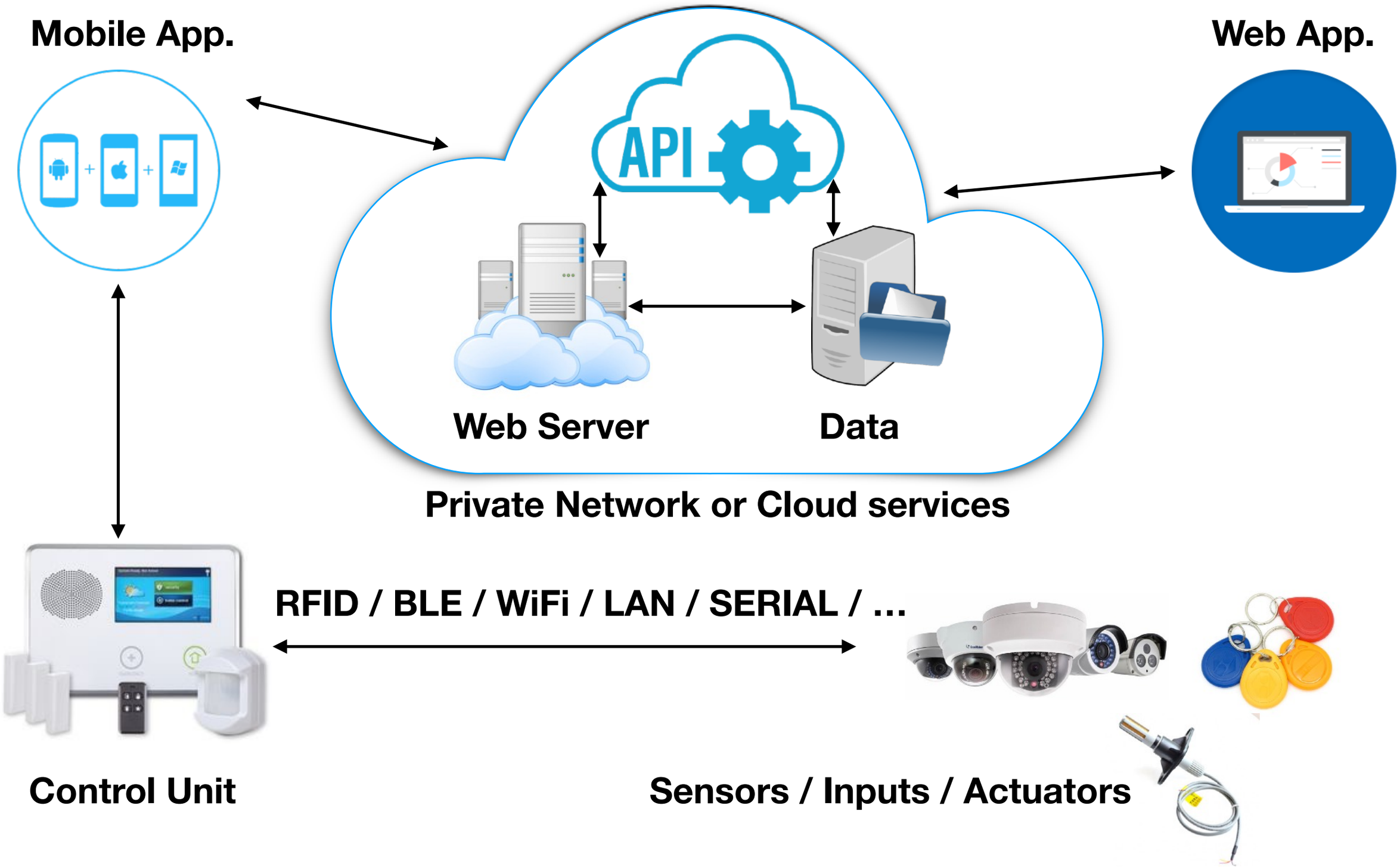
scmagazine.com

Why is so important to take care about security and privacy

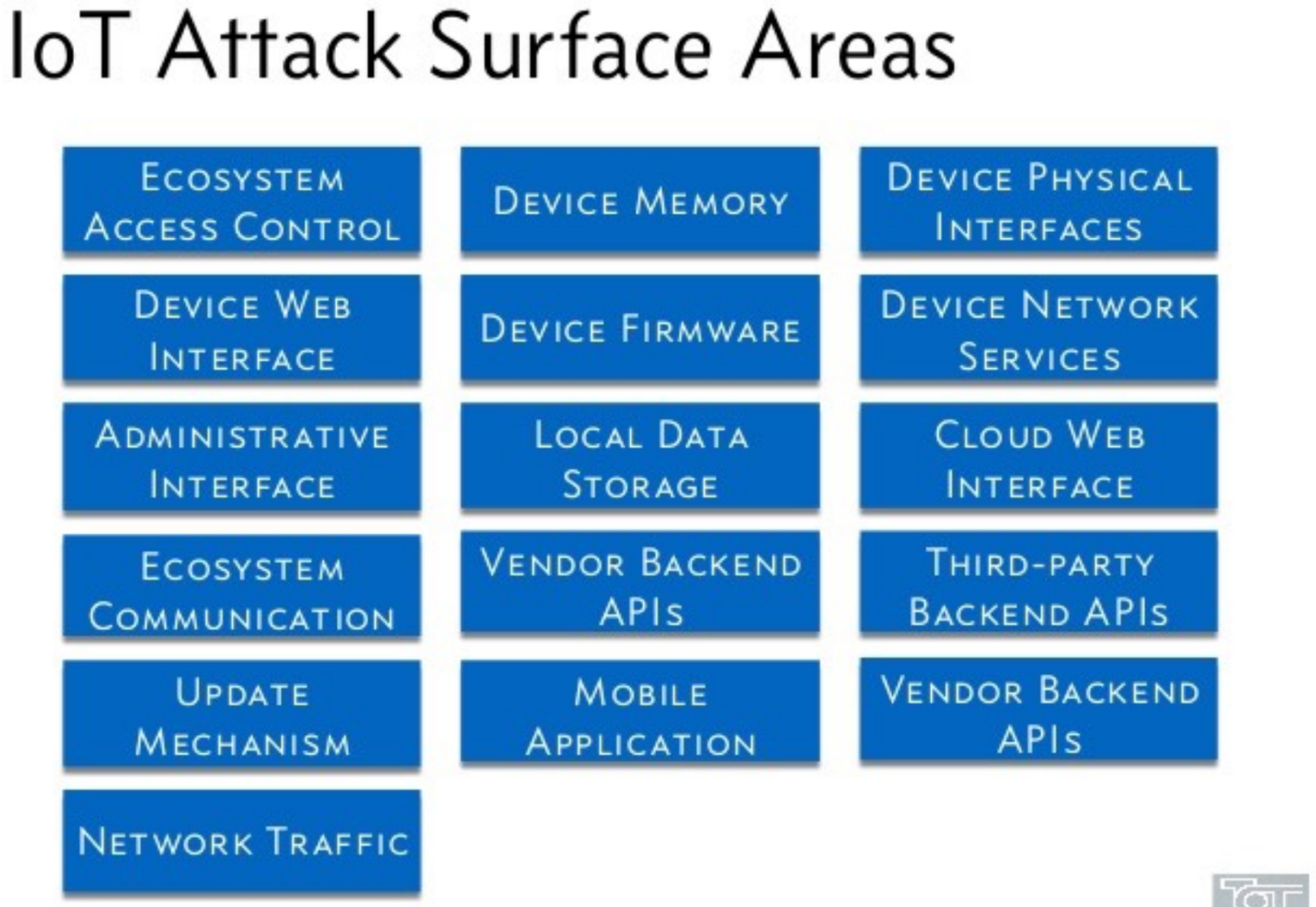


What and where are the main threats

- Common IoT Architecture -



What and where are the main threats



What and where are the main threats

Ecosystem

Interoperability standards
Data governance
System wide failure
Individual stakeholder risks
Implicit trust between components
Access procedures

Ecosystem Communication

Health checks
Heartbeats
Ecosystem commands
De-provisioning
Pushing updates

IoT Ecosystem Example

The Healthcare Internet of Things (IoT) Market Map

Clinical Efficiency

AUGMEDIX
TeleTracking
fruit street
AdhereTech
Obaa
simplifeye
PRISTINE
VOLUNTIS
Connected Therapeutics
awarepoint
Location as a Service
evermind

Clinical-Grade Biometric Sensors

QUANTTUS
vitalconnect
mc10
Senseonics
BL Healthcare
connectedhealth
Sotera WIRELESS
iRhythm
proteus DIGITAL HEALTH
EarlySense
Monica Healthcare
EYENETRA
SilentAlert
Resident Monitor System

Consumer / Home Monitoring

sano
GlucoVista
aira
QARDIO
WHOOP
CHRONO THERAPEUTICS
BIOSERENITY
SUNSPRITE
kinsa
TURINGSENSE
INFOBIONIC
SCANADU
cue
AliveCor
THALMICLABS
ANGEL SENSOR
3rings

Created By

CB INSIGHTS

Infant Monitoring

Sproutling
BABYBE
mimo
Owlet
Rest Assured.

Sleep Monitoring

beddit
NovaSom
hello

Fitness Wearables

sensoria
LUMO
OMsignal
lark
motiv
ATHOS
ATLAS
moov
Withings
Inspire health
MISFIT
JAWBONE

