Что такое hardware hacking, и как им обмазаться

Aanper
zaf0d

Hardware hacking village

August 8-10, 2008

DEF CON 16

It was once a small room filled with people and solder fumes and has since exploded in size and number of people that come through

Кто такой Хакер ?

A person who delights in having an intimate understanding of the internal workings of a system, computers and computer networks in particular.

RFC 1392, Internet Users' Glossary

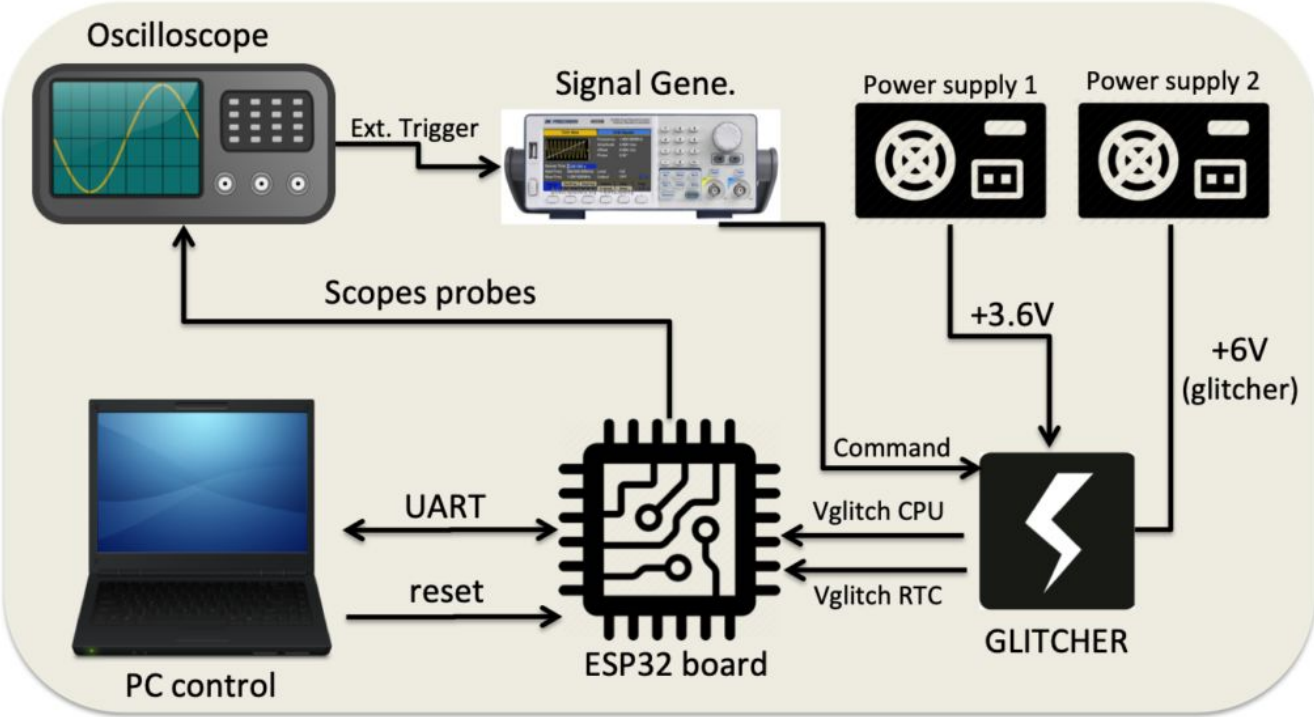
Человек, получающий удовольствие от глубокого понимания внутренней работы систем, компьютеров и компьютерных сетей в частности.

И все таки, зачем?

- Не умея нападать — не сможешь защищаться
- Верификация неизвестных функций сторонних устройств
- Поиск недокументированных возможностей
- Любопытство — понять как это работает

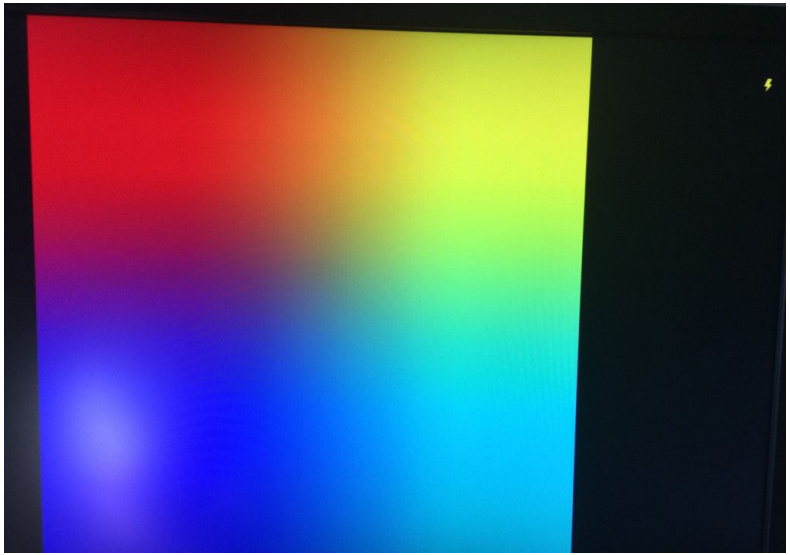
In soviet Russia Therac-25 hacks you

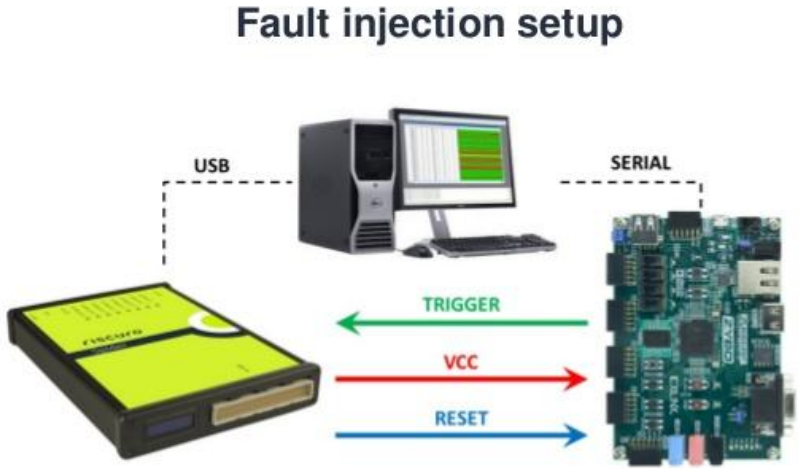
Pwn the ESP32 Secure Boot



https://limitedresults.com/2019/09/pwn-the-esp32-secure-boot/

Escalating Privileges in Linux using Voltage Fault Injection



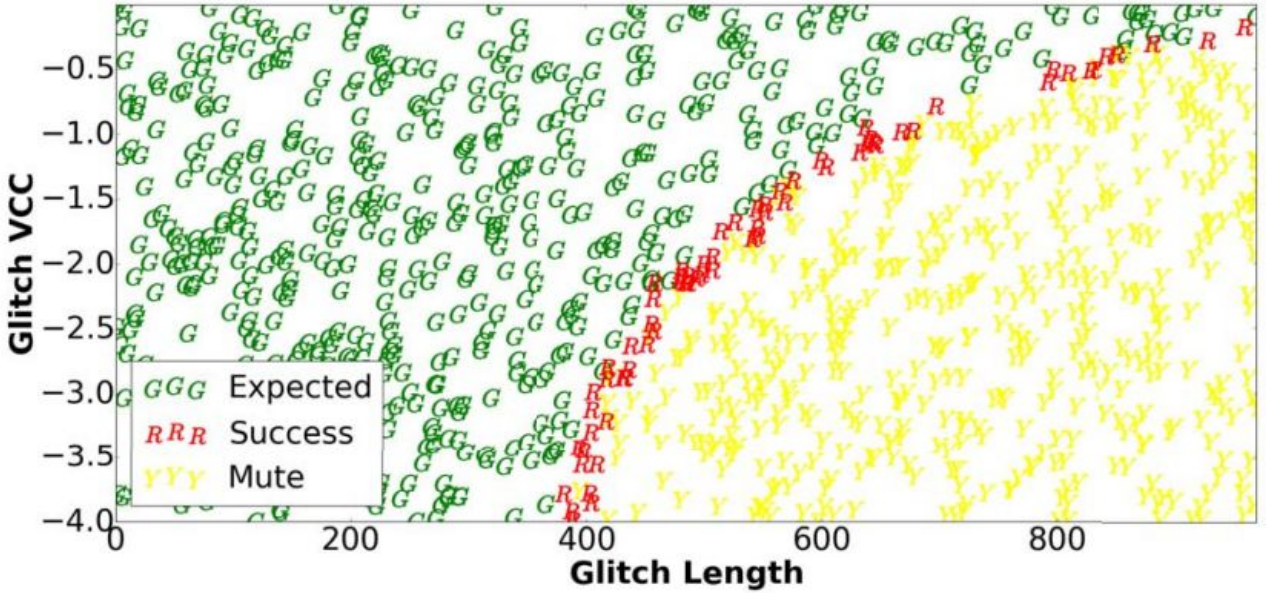


Target

- Fast and feature rich System-on-Chip (SoC)
- ARM Cortex-A9 (32-bit)
- Ubuntu 14.04 LTS (fully patched)

