HARDWARE SECURITY IS HARD:

HOW HARDWARE BOUNDARIES DEFINE PLATFORM SECURITY

@matrosov

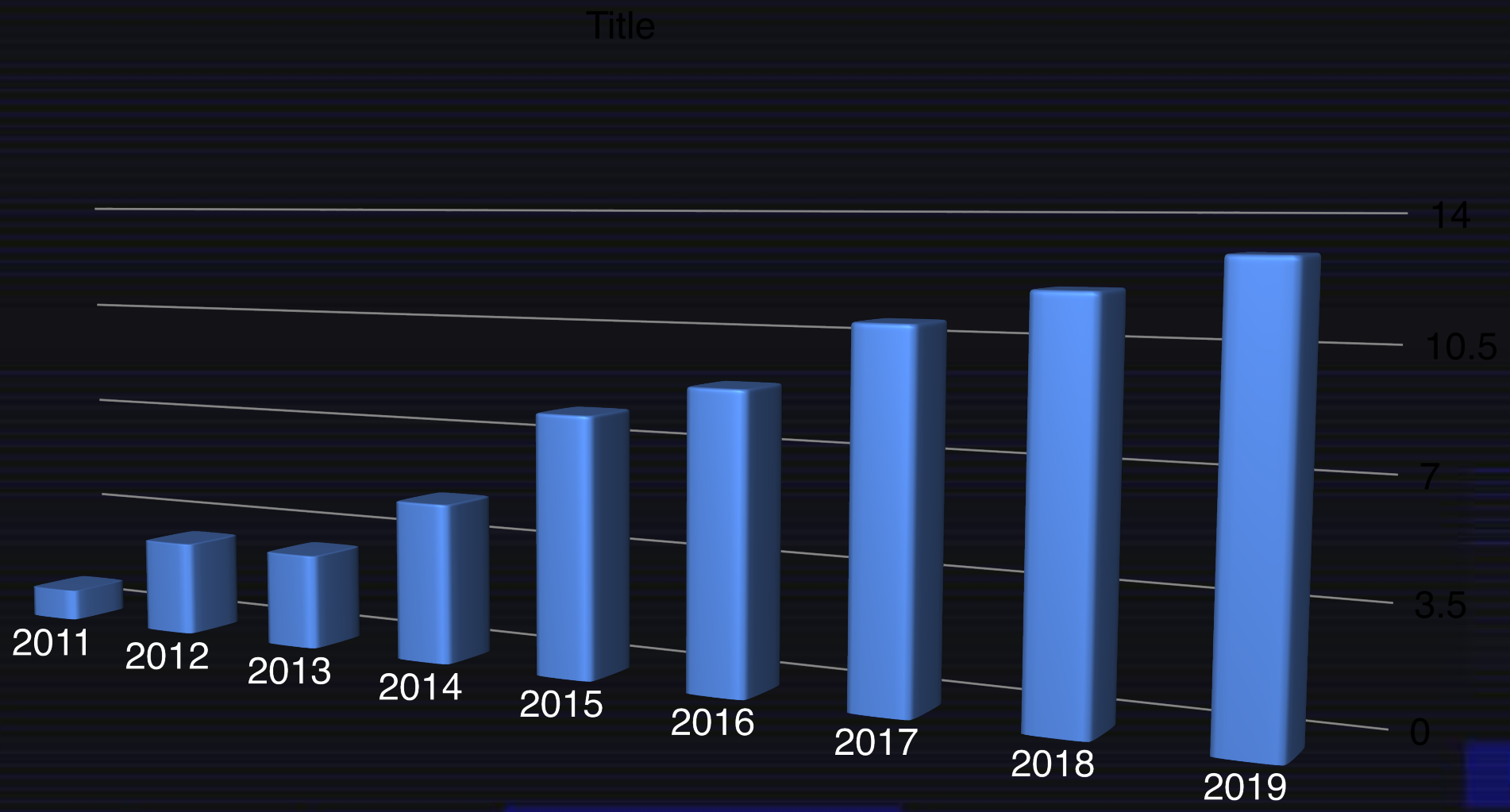
ZERO NIGHTS 2019 EDITION

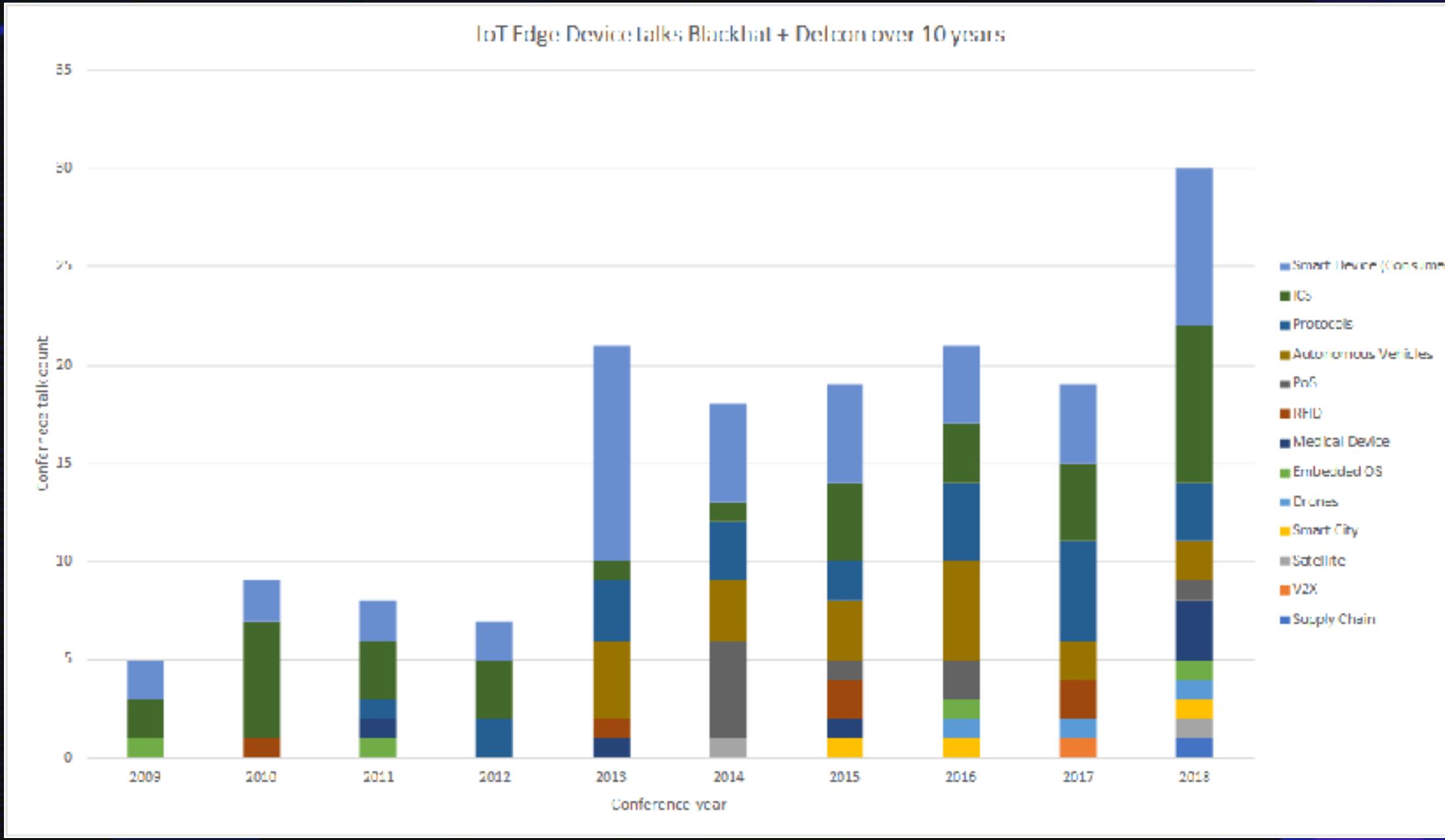
Offensive Security REsearch at

Former Principal Security Researcher @Cylance @Intel @ESET

Doing Security REsearch since 1997

Constant HW security talks growth at ZN




IoT Edge Device talks Blackhat + Defcon over 10 years
35
30
25
20
15
10
5
0
Conference talk count
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
Conference year
Smart Device (Consumer
ICs
Protocols
Autonomous Vehicles
PoS
RFID
Medical Device
Embedded OS
Drones
Smart City
Satellite
V2X
Supply Chain

The Advanced Threats Evolution: REsearchers Arm Race

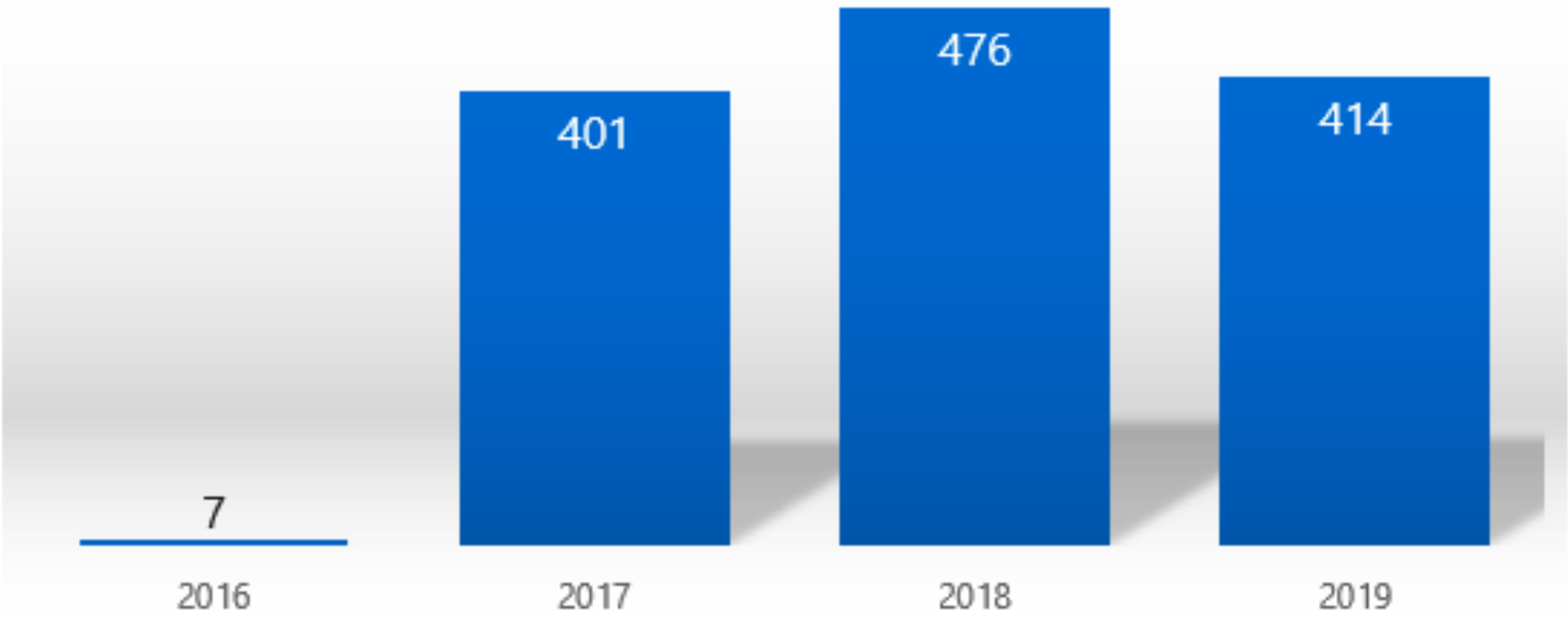
https://www.platformsecuritysummit.com/2019/speaker/matrosov/

