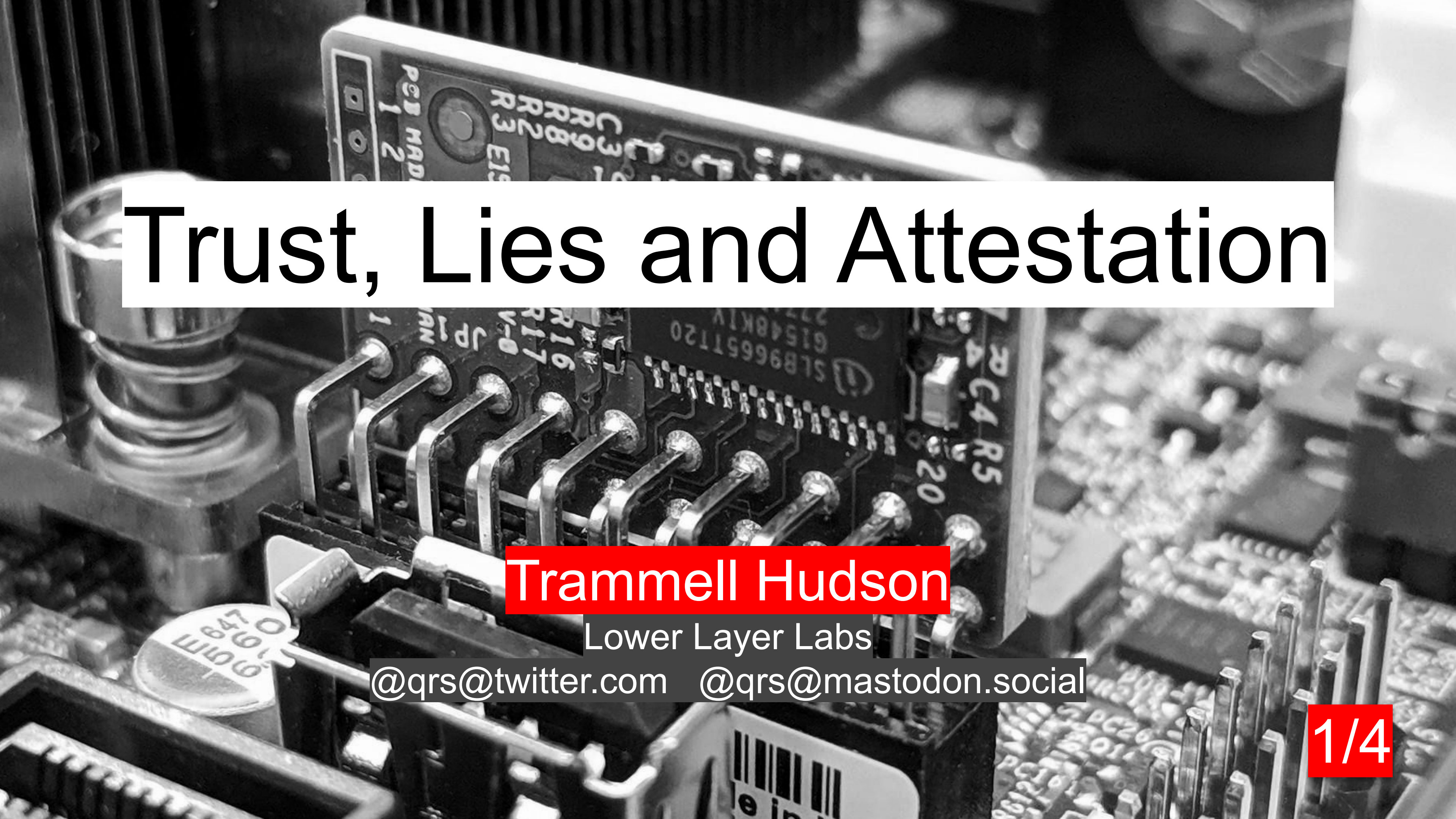


Trust, Lies and Attestation

Trammell Hudson

Lower Layer Labs

@qrs@twitter.com   @qrs@mastodon.social

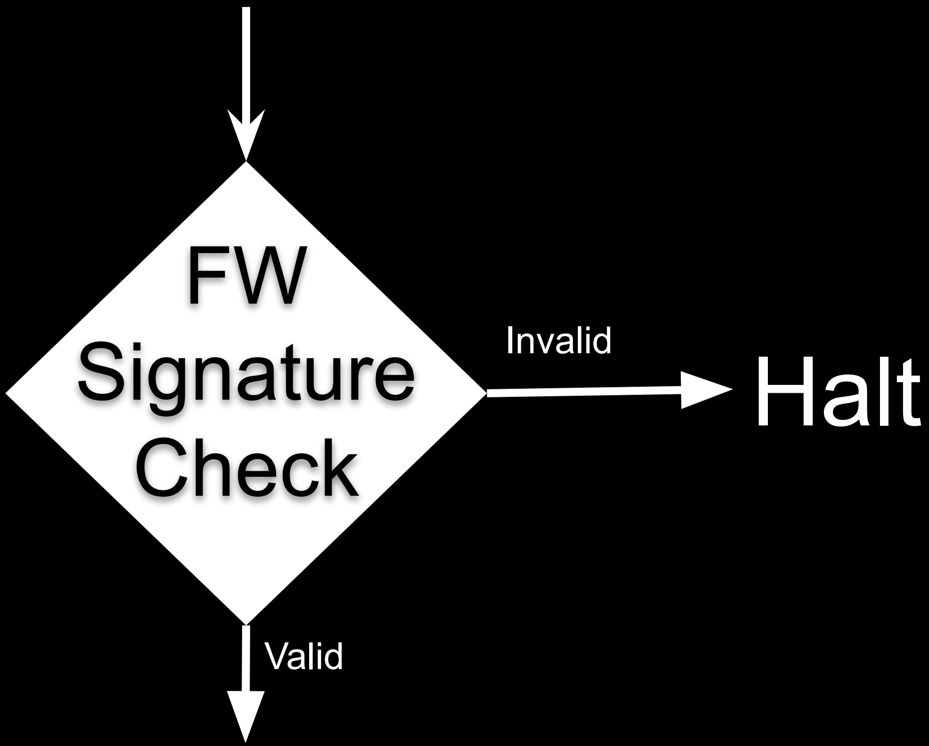
1/4

How do we prevent unauthorized code?

Simple: Turn on Verified Boot

Verified Boot

CPU Reset



FW Signature Check

Invalid

Halt

Valid

Run firmware
validates OS, validates apps

3/4

Thanks for coming to my talk!
Have a wonderful Day 2
At Hardwear.io

Freedom?

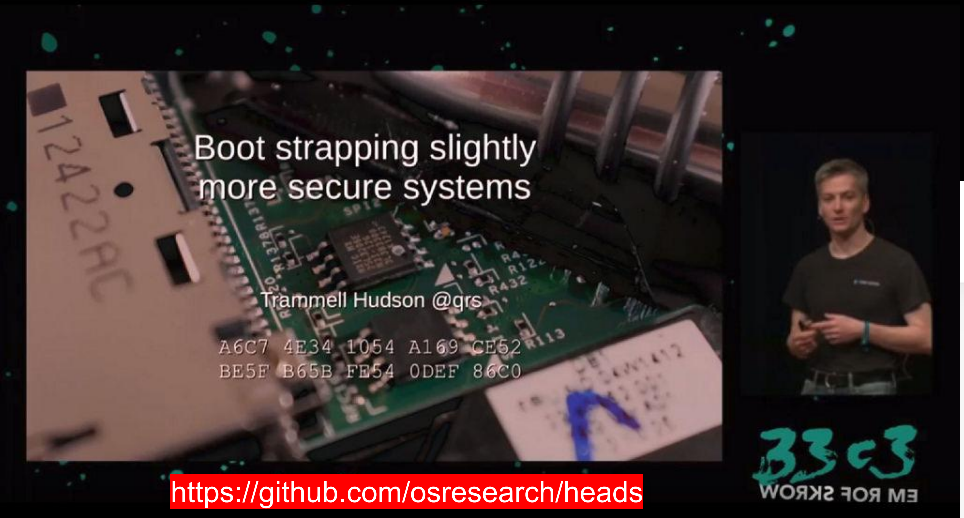
Resilience?

Attestation?

Freedom?

Resilience?

Attestation?



Boot strapping slightly more secure systems

Trammell Hudson @grs

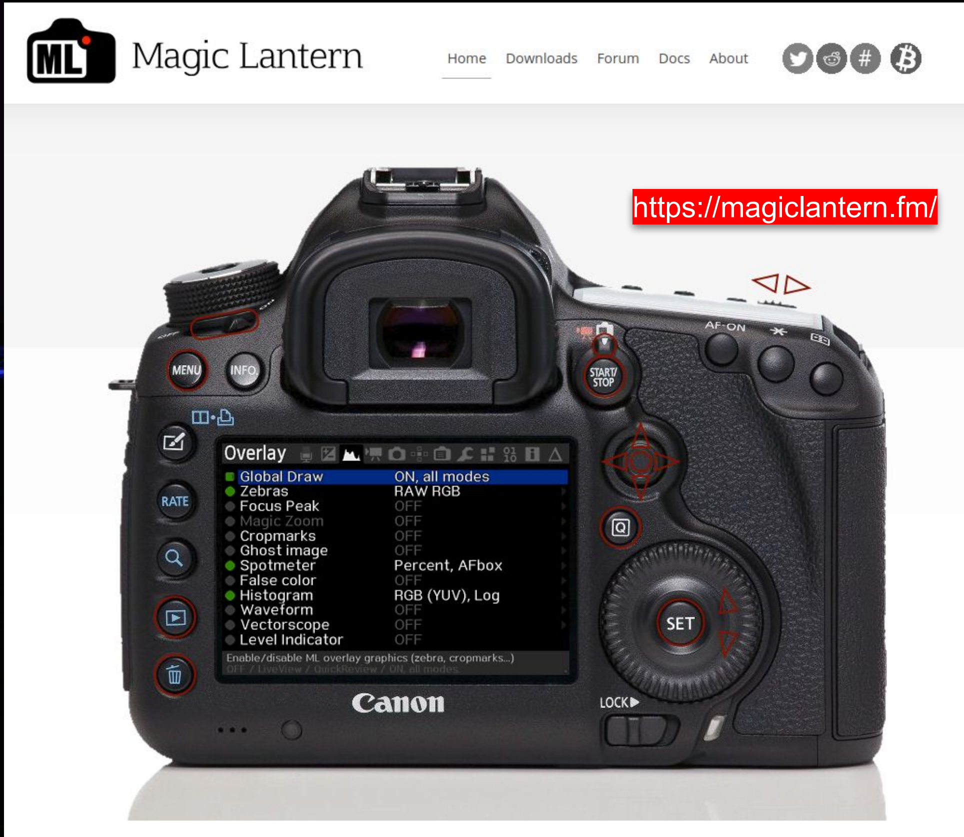
A6C7 4E34 1054 A169 CE52
BE5F B65B FE54 0DEF 86C0

https://github.com/osresearch/heads

Bringing Linux back to the server BIOS with LinuxBoot

Trammell Hudson (Two Sigma Investments)
Ron Minnich (Google)
Jean-Marie Verdun (Horizon Computing)

https://linuxboot.org/



https://magiclantern.fm/

Overlay

Global Draw	ON, all modes
Zebras	RAW RGB
Focus Peak	OFF
Magic Zoom	OFF
Cropmarks	OFF
Ghost image	OFF
Spotmeter	Percent, AFbox
False color	OFF
Histogram	RGB (YUV), Log
Waveform	OFF
Vectorscope	OFF
Level Indicator	OFF

Enable/disable ML overlay graphics (zebra, cropmarks...)
OFF / LiveView / QuickReview / ON, all modes

Freedom

Signing keys
Documentation

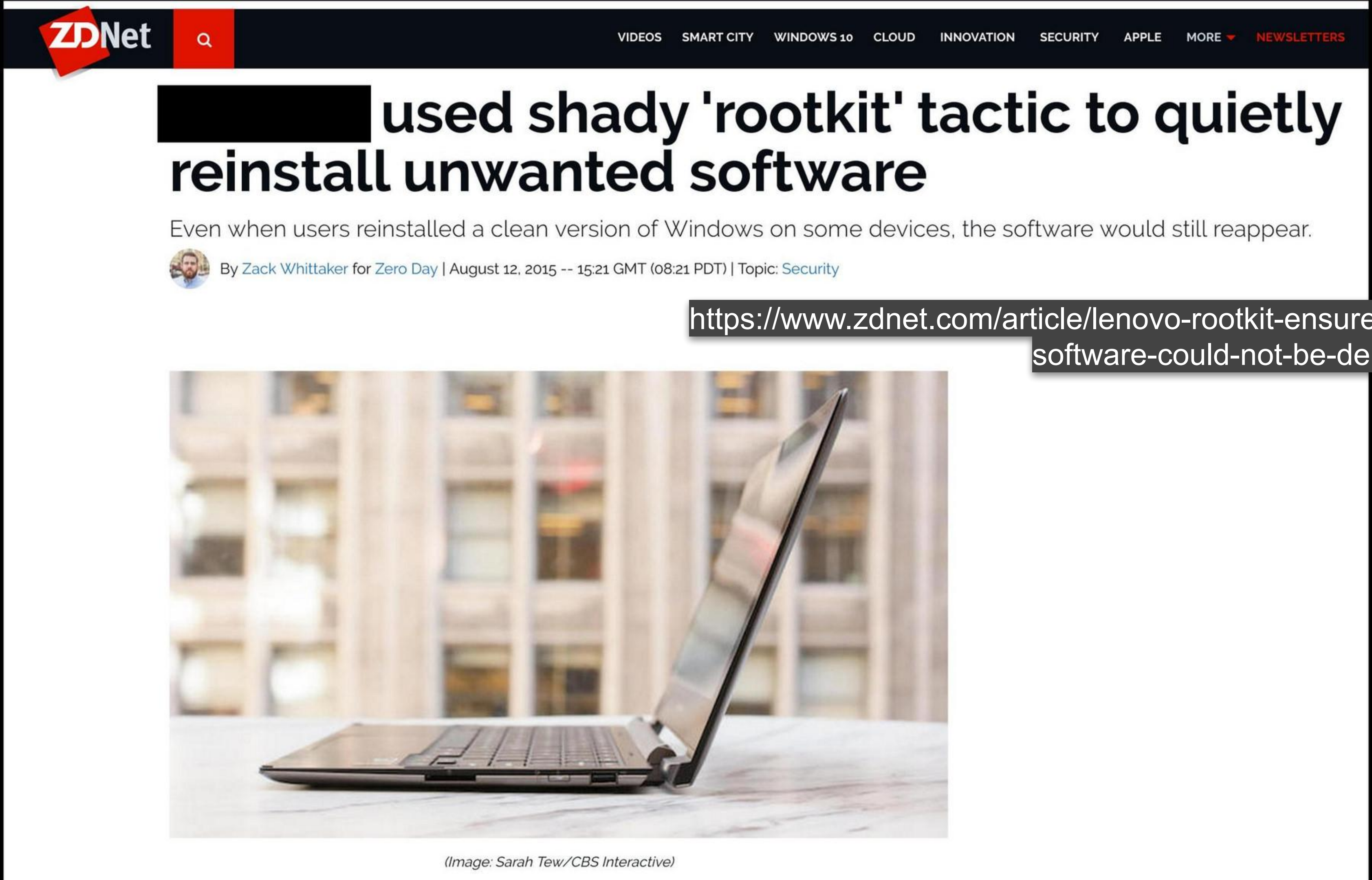
Freedom

Signing keys

Documentation

“Root of Trust for Update”

CC-BY-SA Jared Benedict
https://en.wikipedia.org/wiki/File:Series_2_tivo_front.jpg



[redacted] used shady 'rootkit' tactic to quietly reinstall unwanted software

Even when users reinstalled a clean version of Windows on some devices, the software would still reappear.