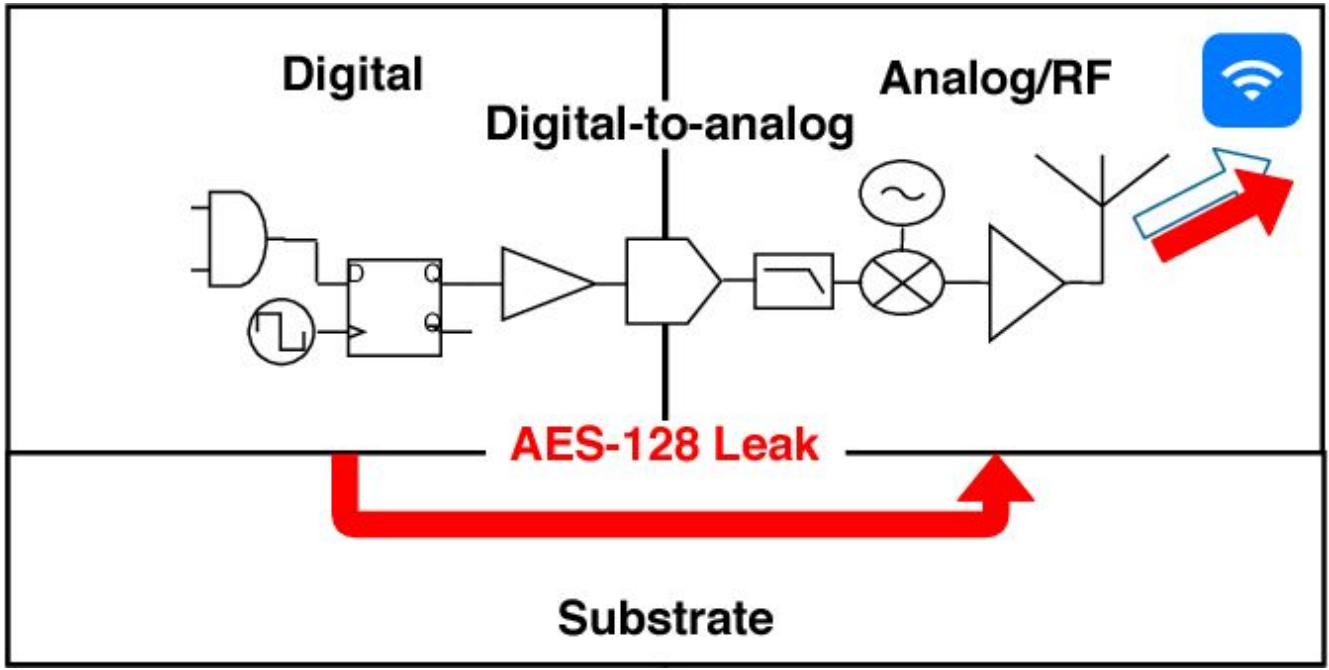
https://www.riscure.com/uploads/2017/10/Riscure_Whitepaper_Escalating_Privileges_in_Linux_using_Fault_Injection.pdf

Escalating Privileges in Linux using Voltage Fault Injection



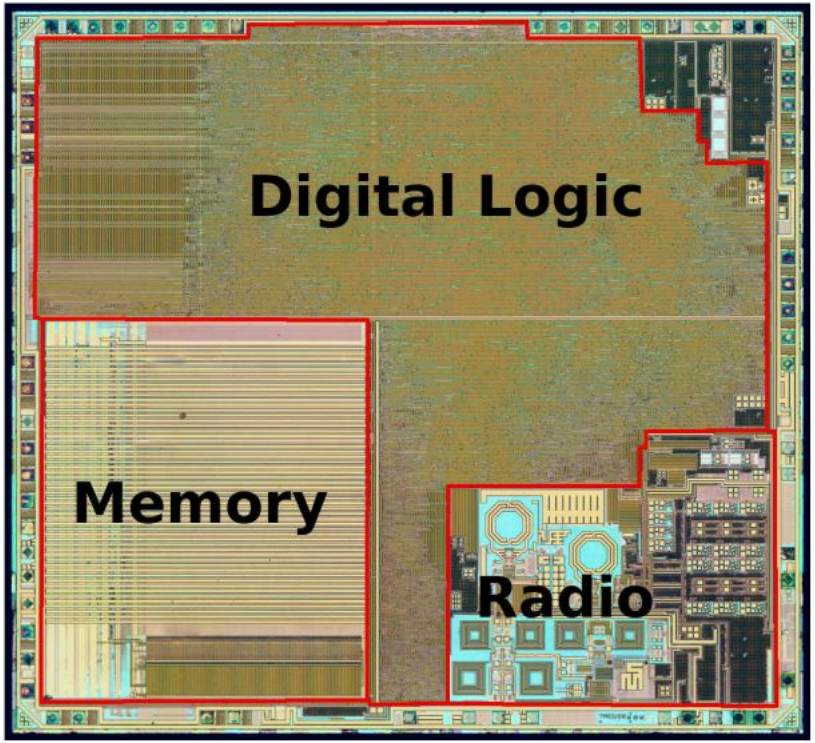
https://www.riscure.com/uploads/2017/10/Riscure_Whitepaper_Escalating_Privileges_in_Linux_using_Fault_Injection.pdf

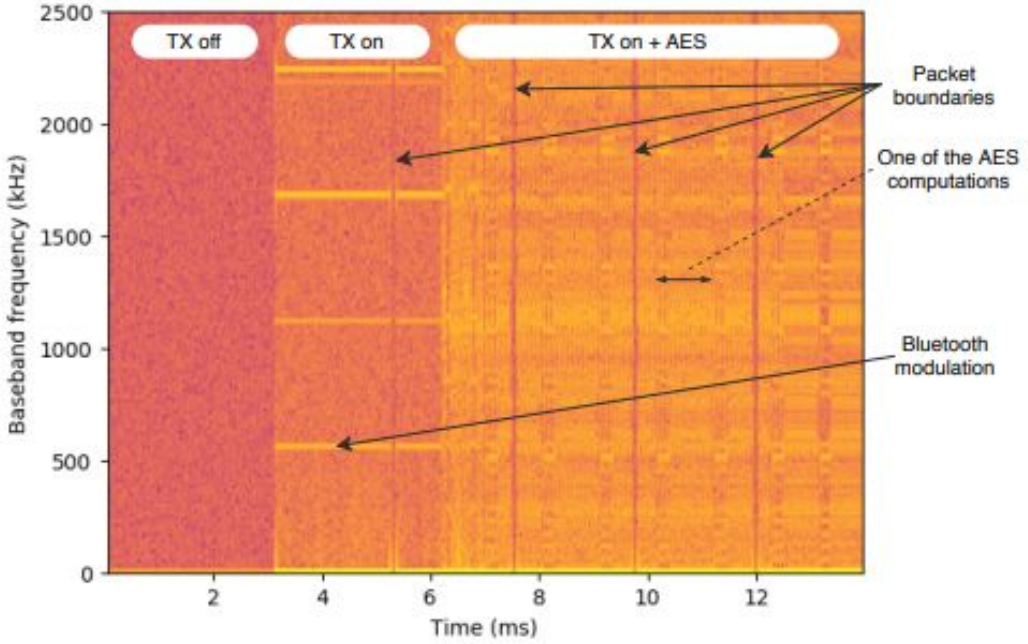
Screaming Channels: When Electromagnetic Side Channels Meet Radio Transceivers



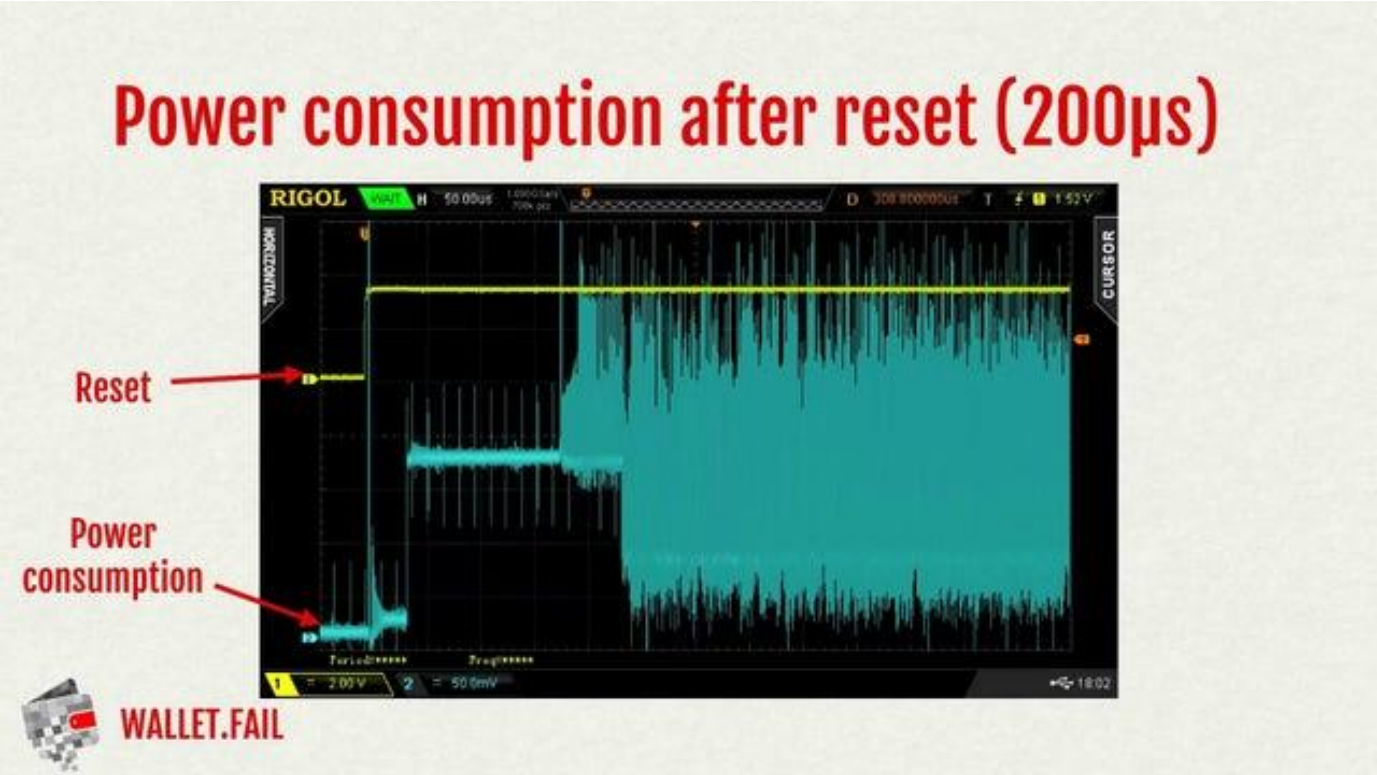
http://www.s3.eurecom.fr/docs/ccs18_camurati_preprint.pdf