Security Industry Visibility Point

Modern Persistence Techniques

https://www.platformsecuritysummit.com/2019/speaker/matrosov/

Number of firmware vulnerabilities



Source: National Vulnerabilities Database

HW TREATS MODEL

||

FW THREAT MODEL

NOWADAYS IT'S HARD TO SPOT REAL BOUNDARIES BETWEEN HARDWARE AND FIRMWARE

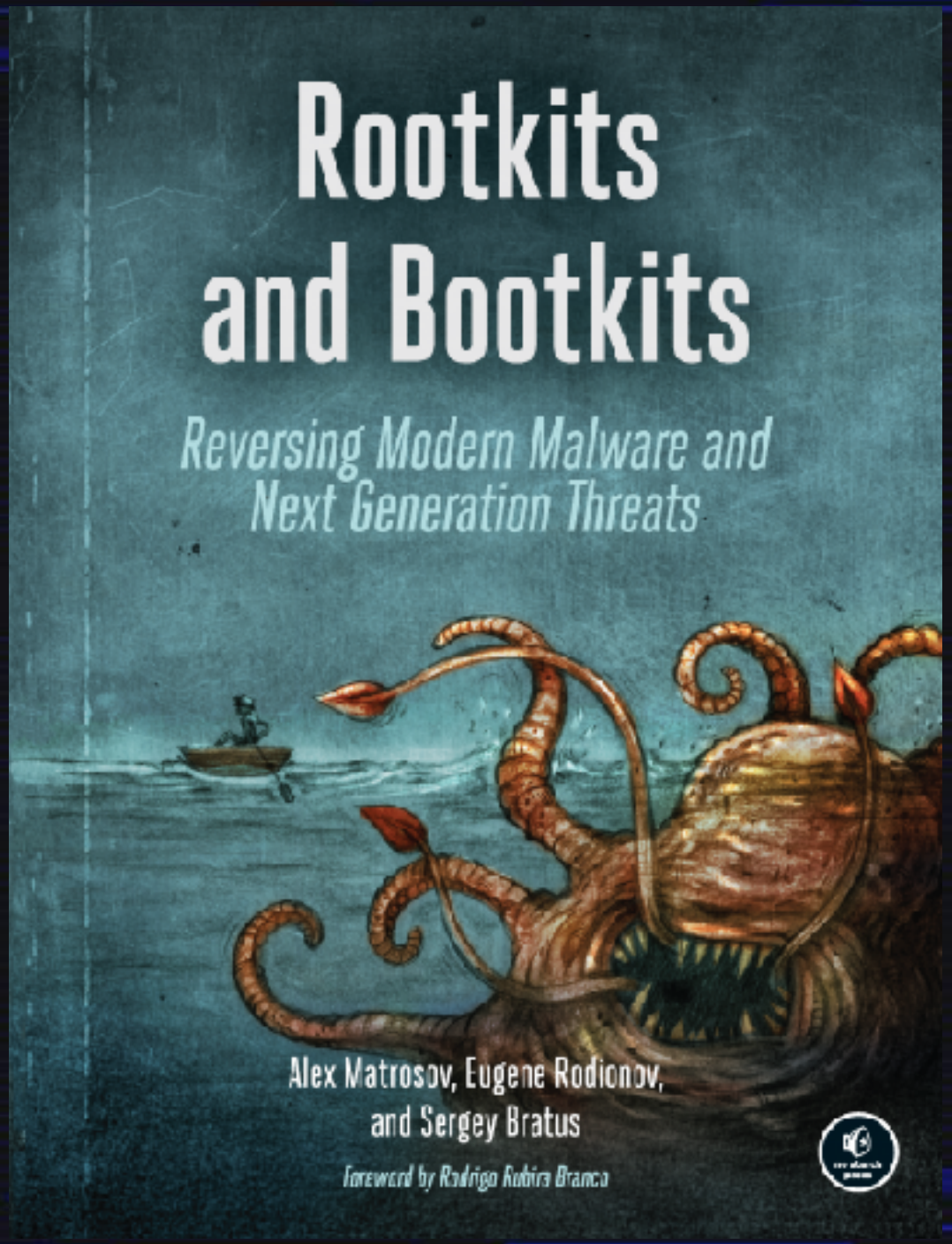
HW TREATS MODEL && FW THREAT MODEL

Identify Threats

- Threats can be identified by analyzing the security requirements and platform diagram
- Threats should be categorized for further analysis
  - Techniques for analyzing threats: STRIDE, DREAD, PASTA, LINDDUN, etc.

https://uefi.org/sites/default/files/resources/UEFI%20SDL%20Webinar_Final%20Slides%20-%20PDF.pdf

IT'S HARD TO FIND REAL SECURITY PROBLEMS IN PLATFORM DIAGRAM AND REQUIREMENTS


Rootkits and Bootkits
Reversing Modern Malware and Next Generation Threats
Alex Matrosov, Eugene Rodionov, and Sergey Bratus
Foreword by Rodrigo Rubira Branco

Rootkits

TRADITIONALLY HARDWARE DESIGN OBJECTIVES ARE DRIVEN BY COST AND PERFORMANCE, BUT NOT SECURITY

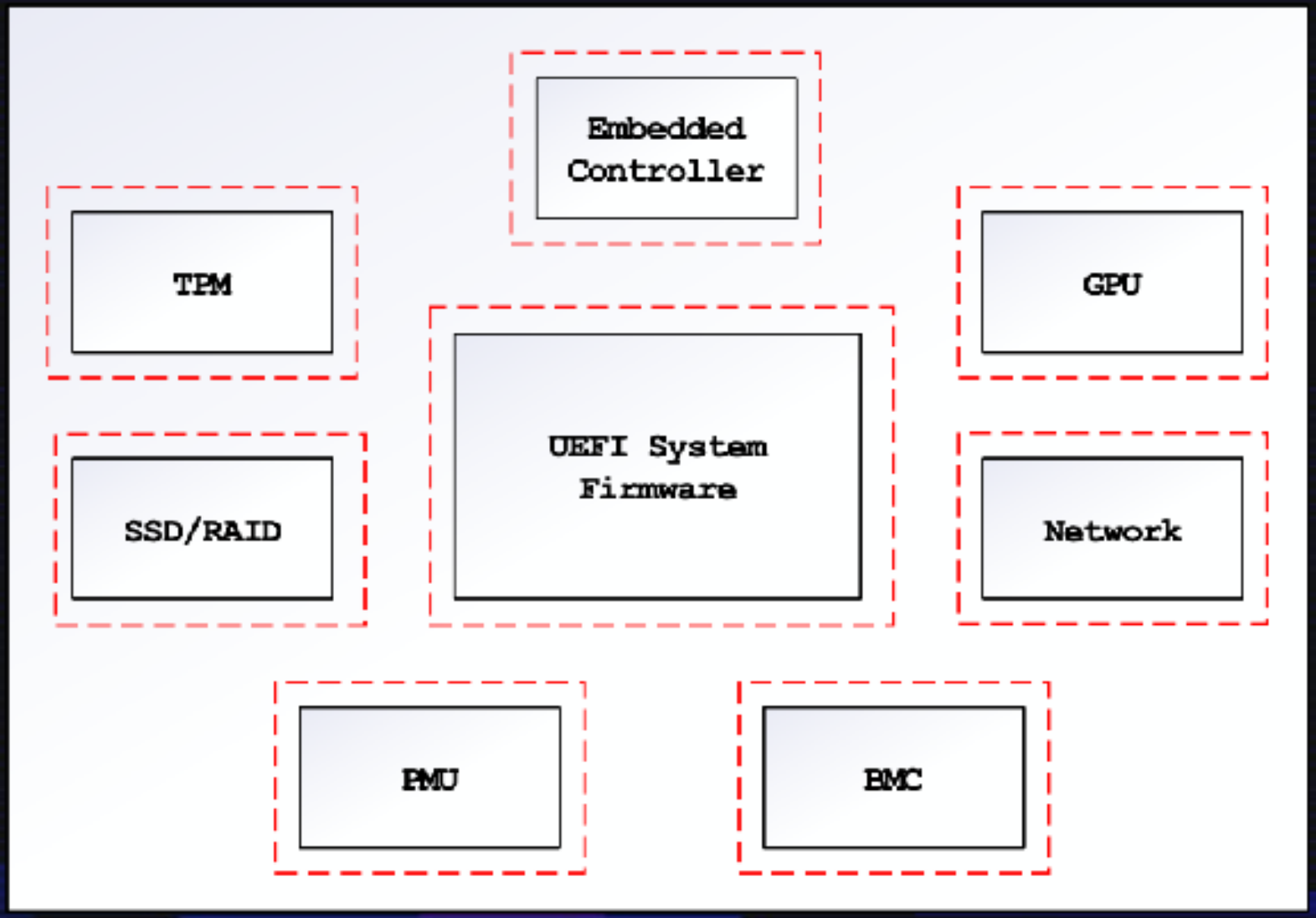
Security Through Obscurity

- Firmware binaries are freely available online
- Tools to analyze binaries are available
- Security researchers are decompiling binaries
  - Most 3rd party reports received include disassembled code

not a binaries technology specs please

https://uefi.org/sites/default/files/resources/UEFI%20SDL%20Webinar_Final%20Slides%20-%20PDF.pdf

HW/FW Security != sum of all Boundaries



ZERONIGHTS.ORG

Hardware Security Boundaries

Most of those chips are:

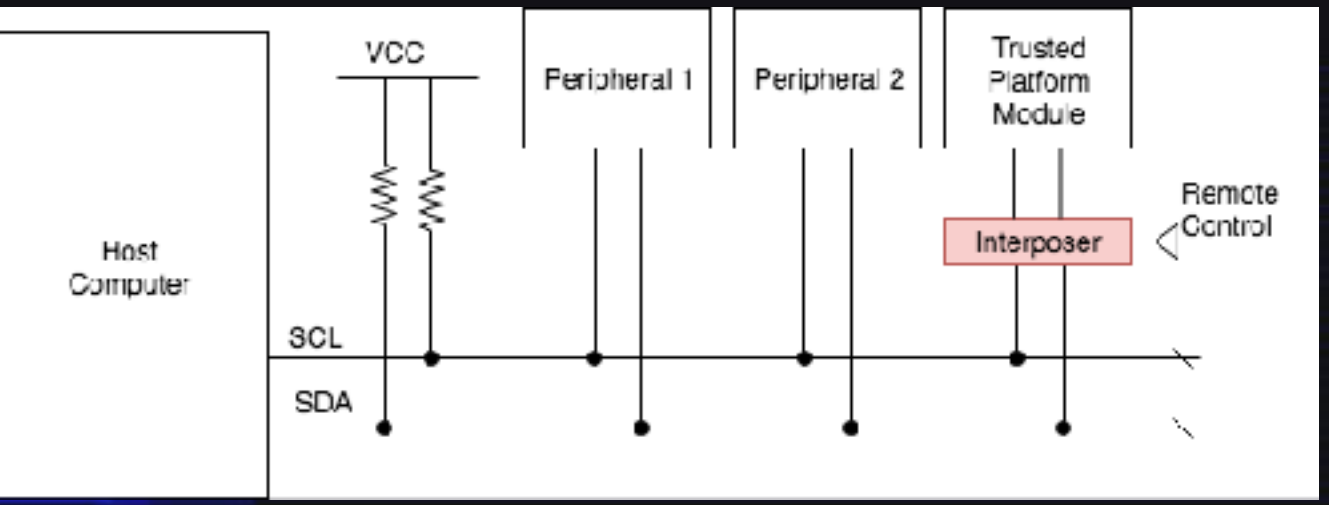
- Not under direct control from hardware vendors
- Involved in security features implementation
- Connected to UEFI firmware (BIOS)
- Considered to generate trusted I/O
- Mostly out of the supervision scope of the main CPU

How can we trust anything that is not under our system control?

