The S in IoT stands for Security

An overview on the Devices, Protocols, Architectures, and Security Threats of the Internet-of-Things Ecosystem

SEPRJ - ISEP, 16/06/2023

João Pedro Dias

$ whoami

João Pedro Dias, PhD

Software Engineer @ KUEHNE+NAGEL

Invited Assistant Professor @ U.PORTO FEUP FACULDADE DE ENGENHARIA UNIVERSIDADE DO PORTO

https://jpdias.me

jpmdias@fe.up.pt

Index

1. The Internet-of-Things *thing*
2. Let’s get *smaller*: IoT devices
3. *The devil is in the details:* looking for vulnerabilities and finding them
4. OWASP Top 10 for IoT
5. Closing remarks

The Internet-of-Things *thing*

The definition by the standards

“An infrastructure of interconnected objects, people, systems and information resources together with intelligent services to allow them to process information of the physical and the virtual world and react.”

ISO/IEC JTC 1 Internet of Things (IoT)

In concrete terms

A network of physical objects — *things* — that are **embedded with sensors, actuators, software**, and other technologies for the purpose of connecting and exchanging data with other devices and systems **over the Internet**.

From Wikipedia, the free encyclopedia

IKEA

0,65 kW
edp re:dy
edp

mi

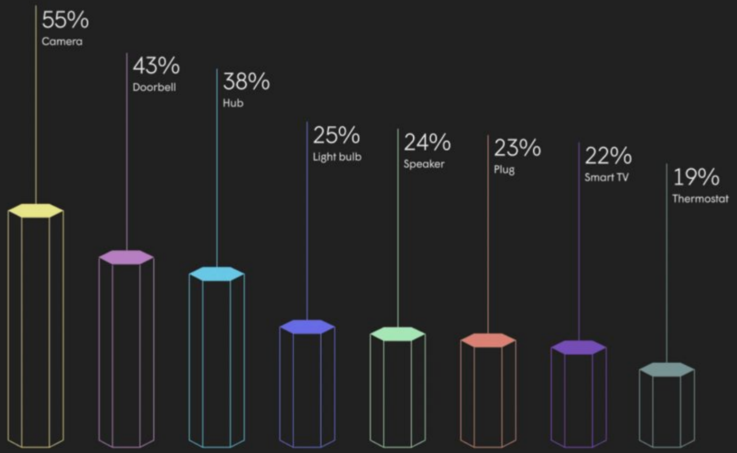
ring
ring

PHILIPS
hue
White and color ambiance
Ambiance blanche et colorée
PHILIPS

nest
70
nest
Google Home
Hands-free smart speaker

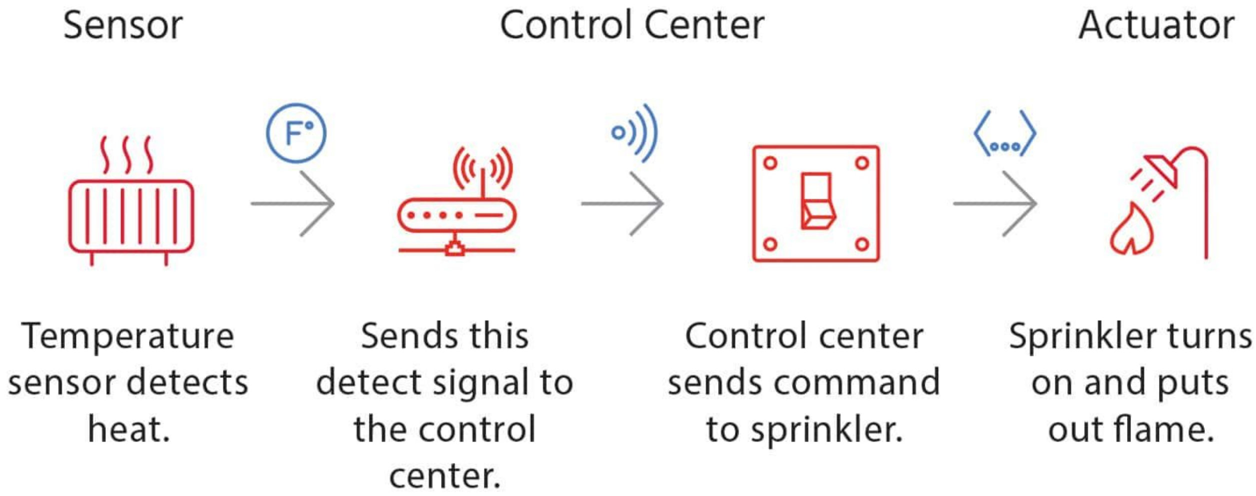
Some stats

“The average house in the U.S. now has 20.2 connected devices, according to a new report based on an analysis of 41 million homes and 1.8 thousand million connected devices. In Europe, the average is 17.4, while the average Japanese house contains only 10.3 smart devices.”



Smart Home: Apple Is The Fastest-Growing Connected Device Company, https://www.forbes.com/sites/johnkoetsier/2022/08/31/smart-home-apple-is-the-fastest-growing-connected-device-company/?sh=39cdf6d07dd4

What happens in an IoT workflow



Sensor

Control Center

Actuator

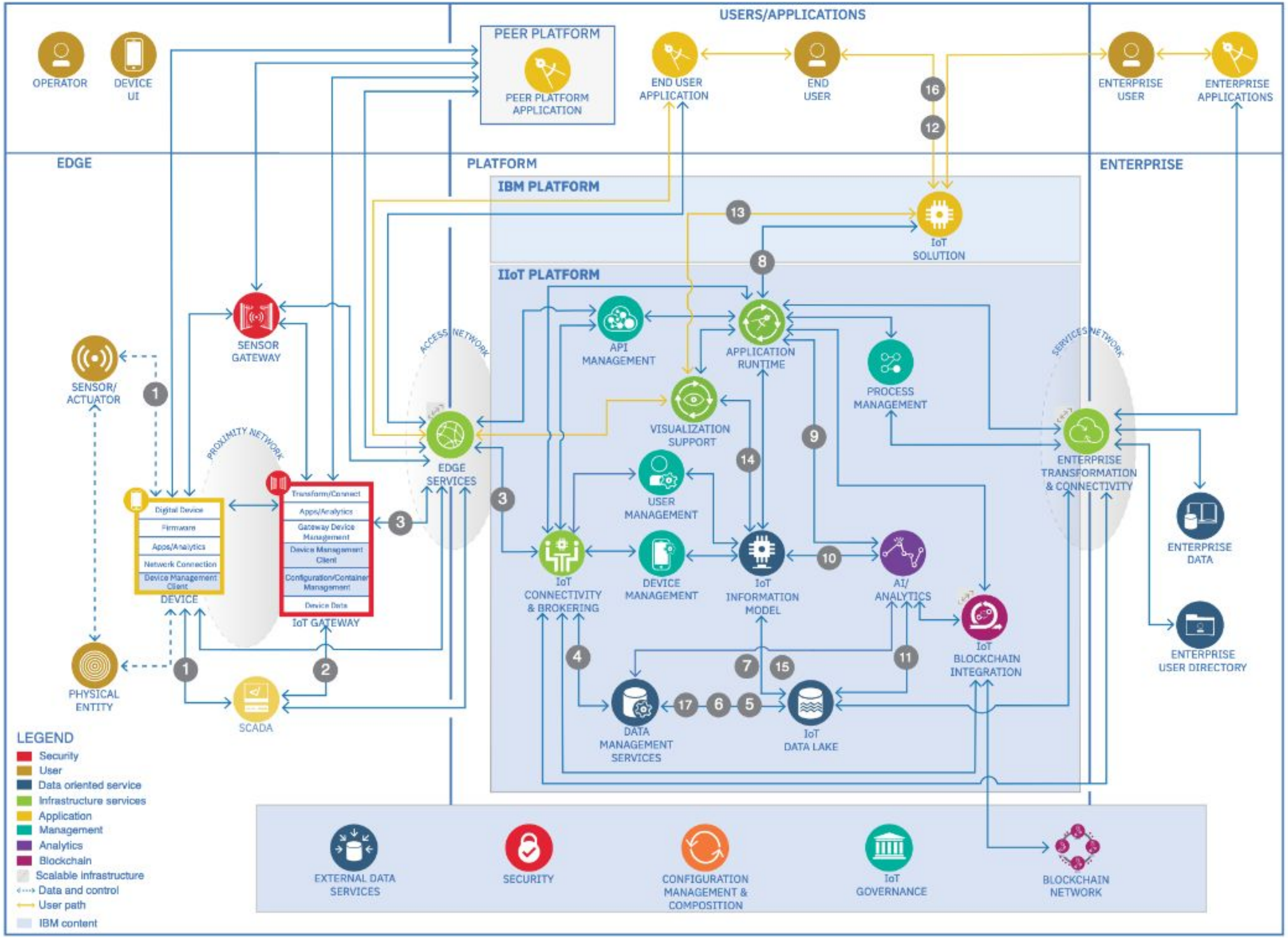
Temperature sensor detects heat.