Screaming Channels: When Electromagnetic Side Channels Meet Radio Transceivers



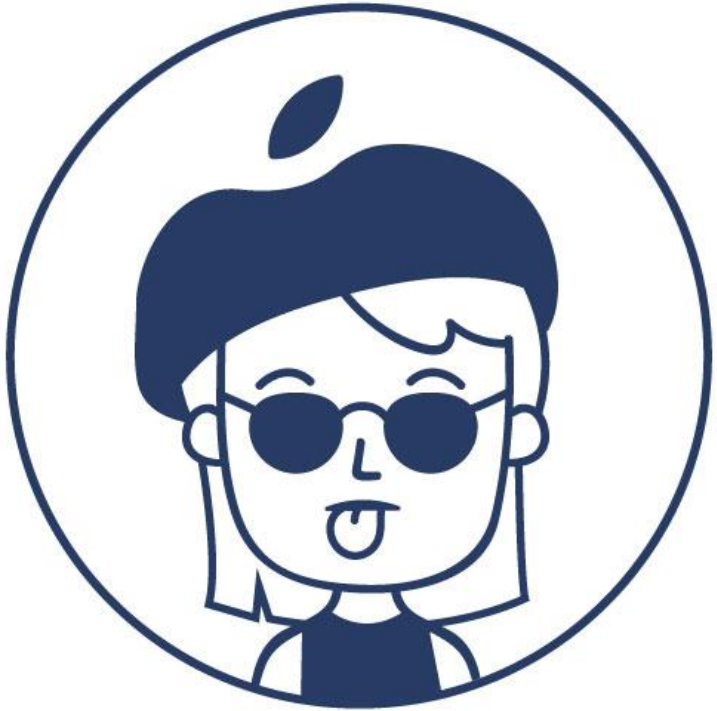


Wallet fail (https://wallet.fail/)



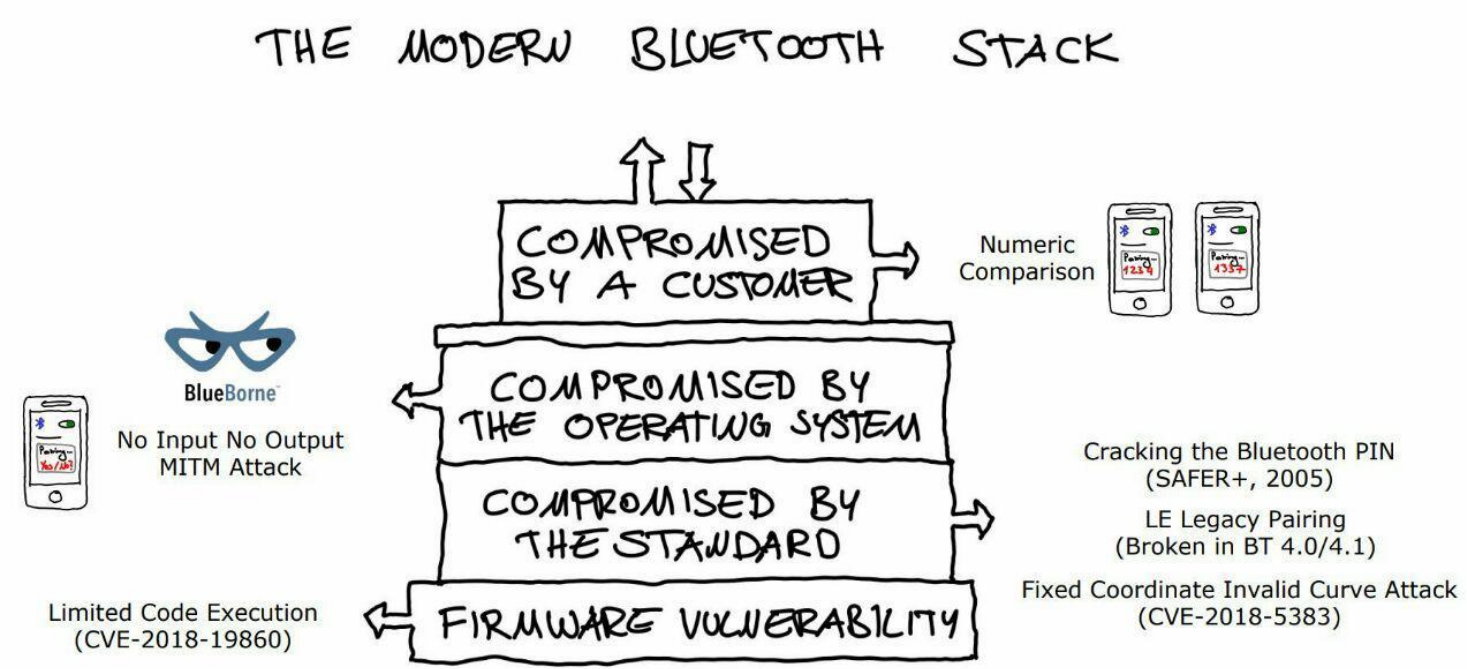
Apple BLEee

TL;DR: If Bluetooth is ON on your Apple device everyone nearby can understand current status of your device, get info about battery, device name, Wi-Fi status, buffer availability, OS version and even get your mobile phone number



https://hexway.io/blog/apple-bleee/

“Bluetooth: With Low Energy comes Low Security”



Slide: https://www.usenix.org/sites/default/files/conference/protected-files/ryan_woot13_slides.pdf
WP: https://www.usenix.org/system/files/conference/woot13/woot13-ryan.pdf