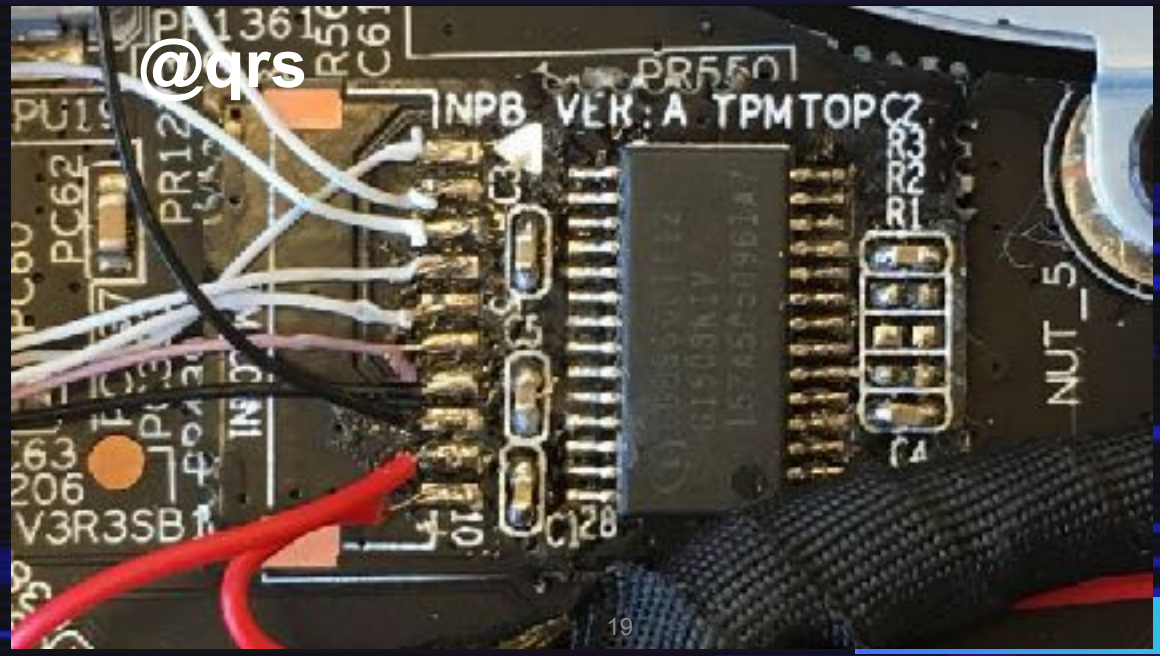
ZERO NIGHTS 2019 EDITION

In current threat model HW is trusted 😈

@uffeux

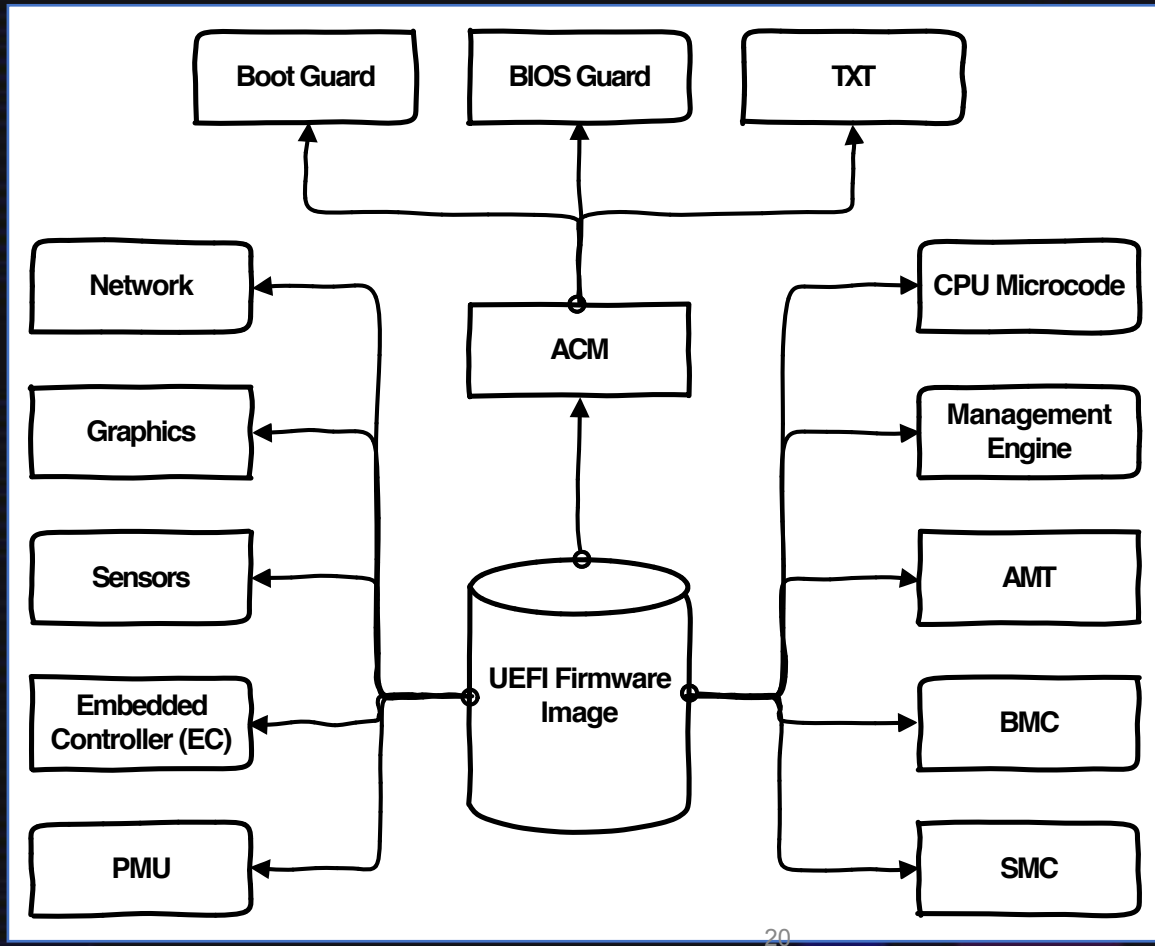


@qrs



How many 3rd-party chips in your laptop?

- TPM module
- USB controller
- Embedded Controller (EC)
- Fingerprint Reader
- Touchpad
- and many others



ZERO NIGHTS 2019 EDITION
ZERONIGHTS.ORG

BMC is inside trusted boundaries

UEFI firmware blindly trust all hardware

But hardware can attack UEFI firmware 😈

https://airbus-seclab.github.io/ilo/ZERONIGHTS2018-Slides-EN-Turning_your_BMC_into_a_revolving_door-perigaud-gazet-czarny.pdf

ZERONIGHTS.ORG

Lenovo Thinkpad EC update process

OS

Lenovo TDK update tool

map EC update image to memory	set NVRAM var 'LenovoEcfwUpdate'

```
while ( v7 - &LenovoEcfwUpdate <= v5 );
memset_(buffer, 0, 1u);
buffer[0] = 1;
TdkBinCreateFromBuff(buffer, 1ui64, &tdk_bin);
result = TdkVariableSet(&a1, &a2, 7u, tdk_bin);
```

Lenovo EcFwUpdateDxe (not SMM)

```
res = LoadFirmware();
if ( res >= 0 )
{
  res = ValidateFirmwareHeader();
  if ( res >= 0 )
  {
    UpdateEcFw(ecfw_bin);
    res = 0i64;
  }
```

BIOS

https://medium.com/@matrosov/breaking-through-another-side-bypassing-firmware-security-boundaries-85807d3fe604

Lenovo Thinkpad EC update process

OS

Len

map EC
image to

```
while ( v7 -
memset_(buff
buffer[0] =
TdkBinCreate
result = Tdk
```

```
case 0x83u:
  v5 = "ECFW image file is invalid";
  break;
case 0x84u:
  v5 = "Failed to load ECFW image file";
  break;
case 0x85u:
  v5 = "This system BIOS supports signed ECFW image only.";
  break;
case 0x86u:
  v5 = "This system BIOS supports unsigned ECFW image only.";
  break;
```

T540p case

ot SMM)

```
Header();
```

BIOS

https://medium.com/@matrosov/breaking-through-another-side-bypassing-firmware-security-boundaries-85807d3fe604

CVE-2019-6171/LEN-27764

Revision History:

Revision	Date	Description
9	2019-11-11	Updated fix targets
8	2019-10-09	Updated fix targets
7	2019-10-06	Updated fix targets and added fixes
6	2019-09-25	Updated fix targets and added fix
5	2019-08-29	Updated fix targets and added fix
4	2019-08-27	Added fixes
3	2019-08-13	Updated fix target for some products
2	2019-08-09	Updated Product Impact
1	2019-08-08	Initial release

Product Impact:

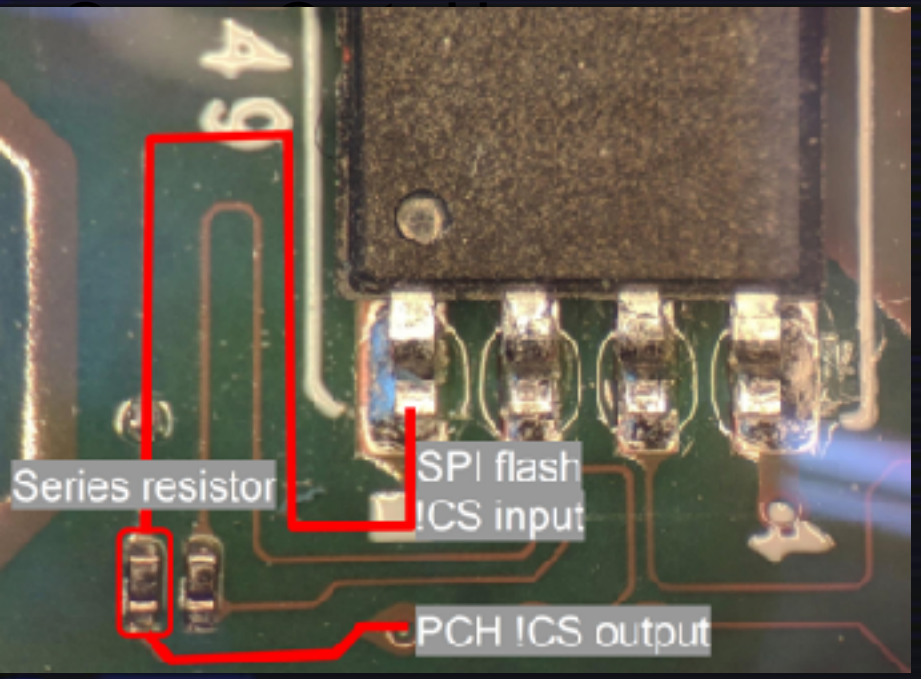
Product	Model	Minimum Fix Version	Download Link	Last Updated
ThinkPad 10	20E5, 20E6	Target available by 2019-11-27		2019-10-09
ThinkPad 13s/Yoga 14s 3RD GEN	20S9, 20GG, 20GB, 20GA	Target available by 2019-11-26		2019-09-25
ThinkPad 13s/Yoga 14s 3RD GEN	20S9, 20GG, 20GB, 20GA	Target available by 2019-11-26		2019-09-25
ThinkPad 13s/Yoga 14s 4TH GEN	20HT, 20HV, 20HS, 20HU	Target available by 2019-11-26		2019-09-25
ThinkPad 13s/Yoga 14s 4TH GEN	20HT, 20HV, 20HS, 20HU	Target available by 2019-11-26		2019-09-25
ThinkPad 13s/Yoga 14s 5TH GEN (GM1)	20LR, 20LQ, 20LN, 20LP	Target available by 2019-11-26		2019-09-25
ThinkPad 13s/Yoga 14s 5TH GEN (HGY-Y)	20LR, 20LQ, 20LN, 20LP	Target available by 2019-11-26		2019-09-25
ThinkPad 13 (SBU)	20G1, 20G2	Target available by 2019-11-26		2019-09-25
ThinkPad 13 (OTA)	20G1, 20G2	Target available by 2019-11-26		2019-09-25
ThinkPad A275	20KC, 20KD	Target available by 2019-11-26		2019-09-25
ThinkPad A285	20MW, 20MX	Target available by 2019-11-26		2019-09-25
ThinkPad A475	20KL, 20KM	Target available by 2019-11-26		2019-09-25
ThinkPad A485	20MU, 20MV	Target available by 2019-11-26		2019-09-25
ThinkPad E450/E450c/E550/E550c	20DC, 20DD, 20E4, 20DF, 20DG, 20D9	Target available by 2019-11-26		2019-09-25
ThinkPad E460/E560	20ET, 20EJ, 20EV, 20EW	Target available by 2019-11-26		2019-09-25
ThinkPad E465/E565	20EX, 20EY	Target available by 2019-11-26		2019-09-25
ThinkPad E470/E570	20H1, 20H2, 20H5, 20H6	Target available by 2019-11-26		2019-09-25
ThinkPad E475/E575	20H4, 20H8	Target available by 2019-11-26		2019-09-25
ThinkPad E480/E580	20KN, 20KQ, 20K5, 20KT	Target available by 2019-11-26		2019-09-25
ThinkPad E485/E585	20KU, 20KV	Target available by 2019-11-26		2019-09-25