Brain Sensors / Neurotechnology

NEUROVIGIL
JAN Medical
Thync
How good feels
muse
ybrain
NeuroSky
halo
neuroscience

www.cbinsights.com

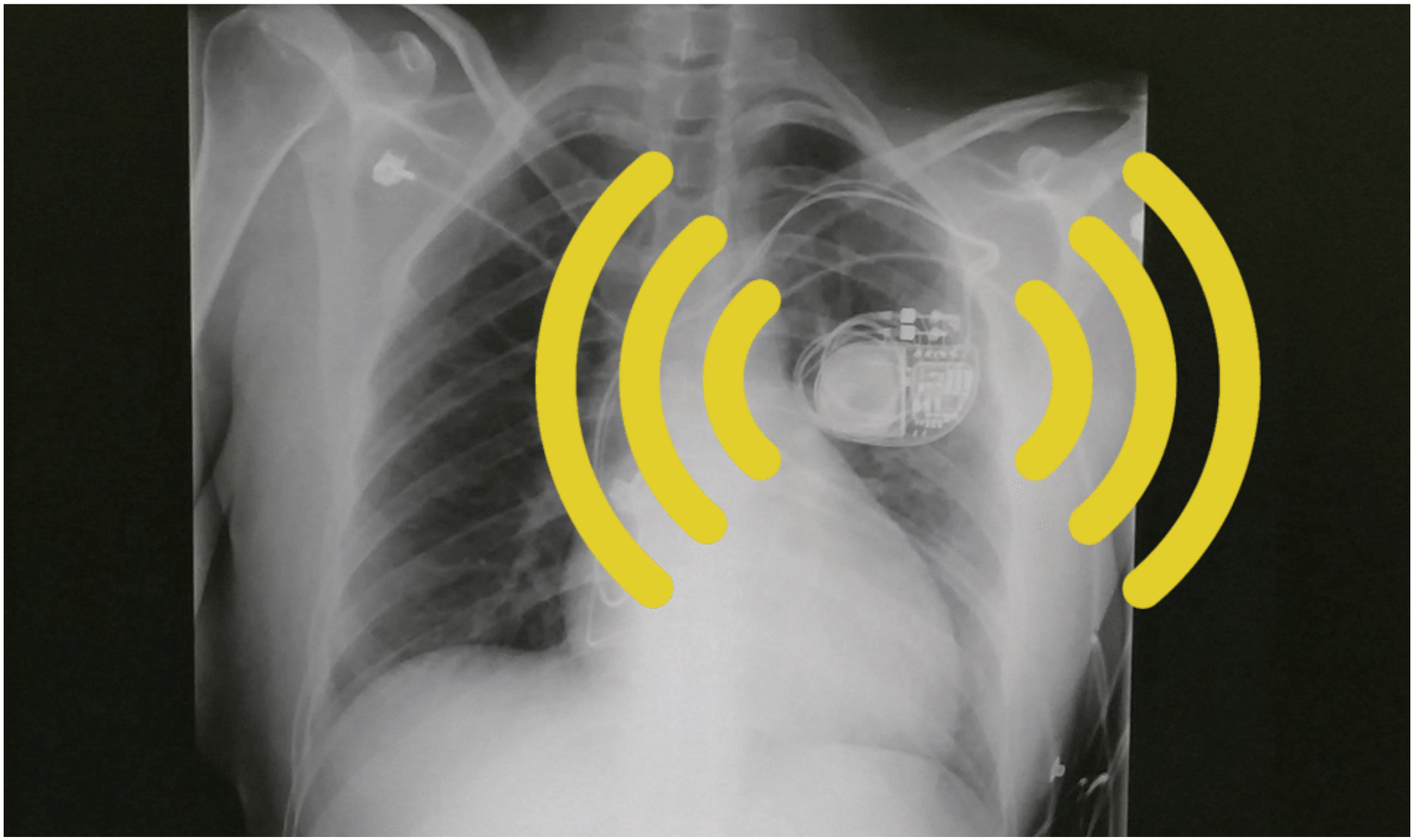
IoT Ecosystem services providers

Business	Hardware	Software	Network	Cloud	AI/ML
Pricing - Upfront - Recurring - Subsidized - Free **Relationship** - Direct - VAR - Service only - None **Distribution** - New distribution models **New info** - Customer Habits - Production tech - Regulations	intel ARDUINO NXP ARM freescale semiconductor	OS WIND RIVER ROCKET WIND RIVER PULSAR LINUX VxWorks yocto PROJECT Windows 10 debian ubuntu Frameworks RAILS php node HTML Java python Microsoft .NET Lua jQuery	Protocols WiFi ZigBee LoRa SIGFOX One network A billion dreams Z-WAVE 6LoWPAN 4G LTE	Platforms amazon web services Microsoft Azure ORACLE CLOUD PLATFORM Google Cloud Platform IBM Bluemix rackspace openstack	Frameworks - Amazon ML - Apache Spark - Apache Singa - Brainstorm - Caffe - Google TensorFlow - Marvin - Microsoft Azure ML - Microsft DMTK - Microsoft CNTK - Mlpack2

Constraining any one dimension affects others

Pace of innovation is picking up

This is also a part of IoT Ecosystem



This is also a part of IoT Ecosystem

What and where are the main threats

Hardware / Device

Sensors

Device Physical Interfaces

Device Memory

Device Firmware

Device Web Interface

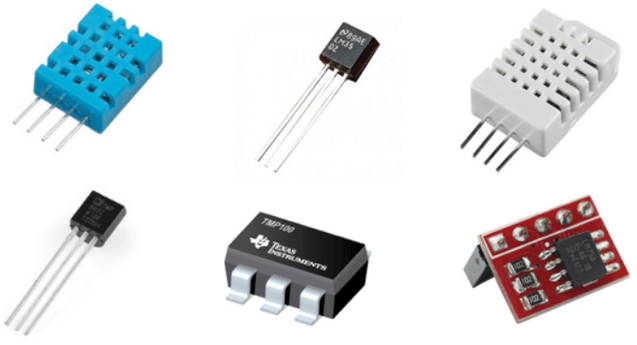
Device Network Services

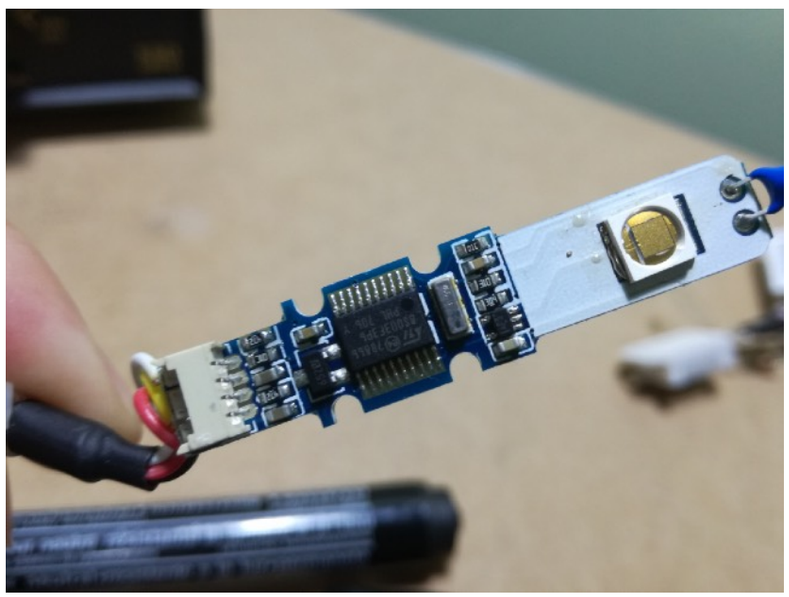
Update Mechanism

What and where are the main threats

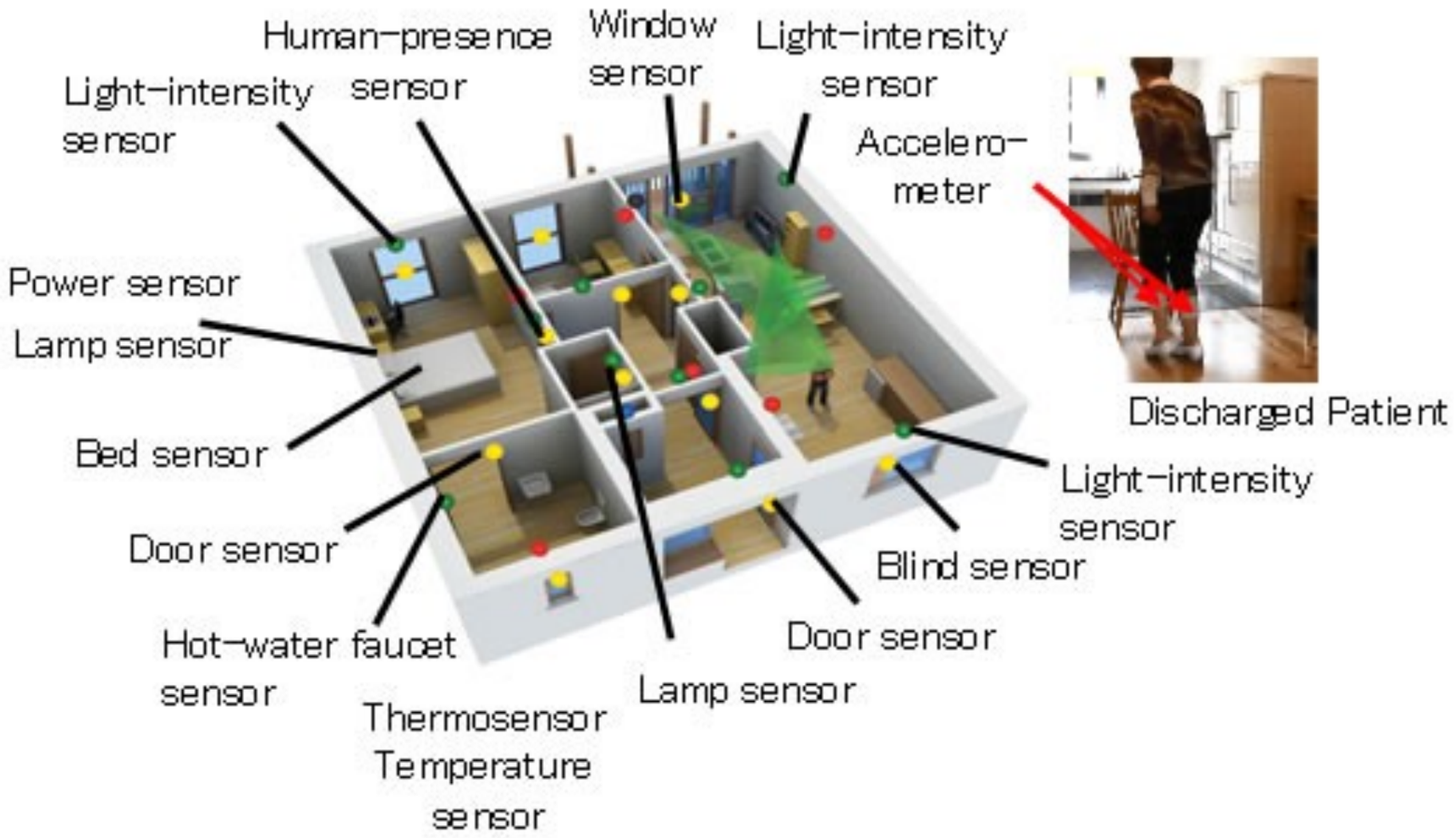
Sensors

Sensing Environment Manipulation
Tampering (Physically)
Damage (Physically)