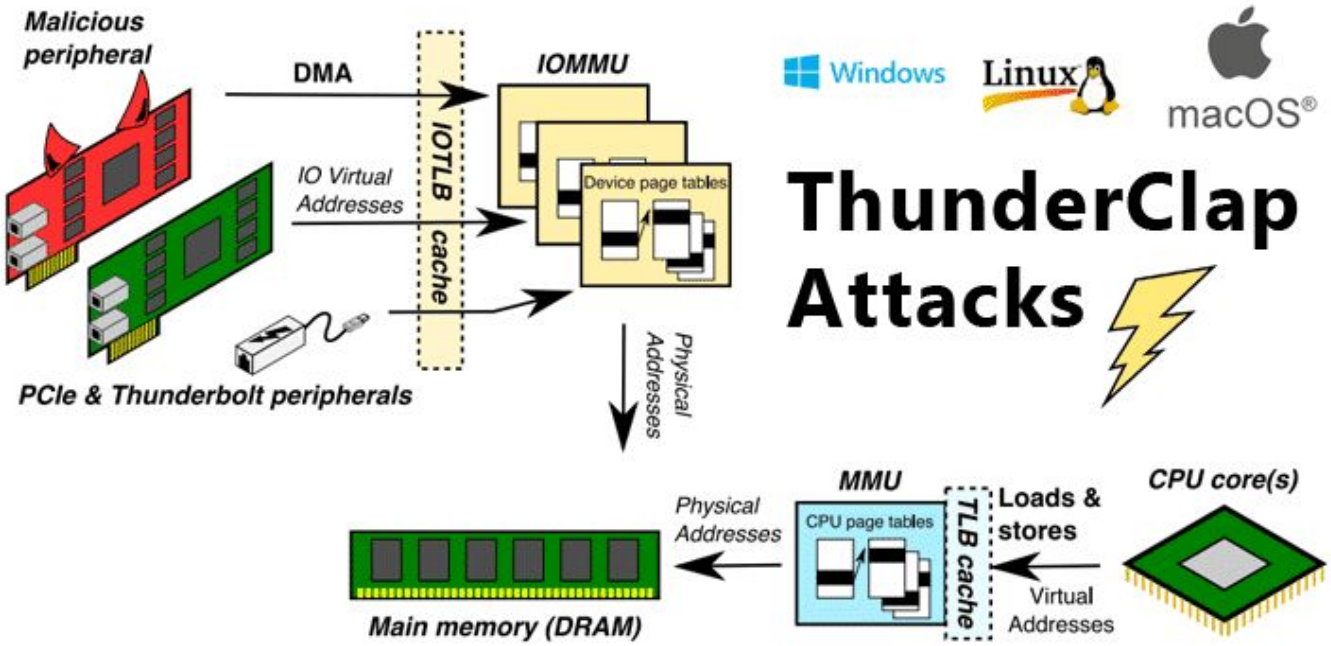
Apple checkm8

https://twitter.com/axi0mx/status/1177542201670168576

Meltdown, spectre and other

DMA attacking over USB-C and Thunderbolt 3

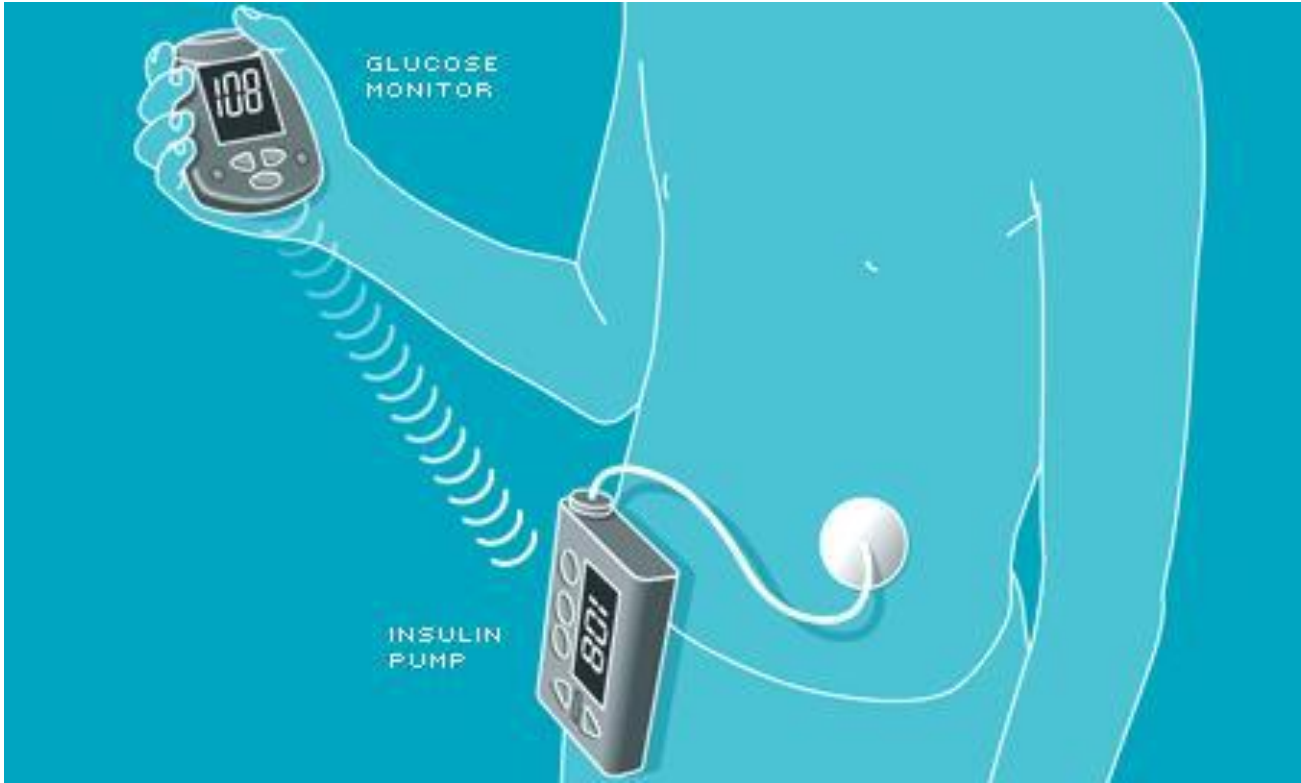
http://thunderclap.io/
http://blog.frizk.net/2016/10/dma-attacking-over-usb-c-and.html



Medtronic MiniMed 508 and Paradigm Series Insulin Pumps

The affected insulin pumps are designed to communicate using a wireless RF with other devices, such as blood glucose meters, glucose sensor transmitters, and CareLink USB devices. This wireless RF communication protocol does not properly implement authentication or authorization. An attacker with adjacent access to one of the affected insulin pump models can inject, replay, modify, and/or intercept data. This vulnerability could also allow attackers to change pump settings and control insulin delivery.

https://www.us-cert.gov/ics/advisories/icsma-19-178-01

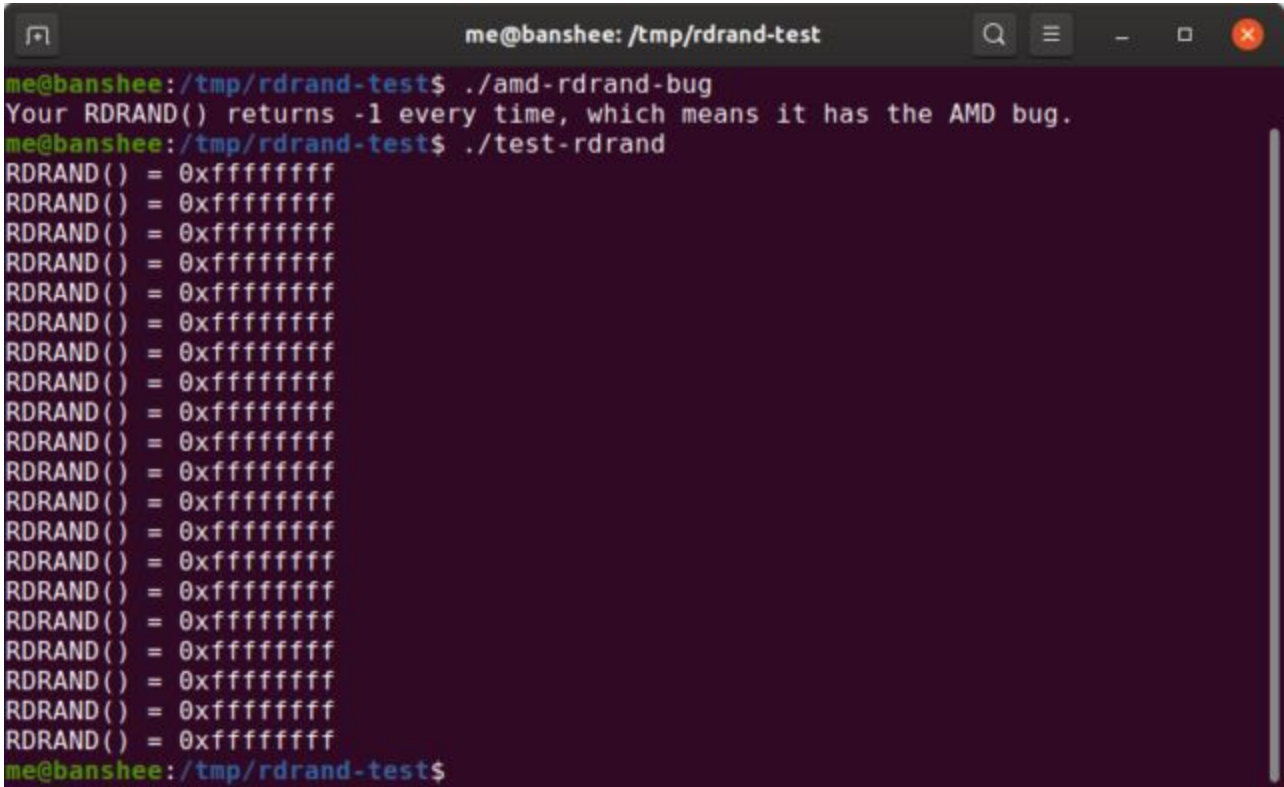


USBAnywhere

https://github.com/eclypsium/USBAnywhere

Ryzen 3000 random bug

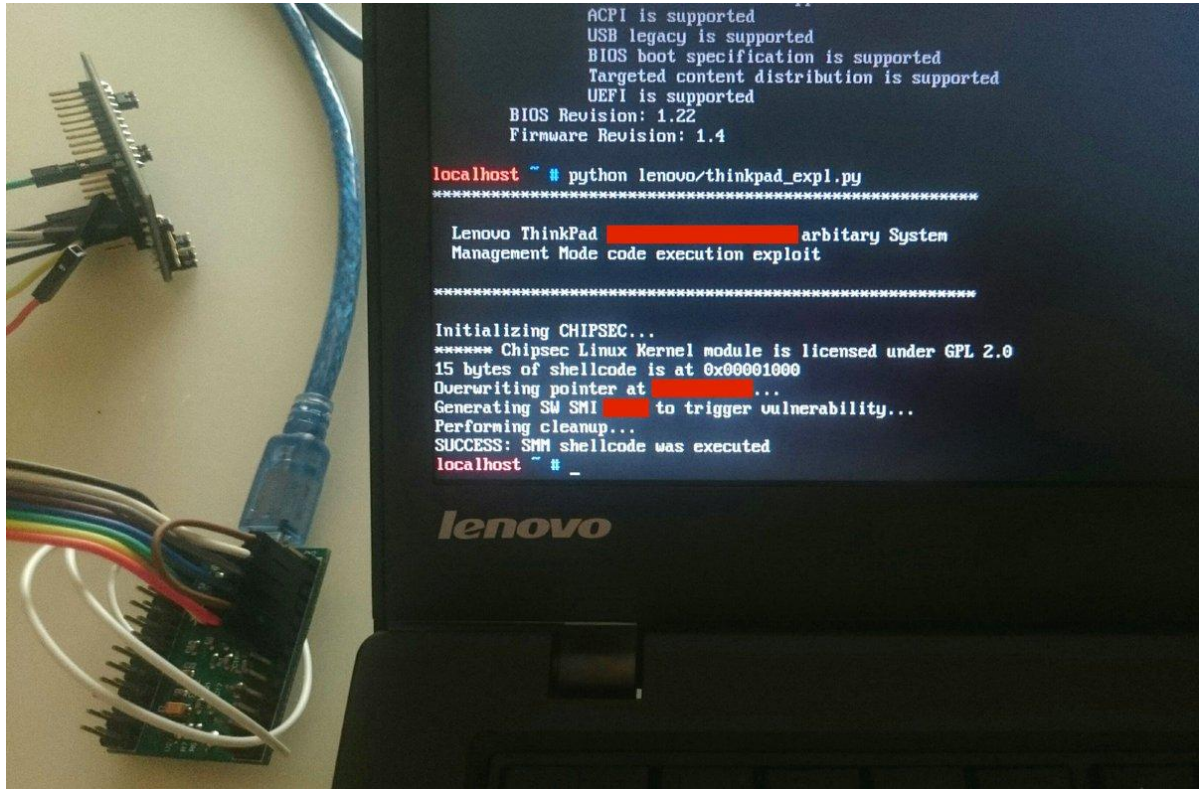
https://community.amd.com/thread/244879



```
me@banshee:/tmp/rdrand-test$ ./amd-rdrand-bug
Your RDRAND() returns -1 every time, which means it has the AMD bug.
me@banshee:/tmp/rdrand-test$ ./test-rdrand
RDRAND() = 0xffffffff
RDRAND() = 0xffffffff
RDRAND() = 0xffffffff
RDRAND() = 0xffffffff
RDRAND() = 0xffffffff
RDRAND() = 0xffffffff
RDRAND() = 0xffffffff
RDRAND() = 0xffffffff
RDRAND() = 0xffffffff
RDRAND() = 0xffffffff
RDRAND() = 0xffffffff
RDRAND() = 0xffffffff
RDRAND() = 0xffffffff
RDRAND() = 0xffffffff
RDRAND() = 0xffffffff
RDRAND() = 0xffffffff
RDRAND() = 0xffffffff
RDRAND() = 0xffffffff
RDRAND() = 0xffffffff
RDRAND() = 0xffffffff
me@banshee:/tmp/rdrand-test$
```