Sends this detect signal to the control center.

Control center sends command to sprinkler.

Sprinkler turns on and puts out flame.

IoT: What Really Happens (architecture-wise)

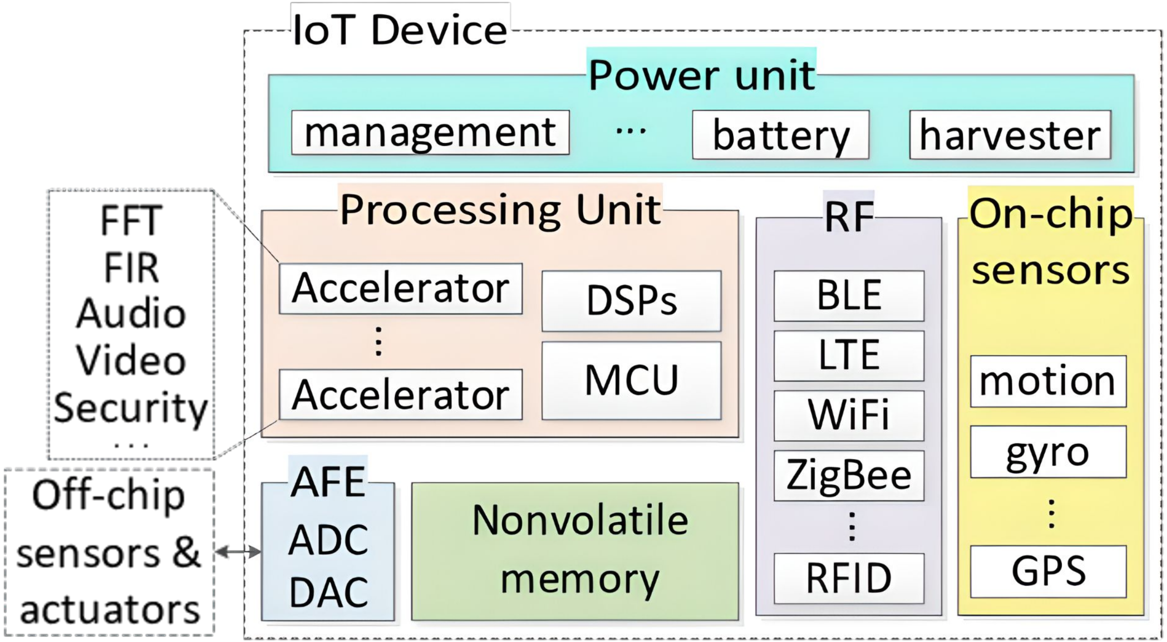


IBM reference architecture,

https://www.ibm.com/cloud/architecture/architectures/iotArchitecture/reference-architecture/

Let’s get *smaller*: IoT devices

General Architecture of an IoT device



James, A., Seth, A., Mukhopadhyay, S.C. (2022). Design Considerations for IoT Node. In: IoT System Design. Smart Sensors, Measurement and Instrumentation, vol 41. Springer, Cham. https://doi.org/10.1007/978-3-030-85863-6_3