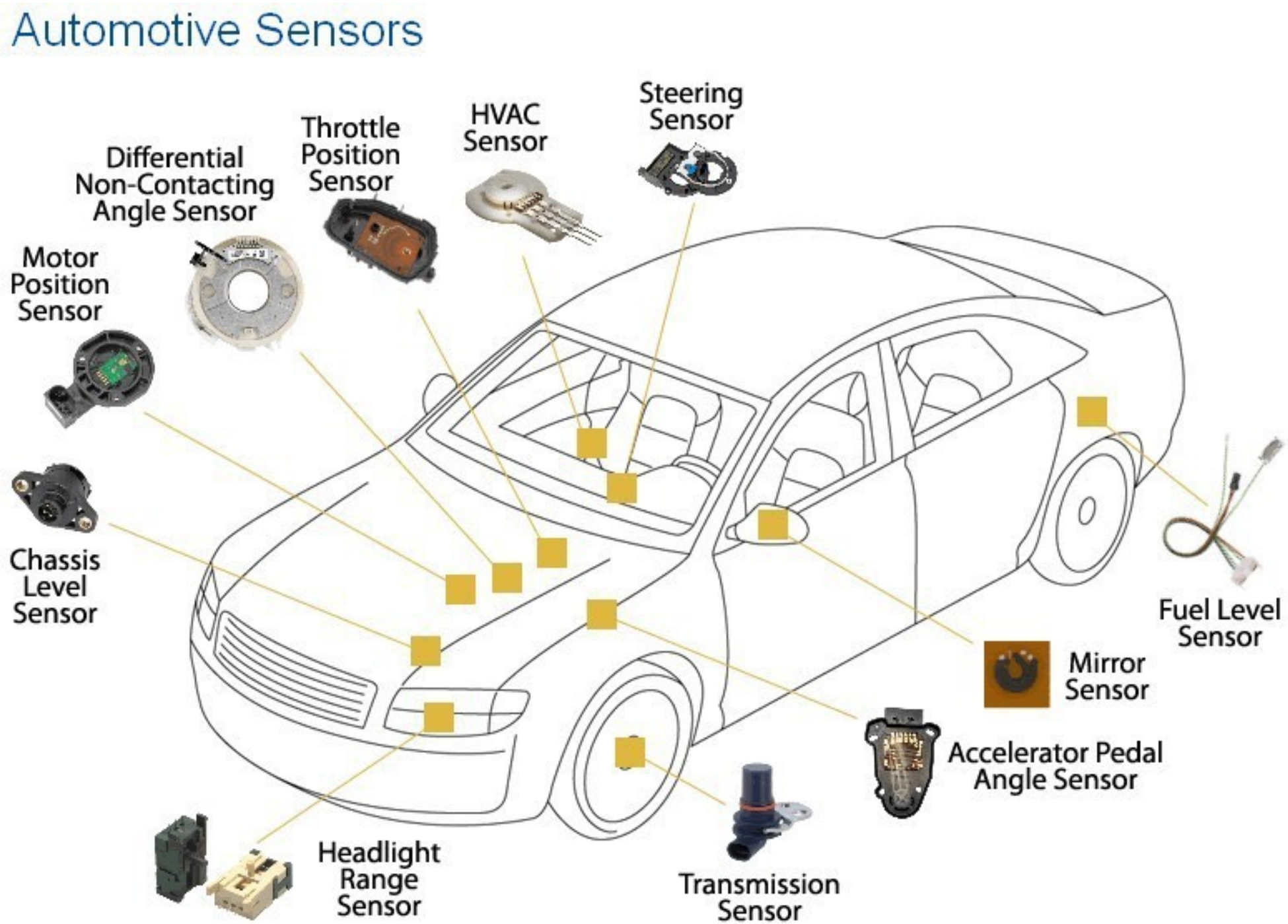




Sensors in Smart Home



Sensors in your Car

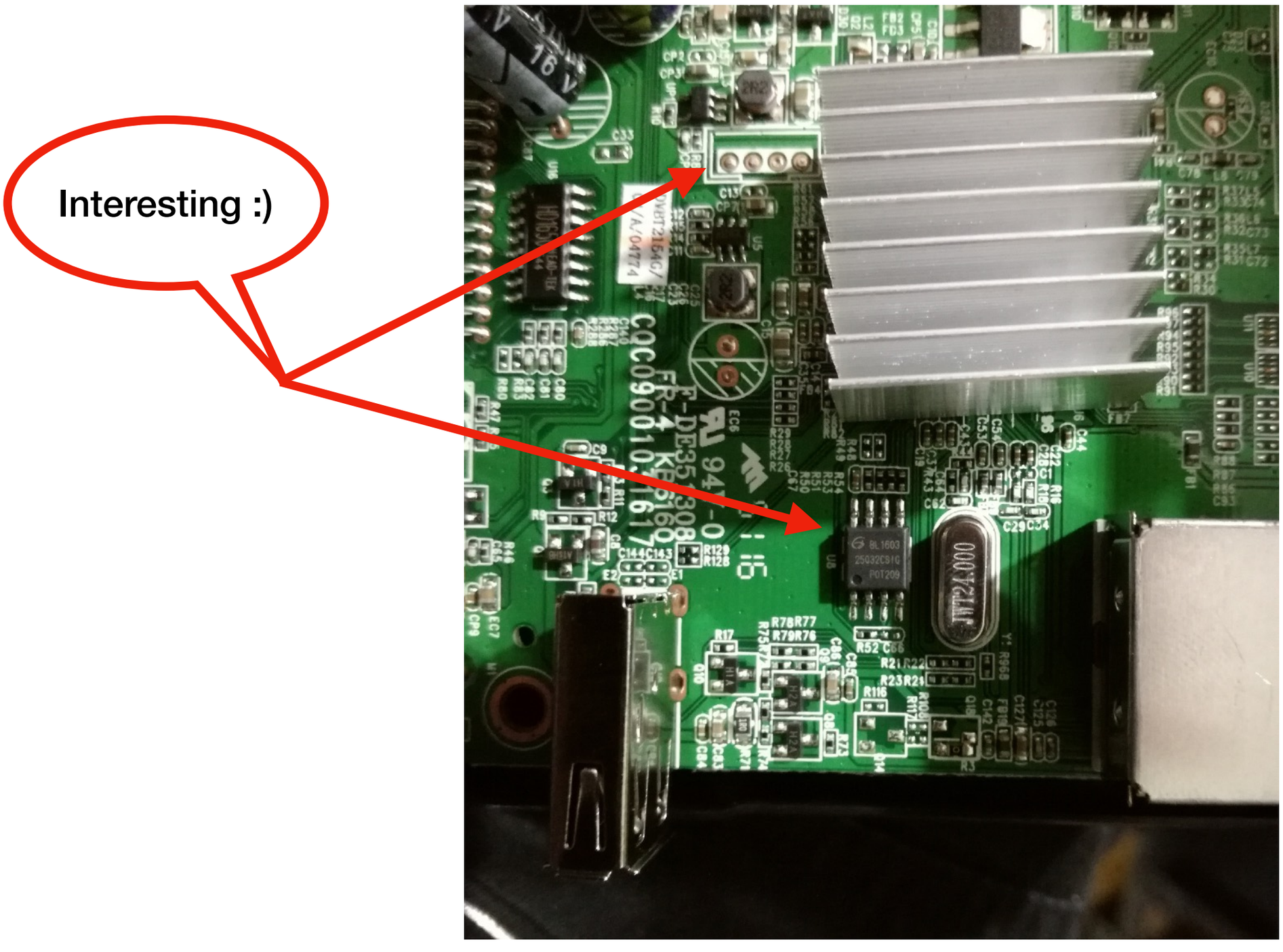


What and where are the main threats

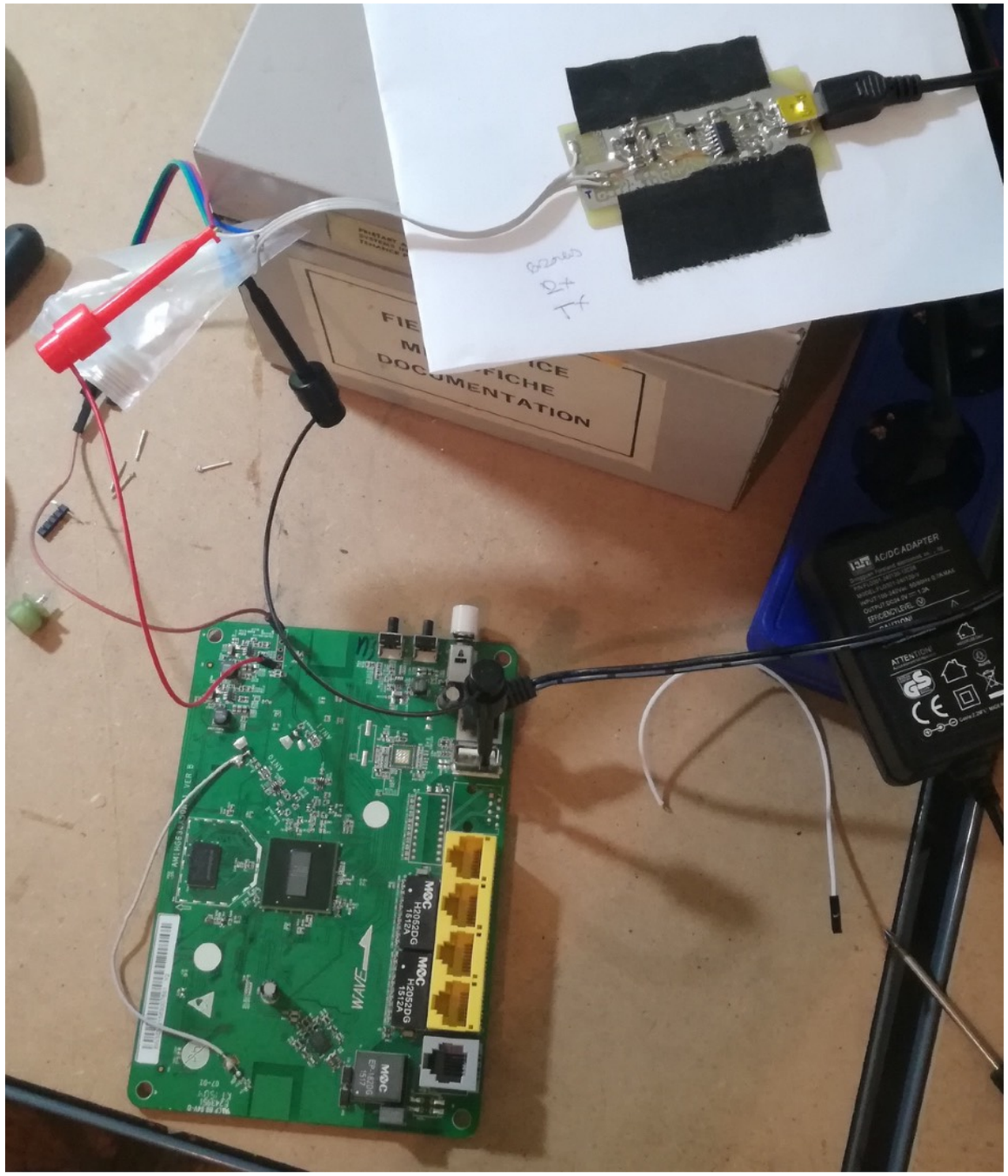
Device Physical Interfaces

Device ID / Serial number exposure
Firmware extraction
User CLI
Admin CLI
Privilege escalation
Reset to insecure state
Removal of storage media
Tamper resistance
UART (Serial)
JTAG / SWD