https://support.lenovo.com/us/en/product_security/len-27764

ZERO NIGHTS 2019 EDITION
ZERONIGHTS.ORG

IN CURRENT REALITIES HW AND FW THREAT MODELING SHOULD BE UNDIVIDED

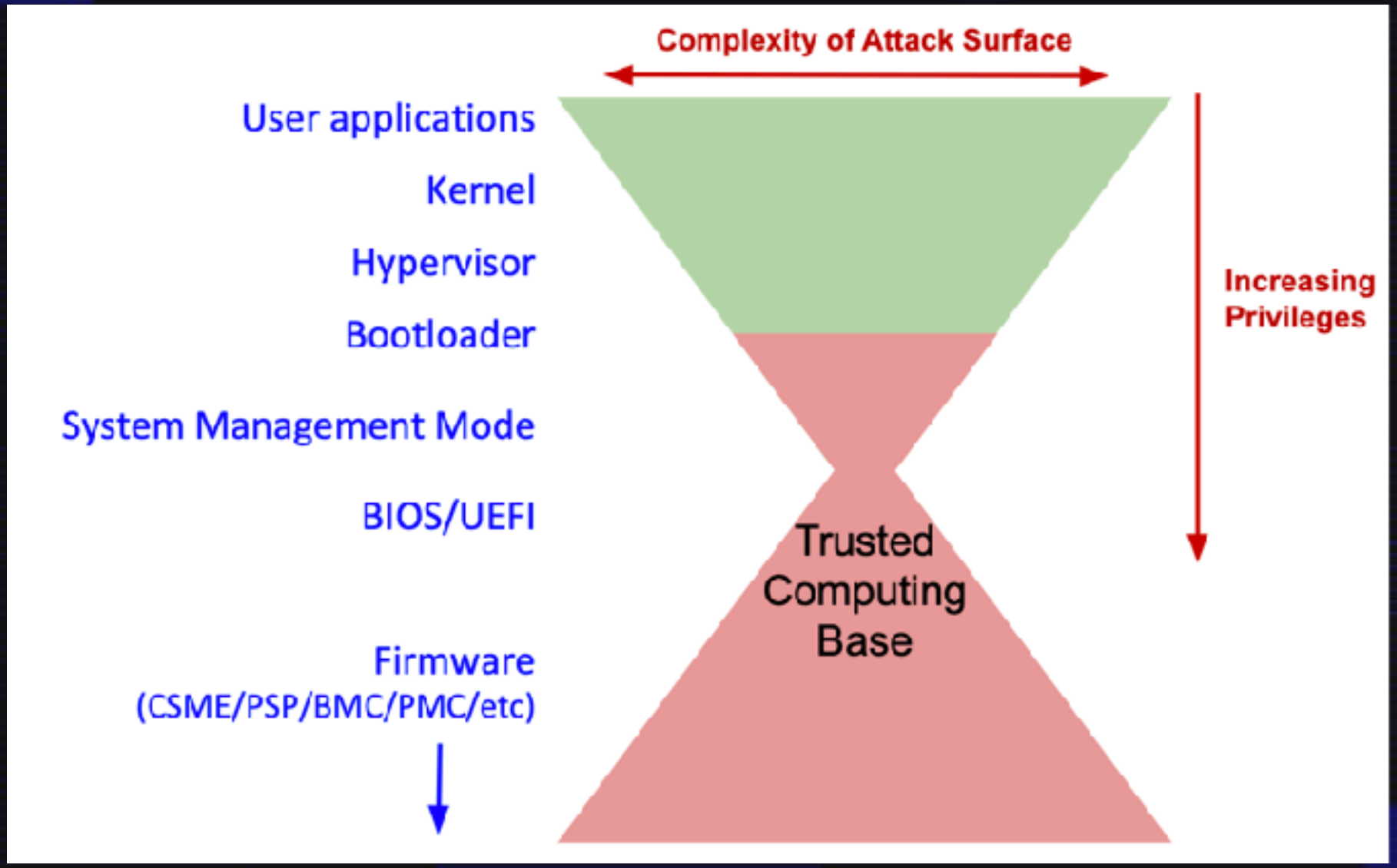
Intel Boot Guard TOCTOU from SPI flash



Authenticated once != trusted forever

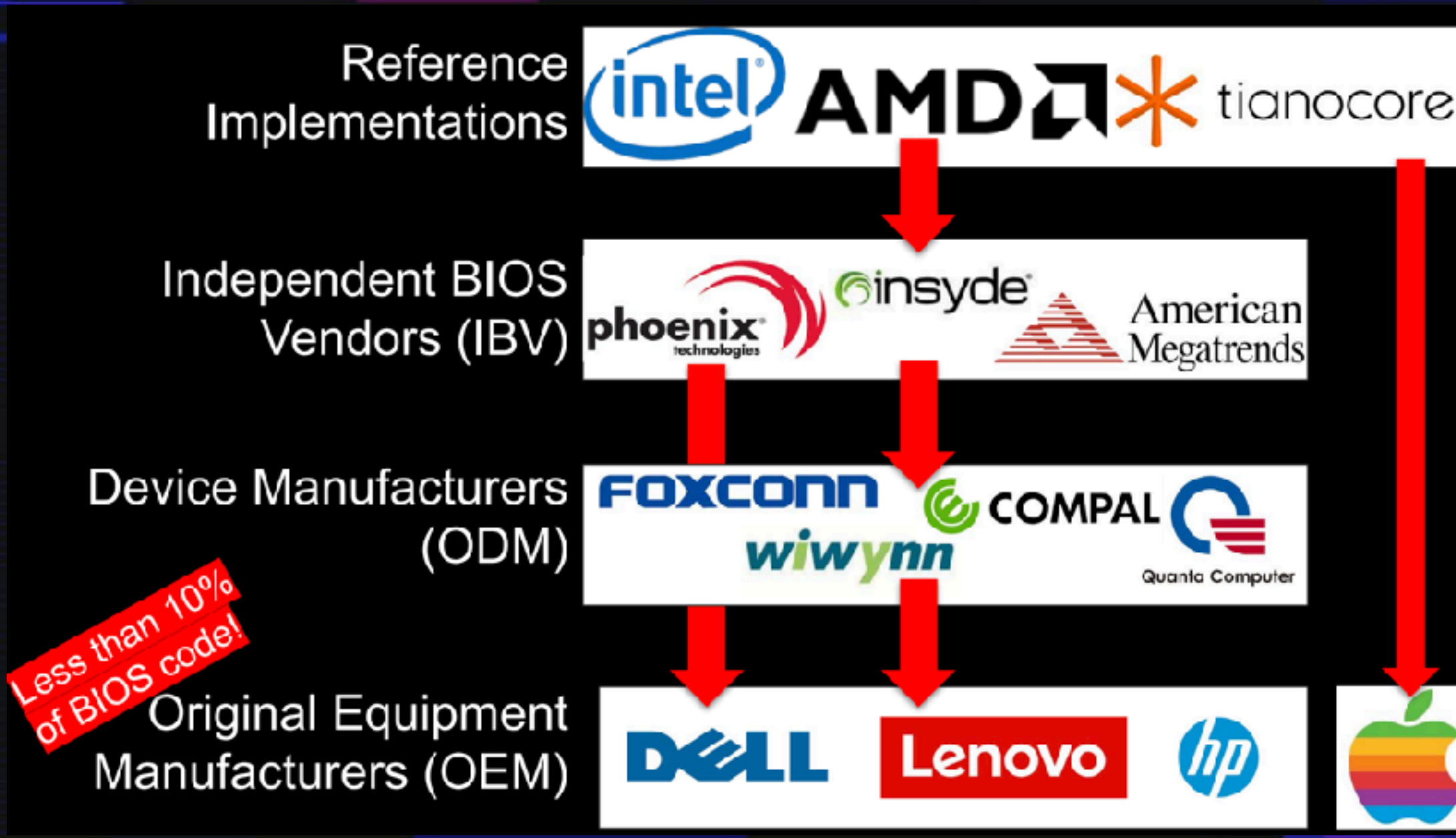
26

https://edk2-docs.gitbooks.io/security-advisory/content/bootguard-toctou-vulnerability.html



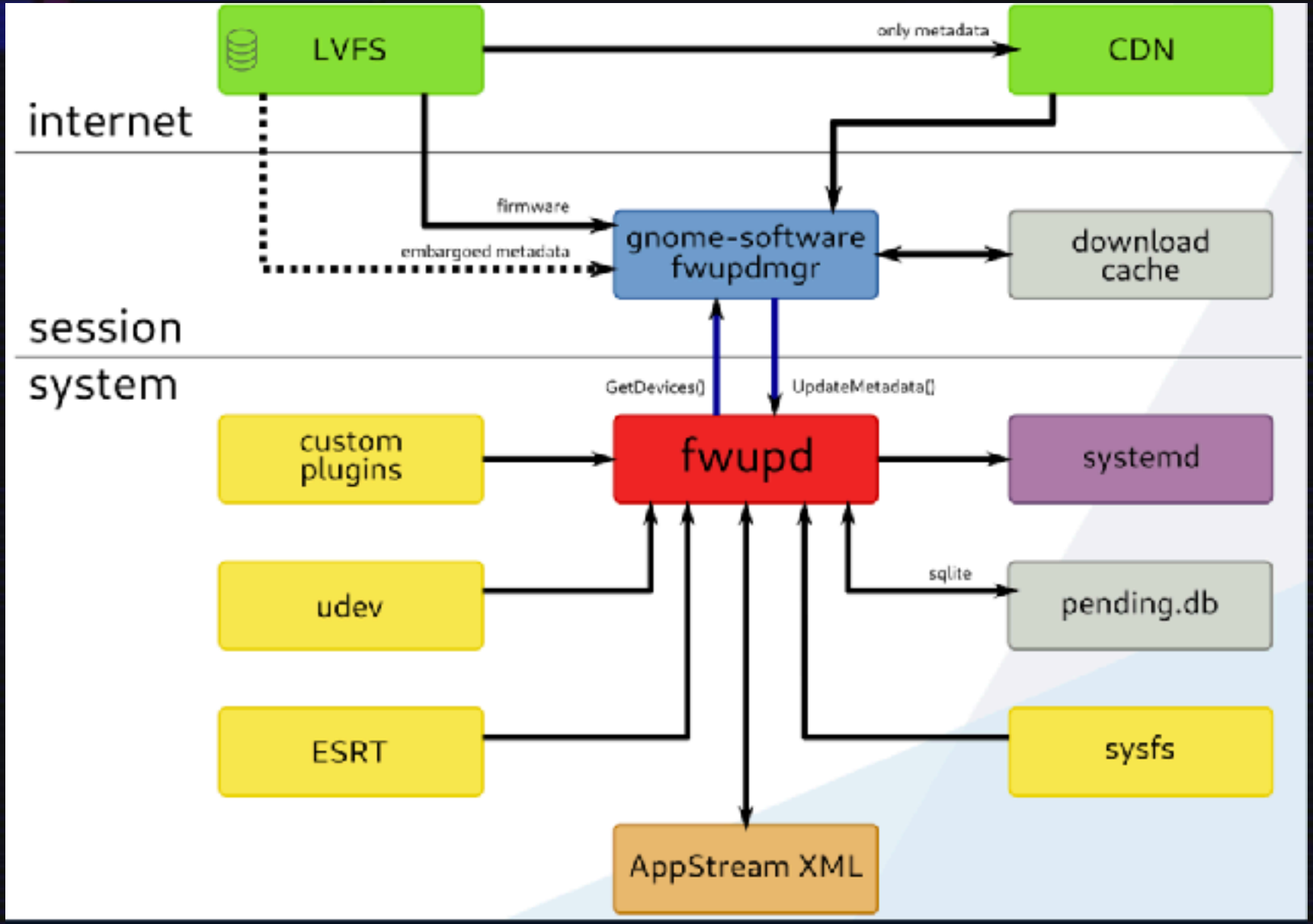
https://www.platformsecuritysummit.com/2019/speaker/wood/