Linux everywhere? *Not so fast*

Real-time Operating Systems

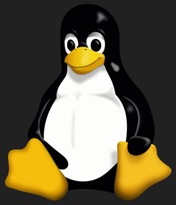
RIOT

freeRTOS

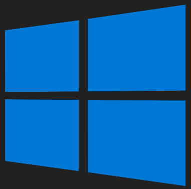
arm MBED OS

Zephyr™

Traditional Operating Systems



yocto PROJECT

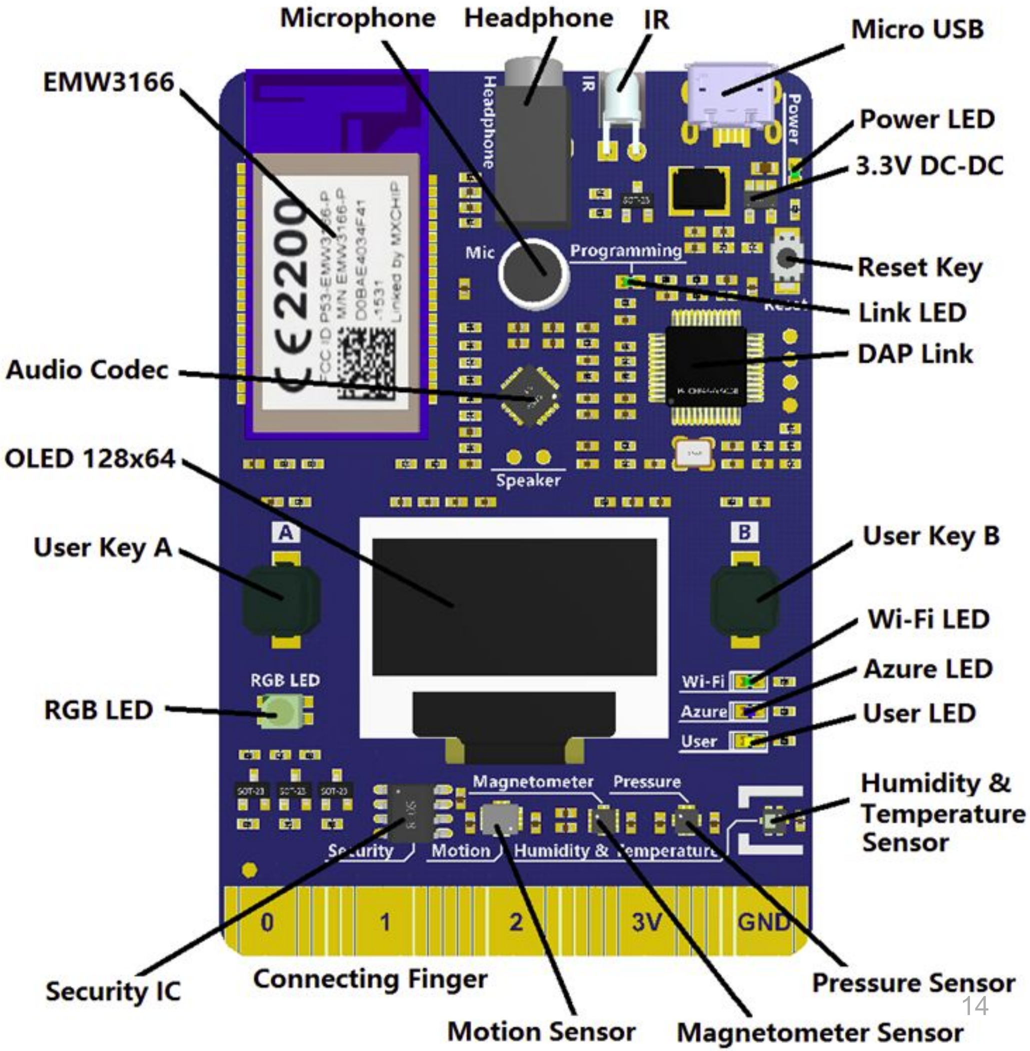


Baremetal

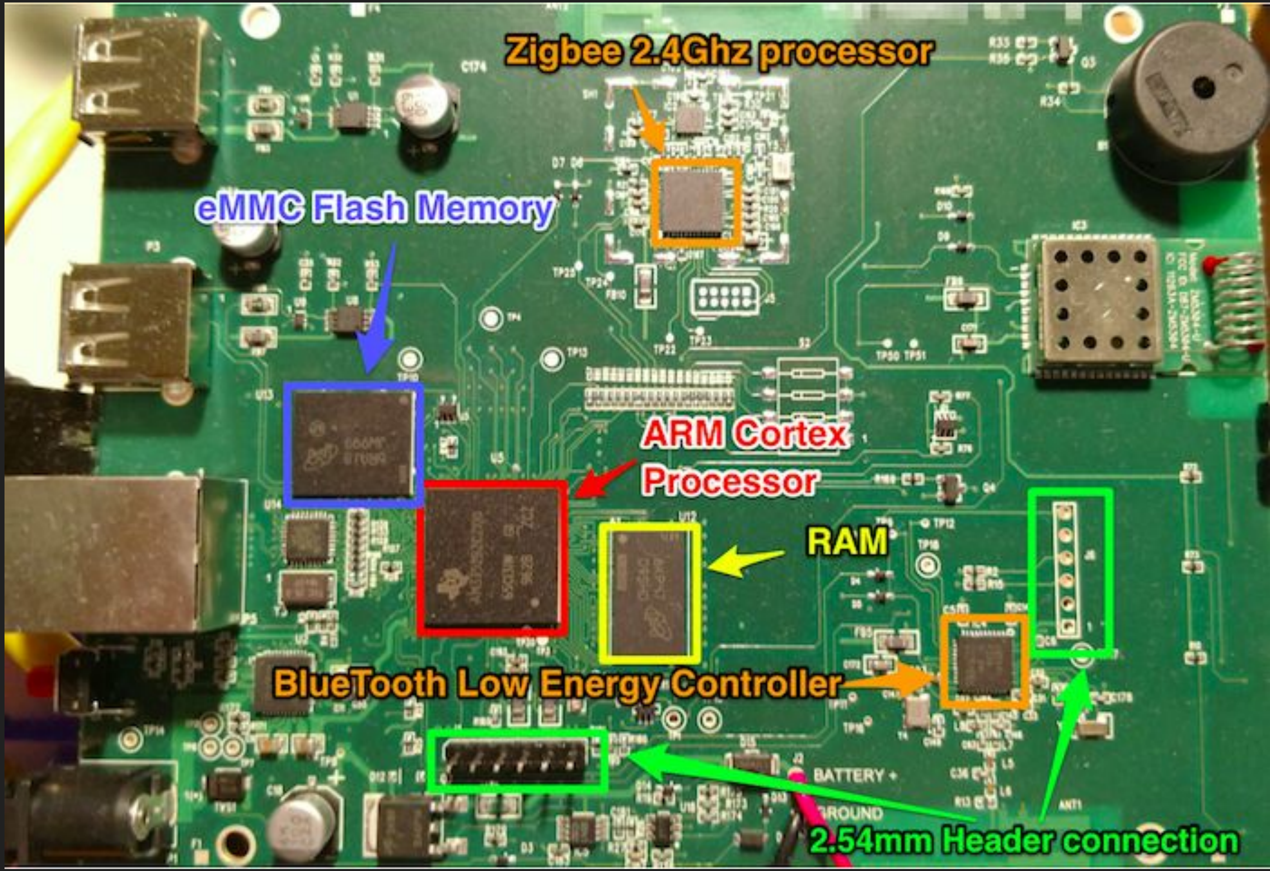
ARDUINO™

Example Device 1: Azure IoT DevKit

An all-in-one IoT kit built for the cloud, https://microsoft.github.io/azure-iot-developer-kit/



Example Device 2: (Unknown) ZigBee Gateway

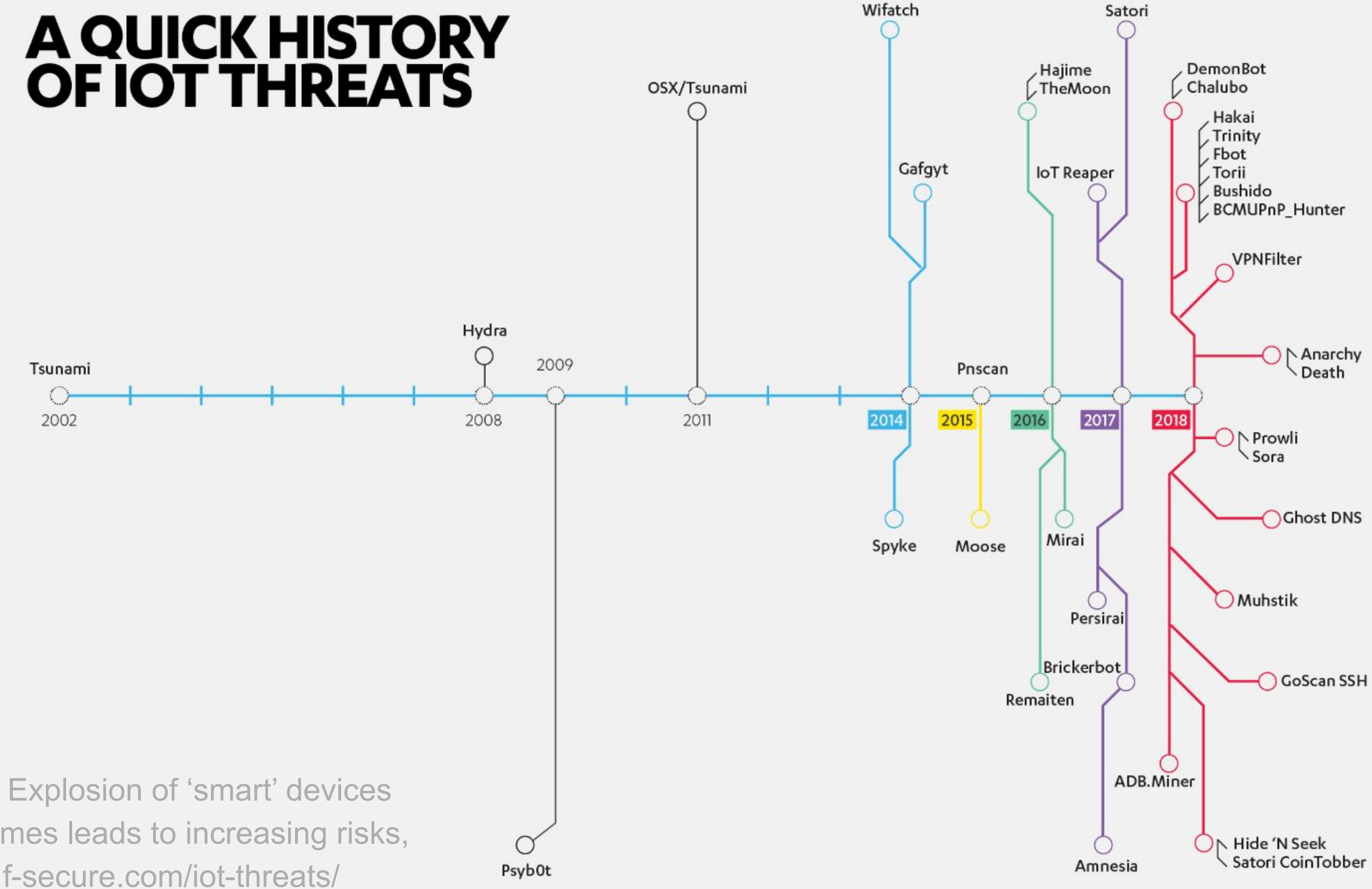


[IoT Security] Introduction to Embedded Hardware Hacking, https://www.rapid7.com/blog/post/2019/02/20/iot-security-introduction-to-embedded-hardware-hacking/