ThinkPwn

https://github.com/Cr4sh/ThinkPwn



Critical Intel Thunderbolt Software and Firmware Updates - ThinkPad

Support

Documentation

Critical Intel Thunderbolt Software and Firmware Updates - ThinkPad

Symptom

Systems may experience any of the following symptoms:

- USB-C port not working
- Intel Thunderbolt controller not visible in the OS/Device Manager
- USB-C or Thunderbolt docking stations not visible or having connectivity problems
- HDMI output not available
- System battery not charging with a USB-C power adapter connected to the USB-C port
- Intel Thunderbolt pop-up error message
- Intel Thunderbolt safe mode error message
- BIOS Thunderbolt communication error or hang during POST

These symptoms may occur after 6 to 12 months of typical usage.

«До Второй мировай войны жизнь была проще.

После нее у нас появились системы»

Фото «первого компьютерного бага»

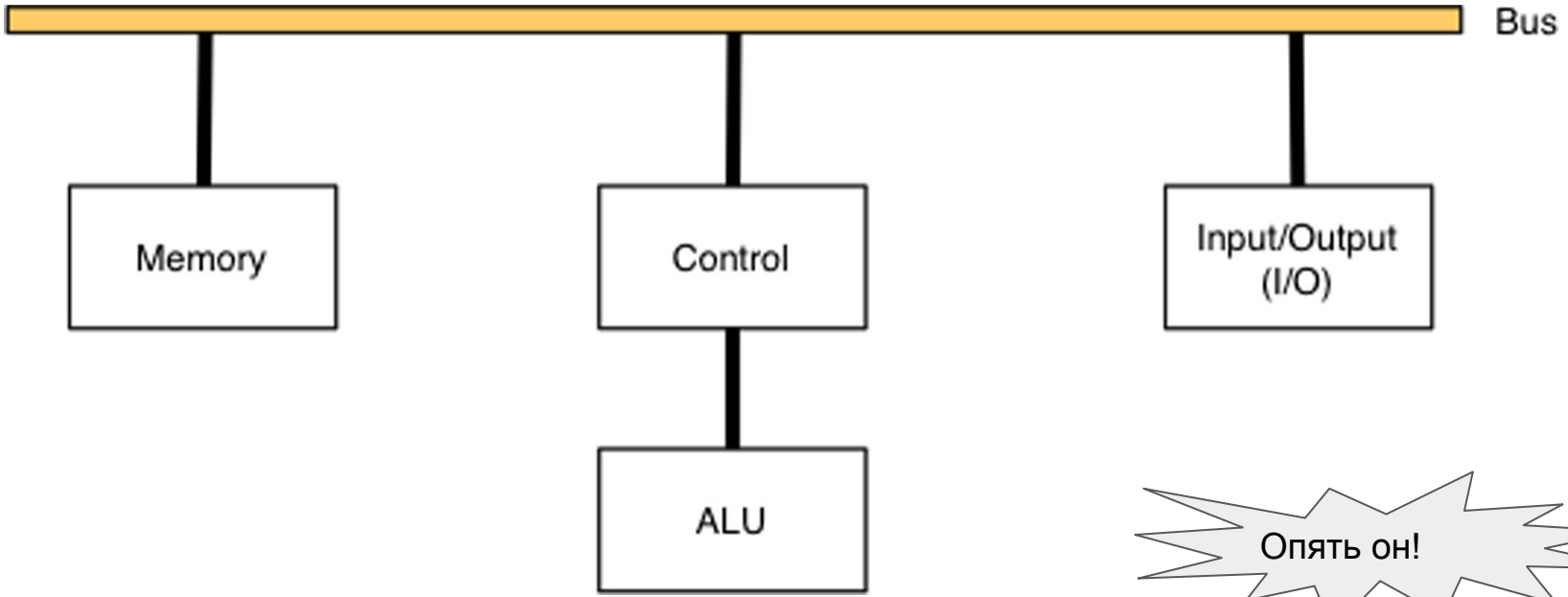
9/9

0800 Arctan started
1000 " stopped - arctan ✓
13°vc (032) MP - MC 2.130476415 (033) PRO 2 2.130476415
correct 2.130676415
1.2700 9.037 847 025
9.037 846 995 correct
4.615925059(-2)
Relays 6-2 in 033 failed special speed test
In relay " 10.00 test.
Relays changed
1100 Started Cosine Tape (Sine check)
1525 Started Multy Adder Test.
1545 Relay #70 Panel F (moth) in relay.
First actual case of bug being found.
1700 closed down.

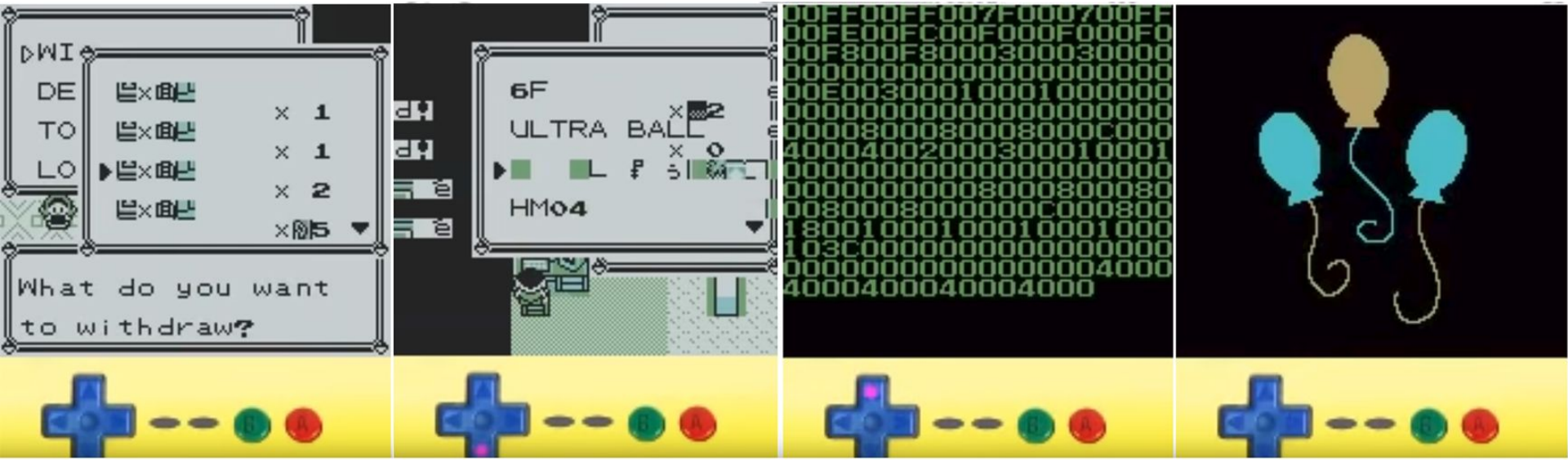
Свойства систем

- Сложность
- Взаимодействие
- Неожиданность и избыточность
- Баги

Архитектура Фон неймана



Weird Machine



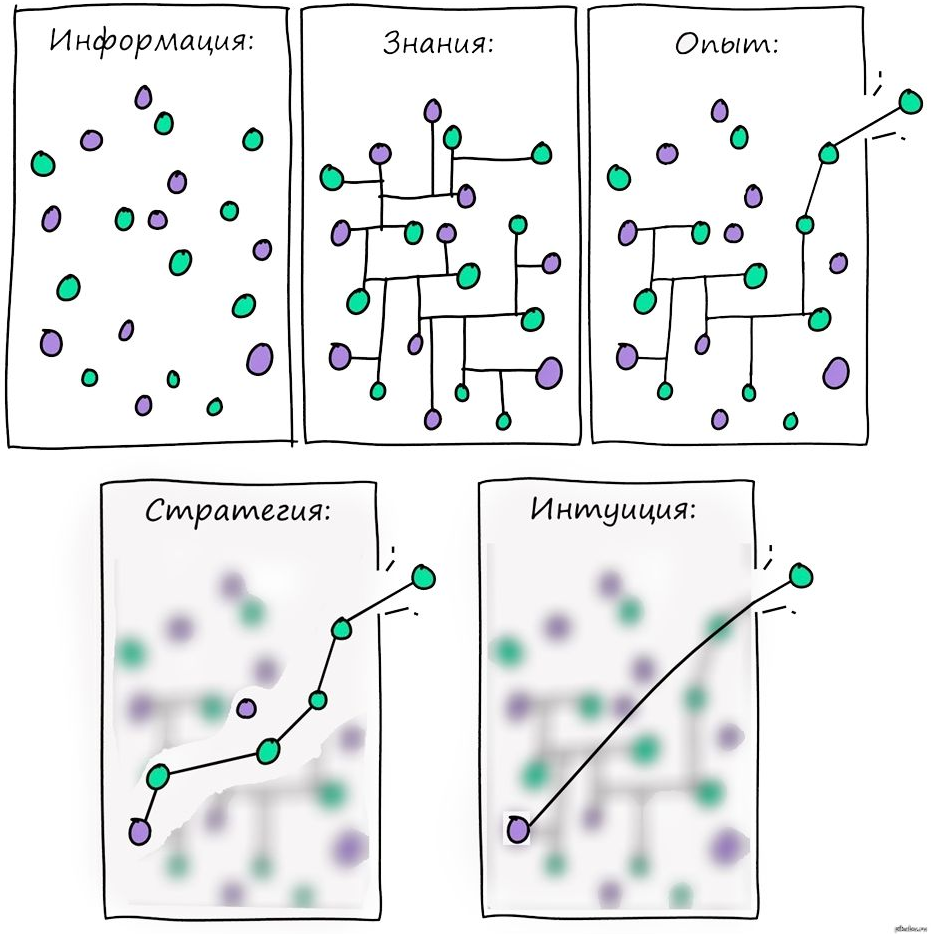
http://aurellem.org/vba-clojure/html/total-control.html