WE TRUST TOO MUCH IN HARDWARE SECURITY BY DEFAULT

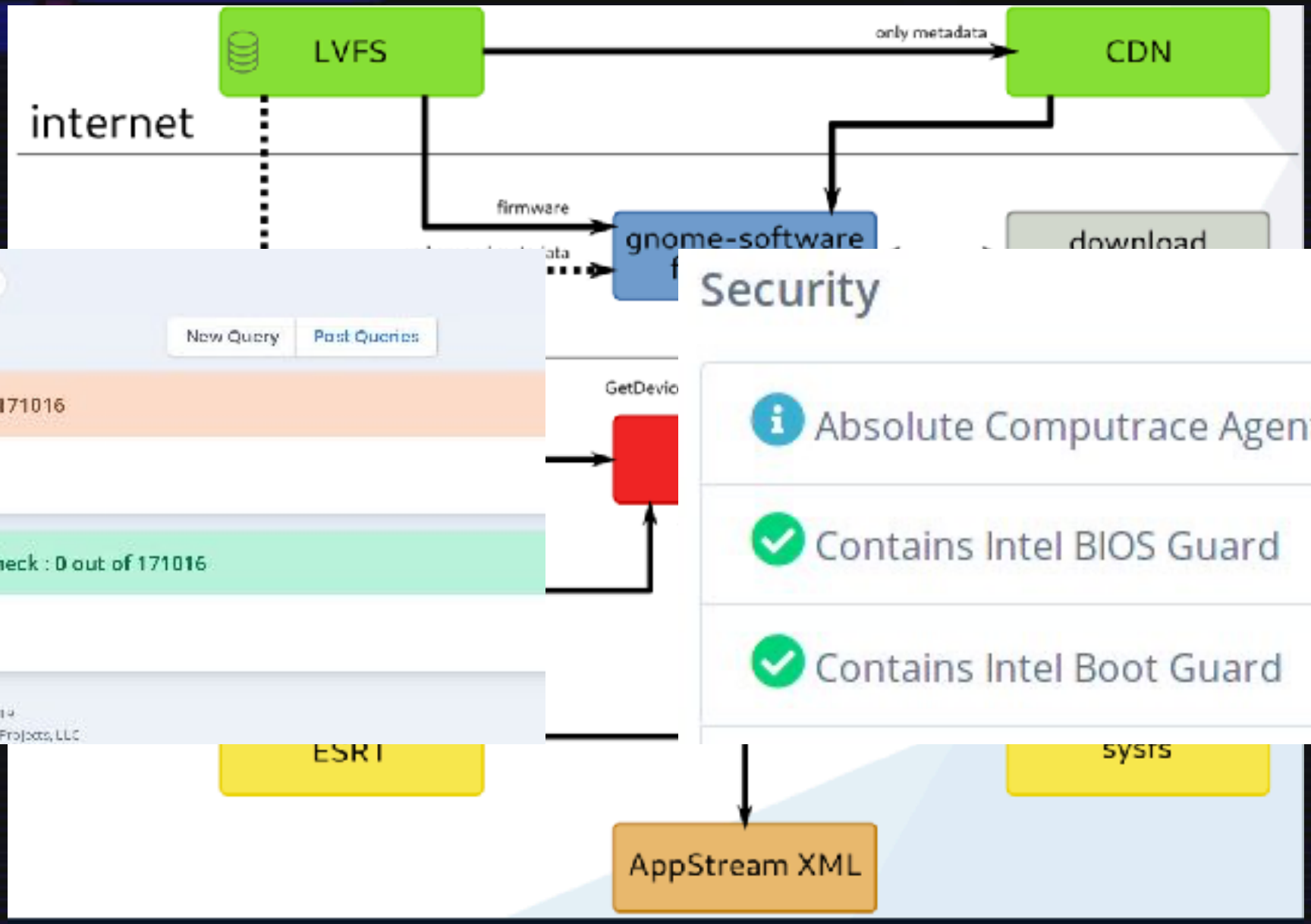


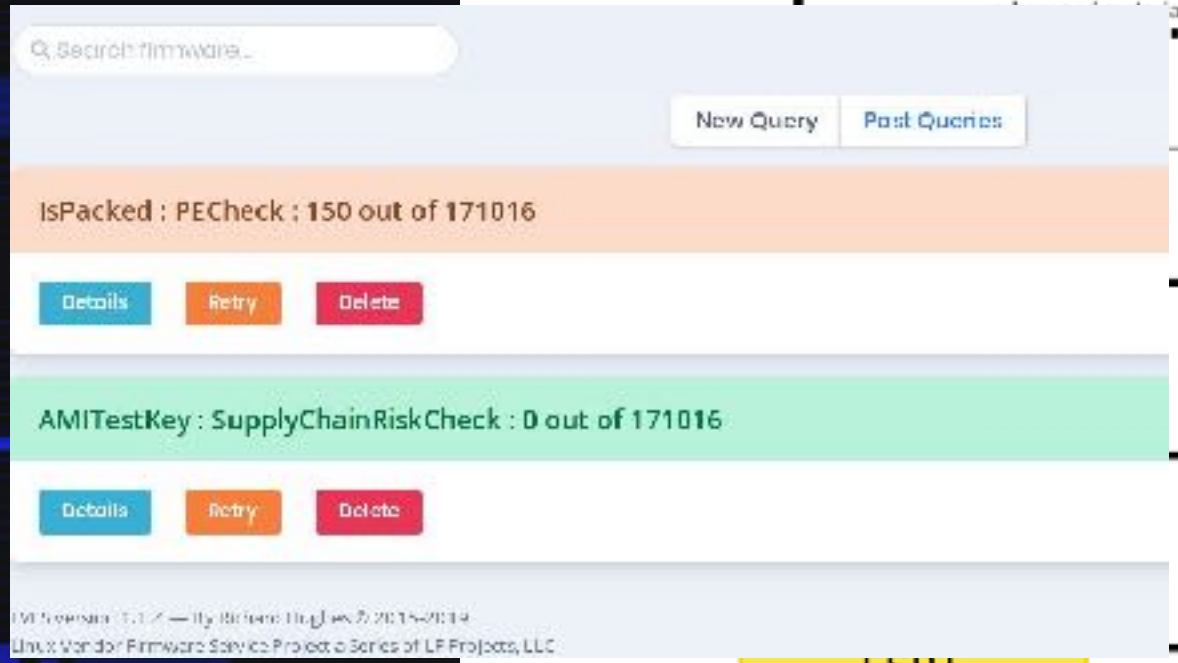
https://media.hardwear.io/roots-of-trust-and-attestation/

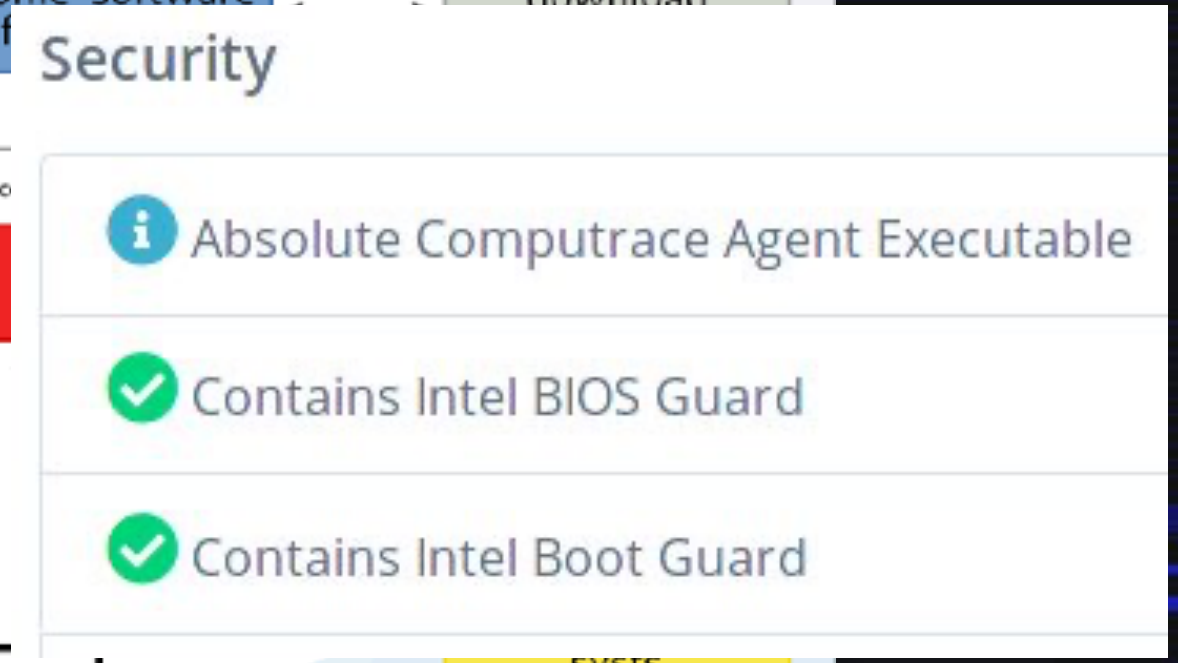
WE TRUST BLINDLY ANYTHING WHICH IS SIGNED AND COME FROM TRUSTED SOURCE



https://osfc.io/uploads/talk/paper/9/Introducing_the_Linux_vendor_Firmware_service.pdf



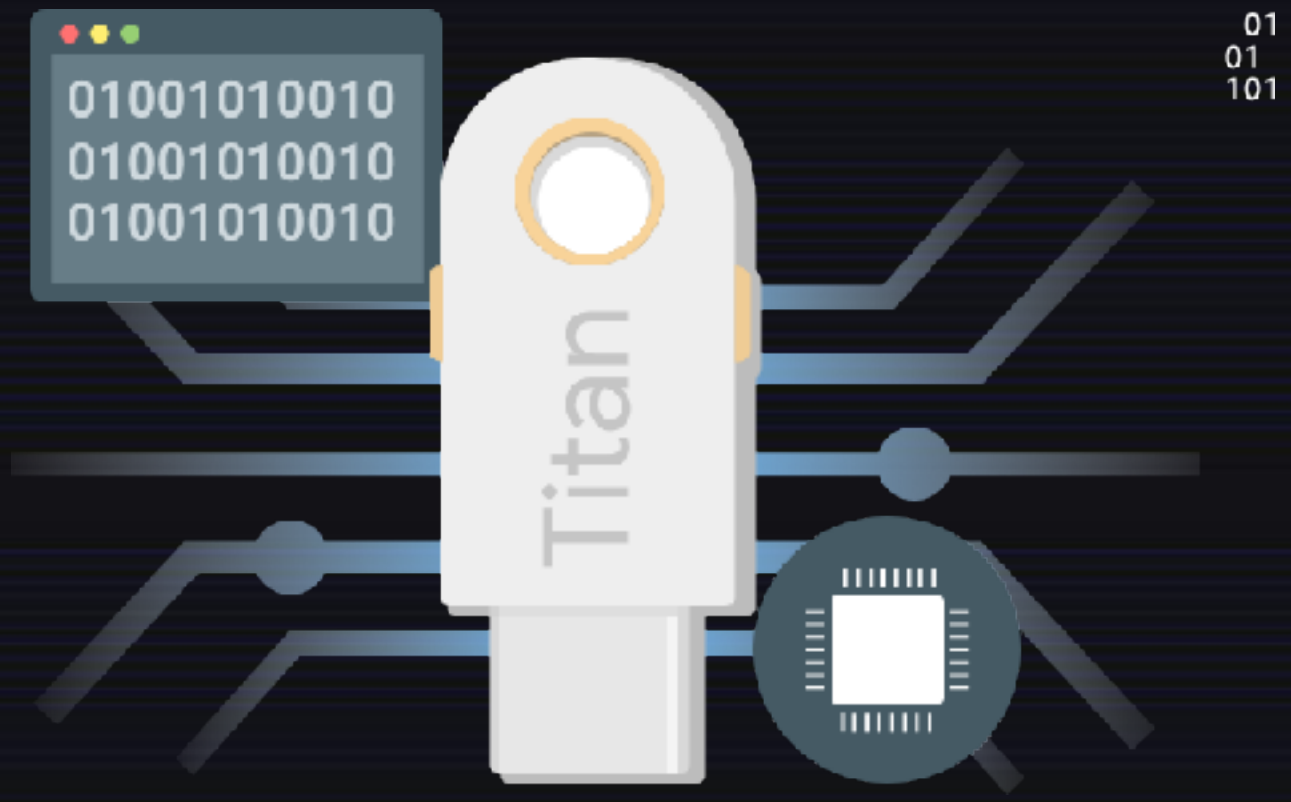




https://osfc.io/uploads/talk/paper/9/Introducing_the_Linux_vendor_Firmware_service.pdf