The devil is in the details:

looking for vulnerabilities and finding them

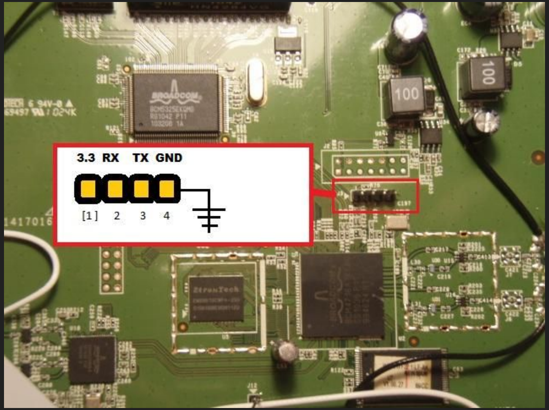
A QUICK HISTORY OF IOT THREATS

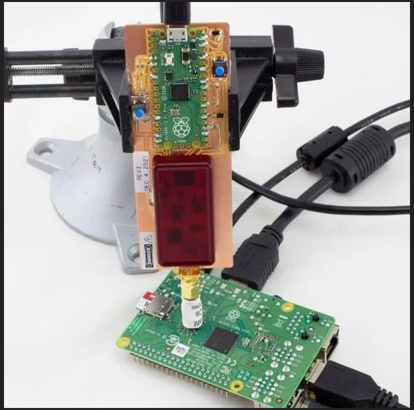


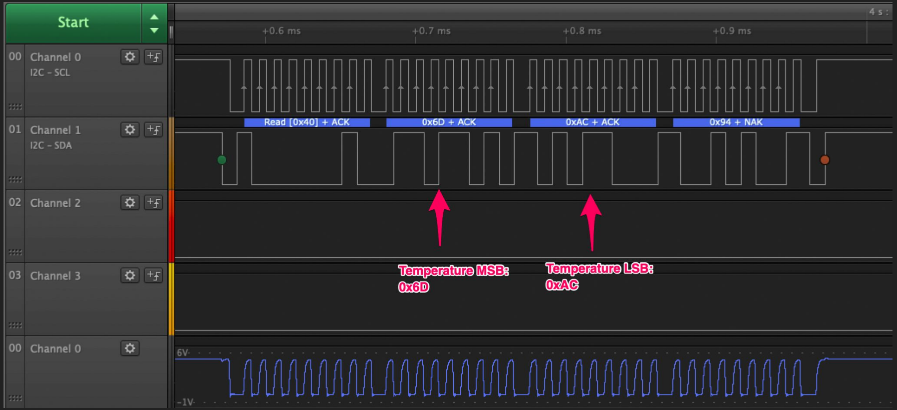
IoT threats: Explosion of 'smart' devices filling up homes leads to increasing risks, https://blog.f-secure.com/iot-threats/

If you have hardware access…

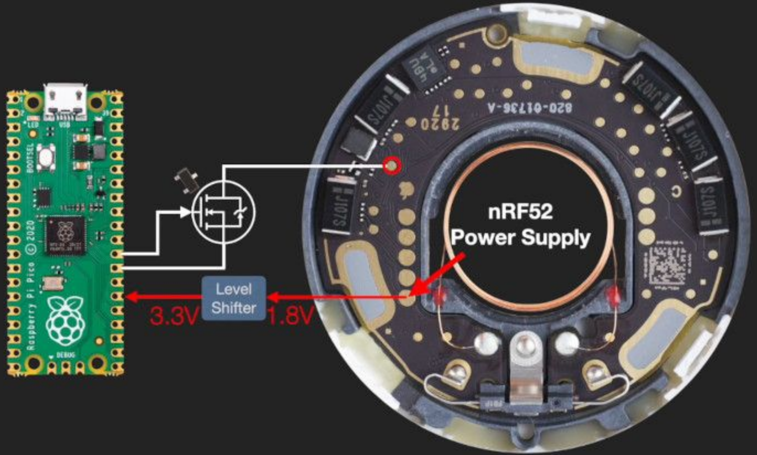
- Local Interfaces (JTAG, Serial, USB,...)
  - Dump flash memory, etc.
- Differential Power Analysis (DPA)
- Glitching (Voltage, Temp, Magnetics)
- Probing

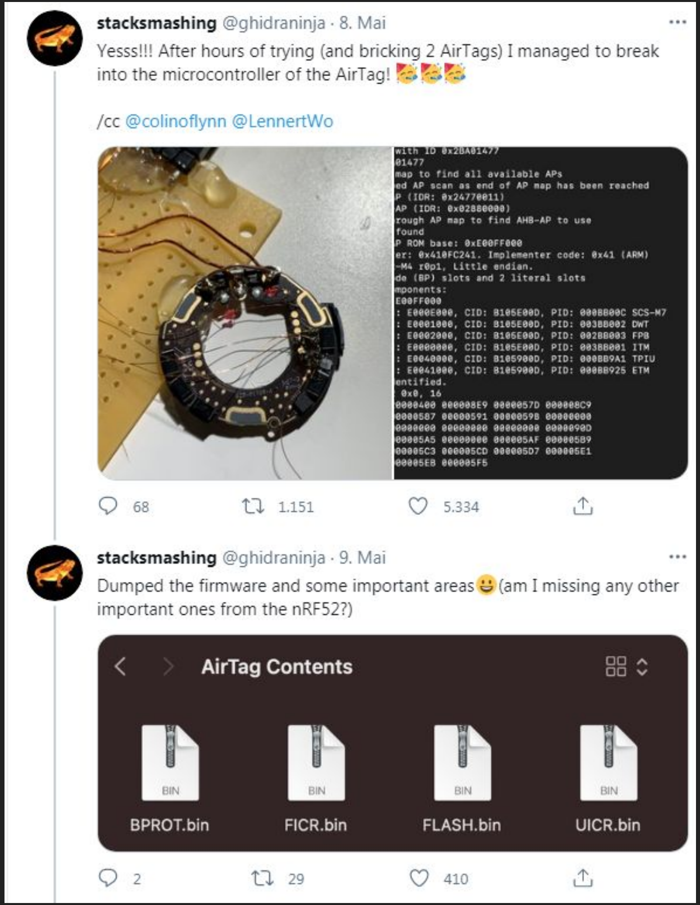






AirTag Glitch Attack example





stacksmashing @ghidraninja · 8. Mai

Yesss!!! After hours of trying (and bricking 2 AirTags) I managed to break into the microcontroller of the AirTag! 🥳🥳🥳

/cc @colinoflynn @LennertWo

```
with ID 0x2BA01477
01477
map to find all available APs
ed AP scan as end of AP map has been reached
P (IDR: 0x24770011)
AP (IDR: 0x02880000)
rough AP map to find AHB-AP to use
found
P ROM base: 0xE00FF000
er: 0x410FC241. Implementer code: 0x41 (ARM)
-M4 r0p1, Little endian.
de (BP) slots and 2 literal slots
mponents:
E00FF000
: E000E000, CID: B105E00D, PID: 000BB00C SCS-M7
: E0001000, CID: B105E00D, PID: 003BB002 DWT
: E0002000, CID: B105E00D, PID: 002BB003 FPB
: E0000000, CID: B105E00D, PID: 003BB001 ITM
: E0040000, CID: B105900D, PID: 000BB9A1 TPIU
: E0041000, CID: B105900D, PID: 000BB925 ETM
entified.
 0x0, 16
0000400 000008E9 0000057D 000008C9
0000587 00000591 0000059B 00000000
0000000 00000000 00000000 0000090D
00005A5 00000000 000005AF 000005B9
00005C3 000005CD 000005D7 000005E1
00005EB 000005F5
```

68 1.151 5.334

stacksmashing @ghidraninja · 9. Mai

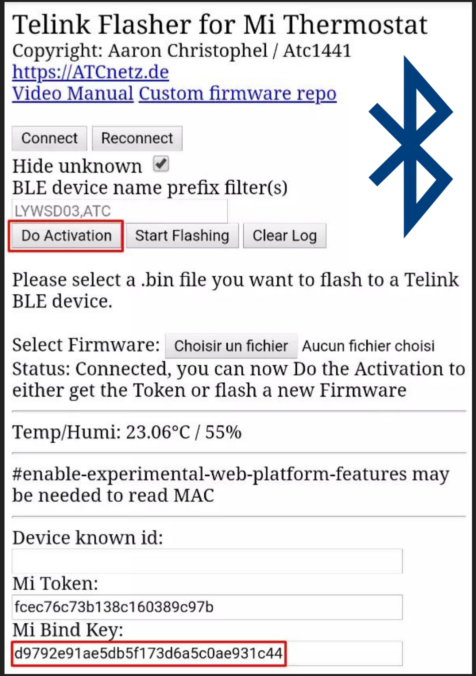
Dumped the firmware and some important areas😃(am I missing any other important ones from the nRF52?)

AirTag Contents

BPROT.bin FICR.bin FLASH.bin UICR.bin

2 29 410

Xiaomi Mi Temperature/Humidity Sensor example



Telink Flasher for Mi Thermostat

Copyright: Aaron Christophel / Atc1441

https://ATCnetz.de

Video Manual Custom firmware repo

Hide unknown ☑

BLE device name prefix filter(s)

LYWSD03,ATC

Please select a .bin file you want to flash to a Telink BLE device.