By Zack Whittaker for Zero Day | August 12, 2015 -- 15:21 GMT (08:21 PDT) | Topic: Security

https://www.zdnet.com/article/lenovo-rootkit-ensured-its-software-could-not-be-deleted/

(Image: Sarah Tew/CBS Interactive)

Why open source firmware is important

Jessie Frazelle - @jessfraz

“Vendors can rarely debug firmware issues…”

https://devopsdays.org/events/2019-chicago/program/jessie-frazelle/

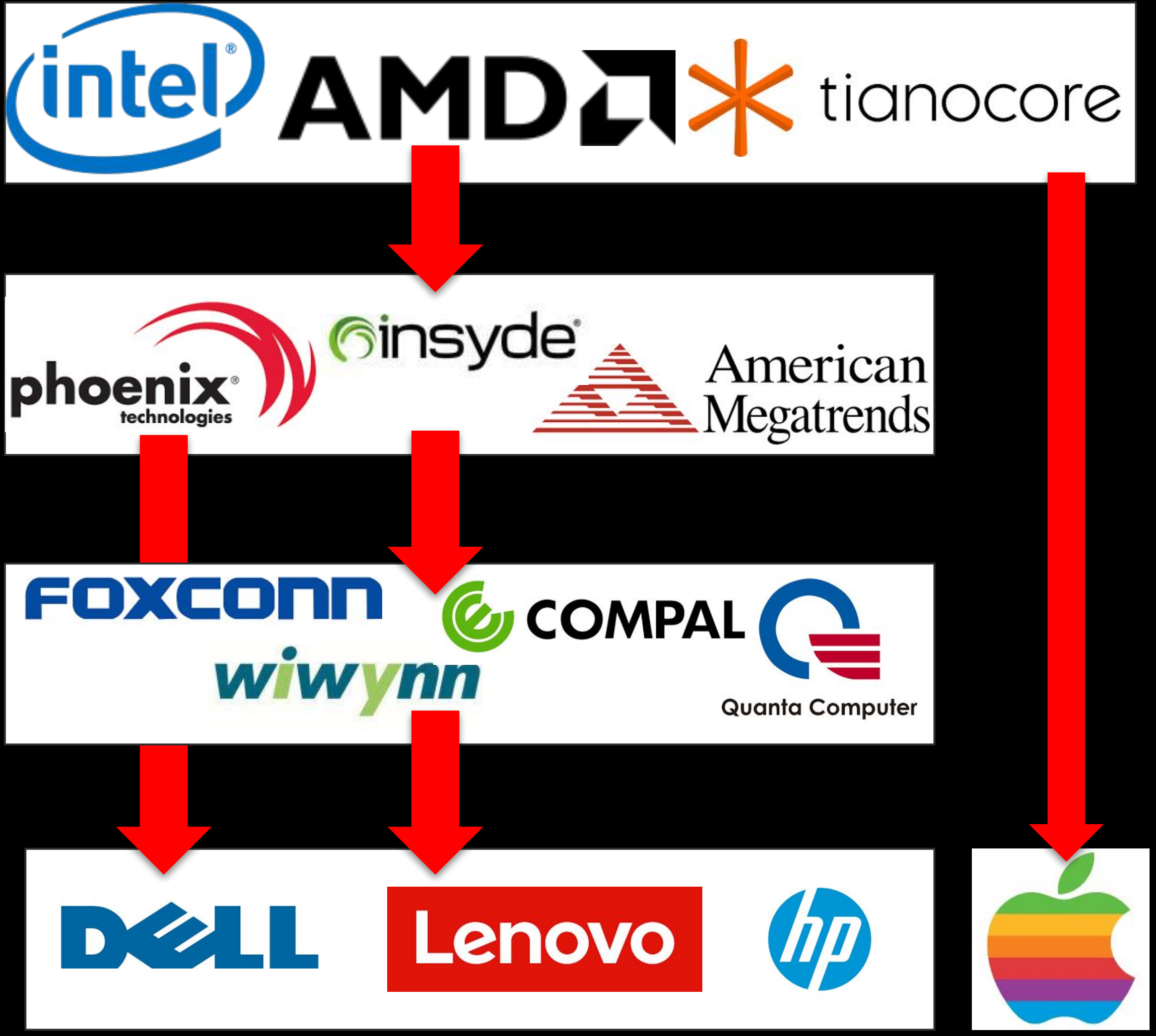
Reference Implementations

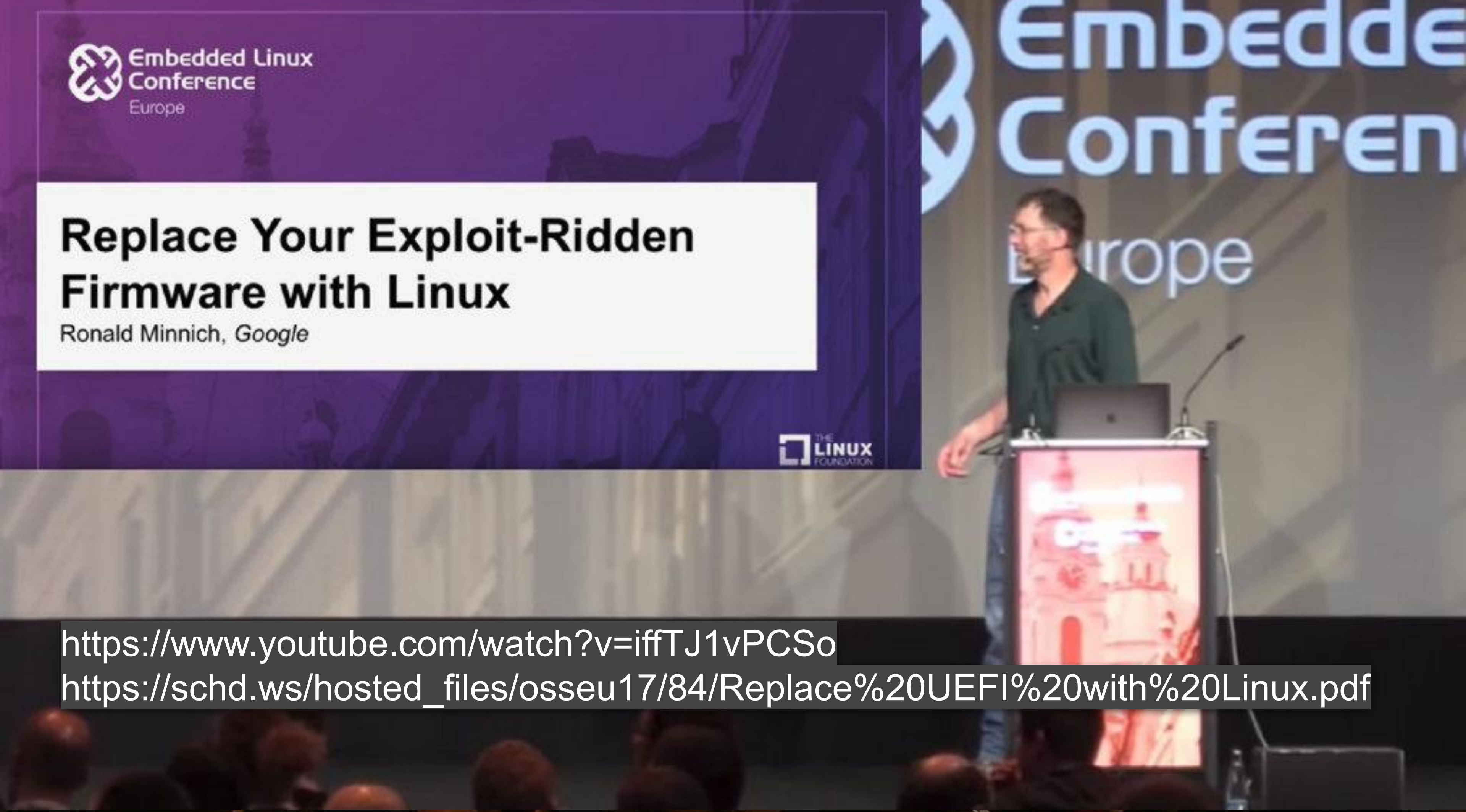
Independent BIOS Vendors (IBV)

Device Manufacturers (ODM)

Less than 10% of BIOS code!

Original Equipment Manufacturers (OEM)





Replace Your Exploit-Ridden Firmware with Linux

Ronald Minnich, *Google*

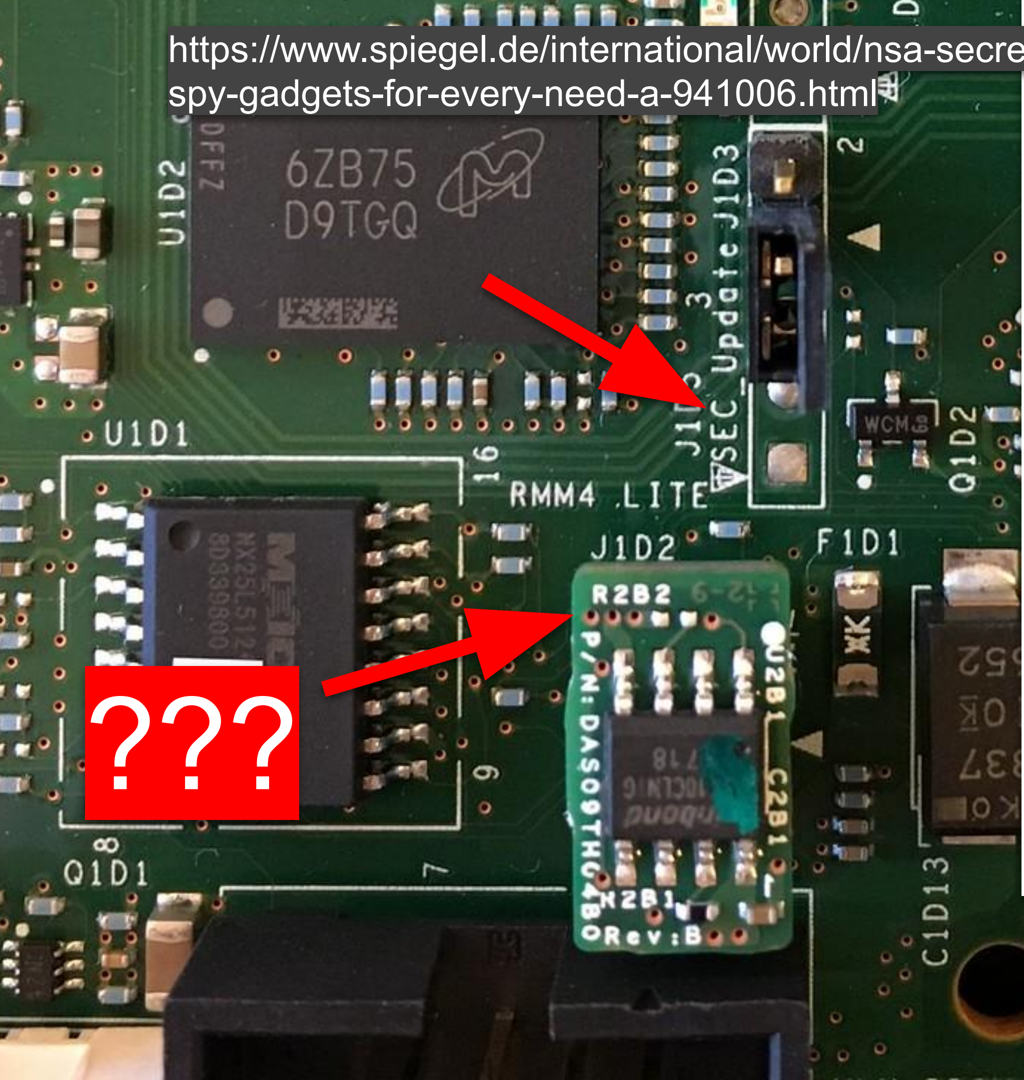
https://www.youtube.com/watch?v=iffTJ1vPCSo
https://schd.ws/hosted_files/osseu17/84/Replace%20UEFI%20with%20Linux.pdf

Freedom

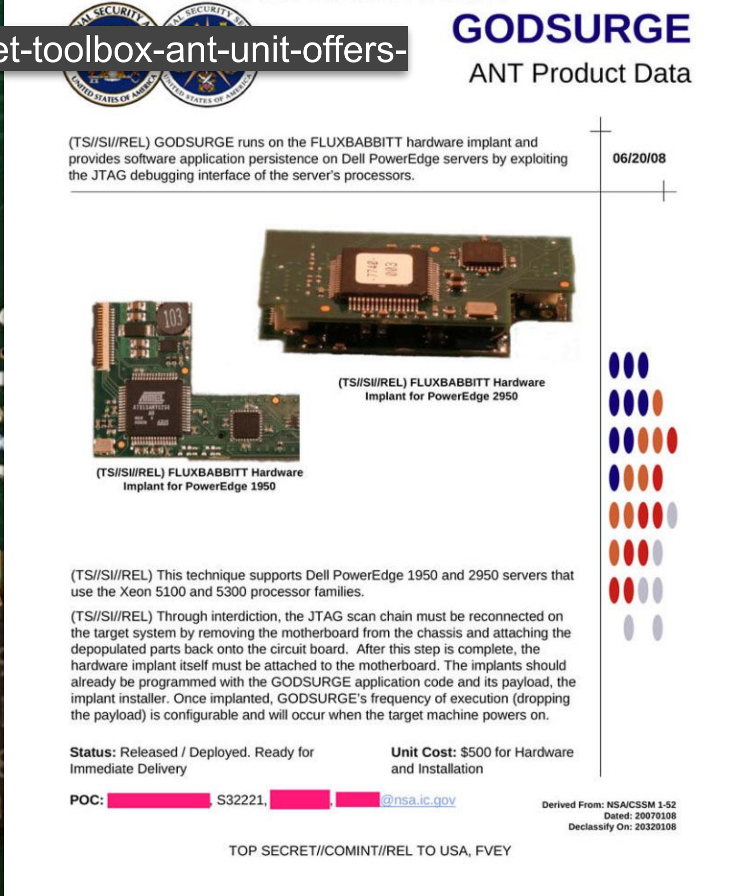
Signing keys

Documentation

https://www.spiegel.de/international/world/nsa-secret-toolbox-ant-unit-offers-spy-gadgets-for-every-need-a-941006.html



???



GODSURGE

ANT Product Data

(TS//SI//REL) GODSURGE runs on the FLUXBABBITT hardware implant and provides software application persistence on Dell PowerEdge servers by exploiting the JTAG debugging interface of the server's processors.

06/20/08

(TS//SI//REL) FLUXBABBITT Hardware Implant for PowerEdge 2950

(TS//SI//REL) FLUXBABBITT Hardware Implant for PowerEdge 1950

(TS//SI//REL) This technique supports Dell PowerEdge 1950 and 2950 servers that use the Xeon 5100 and 5300 processor families.

(TS//SI//REL) Through interdiction, the JTAG scan chain must be reconnected on the target system by removing the motherboard from the chassis and attaching the depopulated parts back onto the circuit board. After this step is complete, the hardware implant itself must be attached to the motherboard. The implants should already be programmed with the GODSURGE application code and its payload, the implant installer. Once implanted, GODSURGE's frequency of execution (dropping the payload) is configurable and will occur when the target machine powers on.

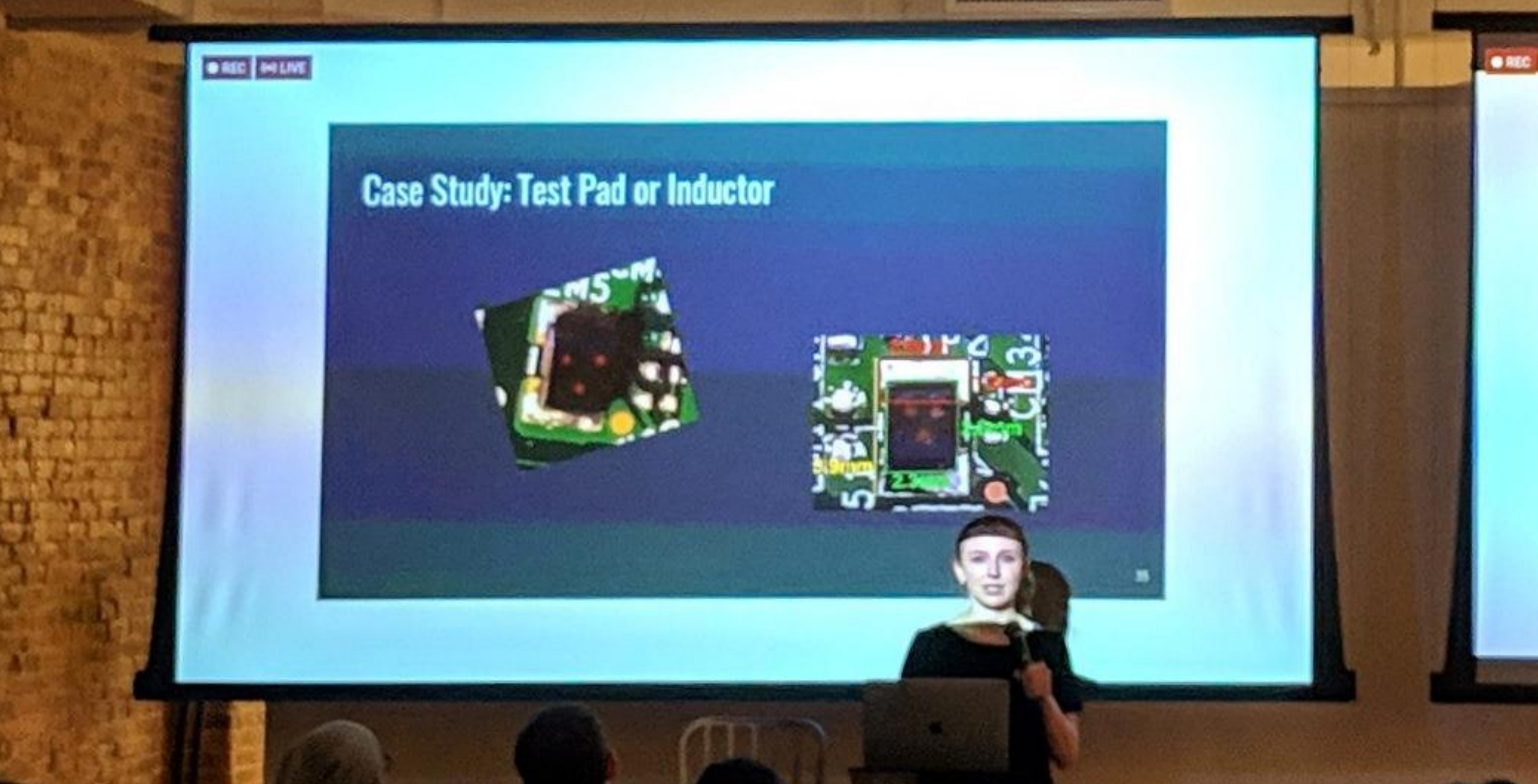
Status: Released / Deployed. Ready for Immediate Delivery