Weird Machine

https://hackaday.com/2014/01/10/teaching-mario-to-play-pong-and-snake-through-innumerable-exploits/

Про коробочки и вот это вот все


Это... веер.!!!
Это... Копье !!!
Это... стена!!!
Это... верёвка!!!
Это... змея!!!
Это... дерево!!!


Информация:
Знания:
Опыт:
Стратегия:
Интуиция:

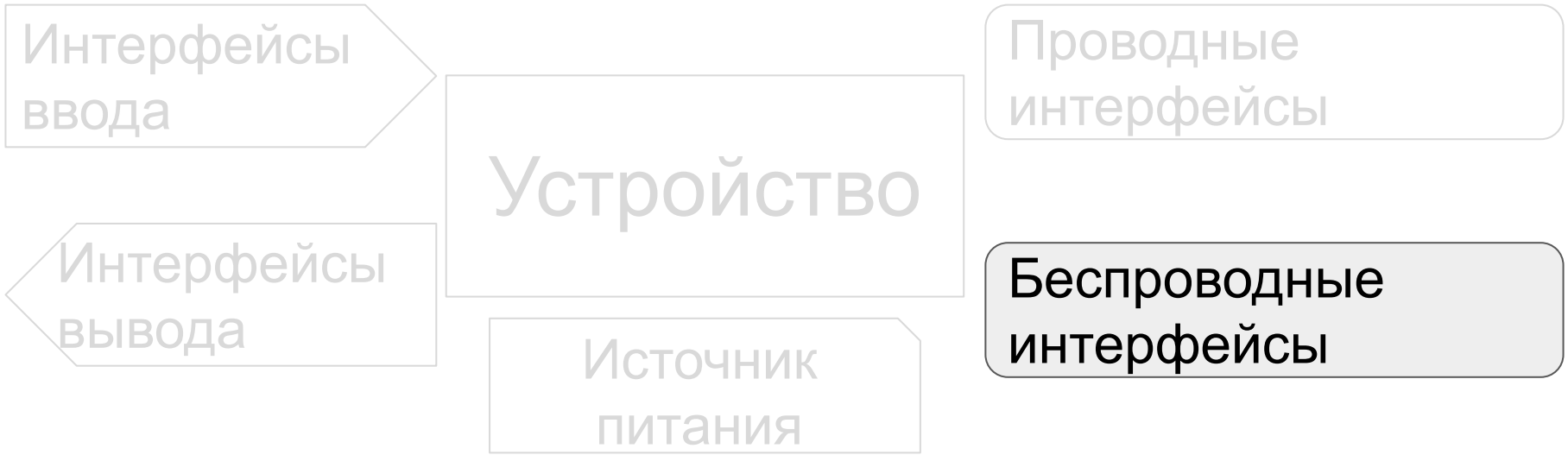
Blackbox


Интерфейсы ввода
Устройство
Проводные интерфейсы
Интерфейсы вывода
Беспроводные интерфейсы
Источник питания

Blackbox

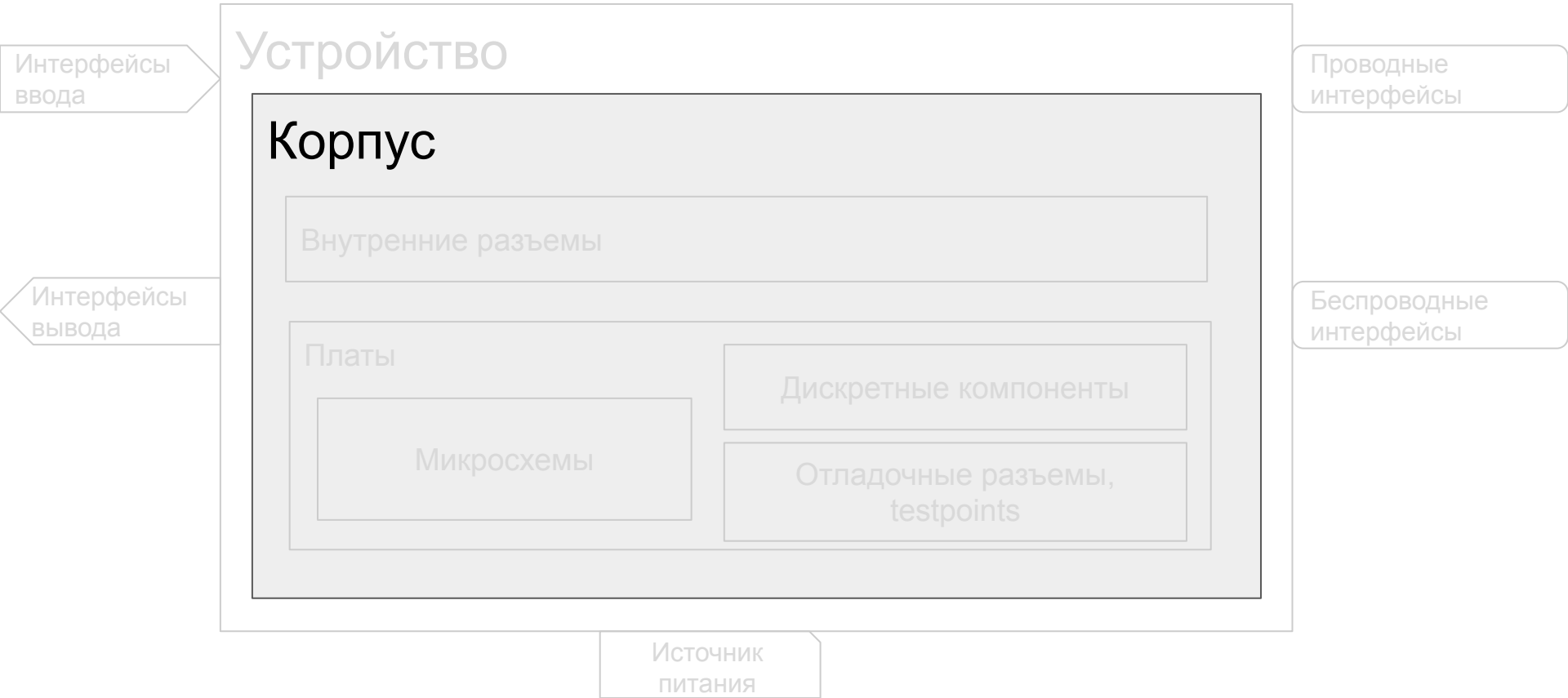

Интерфейсы ввода
Интерфейсы вывода
Устройство
Источник питания
Проводные интерфейсы
Беспроводные интерфейсы