Select Firmware: Choisir un fichier Aucun fichier choisi

Status: Connected, you can now Do the Activation to either get the Token or flash a new Firmware

Temp/Humi: 23.06°C / 55%

#enable-experimental-web-platform-features may be needed to read MAC

Device known id:

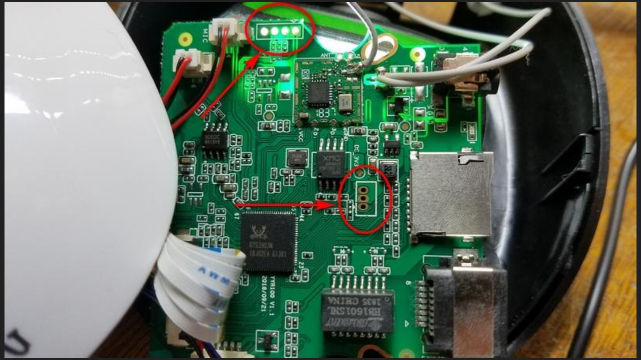
Mi Token:

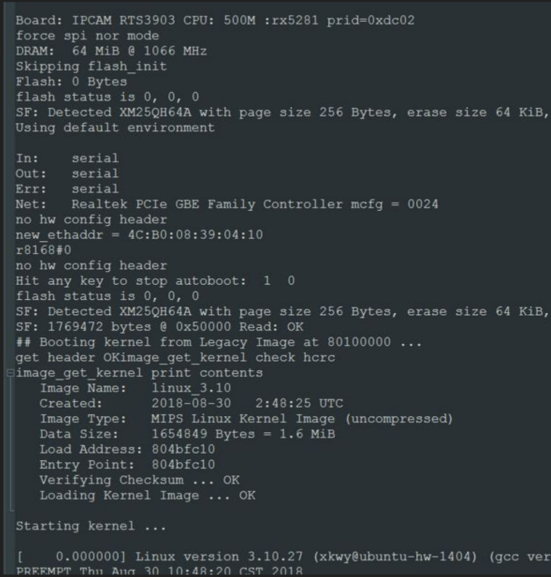
fcec76c73b138c160389c97b

Mi Bind Key:

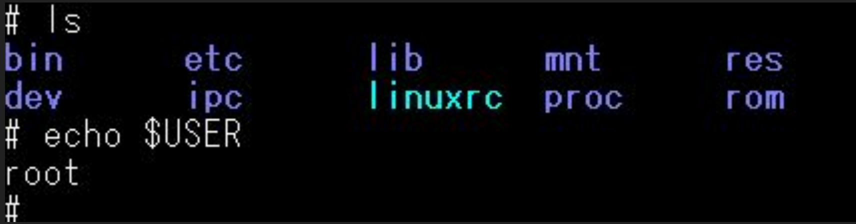
d9792e91ae5db5f173d6a5c0ae931c44

Random IP Camera example

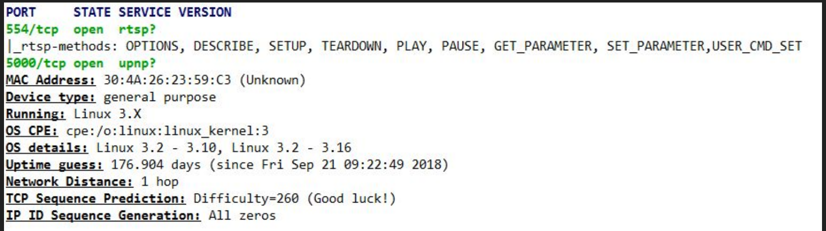




```
Board: IPCAM RTS3903 CPU: 500M :rx5281 prid=0xdc02
force spi nor mode
DRAM:  64 MiB @ 1066 MHz
Skipping flash_init
Flash: 0 Bytes
flash status is 0, 0, 0
SF: Detected XM25QH64A with page size 256 Bytes, erase size 64 KiB,
Using default environment

In:    serial
Out:   serial
Err:   serial
Net:   Realtek PCIe GBE Family Controller mcfg = 0024
no hw config header
new_ethaddr = 4C:B0:08:39:04:10
r8168#0
no hw config header
Hit any key to stop autoboot:  1  0
flash status is 0, 0, 0
SF: Detected XM25QH64A with page size 256 Bytes, erase size 64 KiB,
SF: 1769472 bytes @ 0x50000 Read: OK
## Booting kernel from Legacy Image at 80100000 ...
get header OKimage_get_kernel check hcrc
image_get_kernel print contents
   Image Name:   linux_3.10
   Created:      2018-08-30   2:48:25 UTC
   Image Type:   MIPS Linux Kernel Image (uncompressed)
   Data Size:    1654849 Bytes = 1.6 MiB
   Load Address: 804bfc10
   Entry Point:  804bfc10
   Verifying Checksum ... OK
   Loading Kernel Image ... OK

Starting kernel ...

[    0.000000] Linux version 3.10.27 (xkwy@ubuntu-hw-1404) (gcc ver
PREEMPT Thu Aug 30 10:48:20 CST 2018
```



```
# ls
bin         etc         lib         mnt         res
dev         ipc         linuxrc     proc        rom
# echo $USER
root
#
```

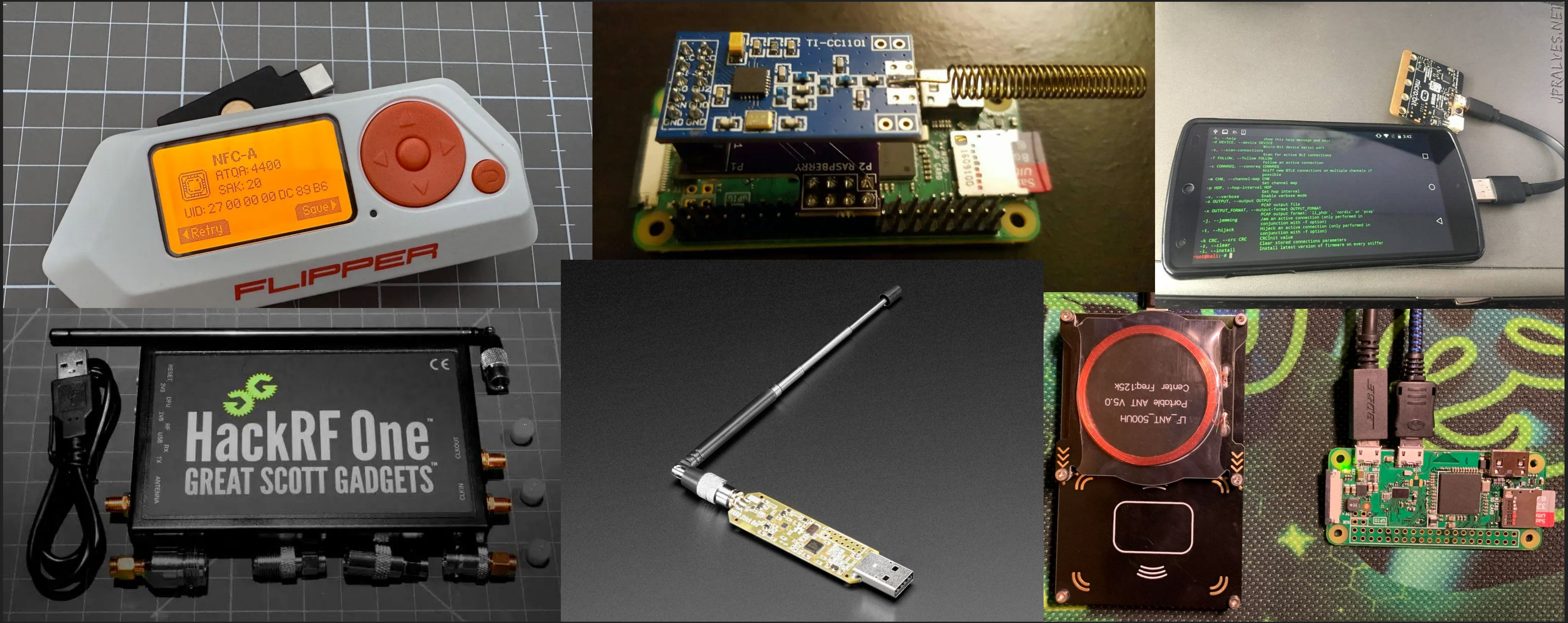


```
PORT     STATE SERVICE VERSION
554/tcp  open  rtsp?
|_rtsp-methods: OPTIONS, DESCRIBE, SETUP, TEARDOWN, PLAY, PAUSE, GET_PARAMETER, SET_PARAMETER,USER_CMD_SET
5000/tcp open  upnp?
MAC Address: 30:4A:26:23:59:C3 (Unknown)
Device type: general purpose
Running: Linux 3.X
OS CPE: cpe:/o:linux:linux_kernel:3
OS details: Linux 3.2 - 3.10, Linux 3.2 - 3.16
Uptime guess: 176.904 days (since Fri Sep 21 09:22:49 2018)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=260 (Good luck!)
IP ID Sequence Generation: All zeros
```