Unit Cost: $500 for Hardware and Installation

POC: [redacted], S32221, [redacted], [redacted]@nsa.ic.gov

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

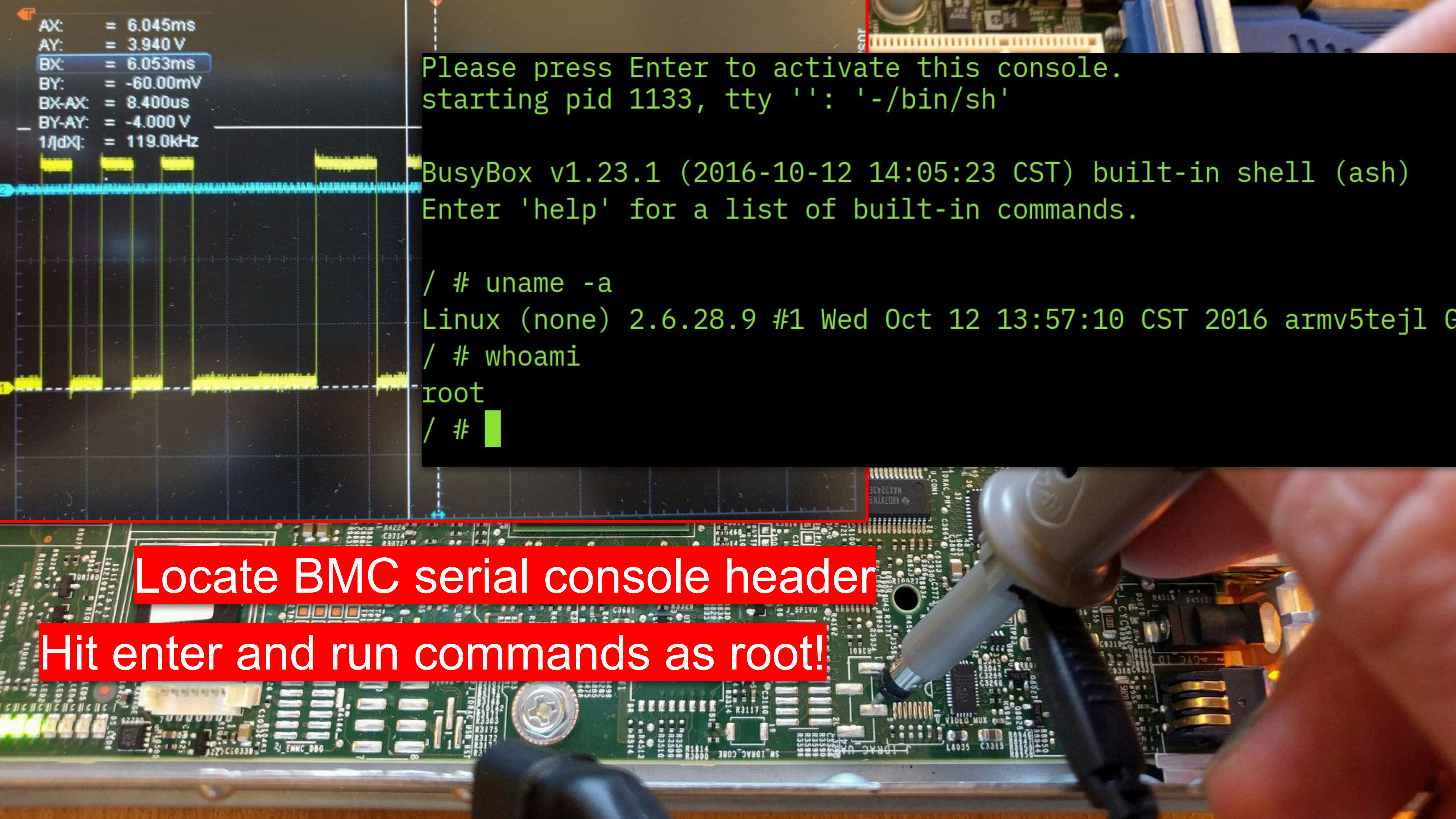
TOP SECRET//COMINT//REL TO USA, FVEY



Case Study: Test Pad or Inductor

Sophia D’Antoine “A Tale of Two Supply Chains”

https://www.riverloopsecurity.com/blog/2018/12/supermicro-validation-1/



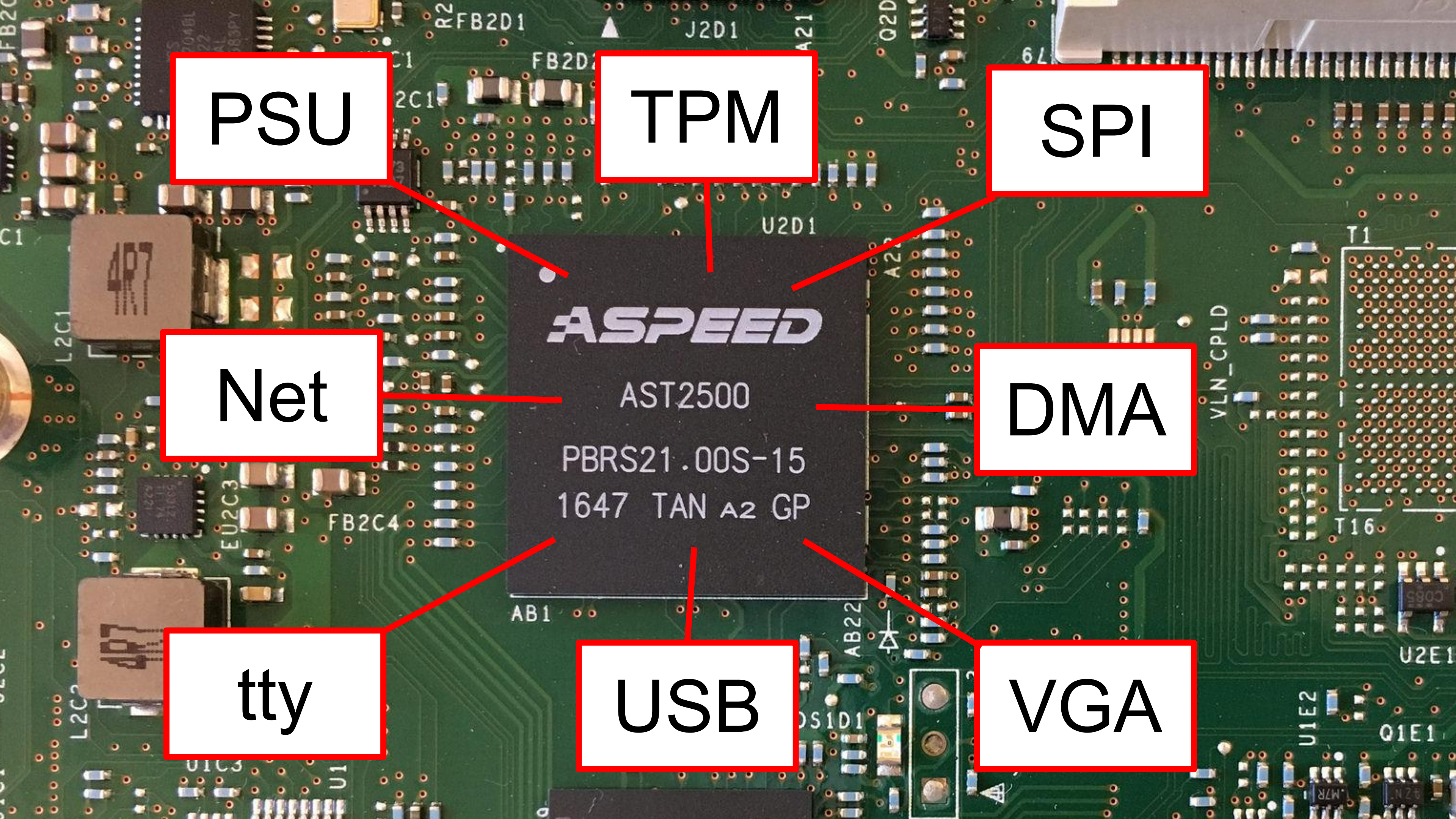
```
Please press Enter to activate this console.
starting pid 1133, tty '': '-/bin/sh'


BusyBox v1.23.1 (2016-10-12 14:05:23 CST) built-in shell (ash)
Enter 'help' for a list of built-in commands.

/ # uname -a
Linux (none) 2.6.28.9 #1 Wed Oct 12 13:57:10 CST 2016 armv5tejl G
/ # whoami
root
/ # 
```

Locate BMC serial console header

Hit enter and run commands as root!



PSU

TPM

SPI

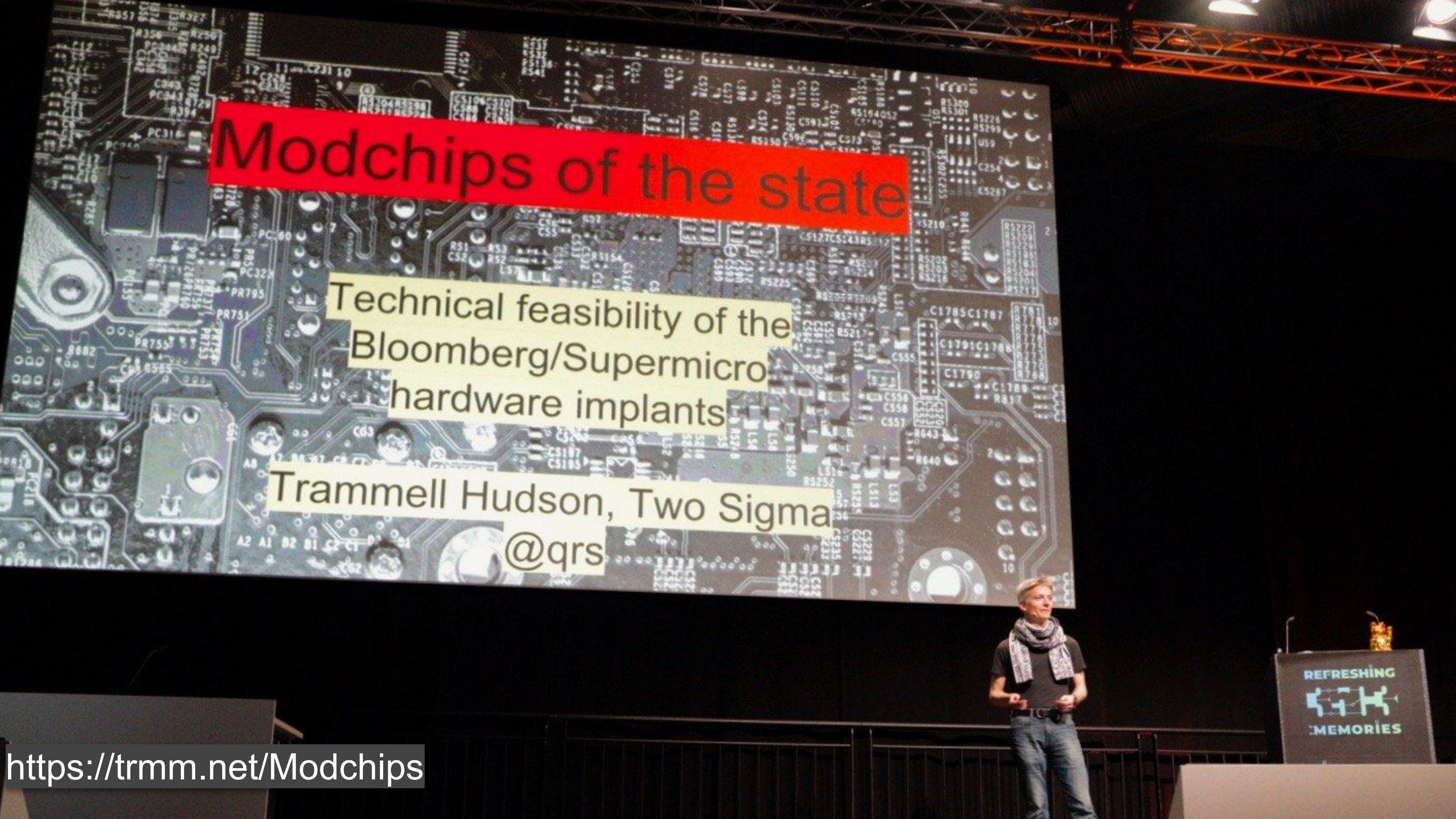
Net

DMA

tty

USB

VGA



Modchips of the state

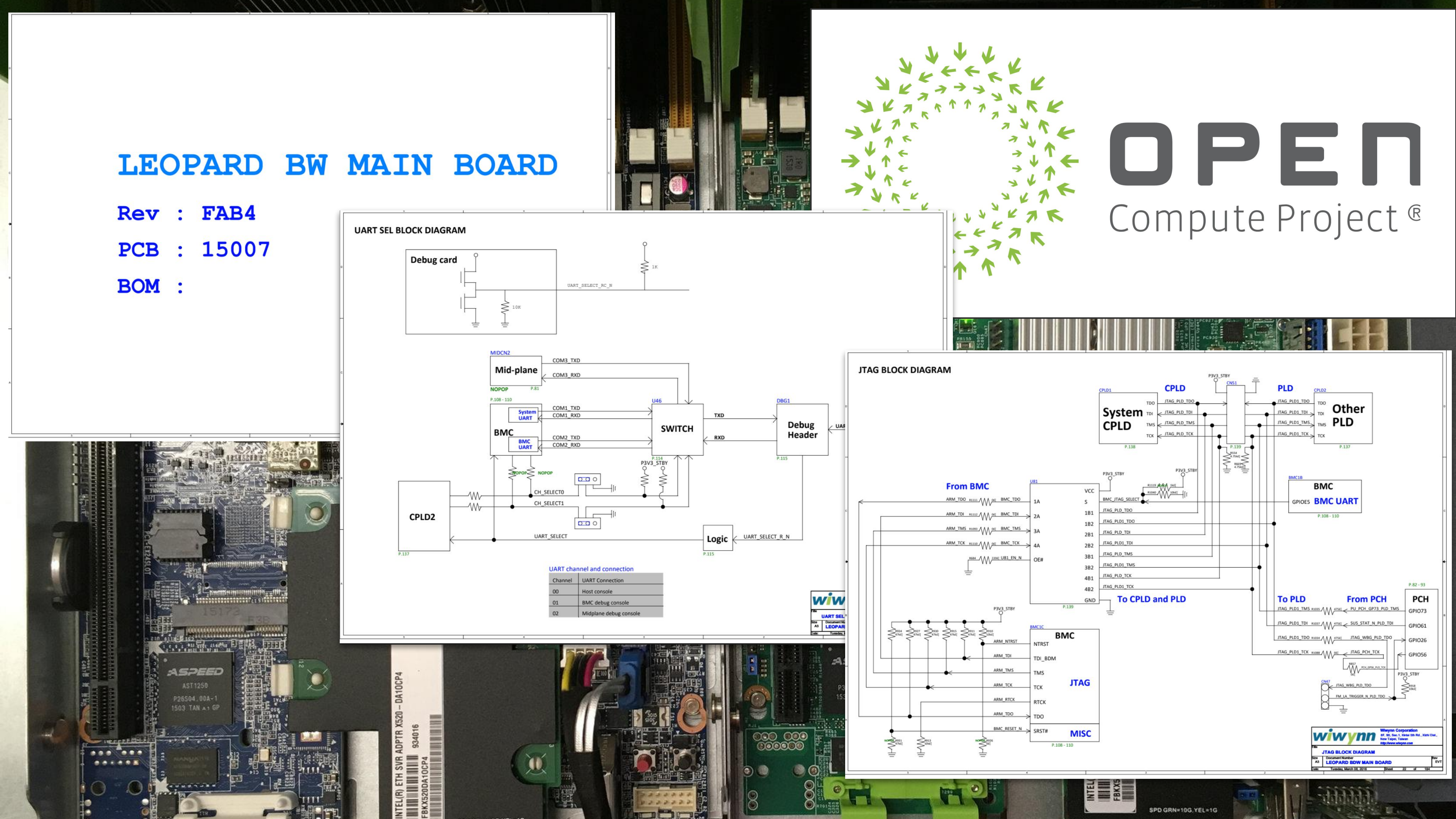
Technical feasibility of the Bloomberg/Supermicro hardware implants

Trammell Hudson, Two Sigma
@qrs

https://trmm.net/Modchips

OPEN
Compute Project ®

https://www.opencompute.org/about



LEOPARD BW MAIN BOARD

Rev : FAB4

PCB : 15007

BOM :