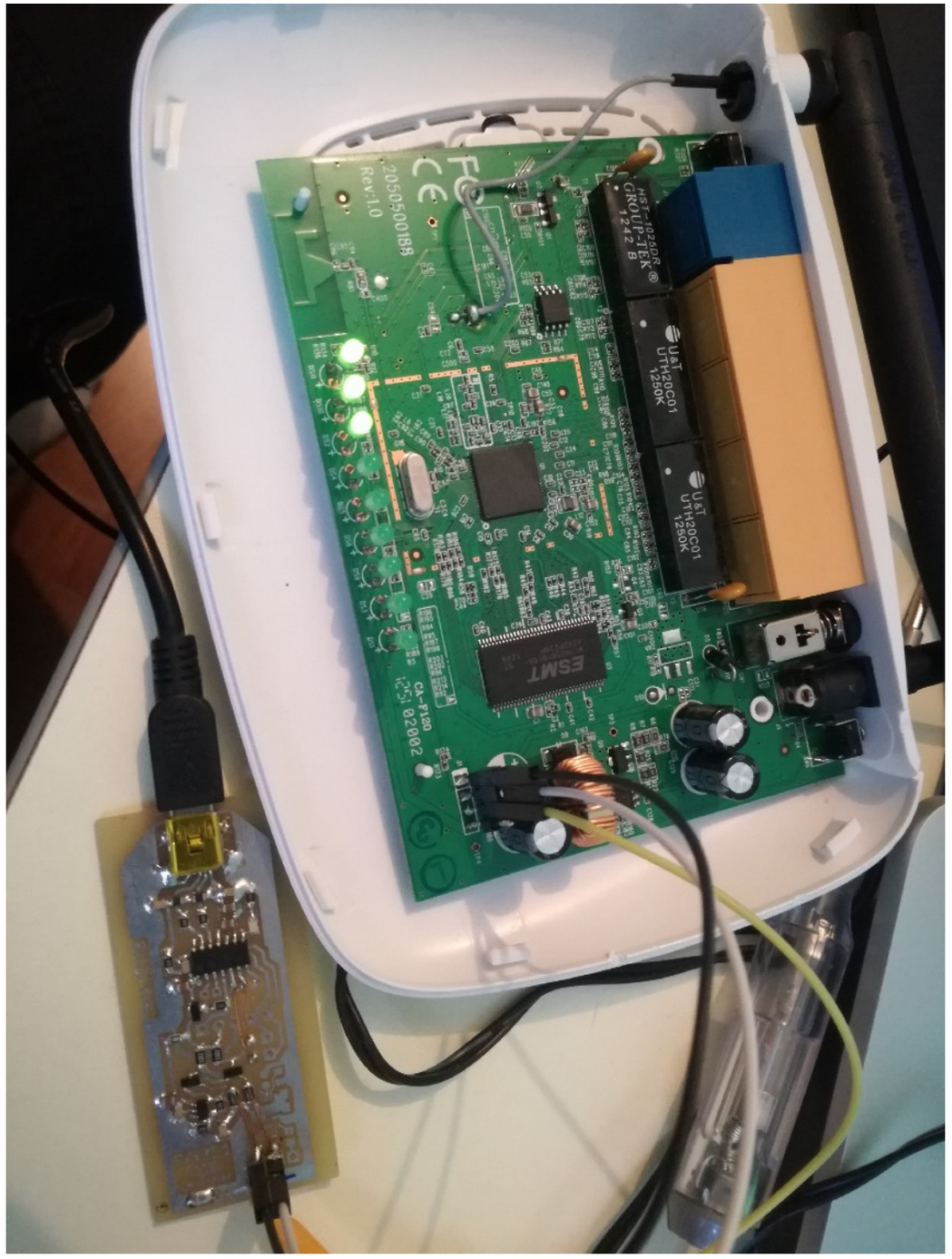
Device Physical Interfaces in MSTAR / Vivax Set-up Box



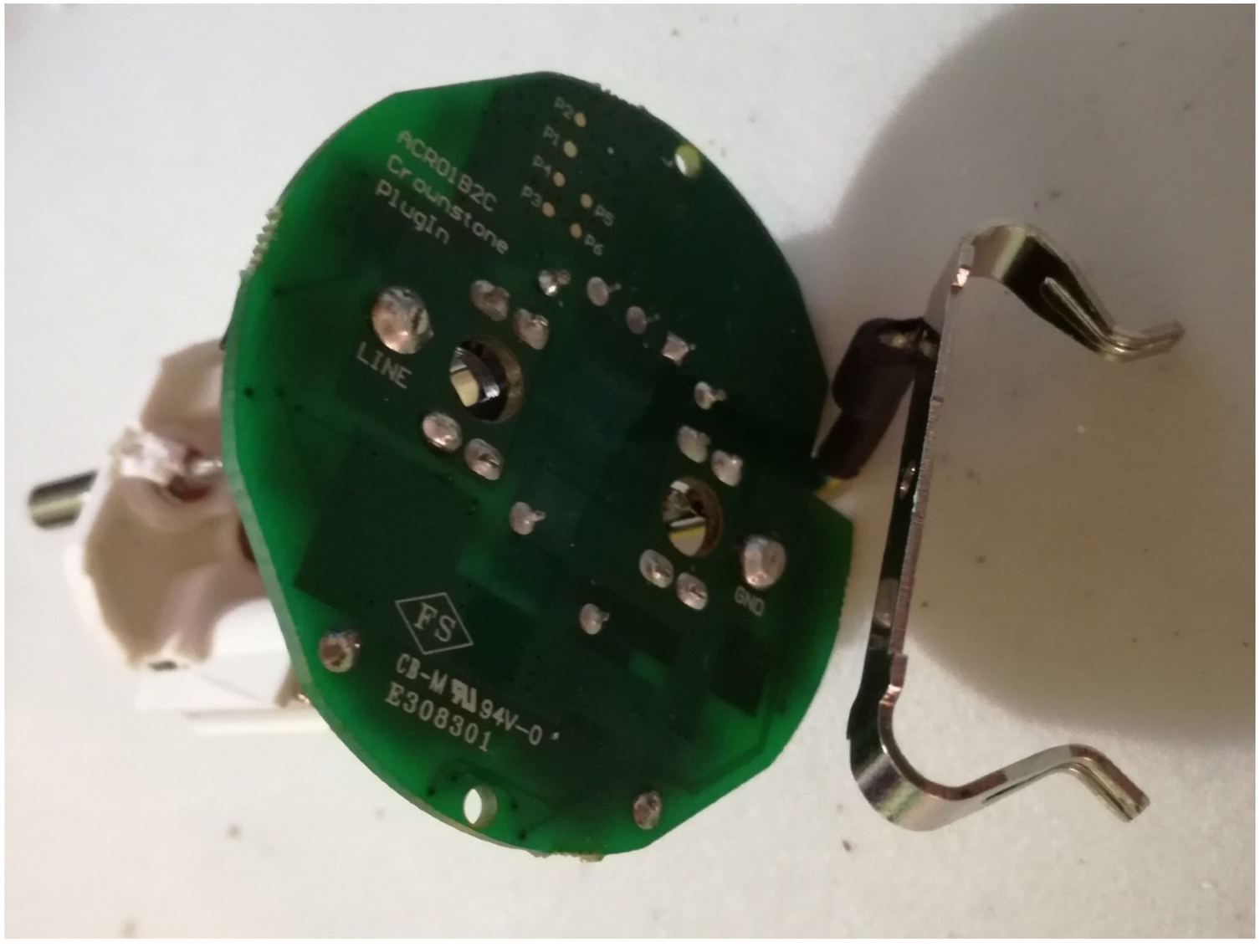
Device Physical Interfaces in HUAWEI / Telekom ADSL routers



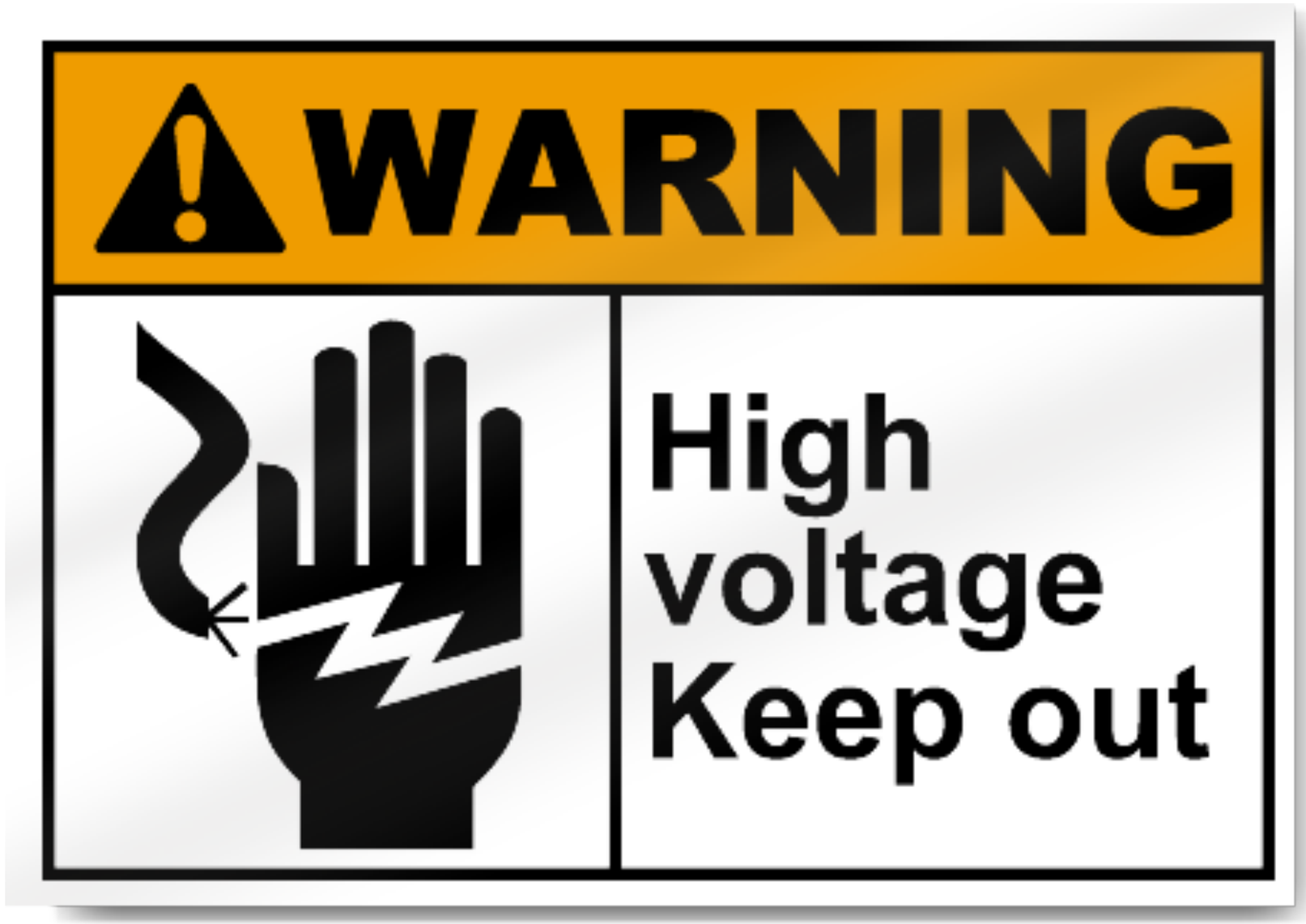
Device Physical Interfaces in TP-LINK router