If you are near enough…

- 433MHz Replay Attacks
    - Or how to open the neighbor garage door
- Zigbee Link key Vulnerability
    - ZigBee standard permits the re-use of link keys for rejoining the network
- Bluetooth LE Link Layer Memory Corruption
    - Crash the device and the device could be remotely restarted
- Bluetooth LE Zero LTK Installation
    - Arbitrary read or write access to the device's functions
- WiFi vulnerabilities
    - Key Reinstallation Attacks, Fragmentation and aggregation attacks, Deauth, …
- Esoteric attacks
    - Laser-Based Audio Injection on Voice-Controllable Systems

Some useful toys

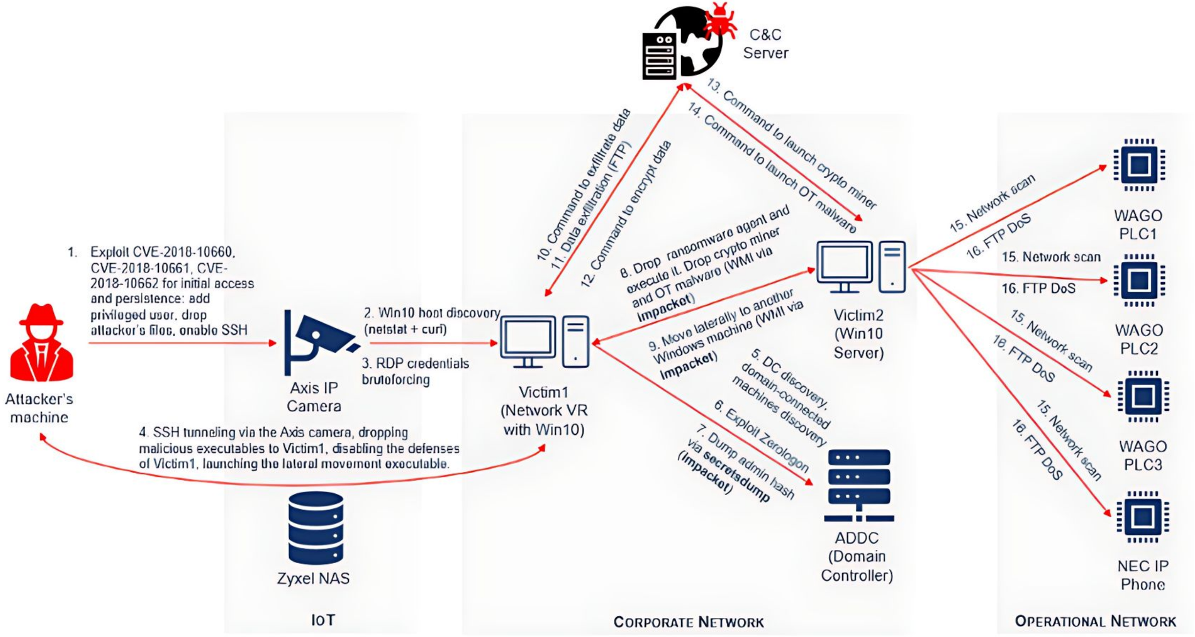


More tools:
https://github.com/yadox666/The-Hackers-Hardware-Toolkit/blob/master/TheHackersHardwareToolkit.pdf

If it is Internet connected…

- Traditional web-related vulnerabilities
  - OWASP Top 10, https://owasp.org/Top10/
  - OWASP API Security Top 10, https://owasp.org/API-Security/editions/2023/en/0x00-header/
- Vulnerabilities from IoT-focused protocols:
  - CoAP
  - MQTT (and variants)
  - XMPP
  - DDS

Anatomy of an Attack



1. Exploit CVE-2018-10660, CVE-2018-10661, CVE-2018-10662 for initial access and persistence: add privileged user, drop attacker's files, enable SSH

2. Win10 host discovery (netstat + curl)

3. RDP credentials bruteforcing

4. SSH tunneling via the Axis camera, dropping malicious executables to Victim1, disabling the defenses of Victim1, launching the lateral movement executable.

5. DC discovery, domain-connected machines discovery

6. Exploit Zerologon

7. Dump admin hash via **secretsdump** (**Impacket**)

8. Drop ransomware agent and execute it. Drop crypto miner and OT malware (WMI via **Impacket**)

9. Move laterally to another Windows machine (WMI via **Impacket**)

10. Command to exfiltrate data

11. Data exfiltration (FTP)

12. Command to encrypt data

13. Command to launch crypto miner

14. Command to launch OT malware

15. Network scan

16. FTP DoS

R4IoT: When Ransomware Meets IoT and OT, https://www.forescout.com/resources/r4iot-next-generation-ransomware-report/

OWASP IoT Top 10 (2018)

OWASP Internet of Things (IoT) Project, https://wiki.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=Main

1 Weak, Guessable, or Hardcoded Passwords

Use of easily bruteforced, publicly available, or unchangeable credentials, including backdoors in firmware or client software that grants unauthorized access to deployed systems.

2 Insecure Network Services

Unneeded or insecure network services running on the device itself, especially those exposed to the internet, that compromise the confidentiality, integrity/authenticity, or availability of information or allow unauthorized remote control…

3 Insecure Ecosystem Interfaces

Insecure web, backend API, cloud, or mobile interfaces in the ecosystem outside of the device that allows compromise of the device or its related components. Common issues include a lack of authentication/authorization, lacking or weak encryption, and a lack of input and output filtering.

4 Lack of Secure Update Mechanism

Lack of ability to securely update the device. This includes lack of firmware validation on device, lack of secure delivery (un-encrypted in transit), lack of anti-rollback mechanisms, and lack of notifications of security changes due to updates.

5 Use of Insecure or Outdated Components

Use of deprecated or insecure software components/libraries that could allow the device to be compromised. This includes insecure customization of operating system platforms, and the use of third-party software or hardware components from a compromised supply chain.

6

Insufficient Privacy Protection

User's personal information stored on the device or in the ecosystem that is used insecurely, improperly, or without permission.

7

Insecure Data Transfer and Storage

Lack of encryption or access control of sensitive data anywhere within the ecosystem, including at rest, in transit, or during processing.

8

Lack of Device Management

Lack of security support on devices deployed in production, including asset management, update management, secure decommissioning, systems monitoring, and response capabilities.

9

Insecure Default Settings

Devices or systems shipped with insecure default settings or lack the ability to make the system more secure by restricting operators from modifying configurations.