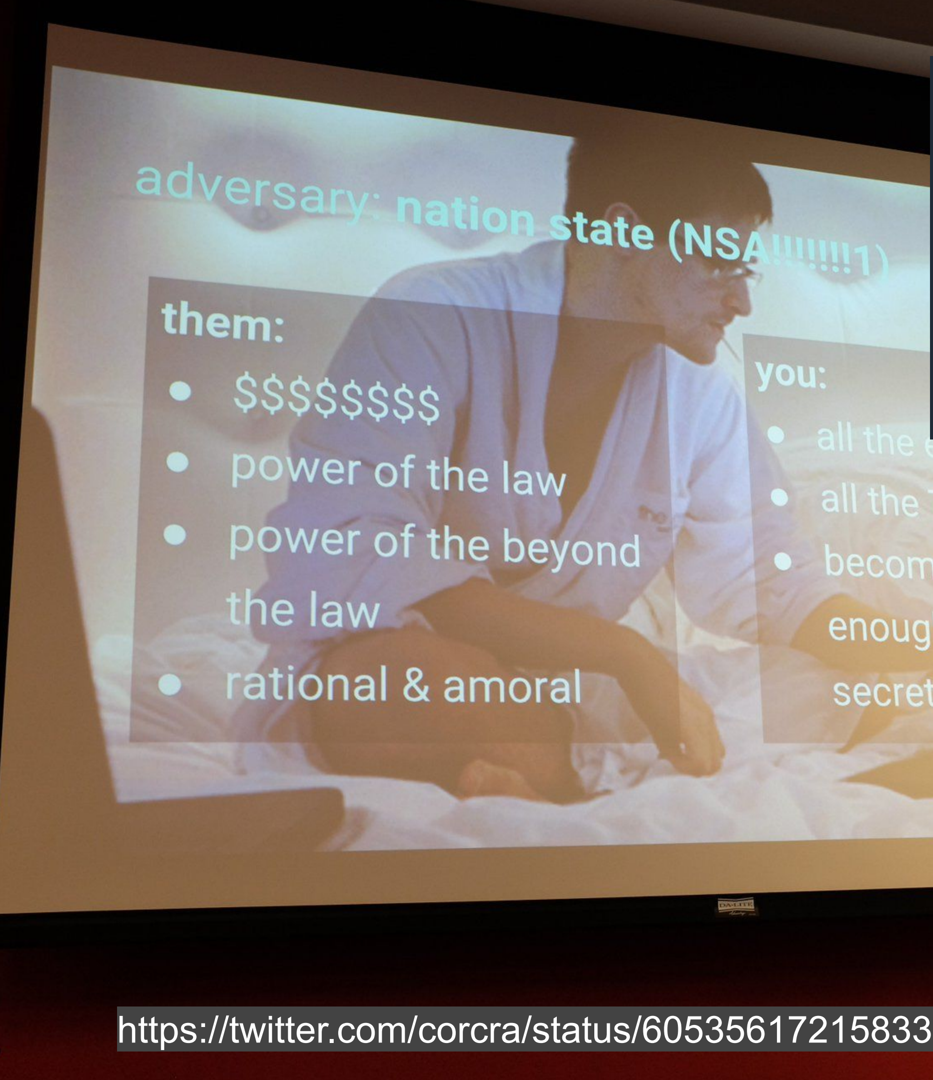
OPEN Compute Project ®

UART SEL BLOCK DIAGRAM

UART channel and connection

Channel	UART Connection
00	Host console
01	BMC debug console
02	Midplane debug console

JTAG BLOCK DIAGRAM



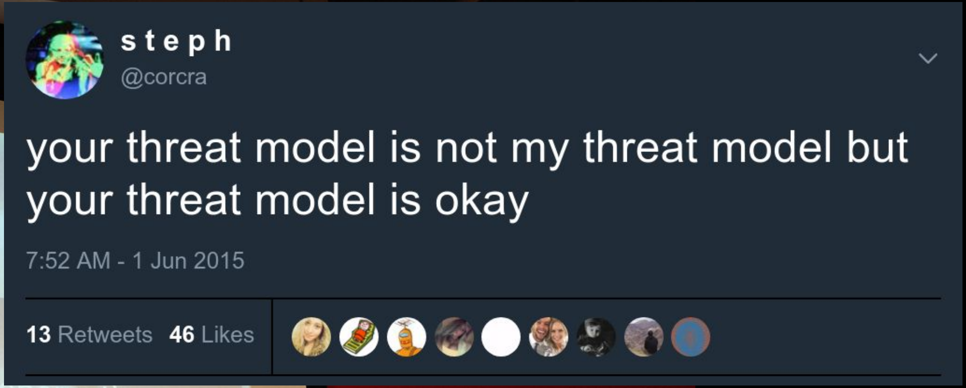
adversary: nation state (NSA!!!!!!!1)

them:

- $$$$$$$$
- power of the law
- power of the beyond the law
- rational & amoral

you:

- all the encryption
- all the Tor
- become famous enough you can't be secretly murdered?



steph
@corcra

your threat model is not my threat model but your threat model is okay

7:52 AM - 1 Jun 2015

13 Retweets **46** Likes

https://twitter.com/corcra/status/605356172158332929

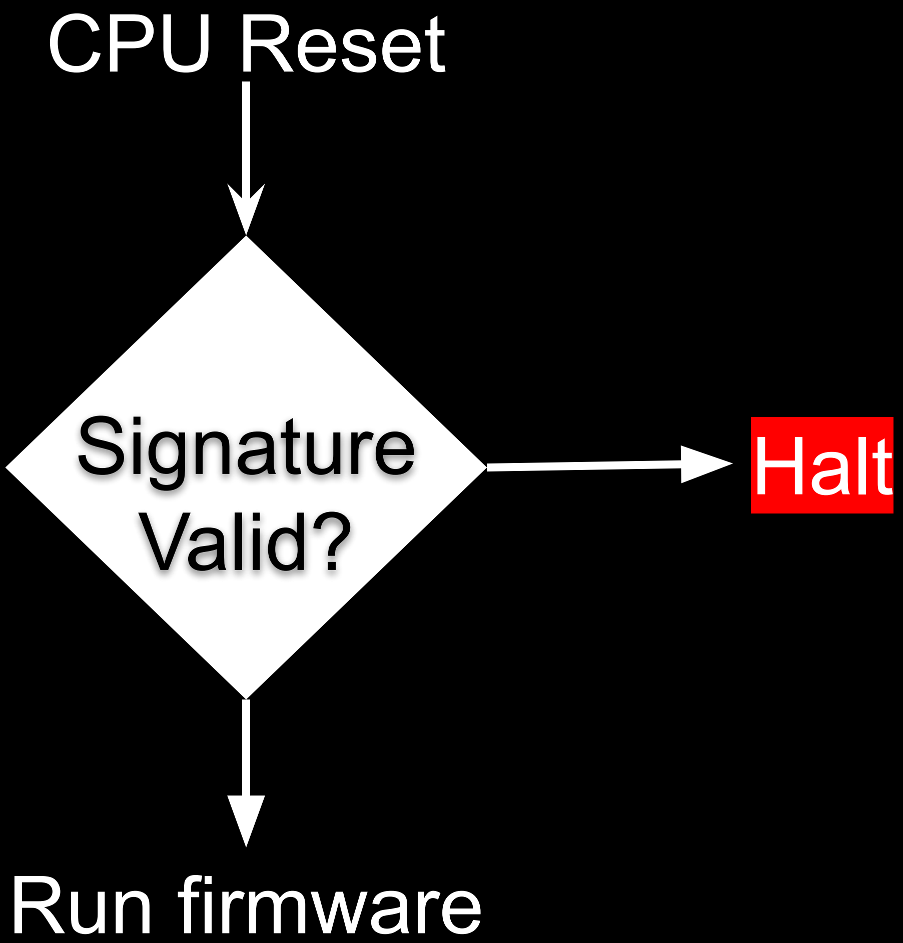
CPU Reset
Halt
Ru ware

Freedom?

Resilience?

Attestation?

Verified Boot

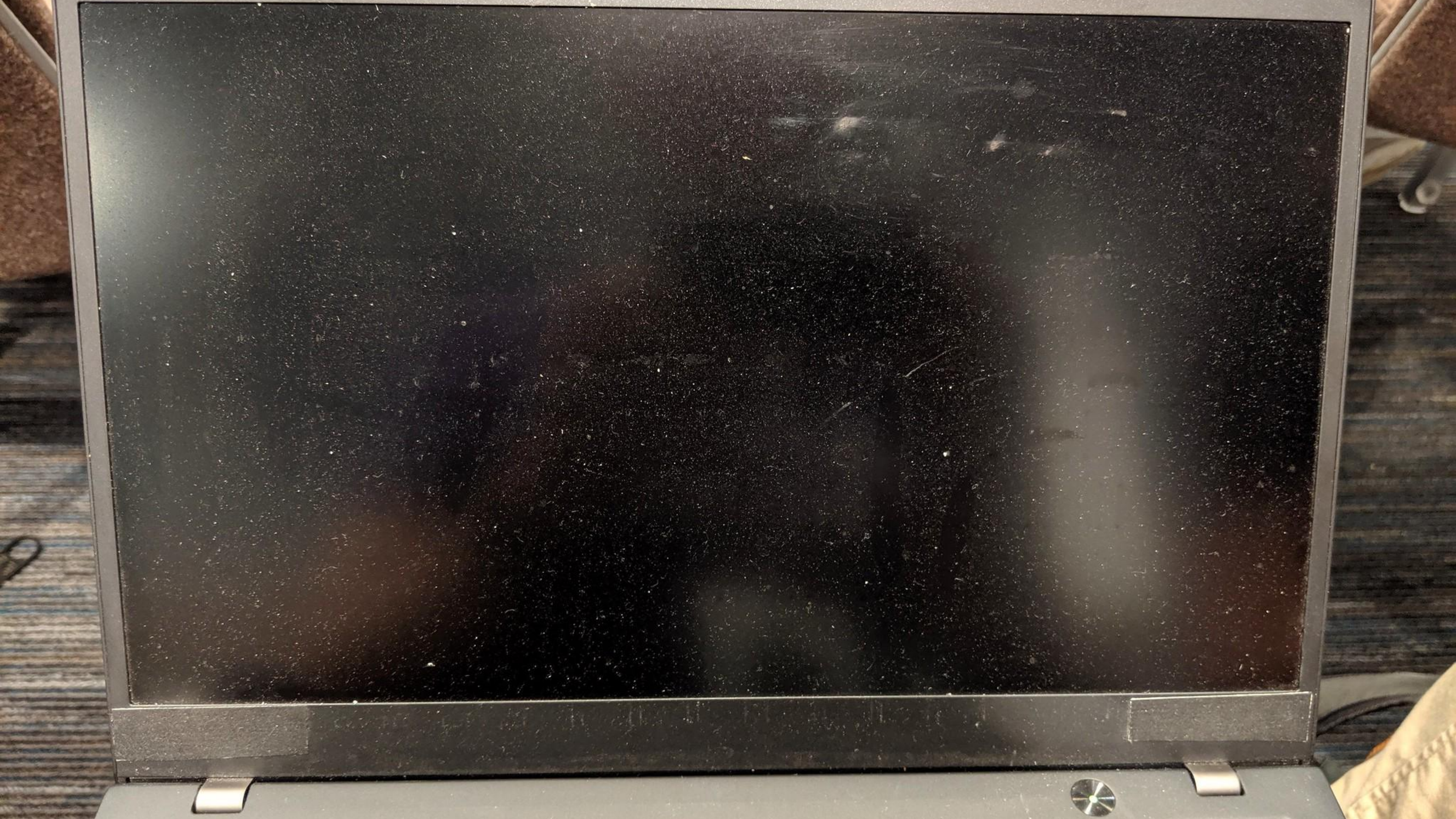


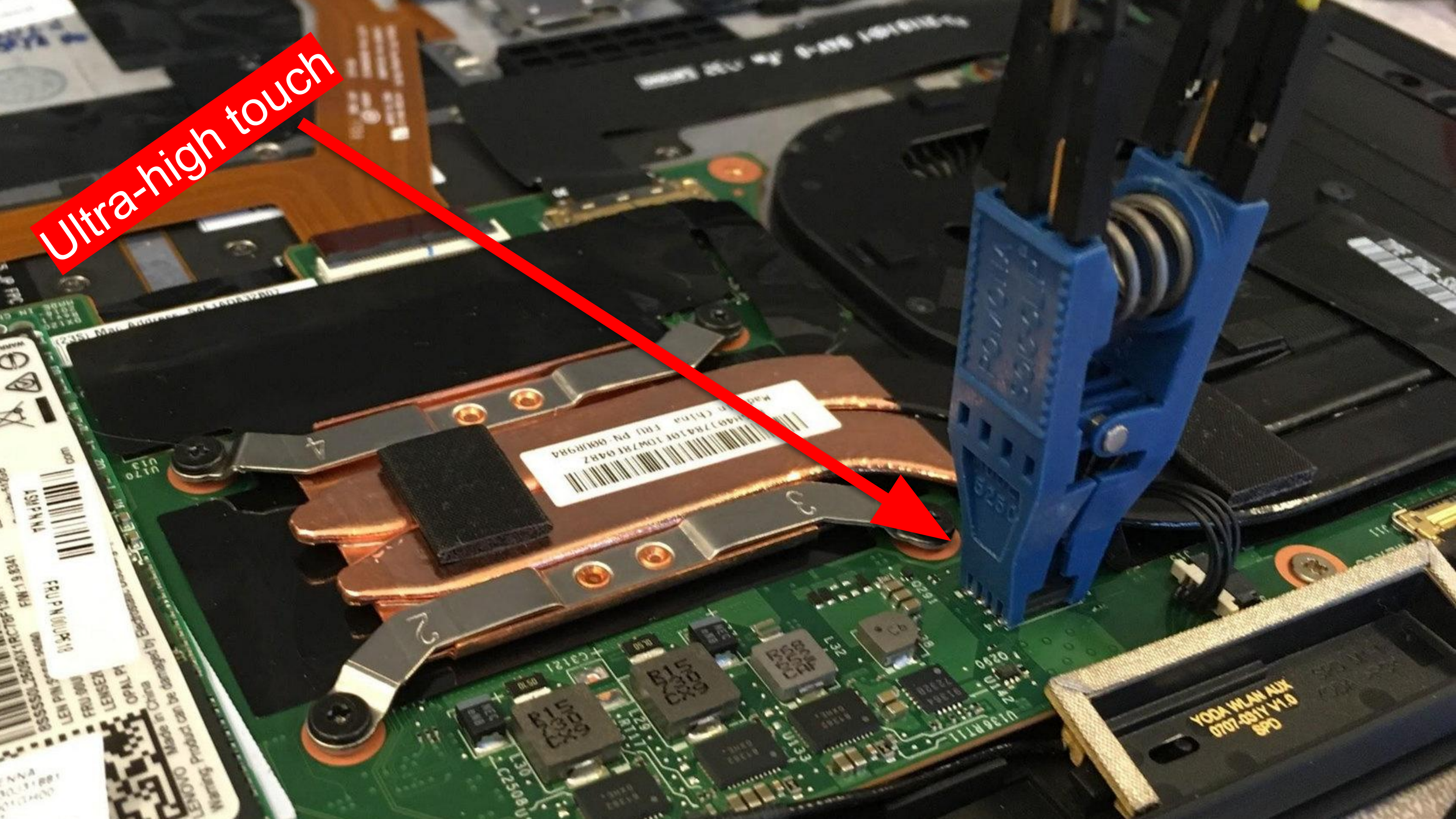
CPU Reset

Signature Valid?