Device Physical Interfaces in Crownstone smart power plugs



Device Physical Interfaces



What and where are the main threats

Device Memory

Sensitive data
Cleartext usernames
Cleartext passwords
Third-party credentials
Encryption keys
PIN codes

What and where are the main threats

Device Firmware

Sensitive data exposure
Backdoor accounts
Hardcoded credentials
Encryption keys
Vulnerable services and software versions
Security related function API exposure
Firmware downgrade possibility

What and where are the main threats

Device Firmware

Hard-coded password exposes up to 46,000 video surveillance DVRs to hacking

Hackers can log into DVRs from RaySharp and six other vendors using a six-digit hard-coded root password

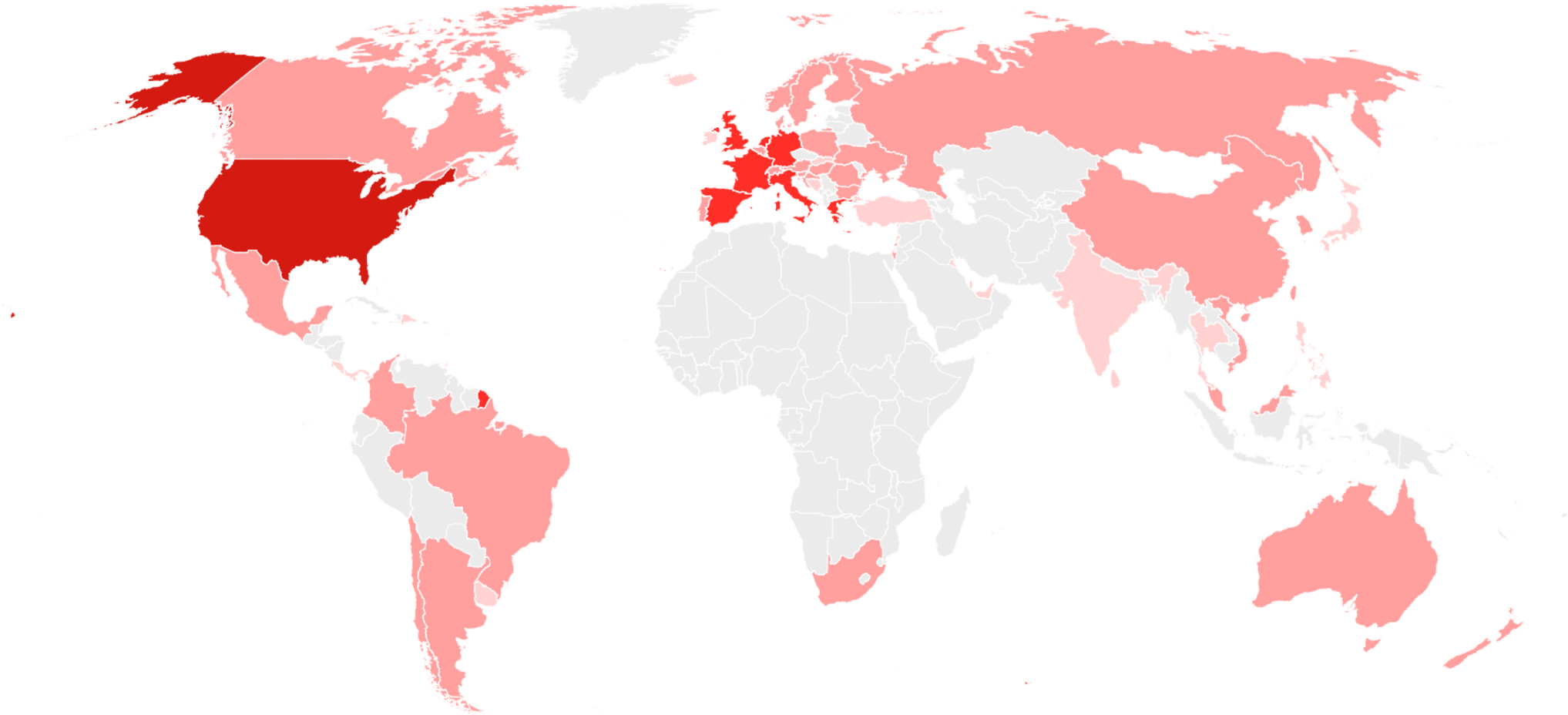
Internet cameras have hard-coded password that can’t be changed

Cameras with multiple brand names are wide open to remote hacking.

Vulnerable Device Firmware

The following devices are known to be vulnerable:

Model Name	System Firmware Version	Application Firmware Version
Opticam i5	1.5.2.11	2.21.1.128
Foscam C2	1.11.1.8	2.72.1.32



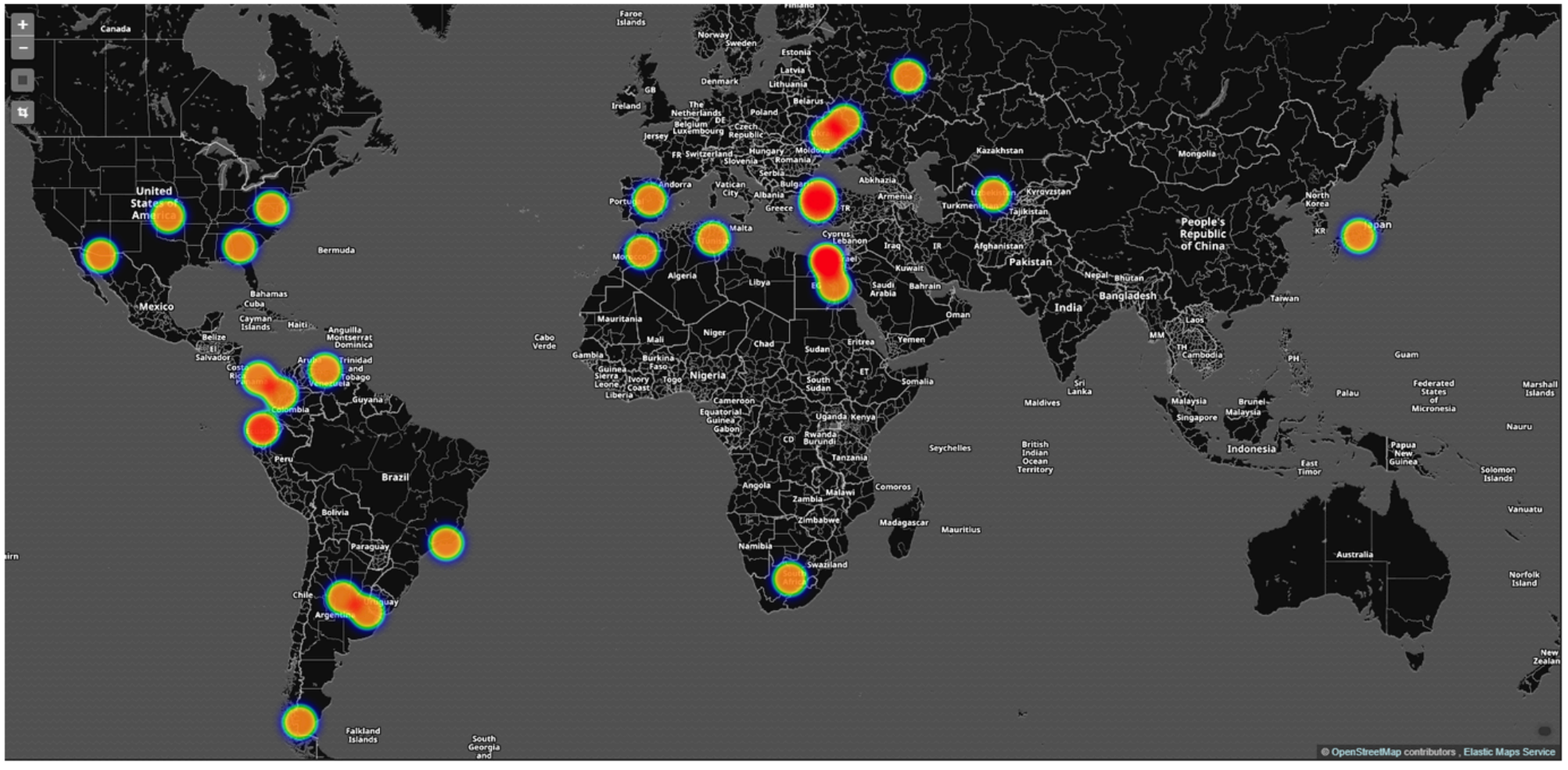
Tens of thousands of potentially vulnerable devices are exposed to the internet around the world.