ZERO TRUST ALSO MEANS "TRUST HW NOT USER". I WILL NEVER CONSIDER HW 100% TRUSTED

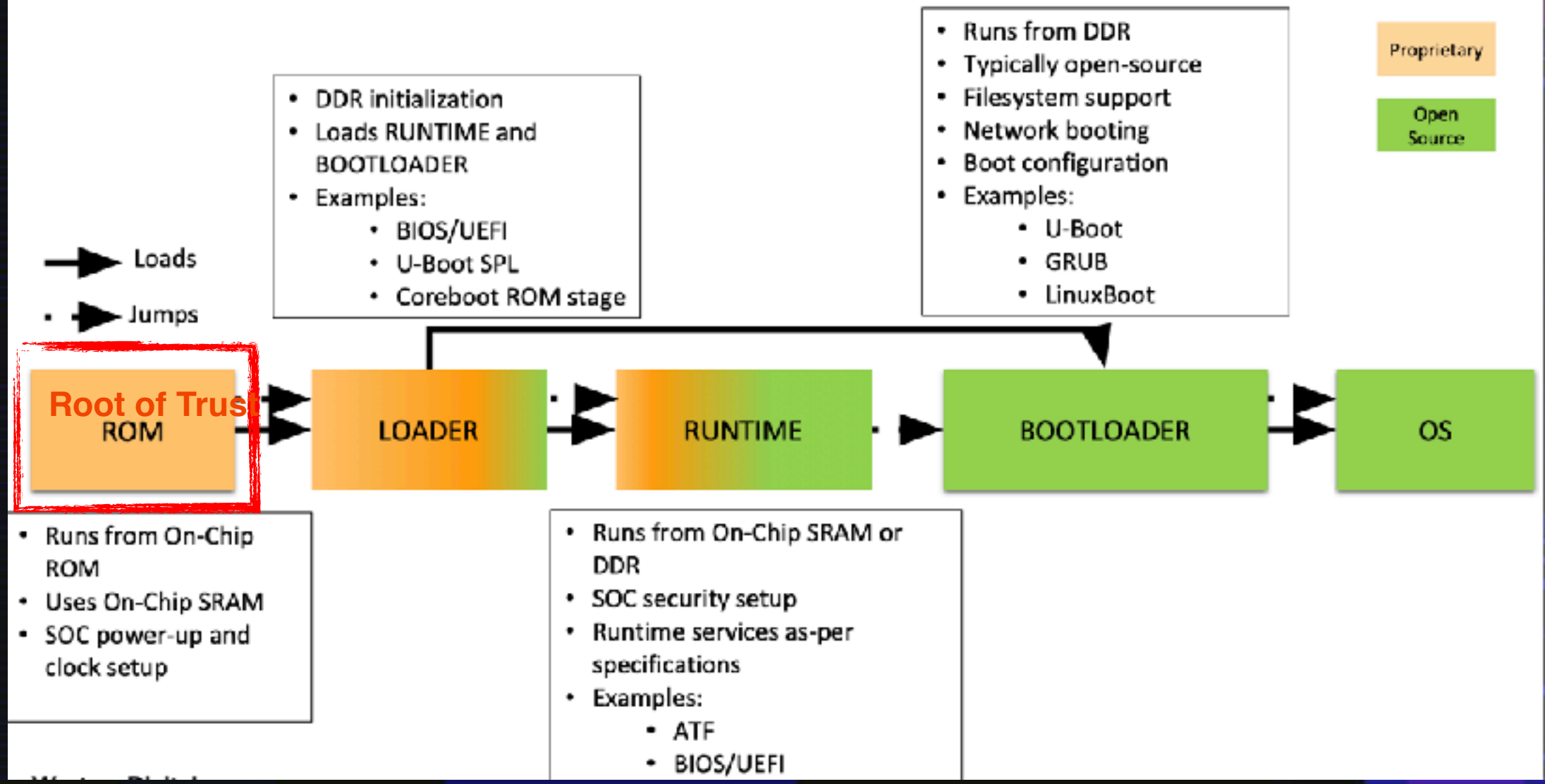
https://www.youtube.com/watch?v=YFE4RqHRYOA



Google recalls some Titan security keys after finding Bluetooth vulnerability

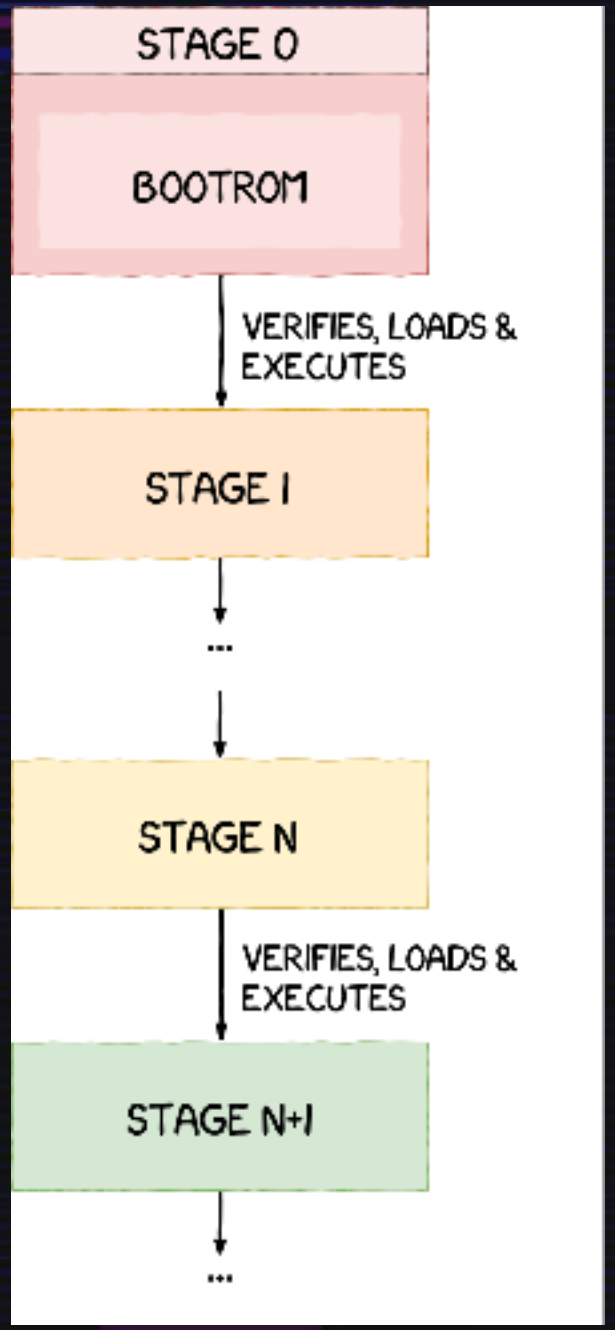
Google recalls some Titan security keys after finding Bluetooth vulnerability

Industry standard boot loaders

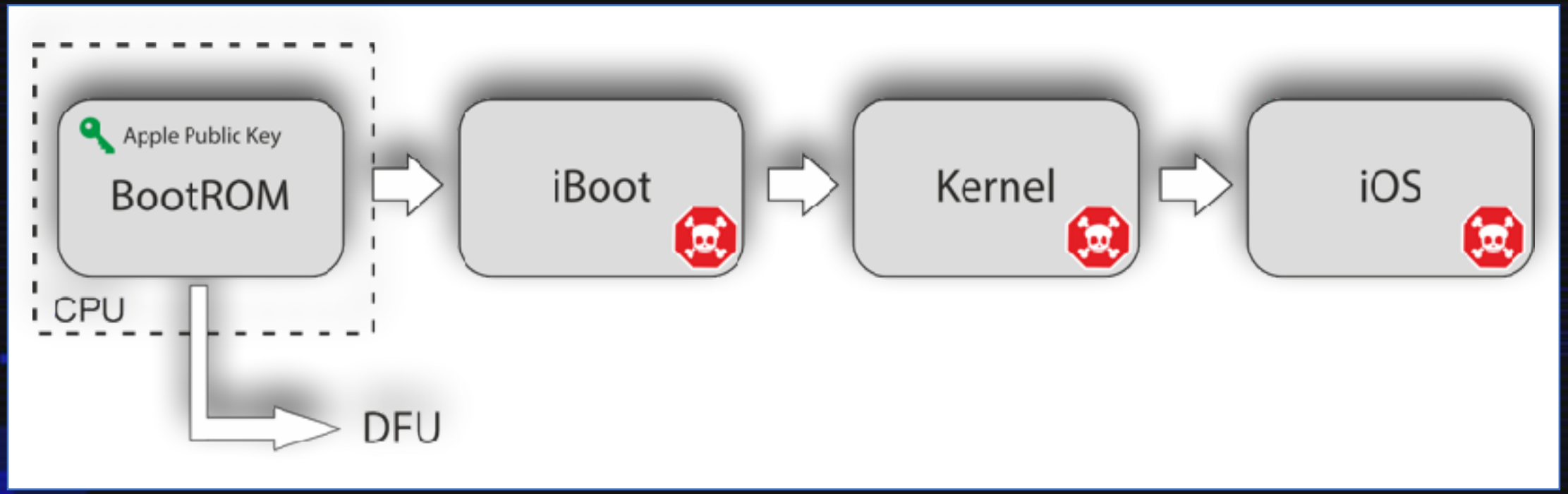


https://osfc.io/uploads/talk/paper/14/The_role_of_open_source_firmware_in_RISC-V.pdf

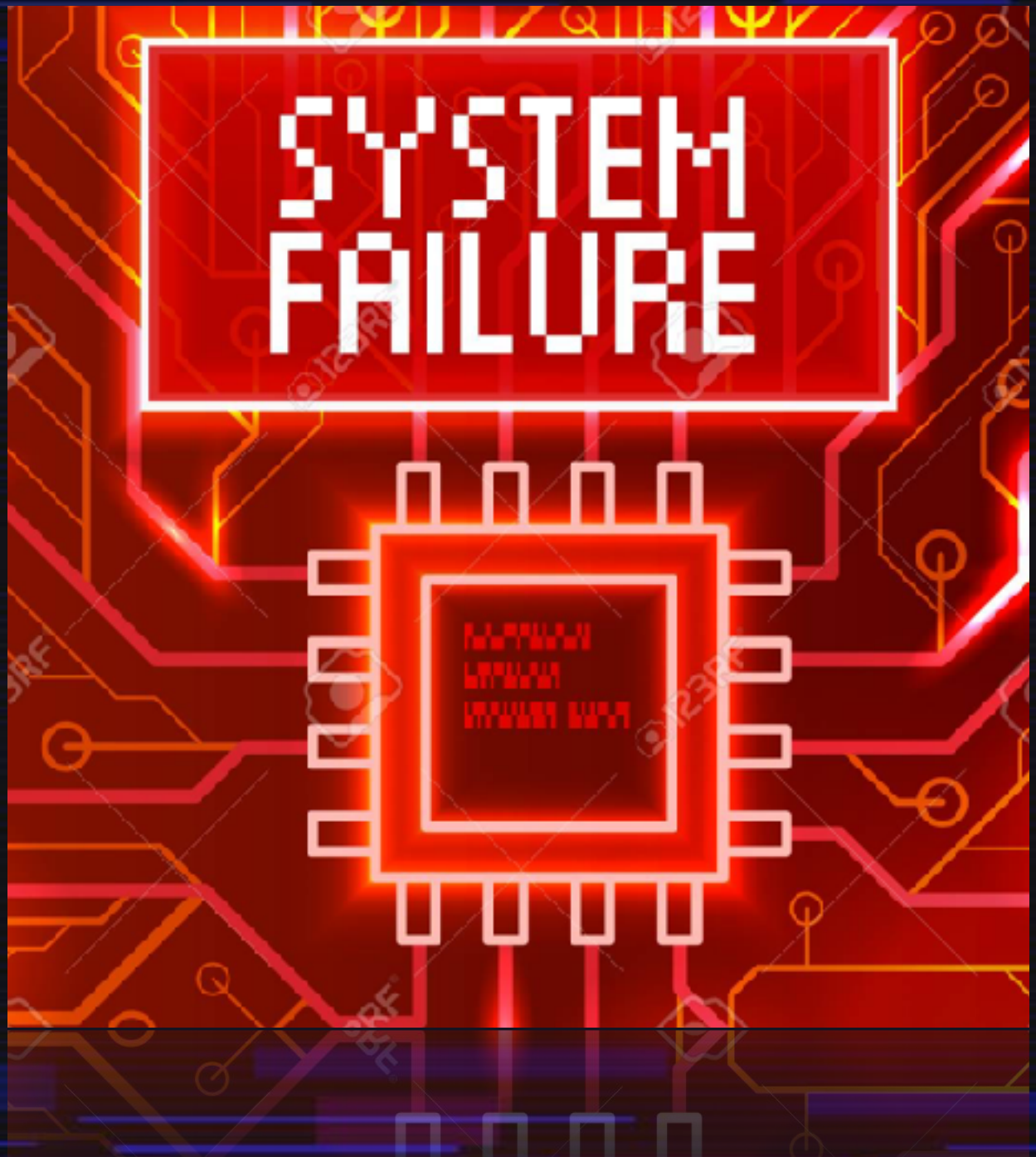
SECURE BOOT FIX EVERYTHING?