Halt

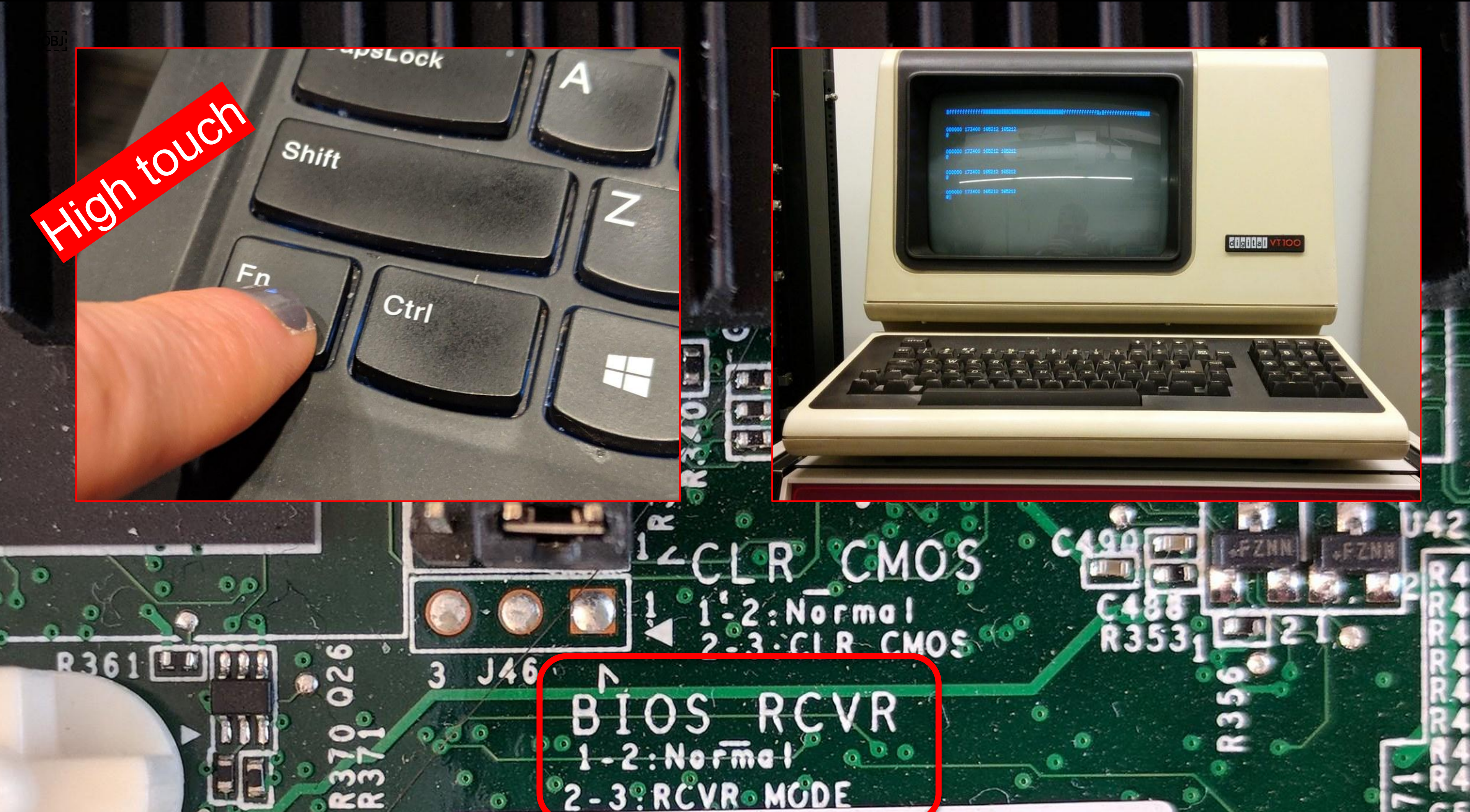
Run firmware



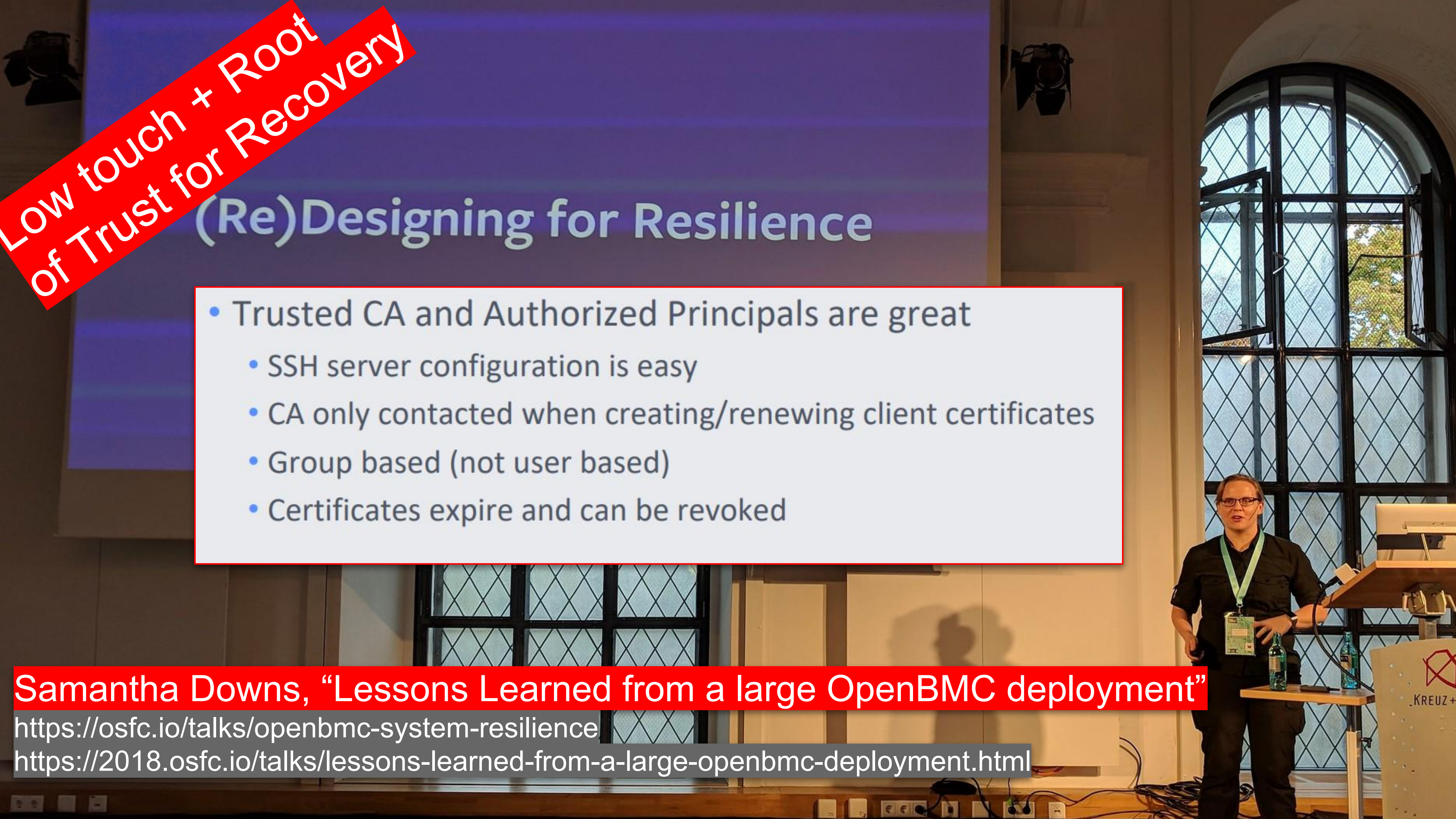


Ultra-high touch

High touch


CapsLock
A
Shift
Z
Fn
Ctrl
digital VT100
CLR CMOS
1-2:Normal
2-3:CLR CMOS
J46
BIOS RCVR
1-2:Normal
2-3:RCVR MODE

Low touch + Root of Trust for Recovery



(Re)Designing for Resilience

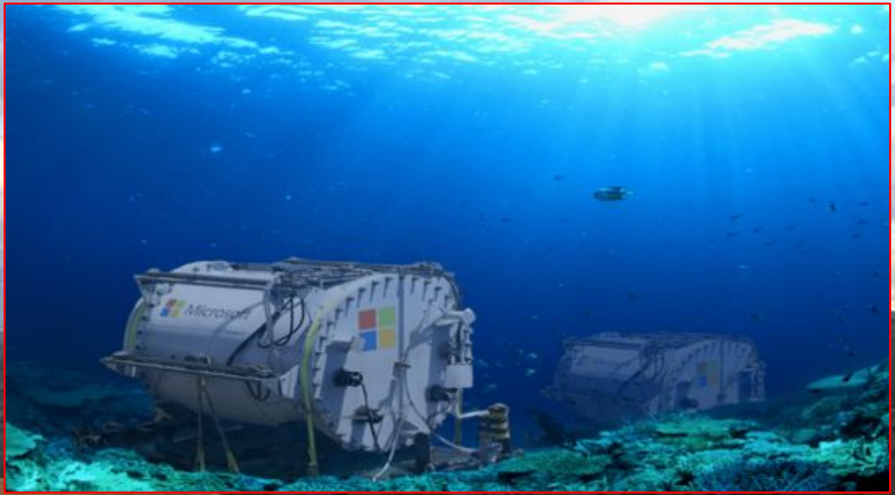
- Trusted CA and Authorized Principals are great
  - SSH server configuration is easy
  - CA only contacted when creating/renewing client certificates
  - Group based (not user based)
  - Certificates expire and can be revoked

Samantha Downs, “Lessons Learned from a large OpenBMC deployment”

https://osfc.io/talks/openbmc-system-resilience

https://2018.osfc.io/talks/lessons-learned-from-a-large-openbmc-deployment.html

[redacted]

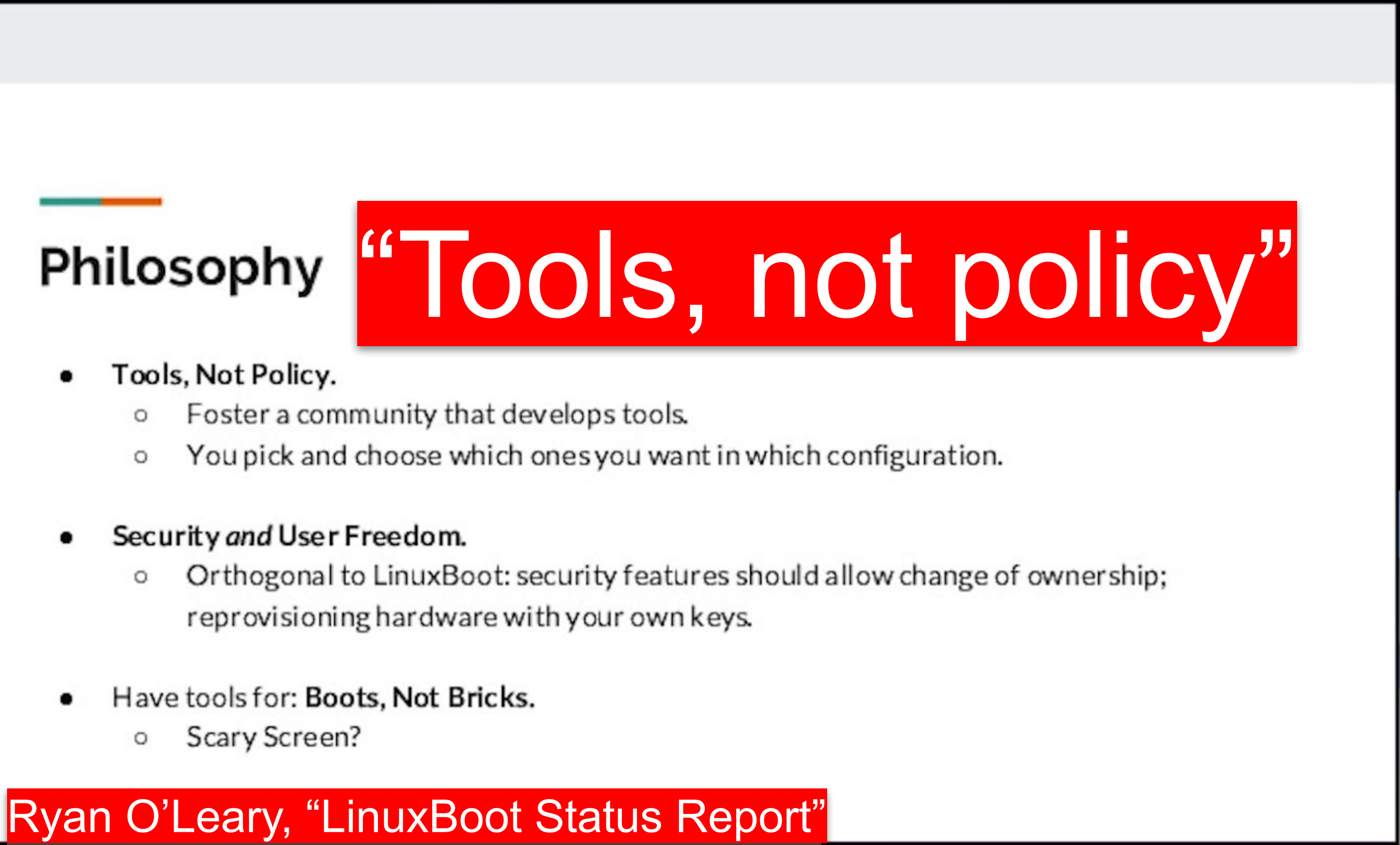


https://natick.research.microsoft.com/

https://commons.wikimedia.org/wiki/File:Edge_Night_02.jpg

https://commons.wikimedia.org/wiki/File:EFF_photograph_of_NSA%27s_Utah_Data_Center.jpg

“Tools, not policy”

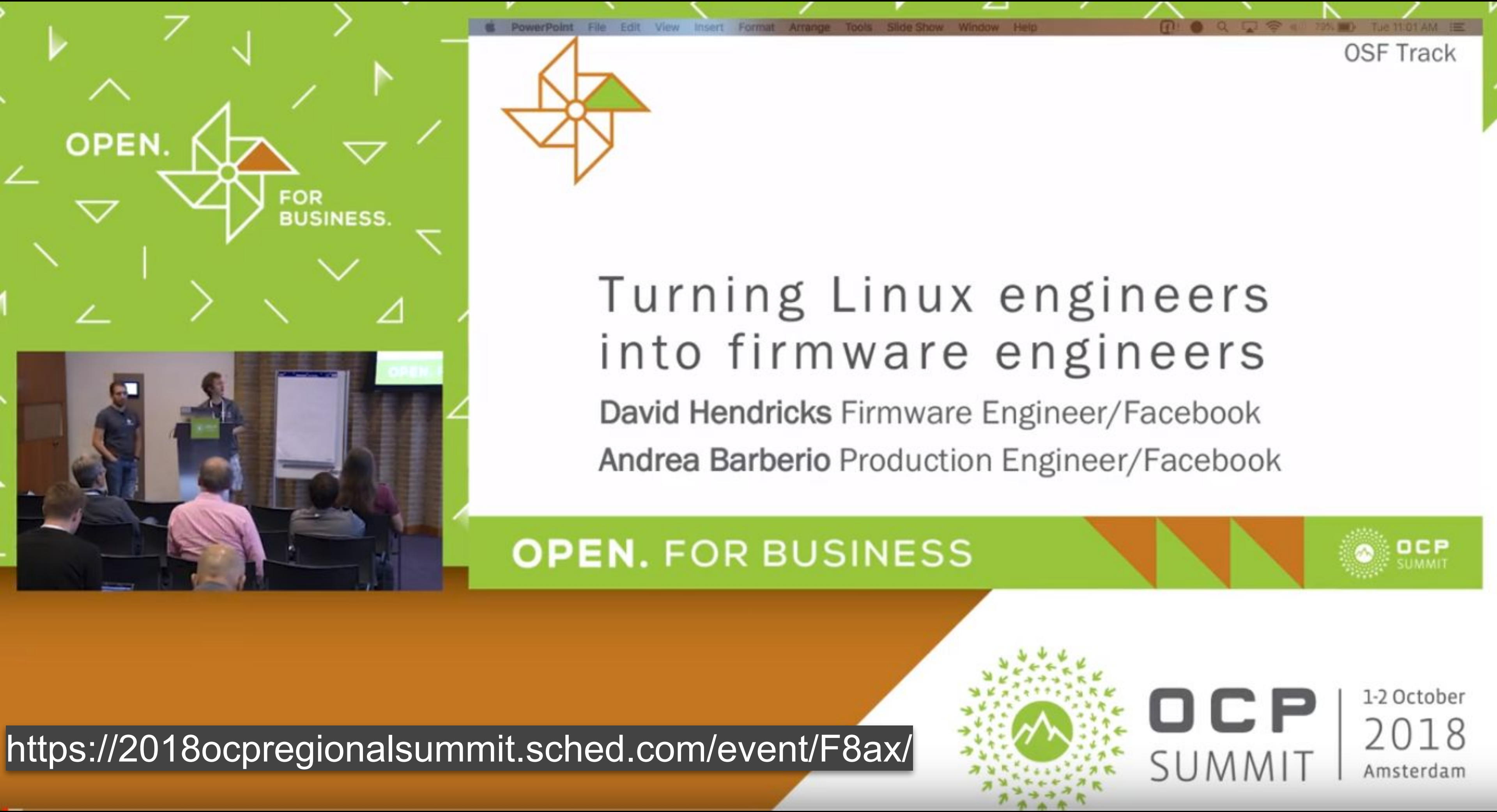


Philosophy

- **Tools, Not Policy.**
  - Foster a community that develops tools.
  - You pick and choose which ones you want in which configuration.
- **Security *and* User Freedom.**
  - Orthogonal to LinuxBoot: security features should allow change of ownership; reprovisioning hardware with your own keys.
- Have tools for: **Boots, Not Bricks.**
  - Scary Screen?

Ryan O’Leary, “LinuxBoot Status Report”

https://2018.osfc.io/talks/linuxboot-status-report.html


PowerPoint File Edit View Insert Format Arrange Tools Slide Show Window Help
Tue 11:01 AM
OPEN.
FOR BUSINESS.

OSF Track

Turning Linux engineers into firmware engineers

David Hendricks Firmware Engineer/Facebook

Andrea Barberio Production Engineer/Facebook

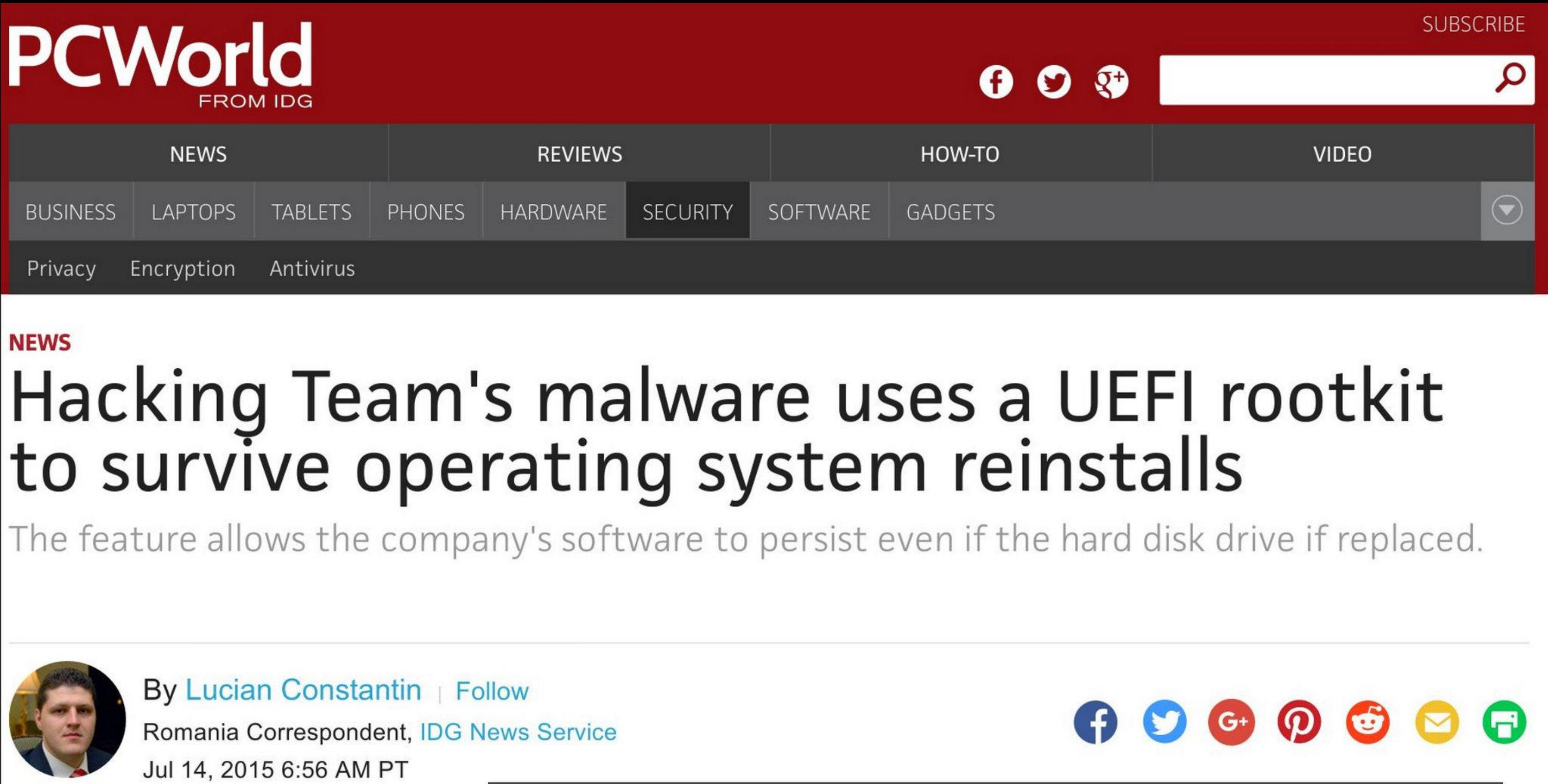
OPEN. FOR BUSINESS

OCP SUMMIT

OCP SUMMIT | 1-2 October 2018 Amsterdam

https://2018ocpregionalsummit.sched.com/event/F8ax/

Recovery from attacks is hard



NEWS

Hacking Team's malware uses a UEFI rootkit to survive operating system reinstalls

The feature allows the company's software to persist even if the hard disk drive if replaced.