What and where are the main threats

Device Network Services

Information disclosure
User or Administrative CLI
Command Injection
Denial of Service
Unencrypted Services
Test / Development Services
Credential management vulnerabilities
Buffer Overflow
UPnP

Huawei HG532 UPNP Botnet



What and where are the main threats

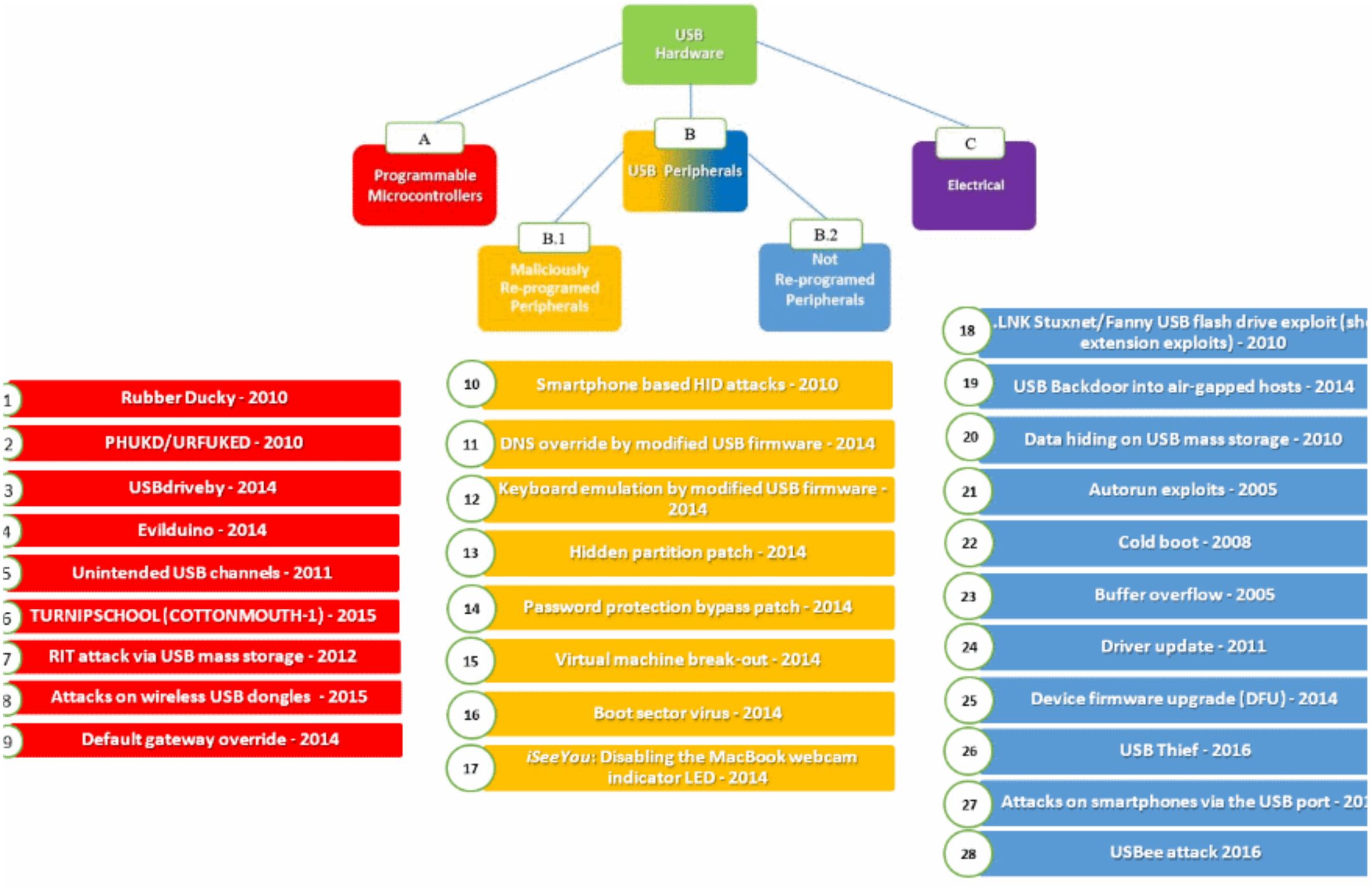
Update Mechanism

Update sent without encryption
Updates not signed
Update location writable
Update verification
Update authentication
Malicious update
Missing update mechanism
No manual update mechanism

USB firmware update

- auto_update / bin / zip / …
- auto_upgrade / bin / zip / …
- …

General USB attacks



What and where are the main threats

Network Traffic

Wireless (WiFi, Z-wave, XBee, Zigbee, Bluetooth, LoRA)
LAN, LAN to Internet
Non-standard, Protocol fuzzing

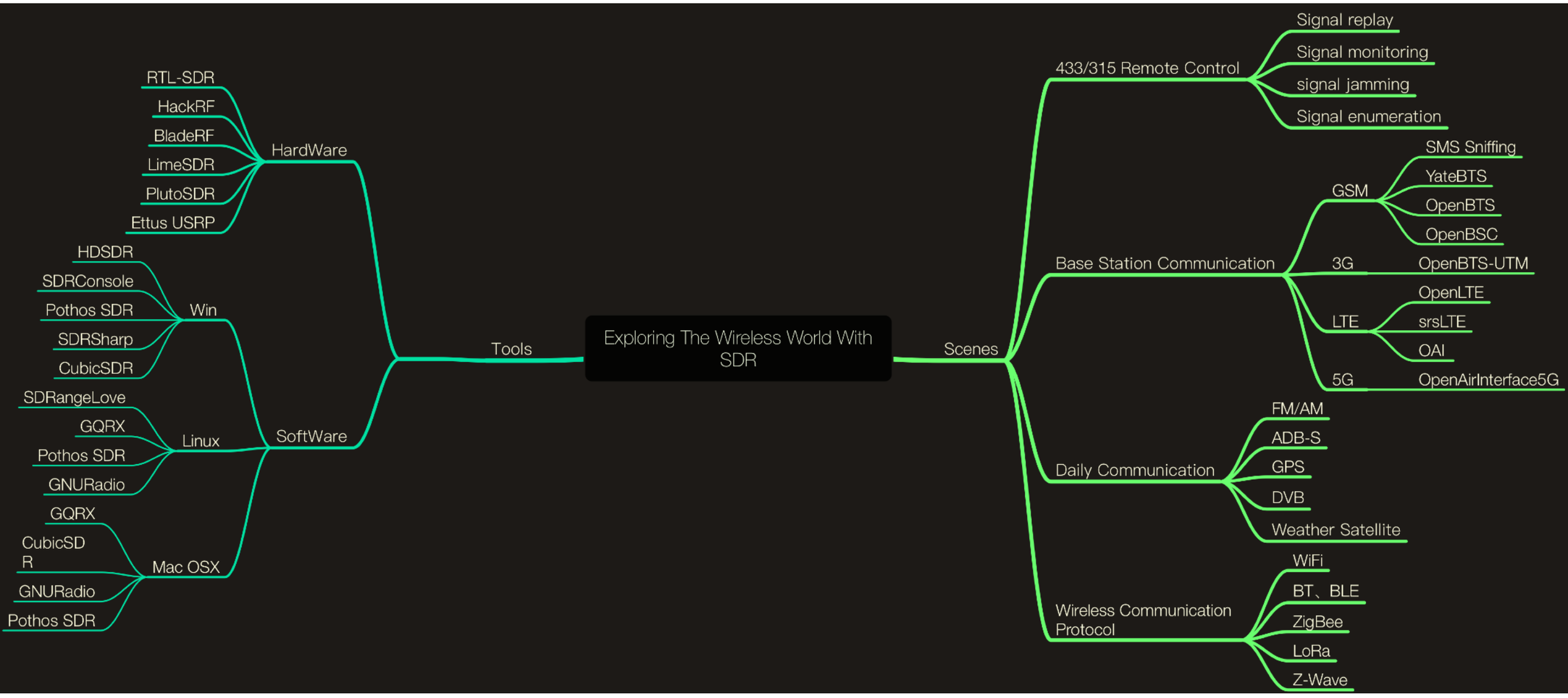
What and where are the main threats

Network Traffic

Rough Devices, MiTM

What and where are the main threats

Network Traffic



What and where are the main threats

Device Web Interface

Standard set of web application vulnerabilities, see:
OWASP Web Top 10
OWASP ASVS
OWASP Testing guide

Credential management vulnerabilities:
Username enumeration
Weak passwords
Account lockout
Known default credentials
Insecure password recovery mechanism

OWASP WEB TOP 10

OWASP Top 10 - 2013	→	OWASP Top 10 - 2017
A1 – Injection	→	A1:2017-Injection
A2 – Broken Authentication and Session Management	→	A2:2017-Broken Authentication
A3 – Cross-Site Scripting (XSS)	↘	A3:2017-Sensitive Data Exposure
A4 – Insecure Direct Object References [Merged+A7]	U	A4:2017-XML External Entities (XXE) [NEW]
A5 – Security Misconfiguration	↘	A5:2017-Broken Access Control [Merged]
A6 – Sensitive Data Exposure	↗	A6:2017-Security Misconfiguration
A7 – Missing Function Level Access Contr [Merged+A4]	U	A7:2017-Cross-Site Scripting (XSS)
A8 – Cross-Site Request Forgery (CSRF)	☒	A8:2017-Insecure Deserialization [NEW, Community]
A9 – Using Components with Known Vulnerabilities	→	A9:2017-Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards	☒	A10:2017-Insufficient Logging&Monitoring [NEW,Comm.]

What and where are the main threats

Mobile Applications

OWASP Top 10 Mobile Risk - Final List 2016	
M1	Improper Platform Usage
M2	Insecure Data Storage
M3	Insecure Communication
M4	Insecure Authentication
M5	Insufficient Cryptography
M6	Insecure Authorization
M7	Client code Quality
M8	Code Tampering
M9	Reverse Engineering
M10	Extraneous Functionality