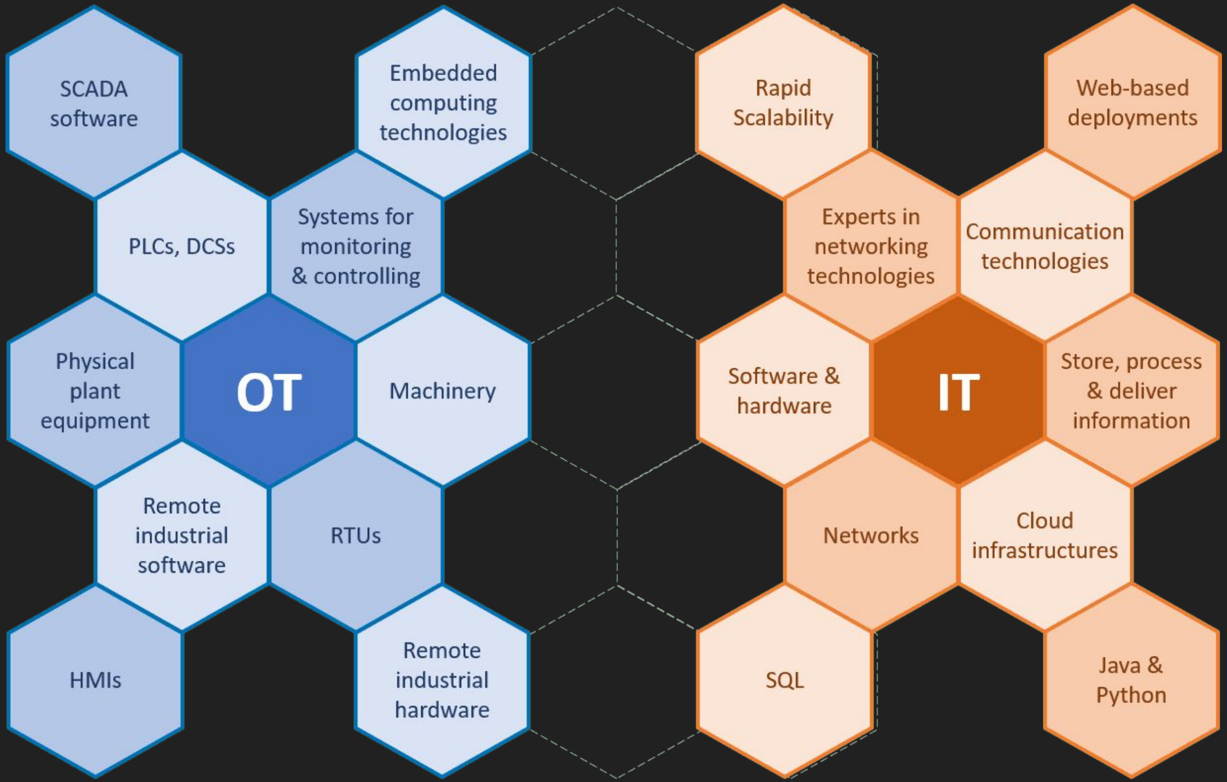
10

Lack of Physical Hardening

Lack of physical hardening measures, allowing potential attackers to gain sensitive information that can help in a future remote attack or take local control of the device.

Closing remarks

Moving from IT to OT (IoT)


SCADA software
Embedded computing technologies
PLCs, DCSs
Systems for monitoring & controlling
Physical plant equipment
OT
Machinery
Remote industrial software
RTUs
HMIs
Remote industrial hardware
Rapid Scalability
Web-based deployments
Experts in networking technologies
Communication technologies
Software & hardware
IT
Store, process & deliver information
Networks
Cloud infrastructures
SQL
Java & Python

Trust but verify (!)

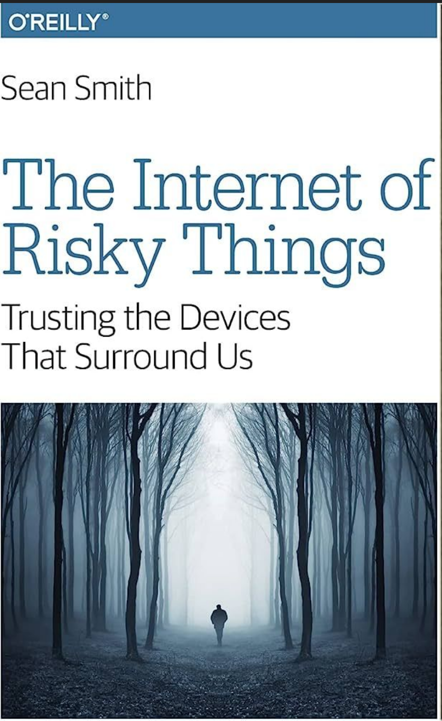
- “Google Calls Hidden Microphone in Its Nest Home Security Devices an 'Error'”
- “Amazon Buys Roomba Company, Will Now Map Inside of Your House”
- “(...) an airport in Rome discovered that one of their security systems, which consisted of over 100 **Hikvision CCTV cameras**, was sending huge packets of data to a chain of IP addresses that ended in China.”
- “Smart lightbulbs could be exporting your personal data to China”
- “Why (Amazon) Ring Doorbells Perfectly Exemplify the IoT Security Crisis: A new wave of reports about the home surveillance cameras getting hijacked by creeps is painfully familiar.”

Some advice from the Internet (Twitter)

- Customers must be notified if security updates are no longer occurring for a given device. (@daeken)
- Proper channels for reporting vulnerabilities. (@daeken)
- Minimize attack surface. (@daeken)
- Keep third-party software up to date. (@daeken)

- No cloud service should ever have access to your sensitive home devices or even know what you're doing. (@creationix)
- Devices should always work when you’re at home, even without Internet connectivity. (@creationix)
- Communicating with devices while at home should have far less latency than is typical. (@creationix)