By Lucian Constantin | Follow

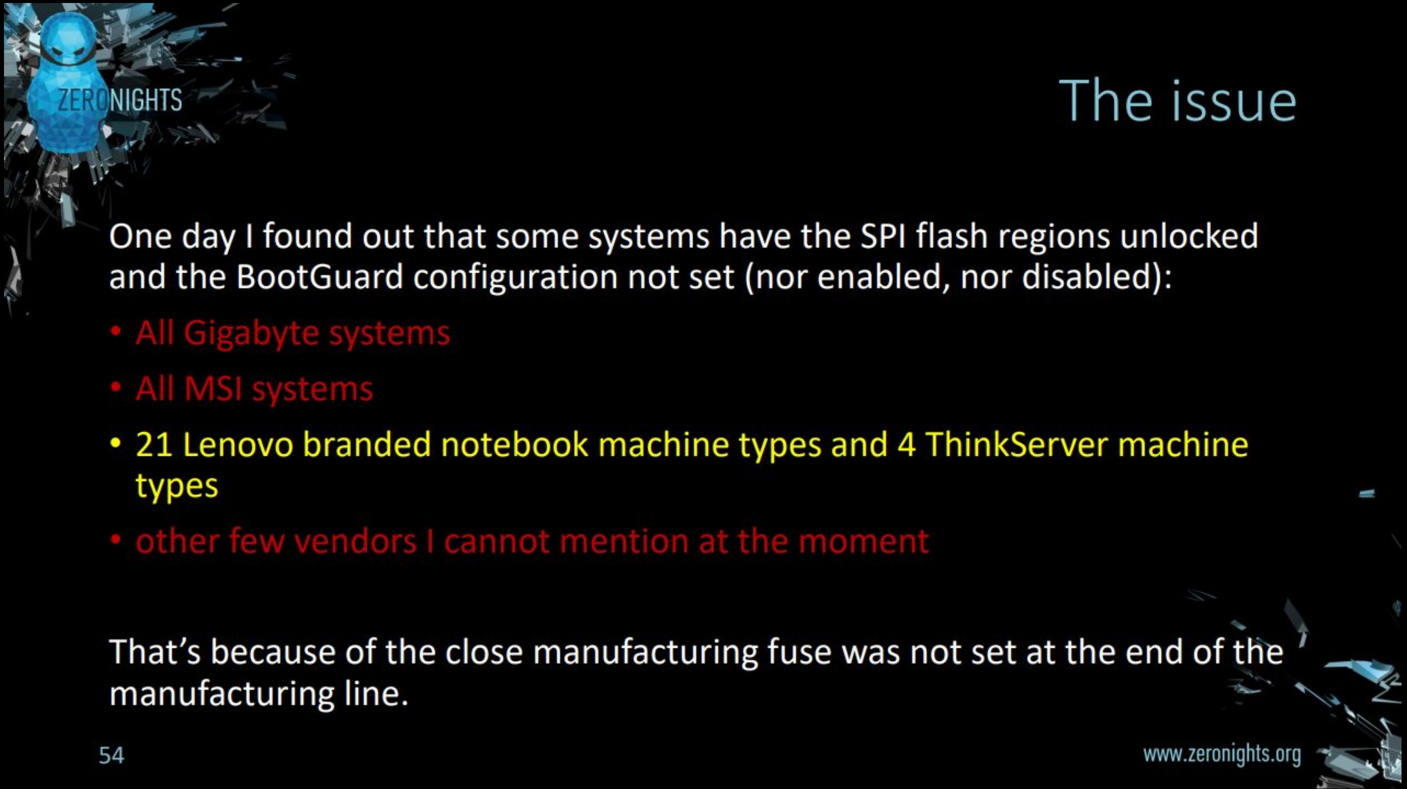
Romania Correspondent, IDG News Service

Jul 14, 2015 6:56 AM PT

https://www.pcworld.com/article/2948092/hacking-teams-malware-uses-uefi-rootkit-to-survive-os-reinstalls.html https://2016.zeronights.ru/wp-content/uploads/2017/03/Intel-BootGuard.pdf

Safeguarding rootkits:
Intel BootGuard

Alexander Ermolov



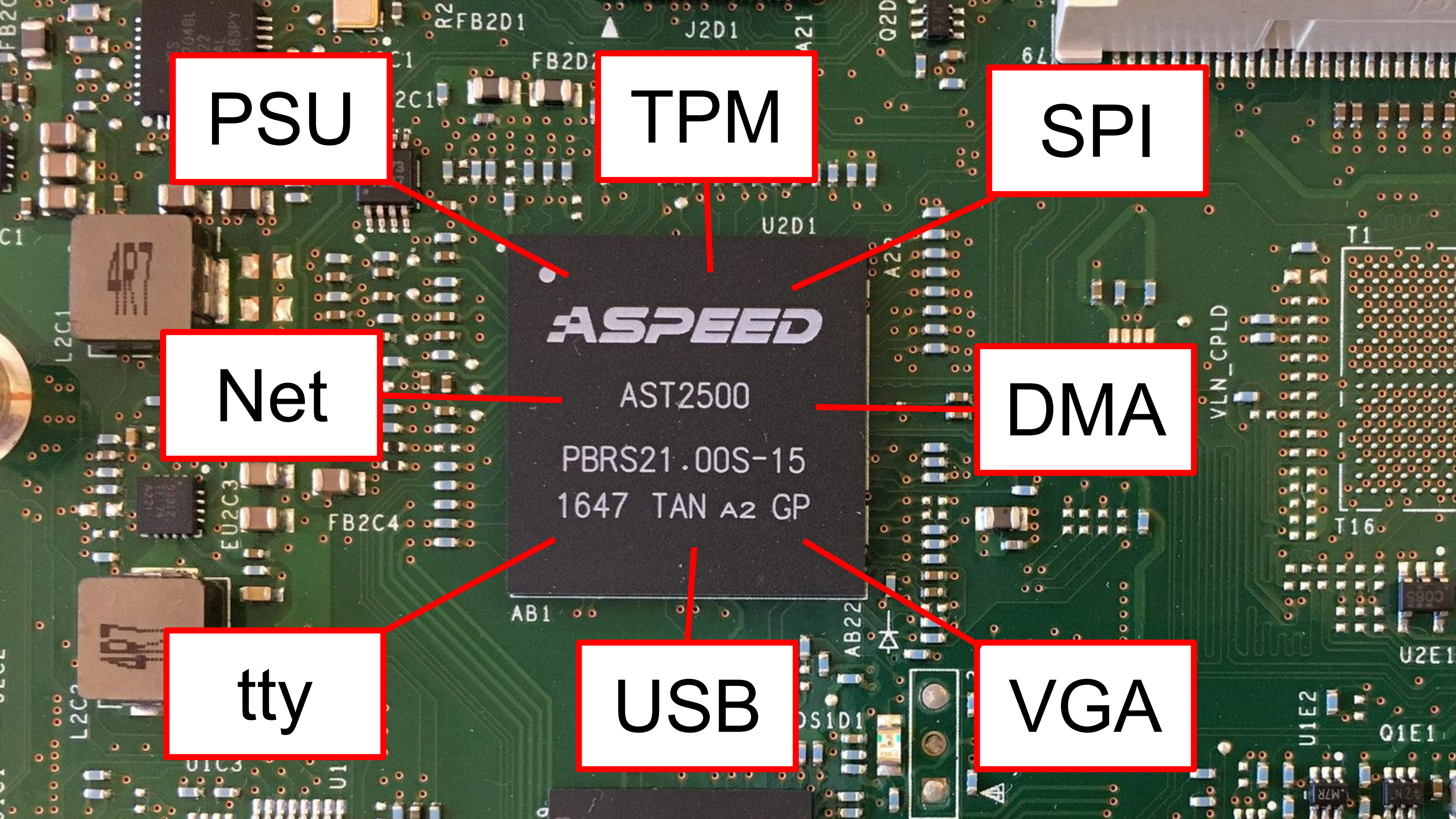
ZERONIGHTS

The issue

One day I found out that some systems have the SPI flash regions unlocked and the BootGuard configuration not set (nor enabled, nor disabled):

- All Gigabyte systems
- All MSI systems
- 21 Lenovo branded notebook machine types and 4 ThinkServer machine types
- other few vendors I cannot mention at the moment

That's because of the close manufacturing fuse was not set at the end of the manufacturing line.



PSU

TPM

SPI

Net

DMA

tty

USB

VGA

The Current State of Industry Servers

- UEFI – limited protection
  - Secure-boot-like functionality
  - No Detect or Recover
  - Platform dependent
- BMC - typically unsecure
- Periphe
  - No
  - Not

“BMC - Typically unsecure
- No protect, no detect, no recovery
- No reliable attestations”

Yigal Edery, Program Manager Azure Security

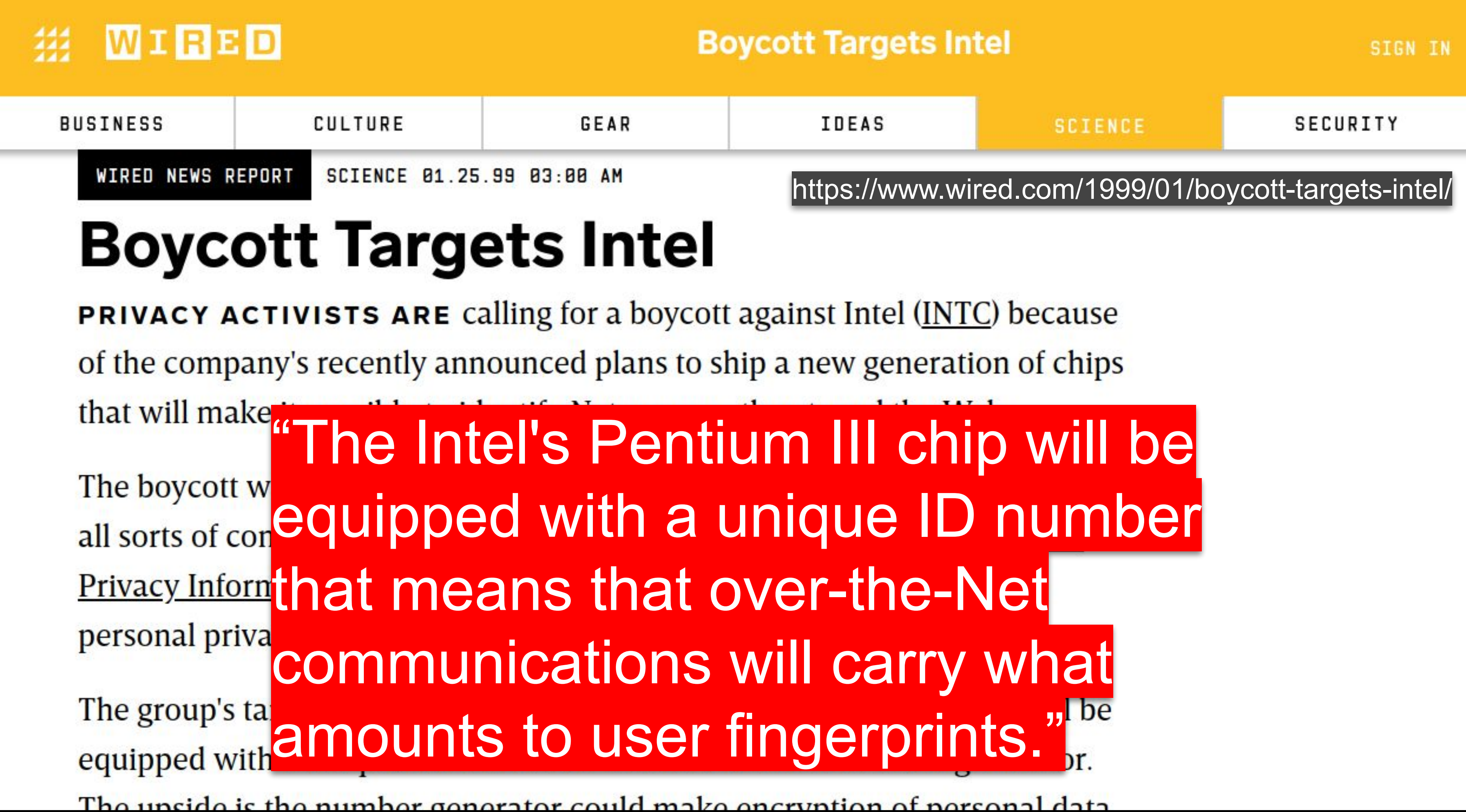
https://2018ocpregionalsummit.sched.com/event/F8b0

CPU Re t
Halt
Ru ware

Freedom?

Resilience?

Attestation?



WIRED NEWS REPORT SCIENCE 01.25.99 03:00 AM

https://www.wired.com/1999/01/boycott-targets-intel/

Boycott Targets Intel

PRIVACY ACTIVISTS ARE calling for a boycott against Intel (INTC) because of the company's recently announced plans to ship a new generation of chips that will make

The boycott w

all sorts of con

Privacy Inforn

personal priva

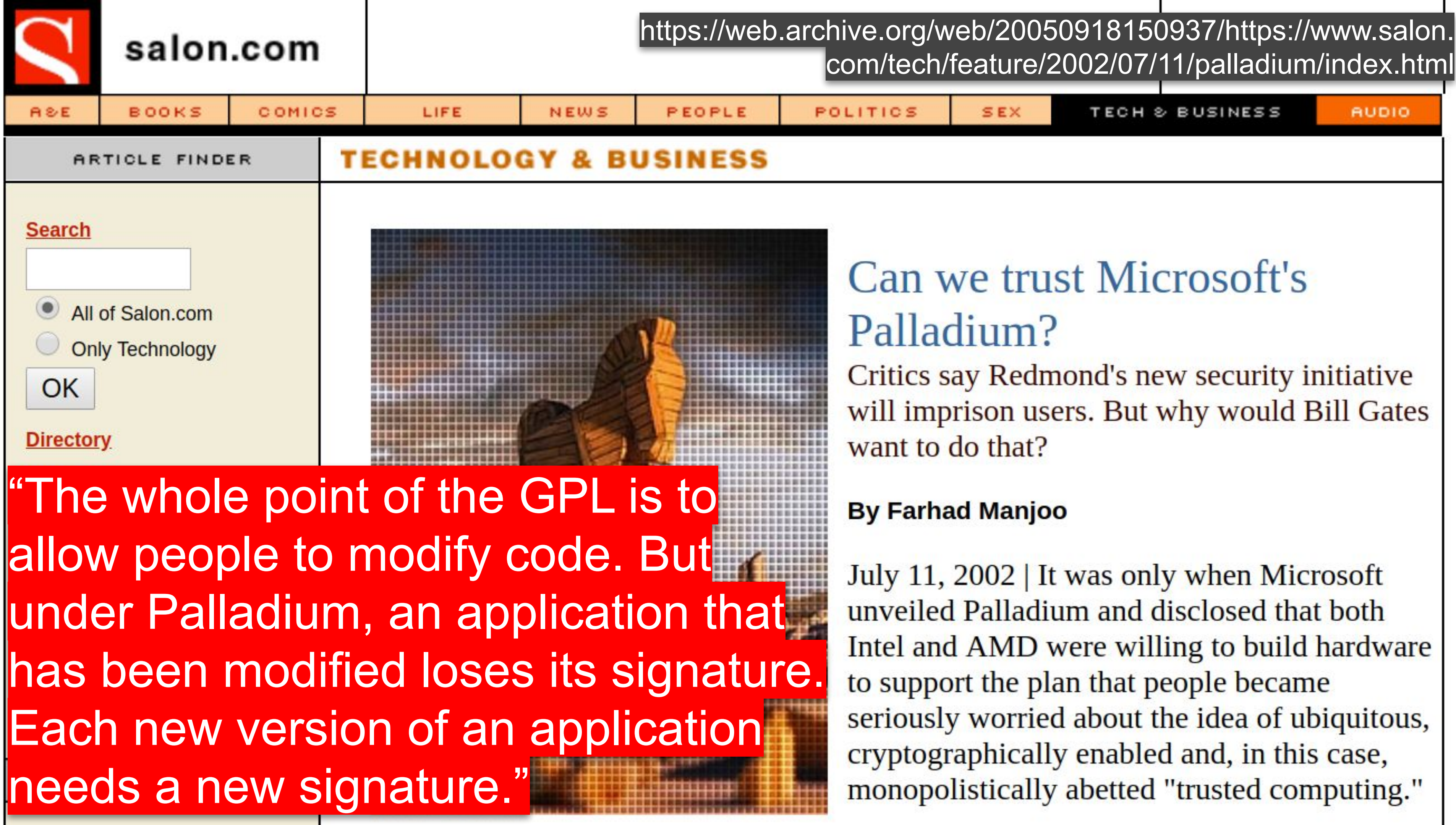
The group's ta l be

equipped with or.