Blackbox

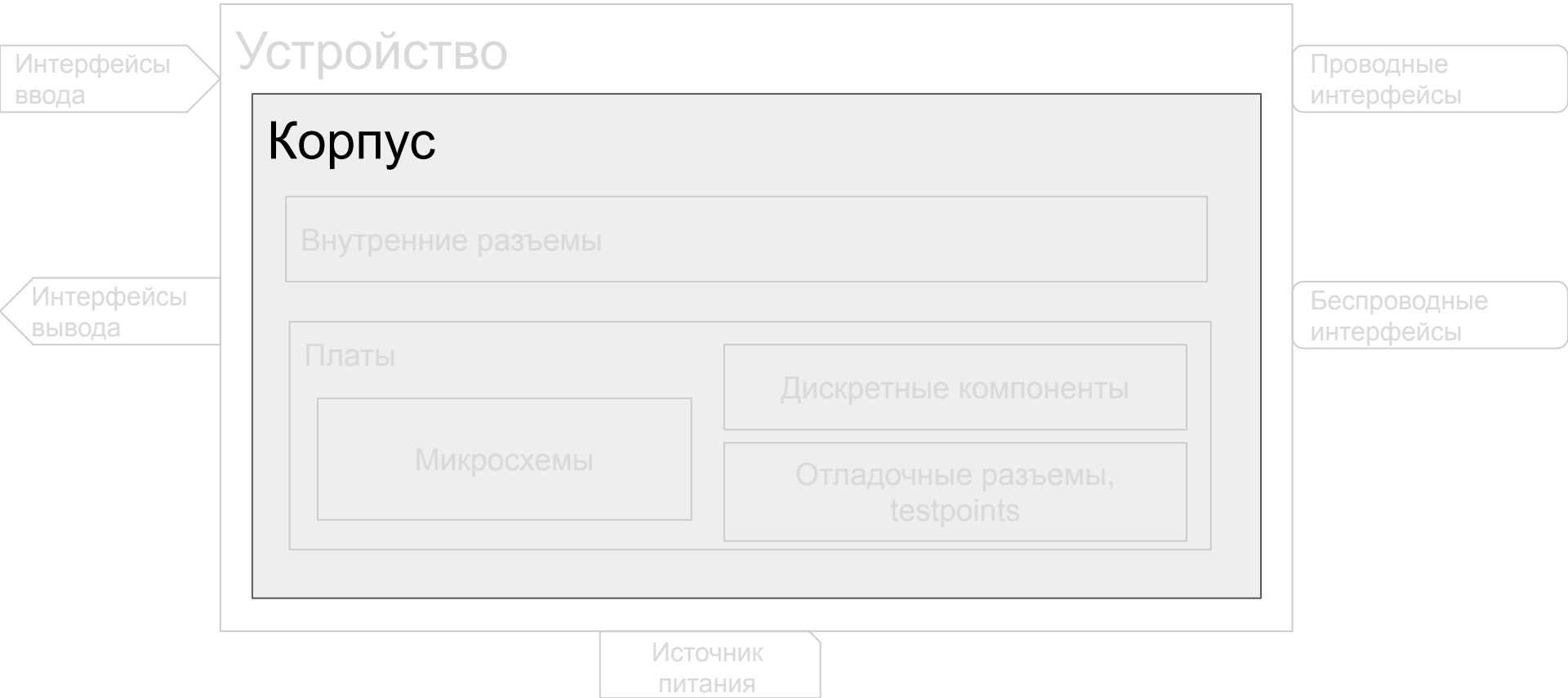

Интерфейсы ввода
Устройство
Проводные интерфейсы
Интерфейсы вывода
Беспроводные интерфейсы
Источник питания