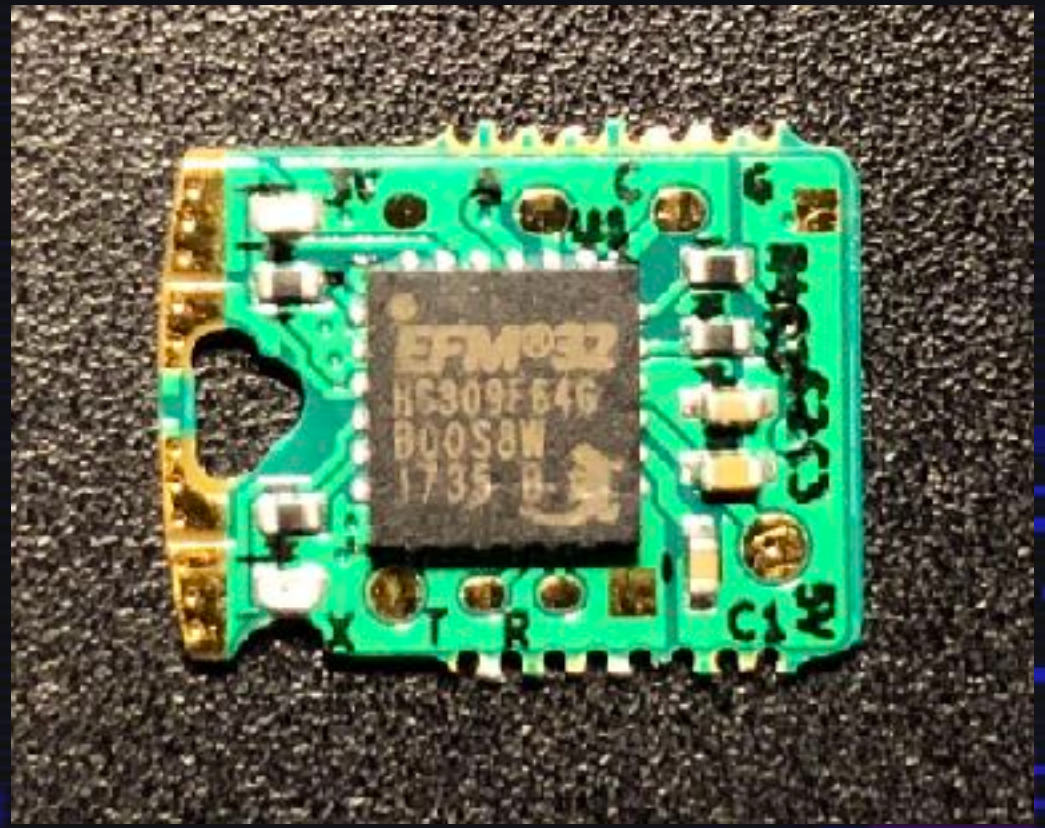


https://blog.quarkslab.com/analysis-of-qualcomm-secure-boot-



https://habr.com/en/company/dsec/blog/472762/


SYSTEM
FAILURE

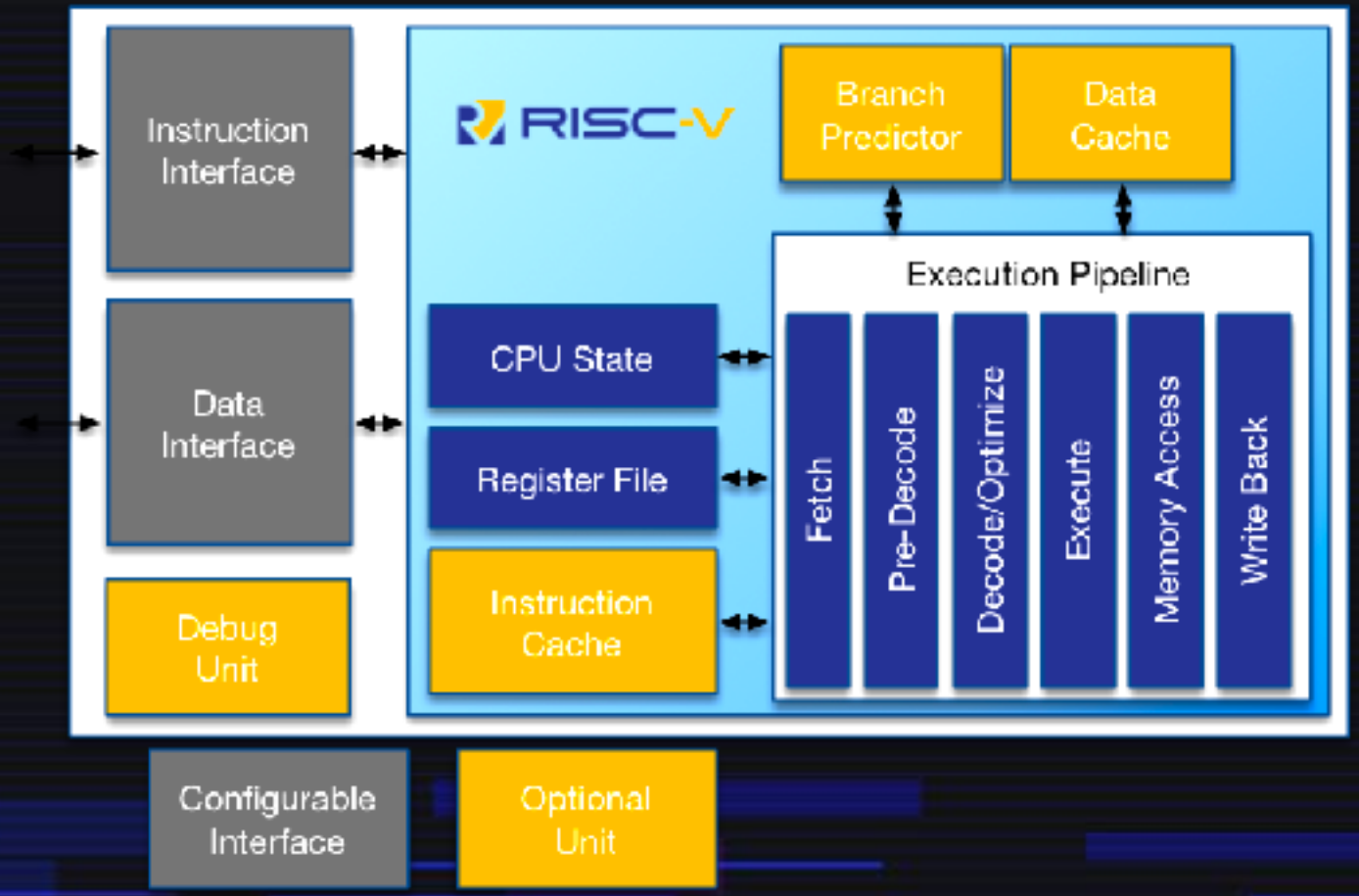


https://www.crowdsupply.com/sutajio-kosagi/tomu

ZERO NIGHTS 2019 EDITION

RISC-V®

RISC-V®


Instruction Interface
Data Interface
Debug Unit
RISC-V
Branch Predictor
Data Cache
Execution Pipeline
CPU State
Register File
Instruction Cache
Fetch
Pre-Decode
Decode/Optimize
Execute
Memory Access
Write Back
Configurable Interface
Optional Unit

Freedom Unleashed SoC

Review

IP Library — Go to Category

Filter

Phase Locked Loop
PLL 40-2400MHz — ODS

Mastering

AI ACCELERATOR

NVIDIA
NVIDIA NVDLA (Deep Learning Accelerator)
NVIDIA Deep Learning Accelerator — Open Source

CONFIGURABLE LOGIC

Flex Logix EFLX-2.5K Embedded FPGA
Embedded FPGA for reprogrammable hardware blocks — ODS

HIGH SPEED INTERFACE

Mobiveil GPEX PCI-Express 4.0 Controller
PCI Express Gen4 Controller — ODS

SECURITY

Rambus
Rambus CryptoManager RT630
A complete solution for chip and system security — ODS

Mastering Subsystems

Gigabit Ethernet Media Access Control

Front Bus
64-bit 300 MHz

System Bus
64-bit 300 MHz

Peripheral Bus
64-bit 200 MHz

U54 Core Complex 500 MHz
U54 Core
BUS MATRIX
L2 Cache

Foundational Blocks

Crystal Oscillator

Phase Locked Loop

SiFive Clock/Reset Control

Memory Bus
32 bit 600 MHz

Memory Subsystem

DDR3/3L/4 Controller

Peripherals

Pulse Width Modulation Peripheral

UART Peripheral

I2C Peripheral

SPI Peripheral

QSPI Interface Peripheral

GPIO Controller

Cadence USB 3.1 Controller

SiFive DMA Engine

SiFive MaskROM

Chip Details

Platform: Freedom Unleashed
Process: TSMC 28nm
Base Design: Application Processor

Chip Settings

CPU Clock: 600 MHz
100MHz — 600 — 900MHz

Peripheral Bus: 200 MHz
50MHz — 200 — 350 — 500MHz

Mastering Bus Clock Ratio

2:1	3:1	4:1

Memory Port Width (bits)