The upside is the number generator could make encryption of personal data

“The Intel's Pentium III chip will be equipped with a unique ID number that means that over-the-Net communications will carry what amounts to user fingerprints.”

https://web.archive.org/web/20050918150937/https://www.salon.com/tech/feature/2002/07/11/palladium/index.html



TECHNOLOGY & BUSINESS

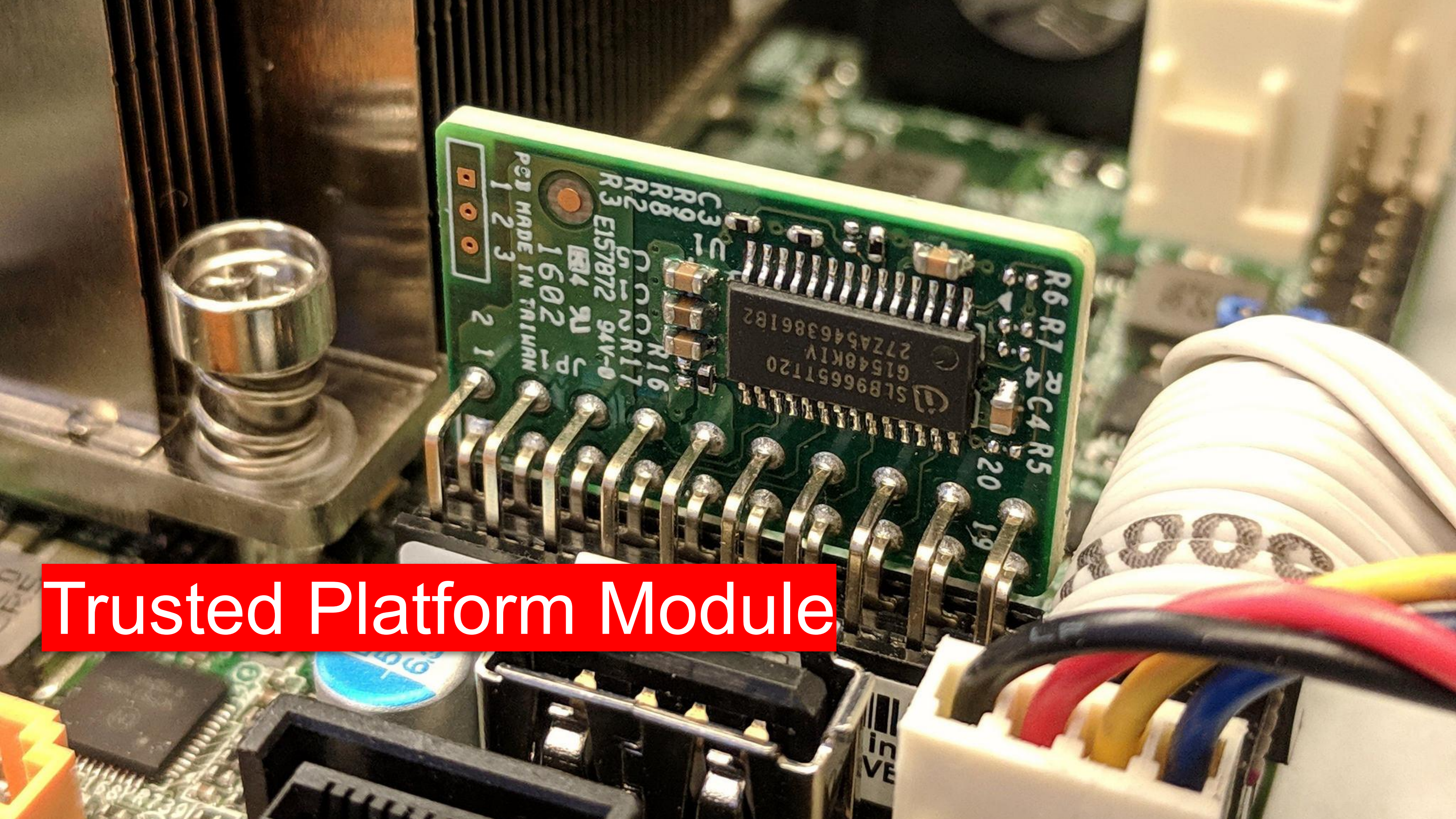
Can we trust Microsoft's Palladium?

Critics say Redmond's new security initiative will imprison users. But why would Bill Gates want to do that?

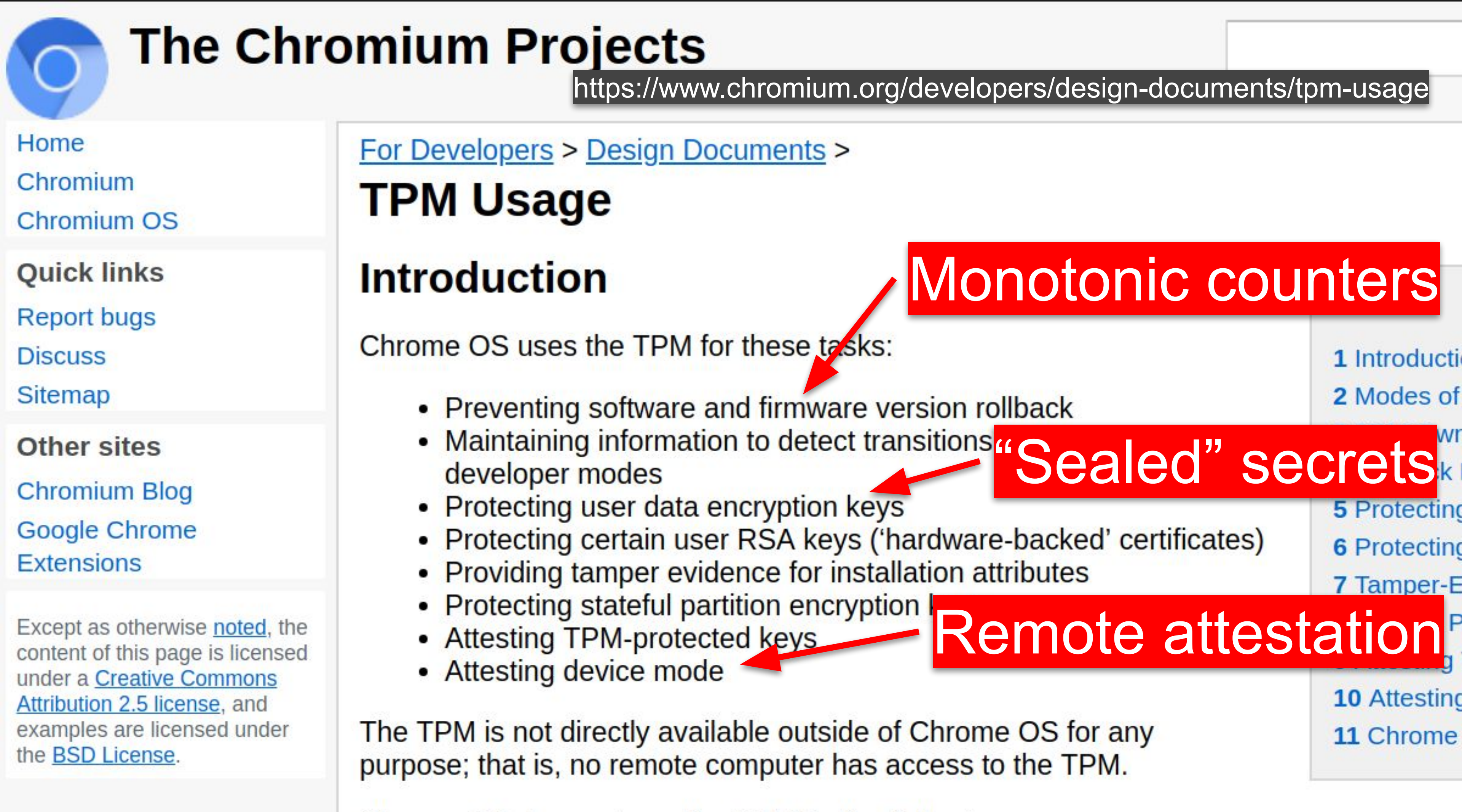
By Farhad Manjoo

July 11, 2002 | It was only when Microsoft unveiled Palladium and disclosed that both Intel and AMD were willing to build hardware to support the plan that people became seriously worried about the idea of ubiquitous, cryptographically enabled and, in this case, monopolistically abetted "trusted computing."

“The whole point of the GPL is to allow people to modify code. But under Palladium, an application that has been modified loses its signature. Each new version of an application needs a new signature.”



Trusted Platform Module



The Chromium Projects

https://www.chromium.org/developers/design-documents/tpm-usage

- Home
- Chromium
- Chromium OS

Quick links

- Report bugs
- Discuss
- Sitemap

Other sites

- Chromium Blog
- Google Chrome Extensions

For Developers > Design Documents >

TPM Usage

Introduction

Chrome OS uses the TPM for these tasks:

- Preventing software and firmware version rollback
- Maintaining information to detect transitions developer modes
- Protecting user data encryption keys
- Protecting certain user RSA keys (‘hardware-backed’ certificates)
- Providing tamper evidence for installation attributes
- Protecting stateful partition encryption k
- Attesting TPM-protected keys
- Attesting device mode

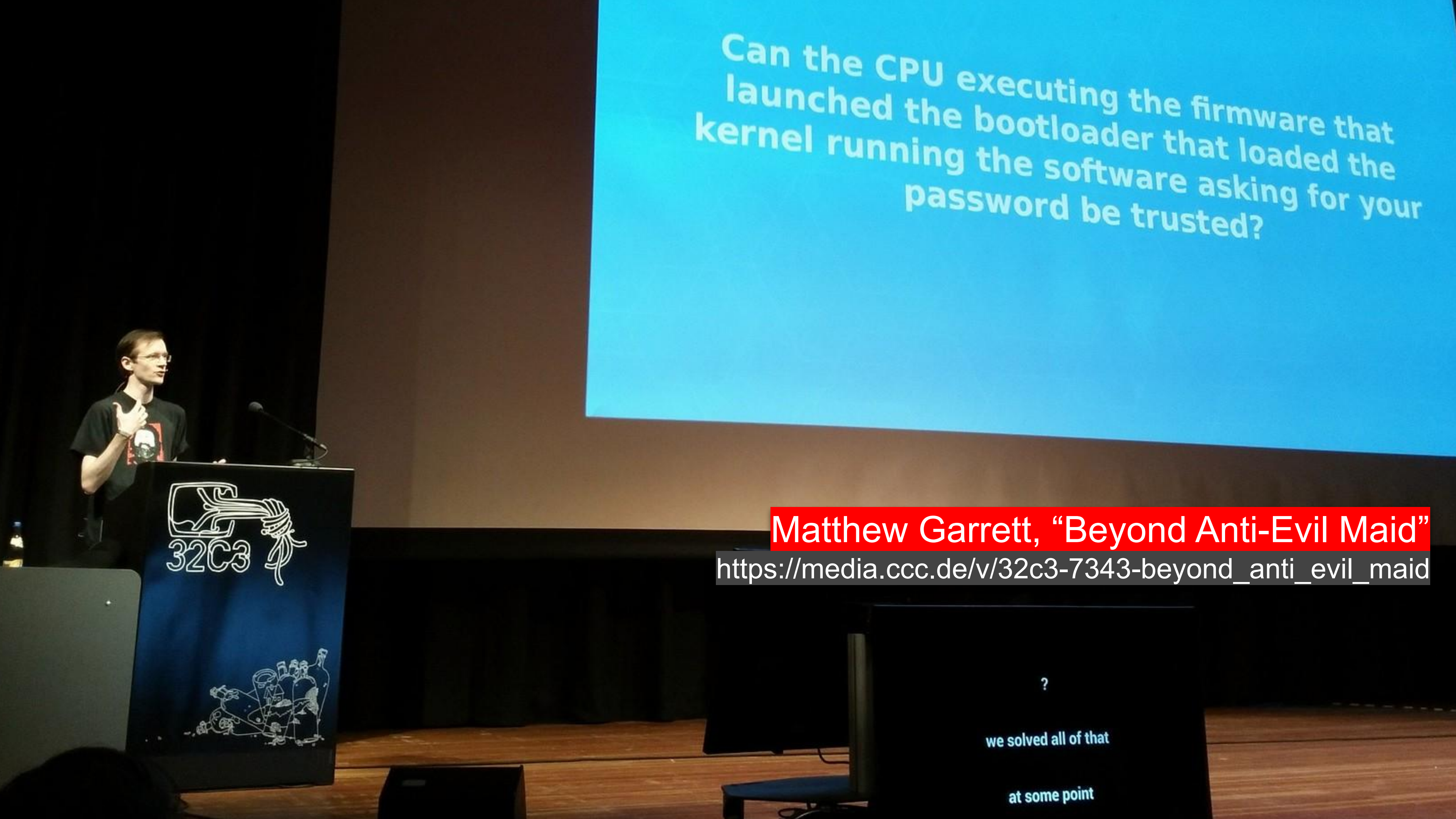
The TPM is not directly available outside of Chrome OS for any purpose; that is, no remote computer has access to the TPM.

Monotonic counters

“Sealed” secrets

Remote attestation

TPMs can be used for good



Can the CPU executing the firmware that launched the bootloader that loaded the kernel running the software asking for your password be trusted?

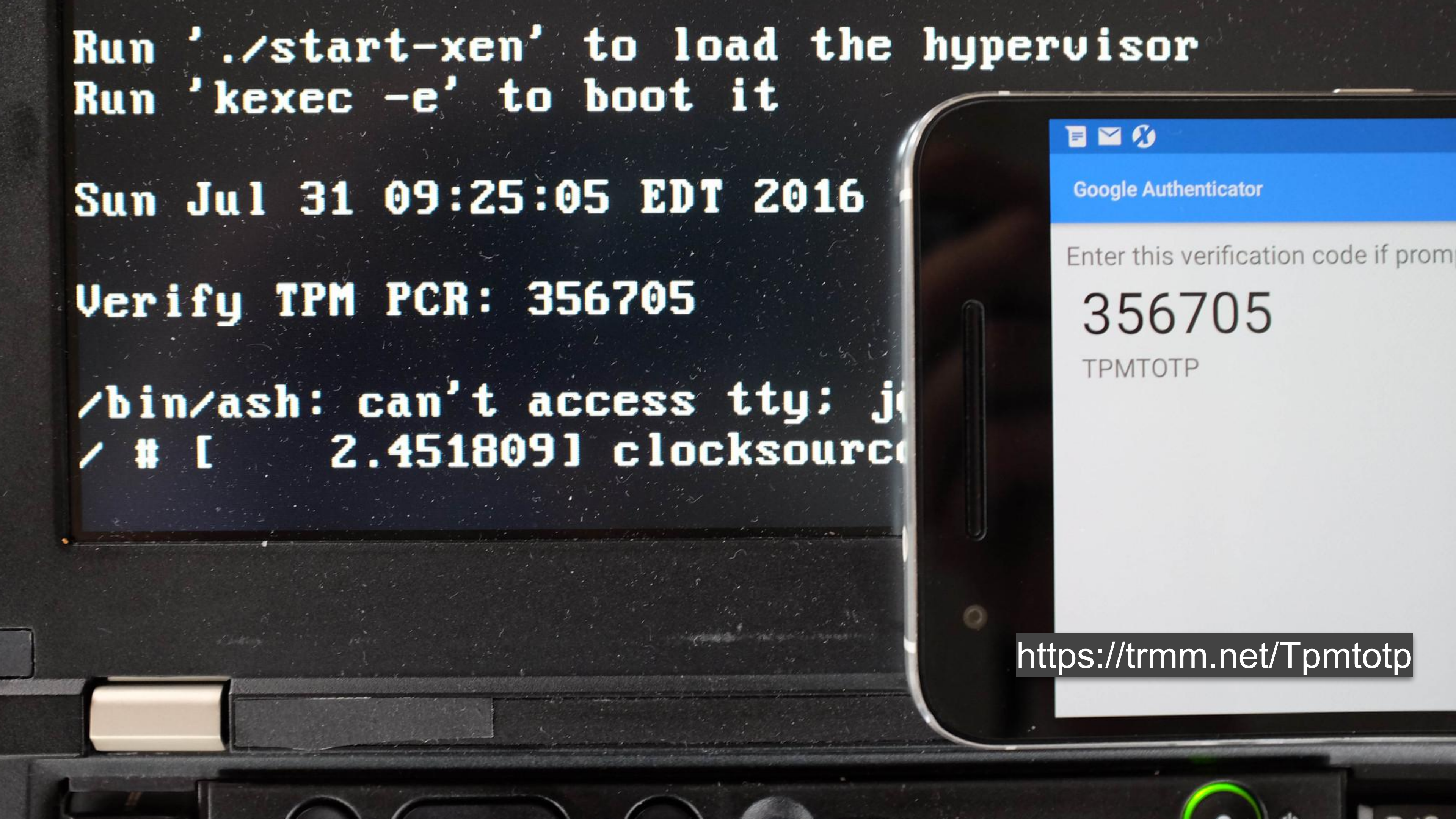
?