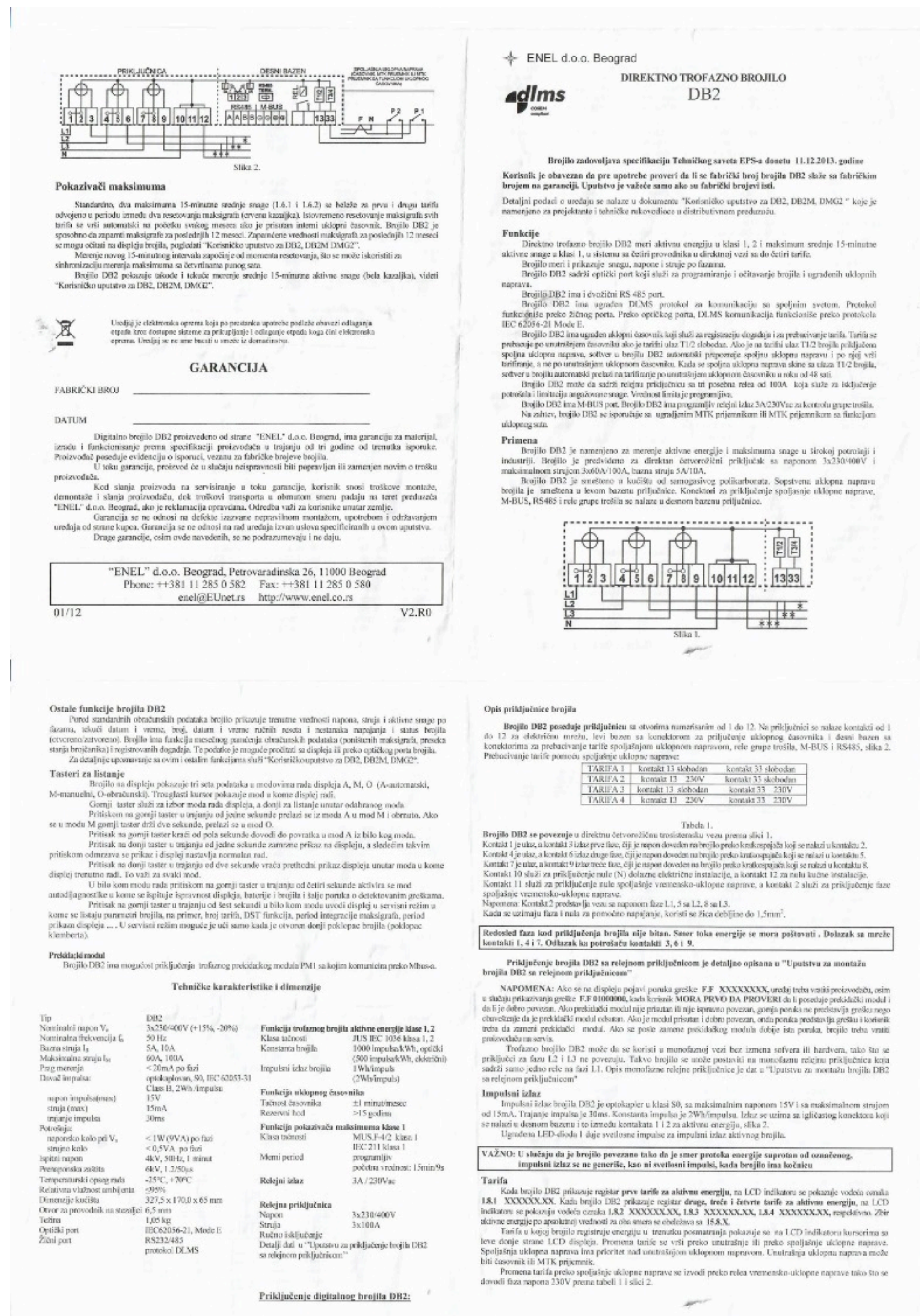
What and where are the main threats

Cloud Services

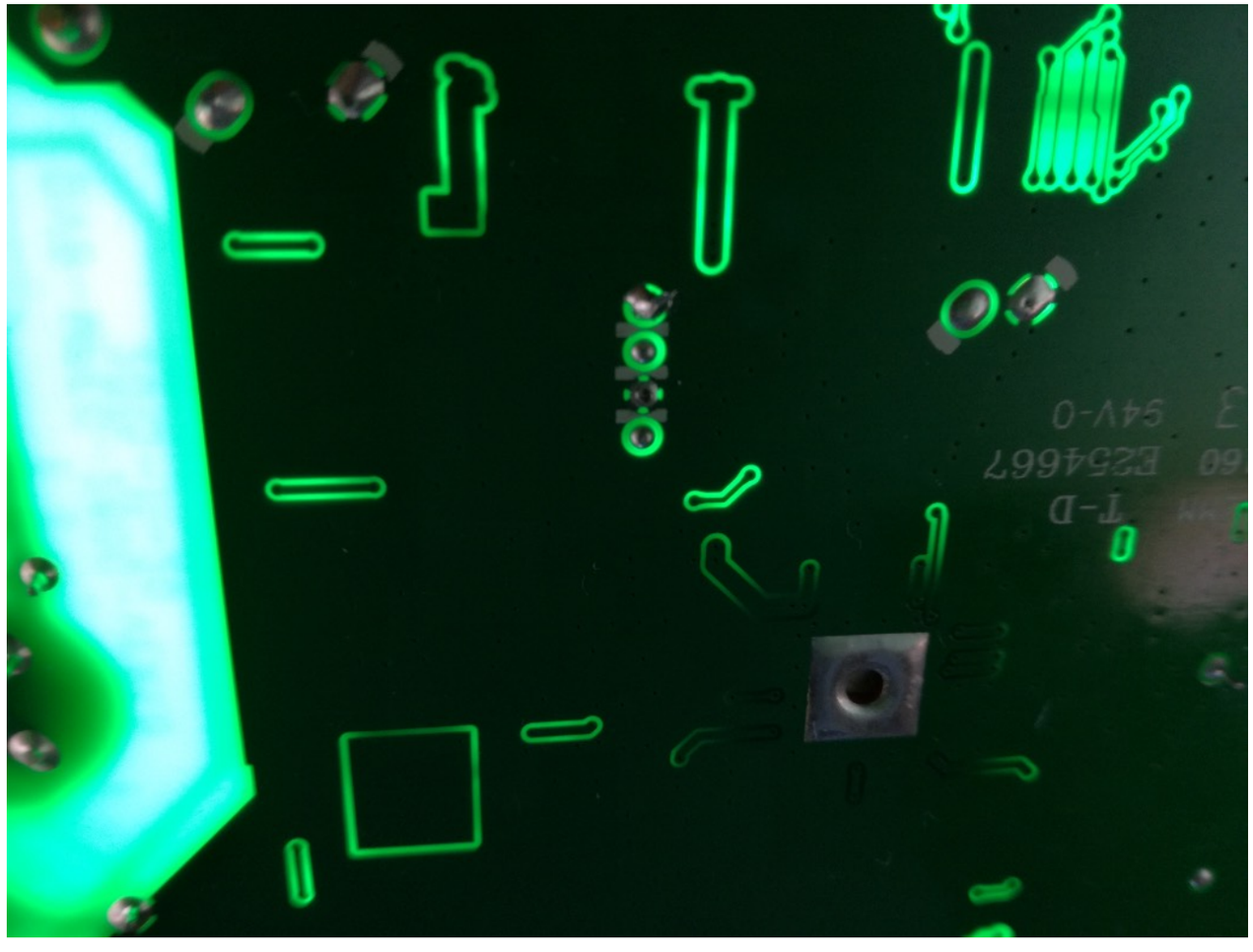
How to do basic security overview of your IoT system

- Information gathering
- Hardware
- Communications / Network
- Software

Read the documentation :)