Open the blackbox

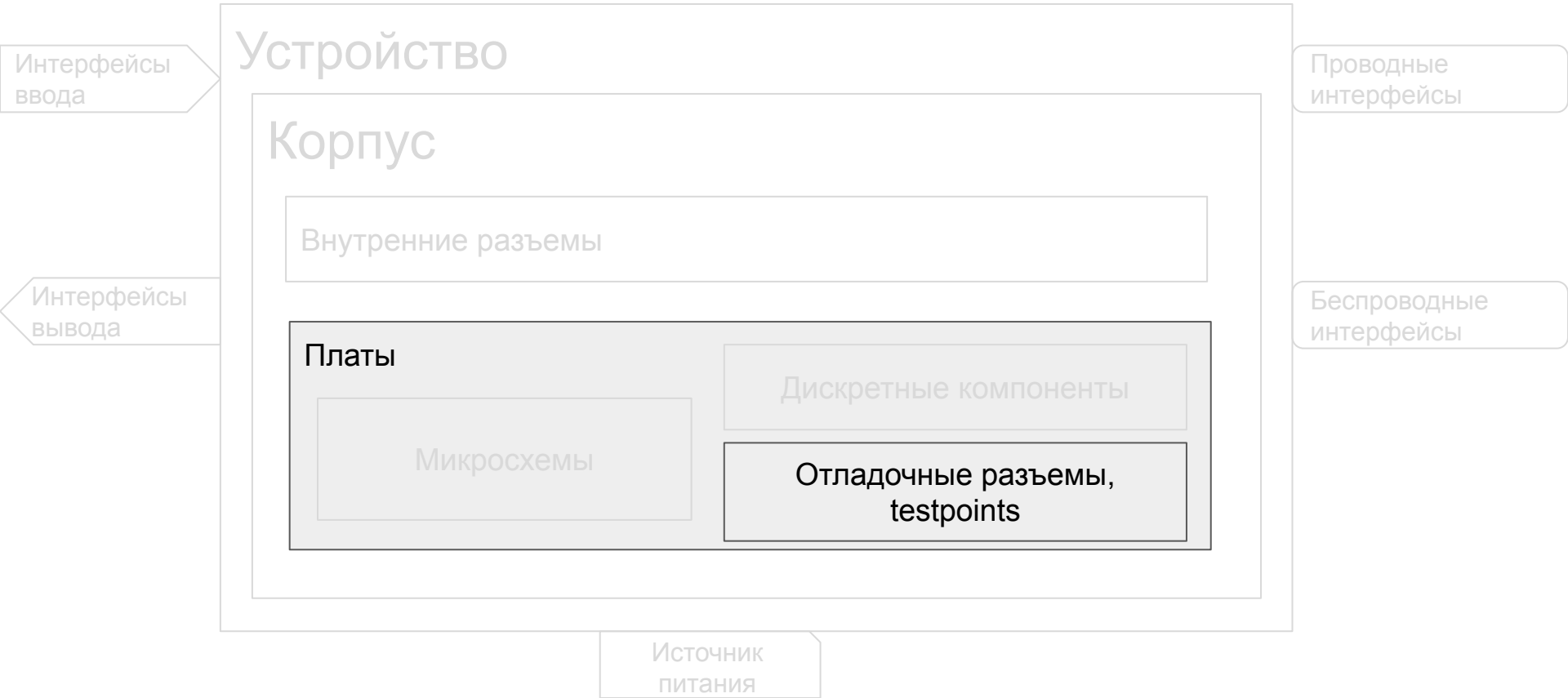
Open the blackbox

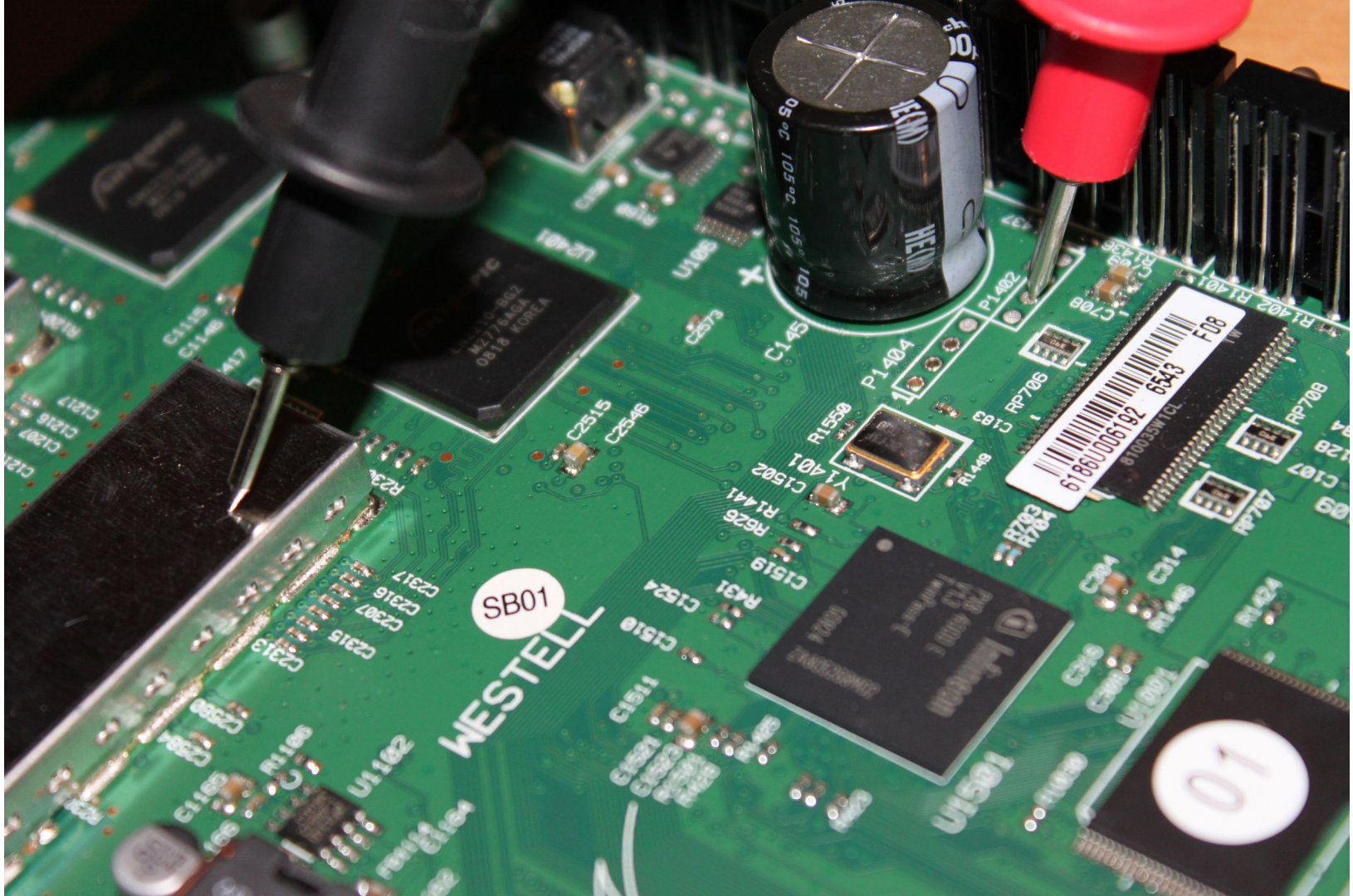


Open the blackbox

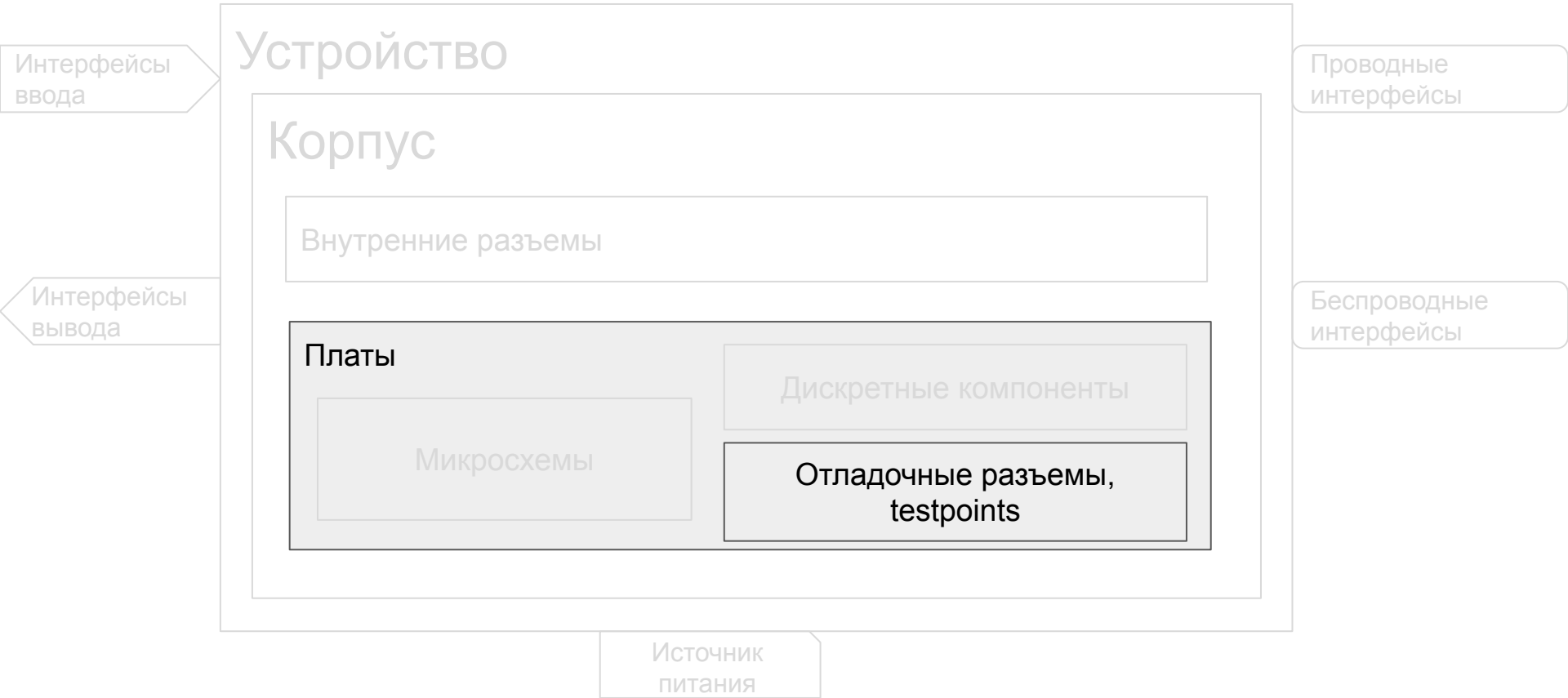


Open the blackbox

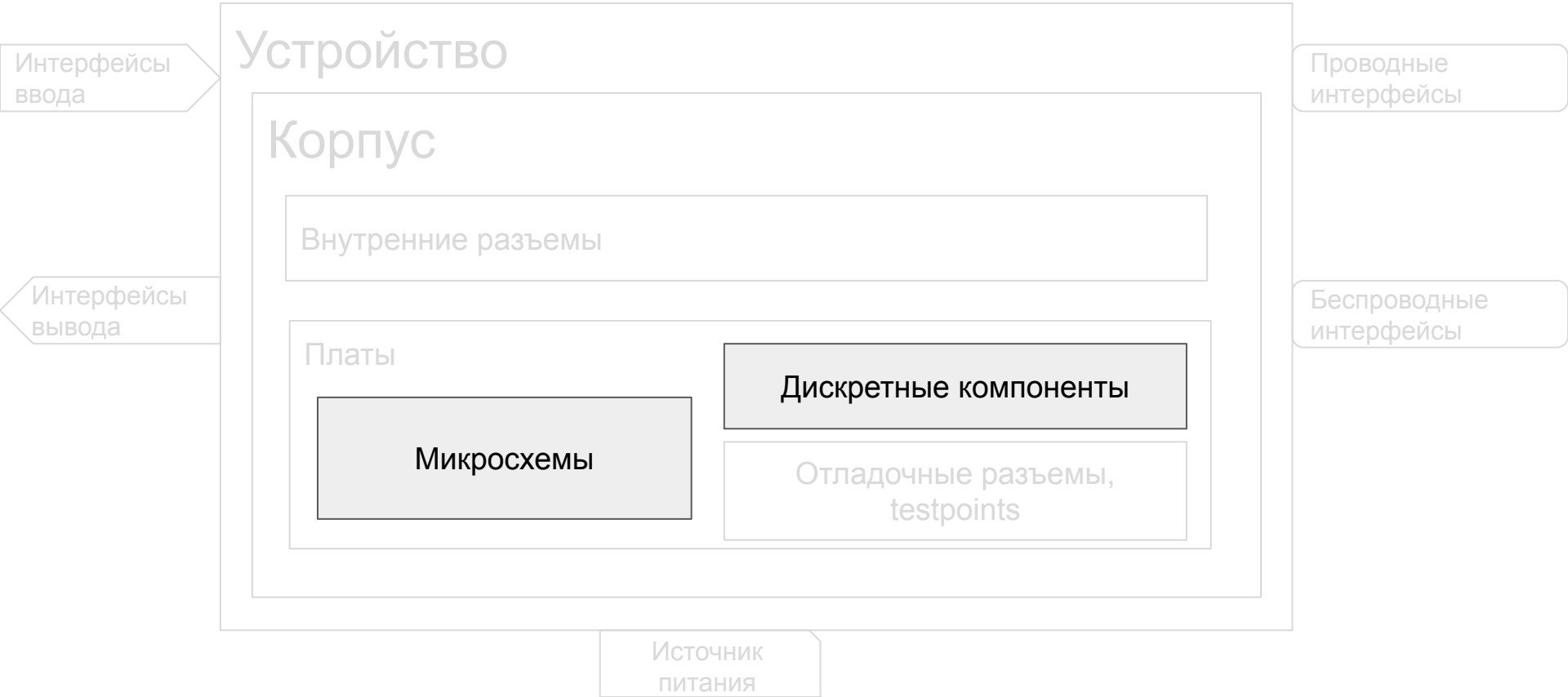



SB01
WESTELL
P1404
P1402
R1558
Y1401
U1102
U1501
01

Open the blackbox

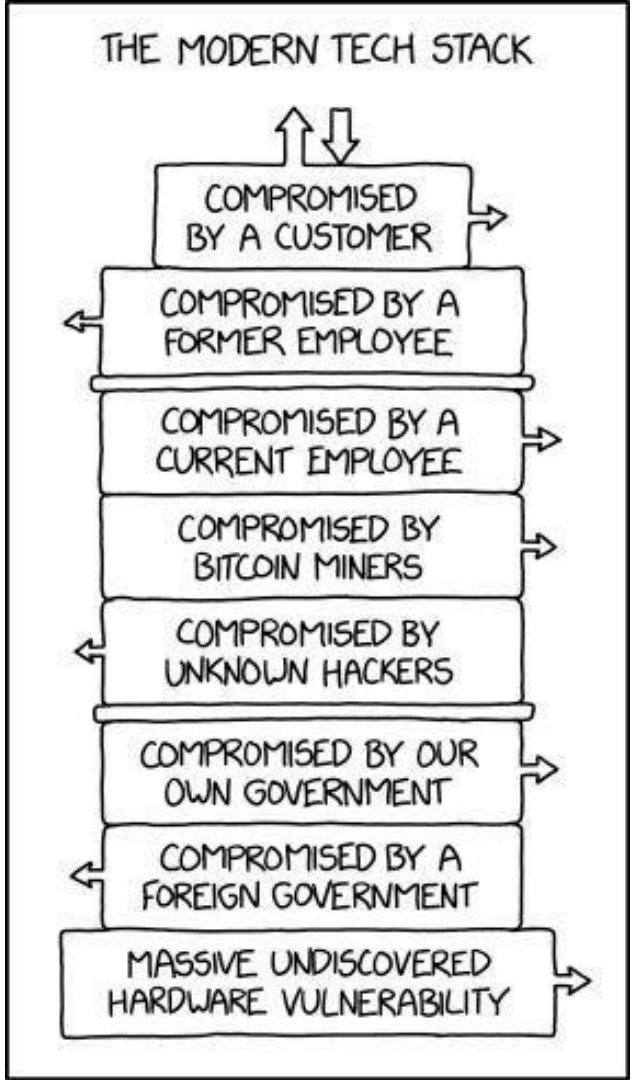


Микросхемы


Устройство
Интерфейсы ввода
Проводные интерфейсы
Корпус
Внутренние разъемы
Интерфейсы вывода
Беспроводные интерфейсы
Платы
Дискретные компоненты
Микросхемы
Отладочные разъемы, testpoints
Источник питания

Инструменты

- отвертка, нож и кусачки
- пинцет
- паяльник, припой и флюс
- куча монтажных проводов, крокодилы
- мультиметр
- осциллограф
- логический анализатор
- USB-UART, SPI, I^2C
- JTAG/SWD
- NAND flash reader
- ...


THE MODERN TECH STACK
COMPROMISED BY A CUSTOMER
COMPROMISED BY A FORMER EMPLOYEE
COMPROMISED BY A CURRENT EMPLOYEE
COMPROMISED BY BITCOIN MINERS
COMPROMISED BY UNKNOWN HACKERS
COMPROMISED BY OUR OWN GOVERNMENT
COMPROMISED BY A FOREIGN GOVERNMENT
MASSIVE UNDISCOVERED HARDWARE VULNERABILITY