Some reading suggestions

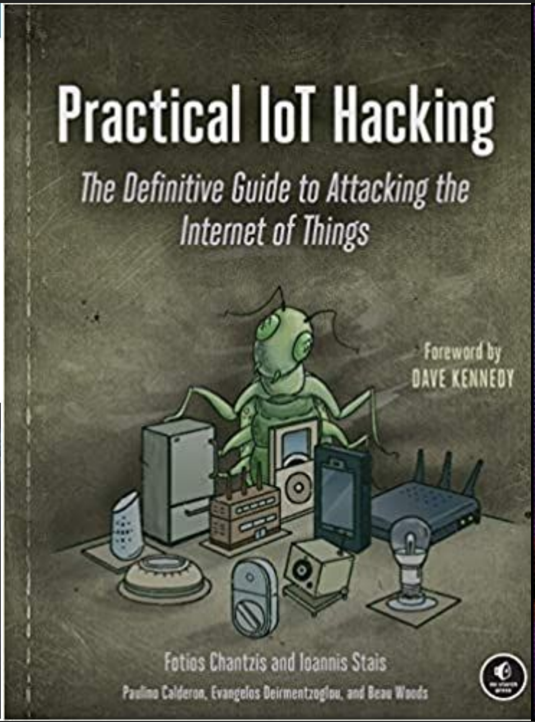


O'REILLY®

Sean Smith

The Internet of Risky Things

Trusting the Devices That Surround Us



Practical IoT Hacking

The Definitive Guide to Attacking the Internet of Things

Foreword by DAVE KENNEDY

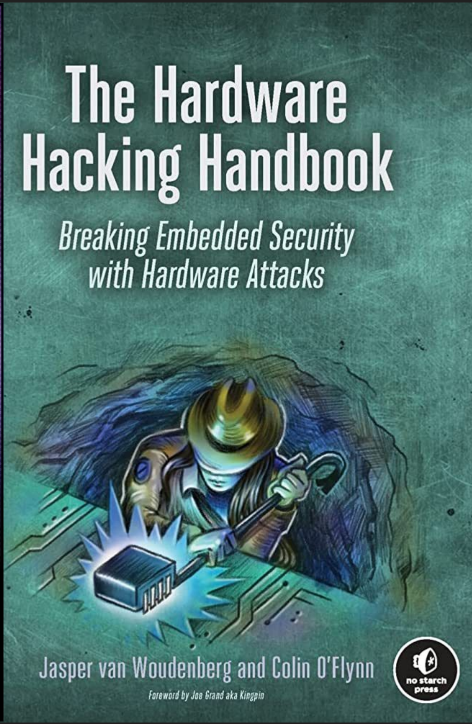
Fotios Chantzis and Ioannis Stais

Paulino Calderon, Evangelos Deirmentzoglou, and Beau Woods

MIKKO HYPPONEN

IF IT'S SMART, IT'S VULNERABLE

WILEY



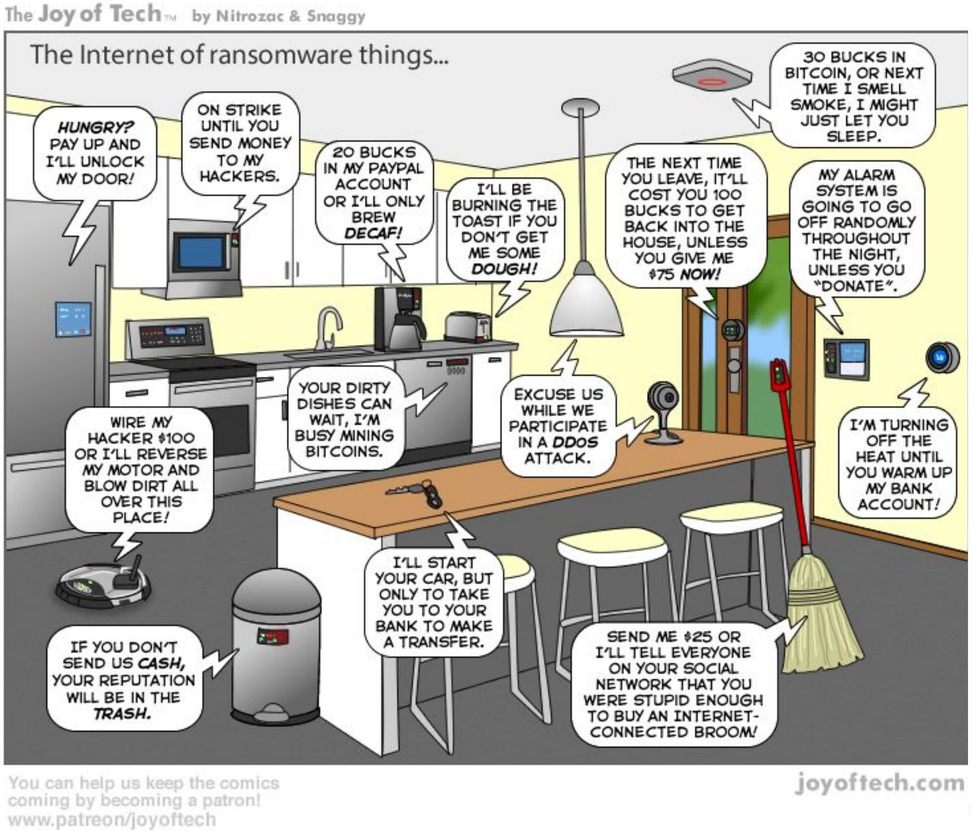
The Hardware Hacking Handbook

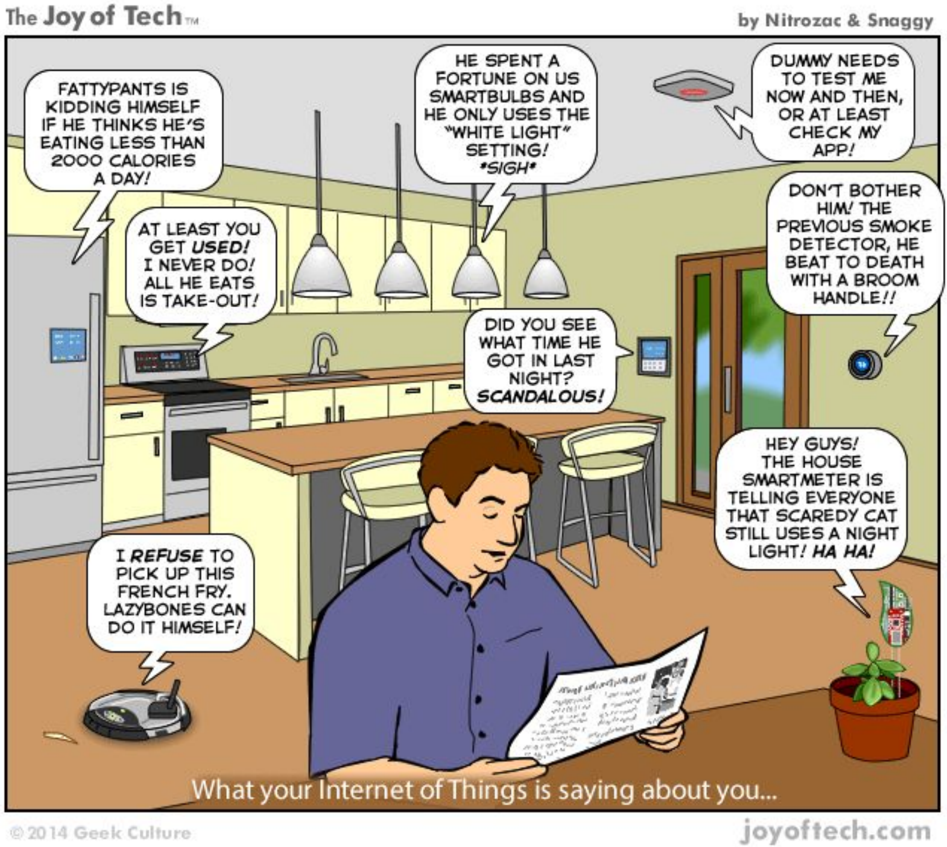
Breaking Embedded Security with Hardware Attacks

Jasper van Woudenberg and Colin O'Flynn

Foreword by Joe Grand aka Kingpin

no starch press


The Joy of Tech™ by Nitrozac & Snaggy
The Internet of ransomware things...
HUNGRY? PAY UP AND I'LL UNLOCK MY DOOR!
ON STRIKE UNTIL YOU SEND MONEY TO MY HACKERS.
20 BUCKS IN MY PAYPAL ACCOUNT OR I'LL ONLY BREW DECAF!
I'LL BE BURNING THE TOAST IF YOU DON'T GET ME SOME DOUGH!
THE NEXT TIME YOU LEAVE, IT'LL COST YOU 100 BUCKS TO GET BACK INTO THE HOUSE, UNLESS YOU GIVE ME $75 NOW!
30 BUCKS IN BITCOIN, OR NEXT TIME I SMELL SMOKE, I MIGHT JUST LET YOU SLEEP.
MY ALARM SYSTEM IS GOING TO GO OFF RANDOMLY THROUGHOUT THE NIGHT, UNLESS YOU "DONATE".
YOUR DIRTY DISHES CAN WAIT, I'M BUSY MINING BITCOINS.
EXCUSE US WHILE WE PARTICIPATE IN A DDoS ATTACK.
I'M TURNING OFF THE HEAT UNTIL YOU WARM UP MY BANK ACCOUNT!
WIRE MY HACKER $100 OR I'LL REVERSE MY MOTOR AND BLOW DIRT ALL OVER THIS PLACE!
I'LL START YOUR CAR, BUT ONLY TO TAKE YOU TO YOUR BANK TO MAKE A TRANSFER.
IF YOU DON'T SEND US CASH, YOUR REPUTATION WILL BE IN THE TRASH.
SEND ME $25 OR I'LL TELL EVERYONE ON YOUR SOCIAL NETWORK THAT YOU WERE STUPID ENOUGH TO BUY AN INTERNET-CONNECTED BROOM!
You can help us keep the comics coming by becoming a patron! www.patreon/joyoftech
joyoftech.com


The Joy of Tech™
by Nitrozac & Snaggy
FATTYPANTS IS KIDDING HIMSELF IF HE THINKS HE'S EATING LESS THAN 2000 CALORIES A DAY!
HE SPENT A FORTUNE ON US SMARTBULBS AND HE ONLY USES THE "WHITE LIGHT" SETTING! *SIGH*
DUMMY NEEDS TO TEST ME NOW AND THEN, OR AT LEAST CHECK MY APP!
AT LEAST YOU GET USED! I NEVER DO! ALL HE EATS IS TAKE-OUT!
DON'T BOTHER HIM! THE PREVIOUS SMOKE DETECTOR, HE BEAT TO DEATH WITH A BROOM HANDLE!!
DID YOU SEE WHAT TIME HE GOT IN LAST NIGHT? SCANDALOUS!
HEY GUYS! THE HOUSE SMARTMETER IS TELLING EVERYONE THAT SCAREDY CAT STILL USES A NIGHT LIGHT! HA HA!
I REFUSE TO PICK UP THIS FRENCH FRY. LAZYBONES CAN DO IT HIMSELF!
What your Internet of Things is saying about you...
© 2014 Geek Culture
joyoftech.com

That's all folks!

João Pedro Dias
jpmdias@fe.up.pt
https://jpdias.me

*If you can't fix it,
you don't own it.* *(iFixit)*