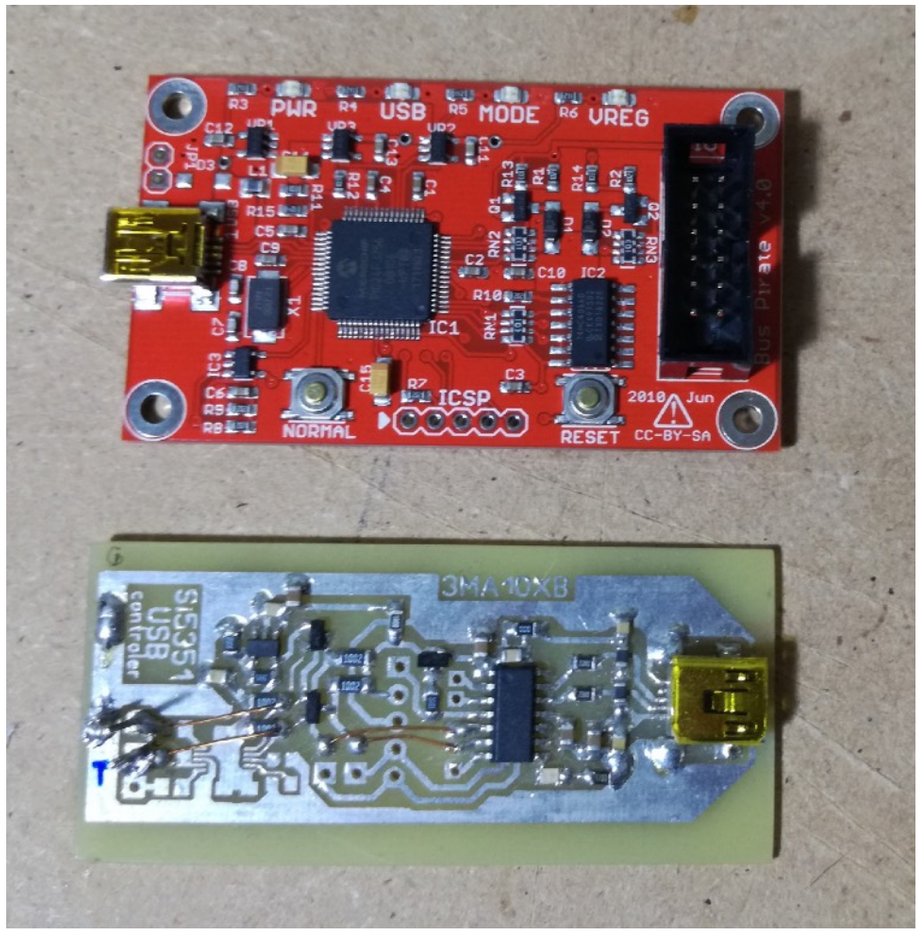


Play with Hardware



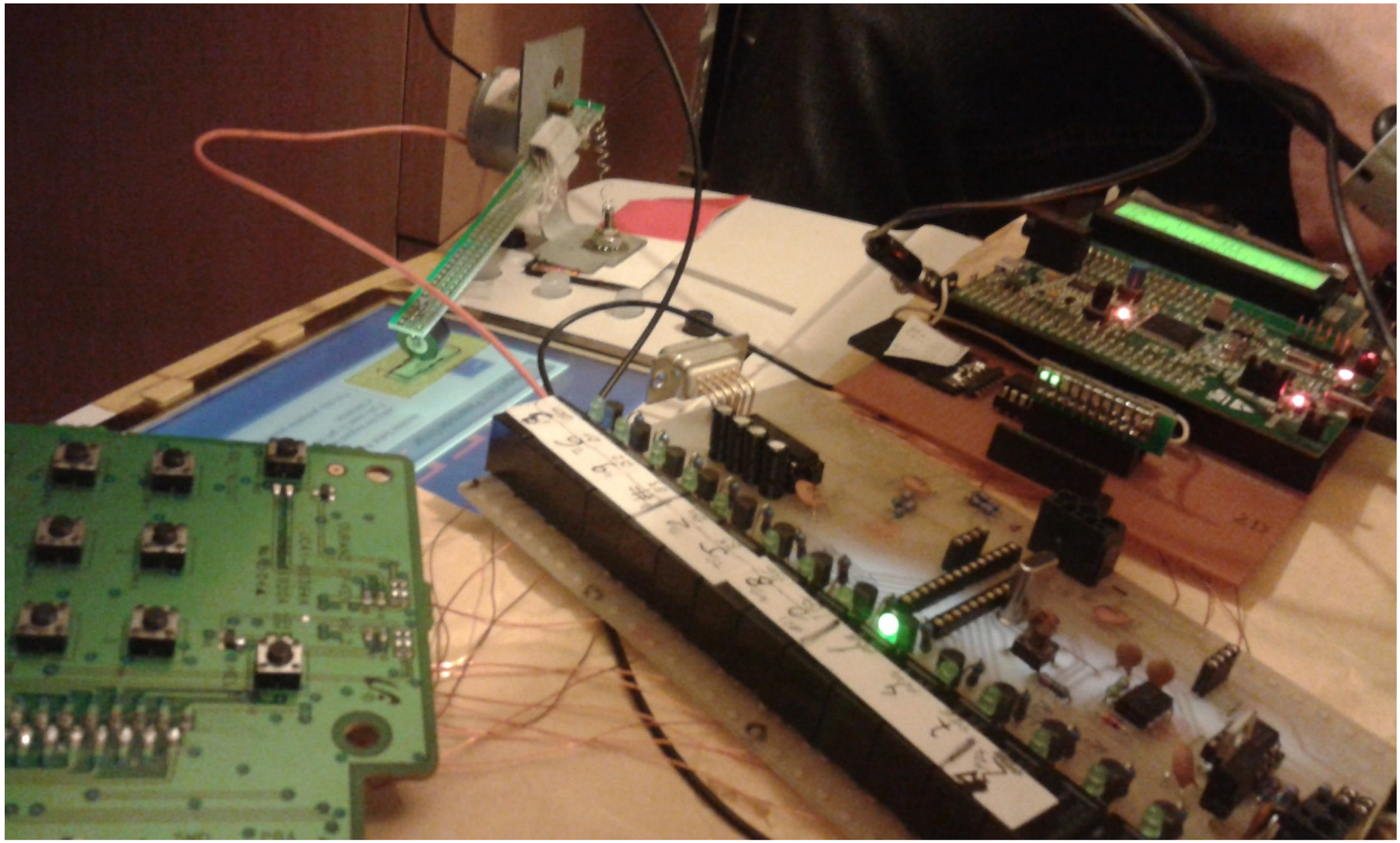
Play with hardware

BUS PIRATE / ANY UART DEVICE / RASPBERRY PI / LOGIC ANALYZER

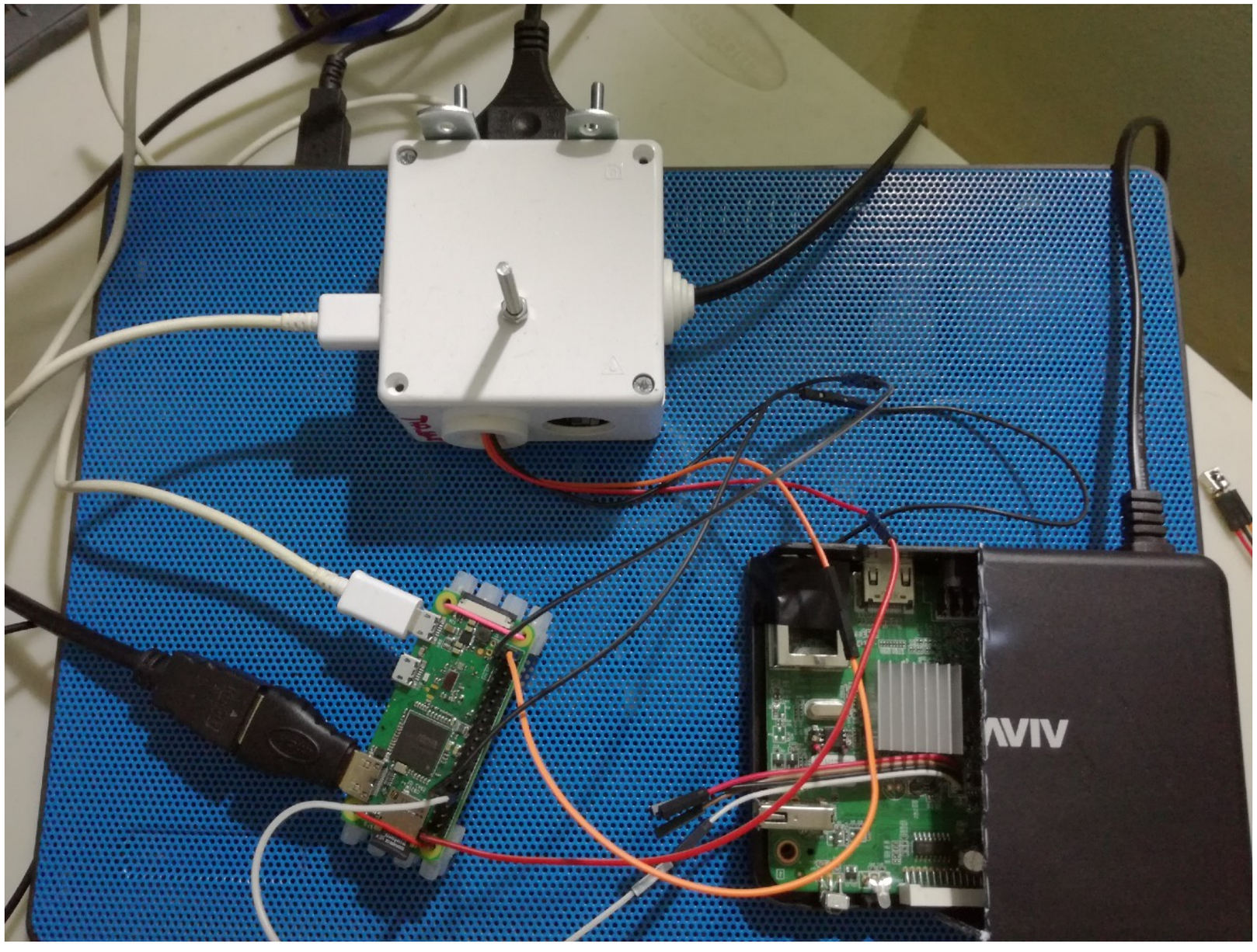


Play with hardware

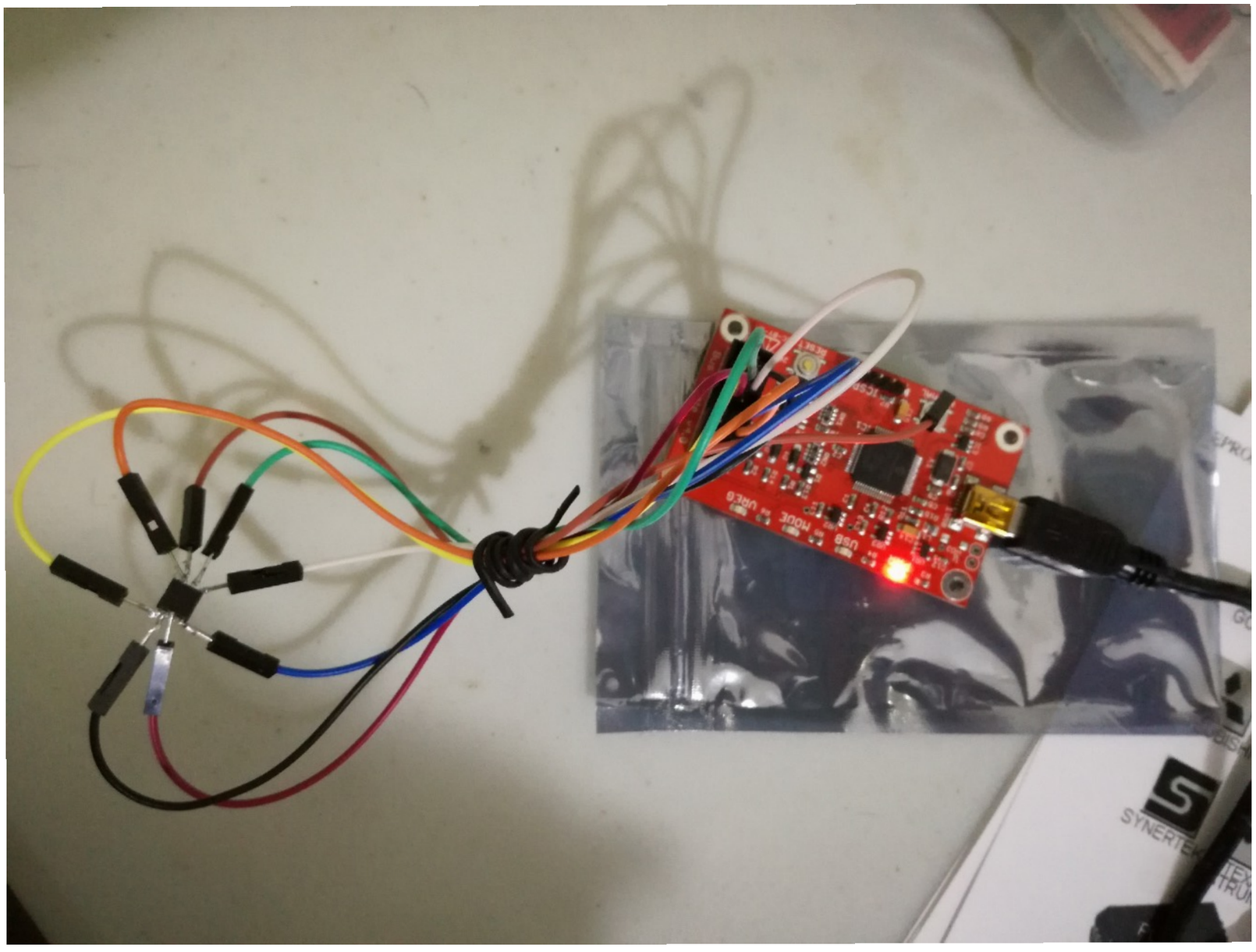
Play with hardware



Play with hardware



Dump Firmware



Check communications

RADIO

GNURadio

THE FREE & OPEN SOFTWARE RADIO ECOSYSTEM

Check communications

BlueBorne

A new attack vector exposes almost every connected device.

Check communications

BlueZ

nRF Connect

A BLUETOOTH LOW ENERGY TOOL FOR DEVELOPMENT AND EXPLORATION

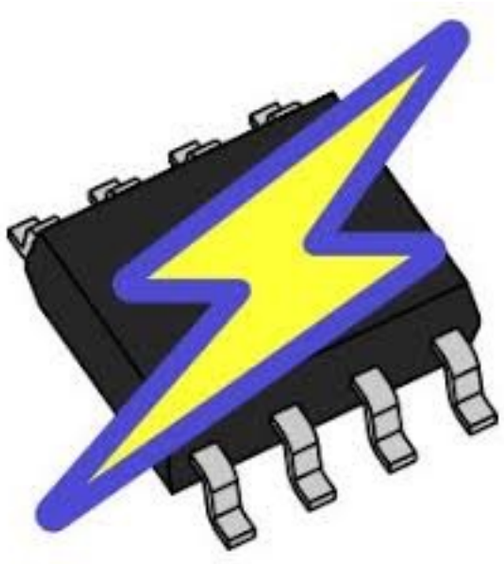
bleno

gitter join chat

A Node.js module for implementing BLE (Bluetooth Low Energy) peripherals.

Need a BLE central module? See noble.

Analyze firmware



Check network services

Analyze web applications and services

Nikto

Analyze mobile applications

QARK

build passing

Quick Android Review Kit

DEMO TIME

QUESTIONS

Thank you for your time!

You can contact me via e-mail:

ivanm@security-net.biz

“If you think you are too small to make a difference, try sleeping with a mosquito.” - Dalai Lama XIV