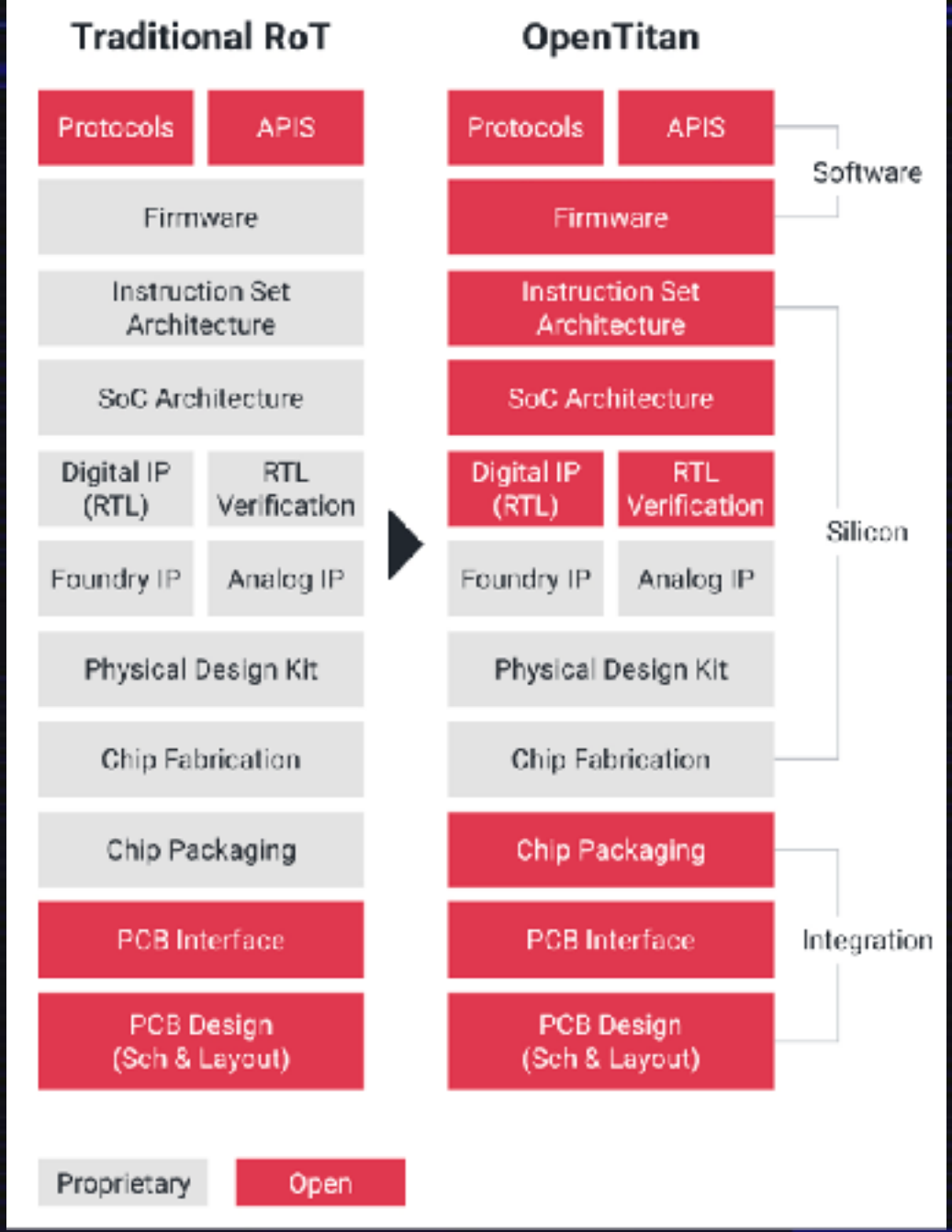
32	64	128

CPU Clock speed and Bus Clock Ratio determine Front and System Bus speeds.

Bus widths are determined by the choice of Core IP.

Memory Bus speed is determined by IP in the Memory Subsystem.

https://www.sifive.com/chip-designer



https://security.googleblog.com/2019/11/opentitan-open-sourcing-

Fault injection attacks do not scale well, but their results do! Whenever something is extracted (E.g secrets, keys, firmware and vulnerabilities identified in the firmware), it will be distributable! Fault injection attacks are a first step in a complete chain of attacks!

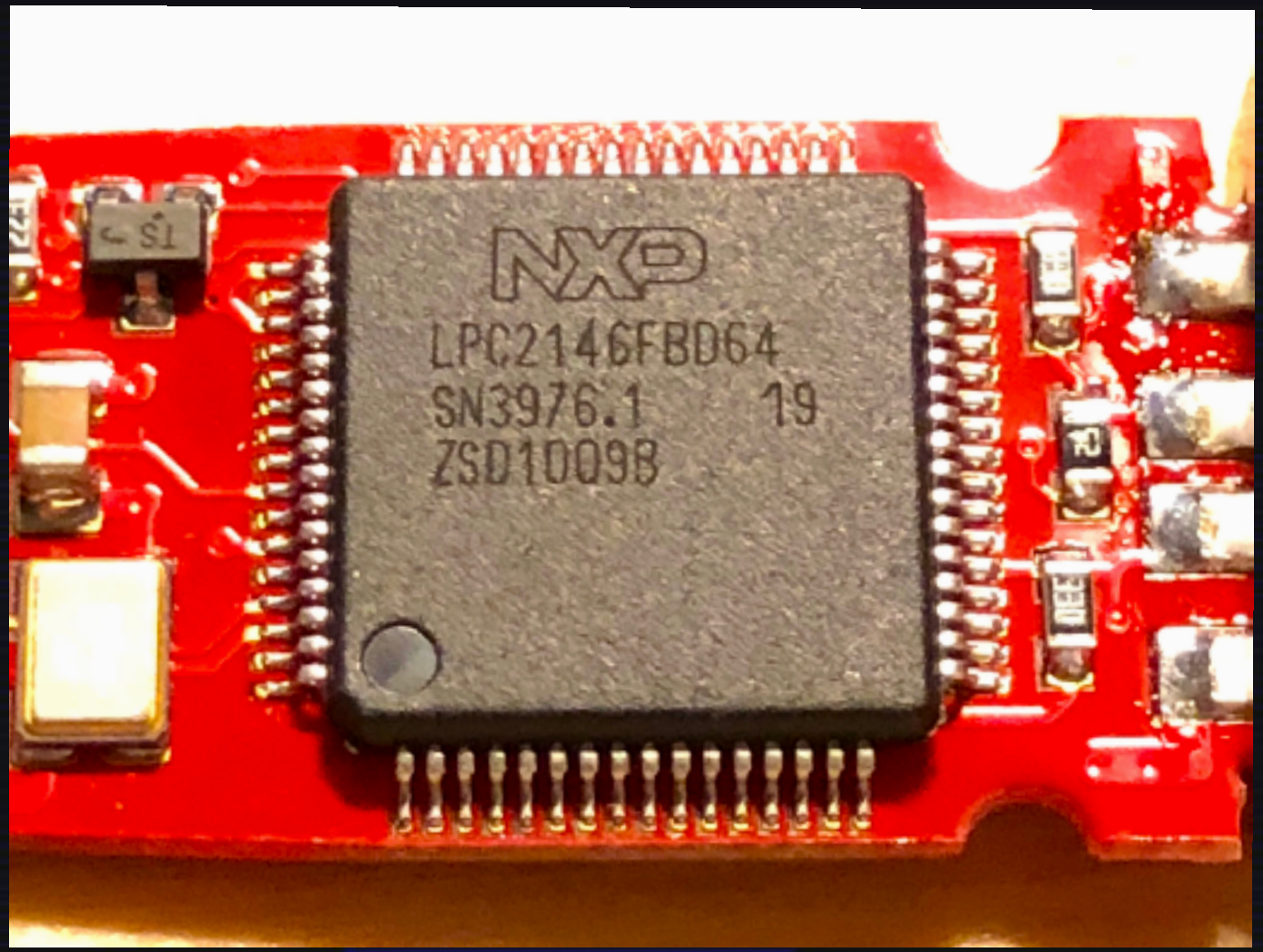
Niek Timmers (@tieknimmers)

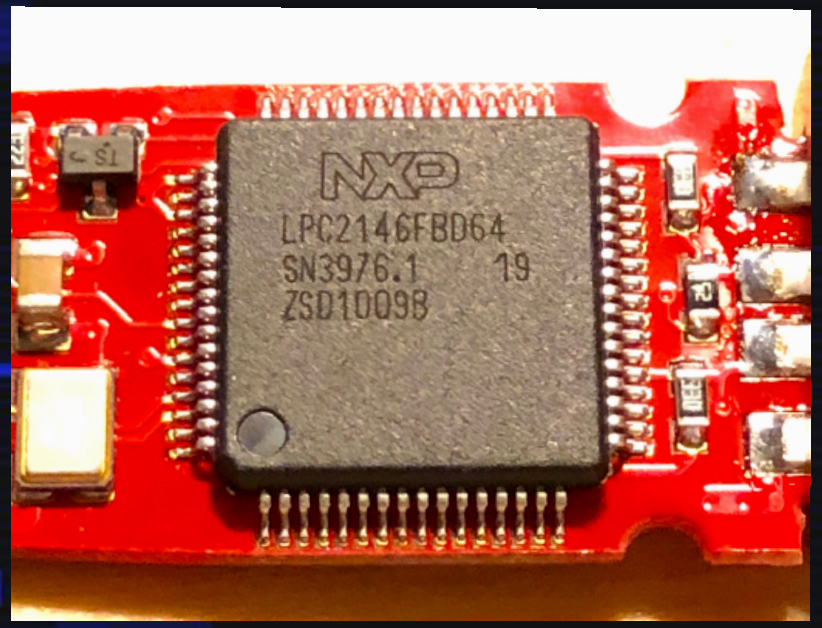
Hardware Security Chip

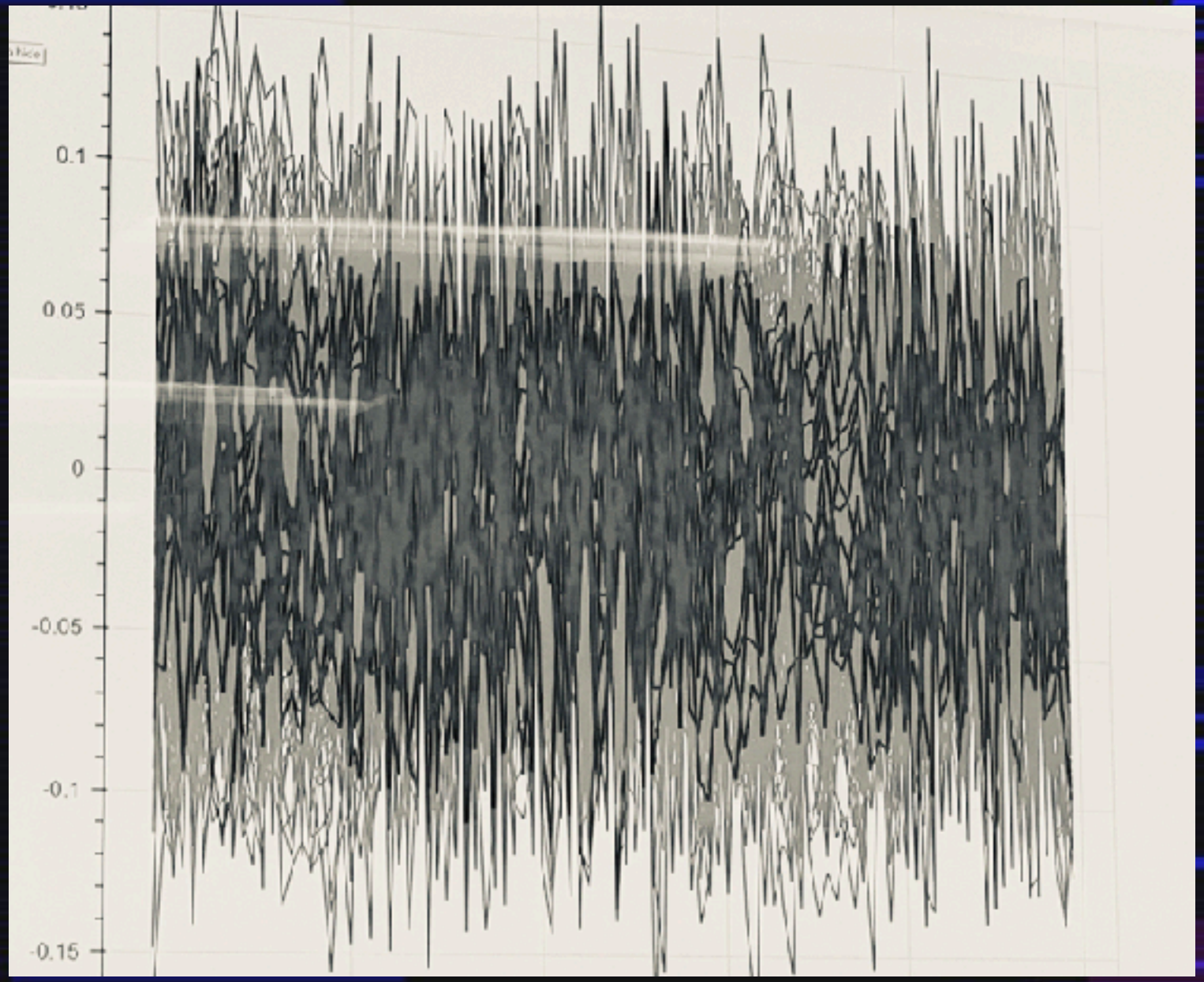
E-Fuses

- ECC Private Keys
- AES Key
- Boot Key

- AES
- SHA2
- ECC
- RSA
- RNG


NXP
LPC2146FBD64
SN3976.1 19
ZSD10098


NXP
LPC2146FBD64
SN3976.1 19
ZSD10098


0.1
0.05
0
-0.05
-0.1
-0.15

HARDWARE SECURITY IS HARD!

WE REALLY NEED TO RETHINK MEANING OF HW SECURITY IN REALITIES OF MODERN THREATS

THANK YOU!

@matrosov