we solved all of that

at some point

Matthew Garrett, “Beyond Anti-Evil Maid”

https://media.ccc.de/v/32c3-7343-beyond_anti_evil_maid



```
Run './start-xen' to load the hypervisor
Run 'kexec -e' to boot it

Sun Jul 31 09:25:05 EDT 2016

Verify TPM PCR: 356705

/bin/ash: can't access tty; jo
/ # [    2.451809] clocksource
```

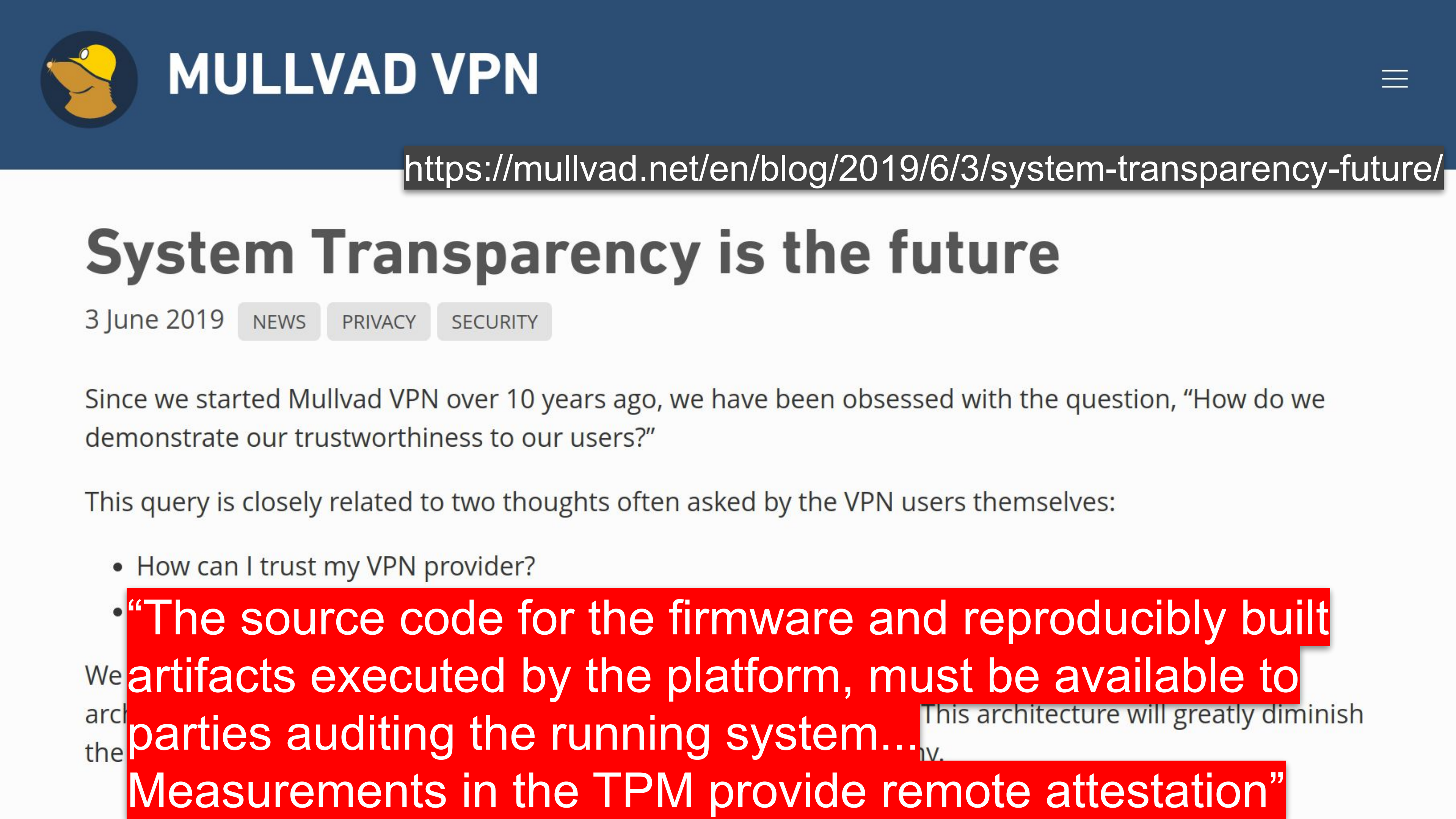
Google Authenticator

Enter this verification code if prom

356705

TPMTOTP

https://trmm.net/Tpmtotp



MULLVAD VPN

https://mullvad.net/en/blog/2019/6/3/system-transparency-future/

System Transparency is the future

3 June 2019 NEWS PRIVACY SECURITY

Since we started Mullvad VPN over 10 years ago, we have been obsessed with the question, “How do we demonstrate our trustworthiness to our users?”

This query is closely related to two thoughts often asked by the VPN users themselves:

- How can I trust my VPN provider?
-

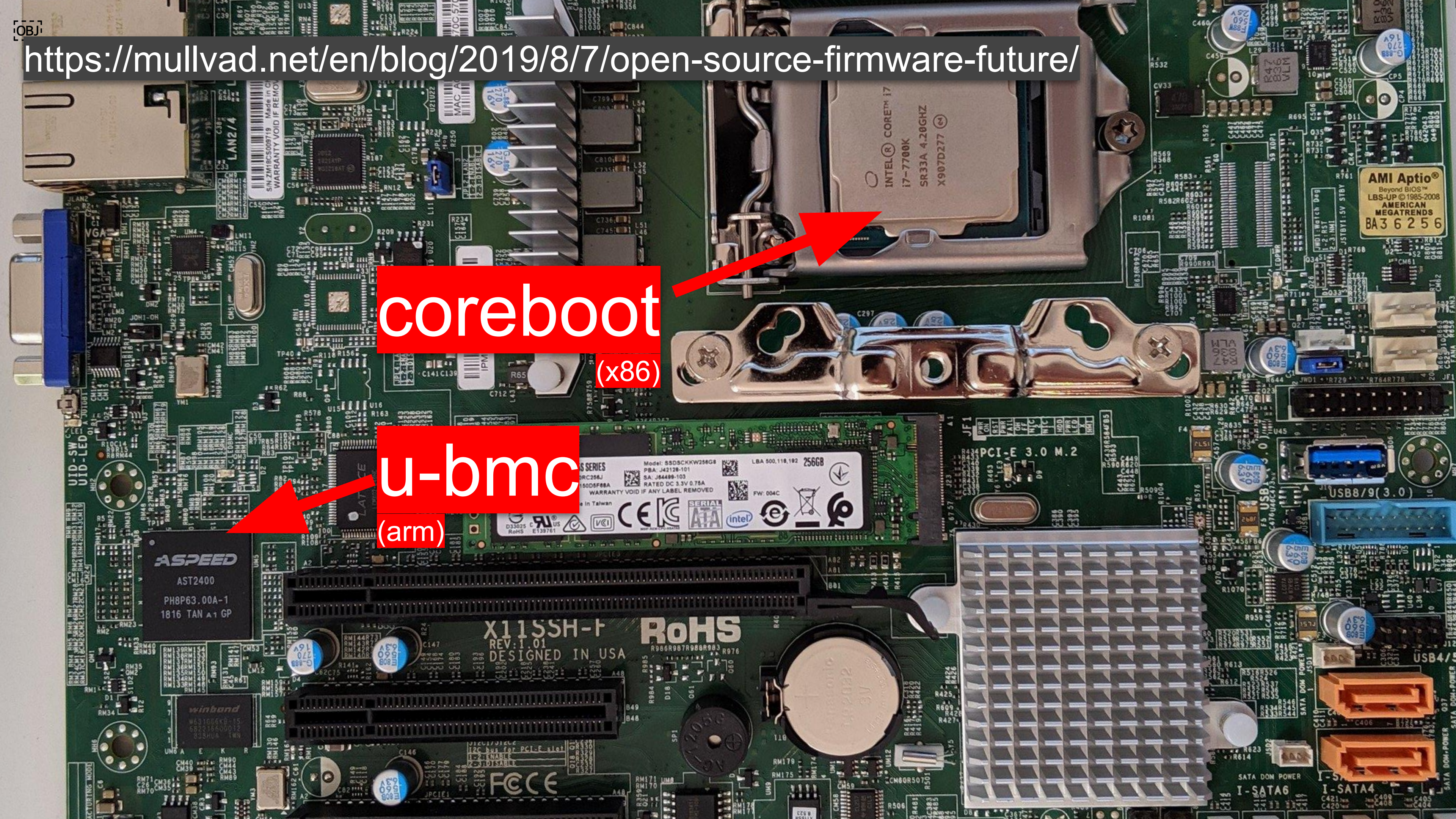
We

arc This architecture will greatly diminish

the ny.

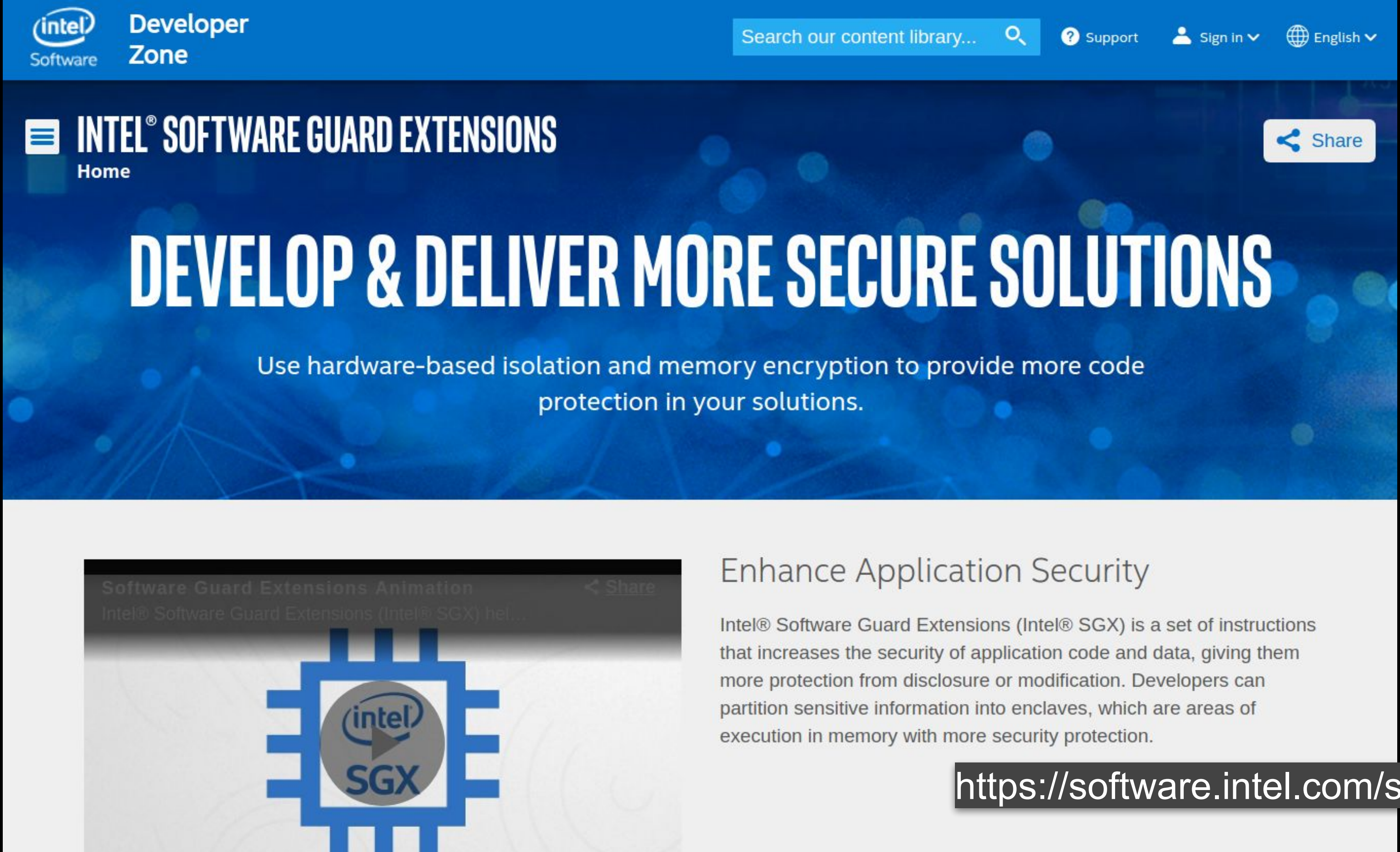
“The source code for the firmware and reproducibly built artifacts executed by the platform, must be available to parties auditing the running system...
Measurements in the TPM provide remote attestation”

https://mullvad.net/en/blog/2019/8/7/open-source-firmware-future/



coreboot (x86)

u-bmc (arm)



INTEL® SOFTWARE GUARD EXTENSIONS

DEVELOP & DELIVER MORE SECURE SOLUTIONS

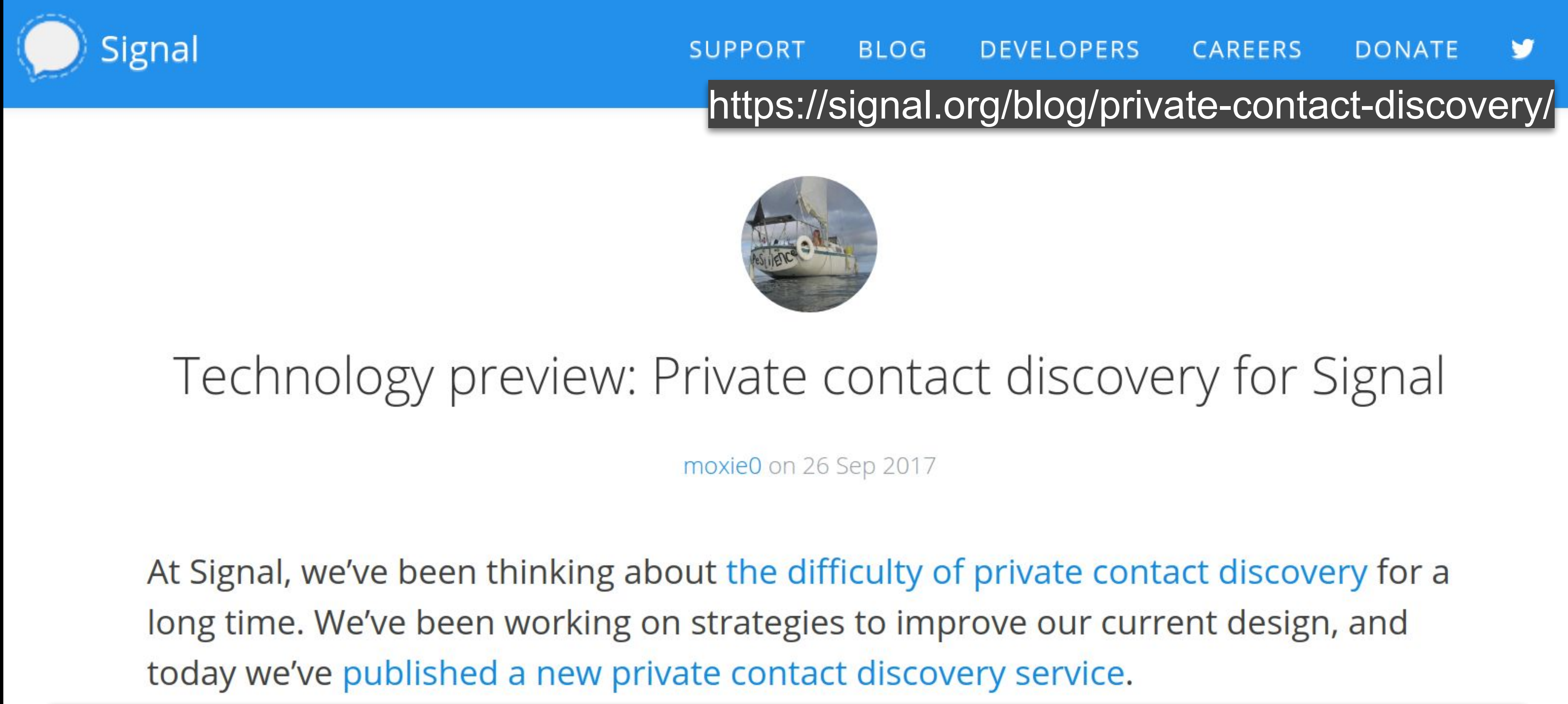
Use hardware-based isolation and memory encryption to provide more code protection in your solutions.

Intel® Software Guard Extensions (Intel® SGX) hel...

Enhance Application Security

Intel® Software Guard Extensions (Intel® SGX) is a set of instructions that increases the security of application code and data, giving them more protection from disclosure or modification. Developers can partition sensitive information into enclaves, which are areas of execution in memory with more security protection.

https://software.intel.com/sgx



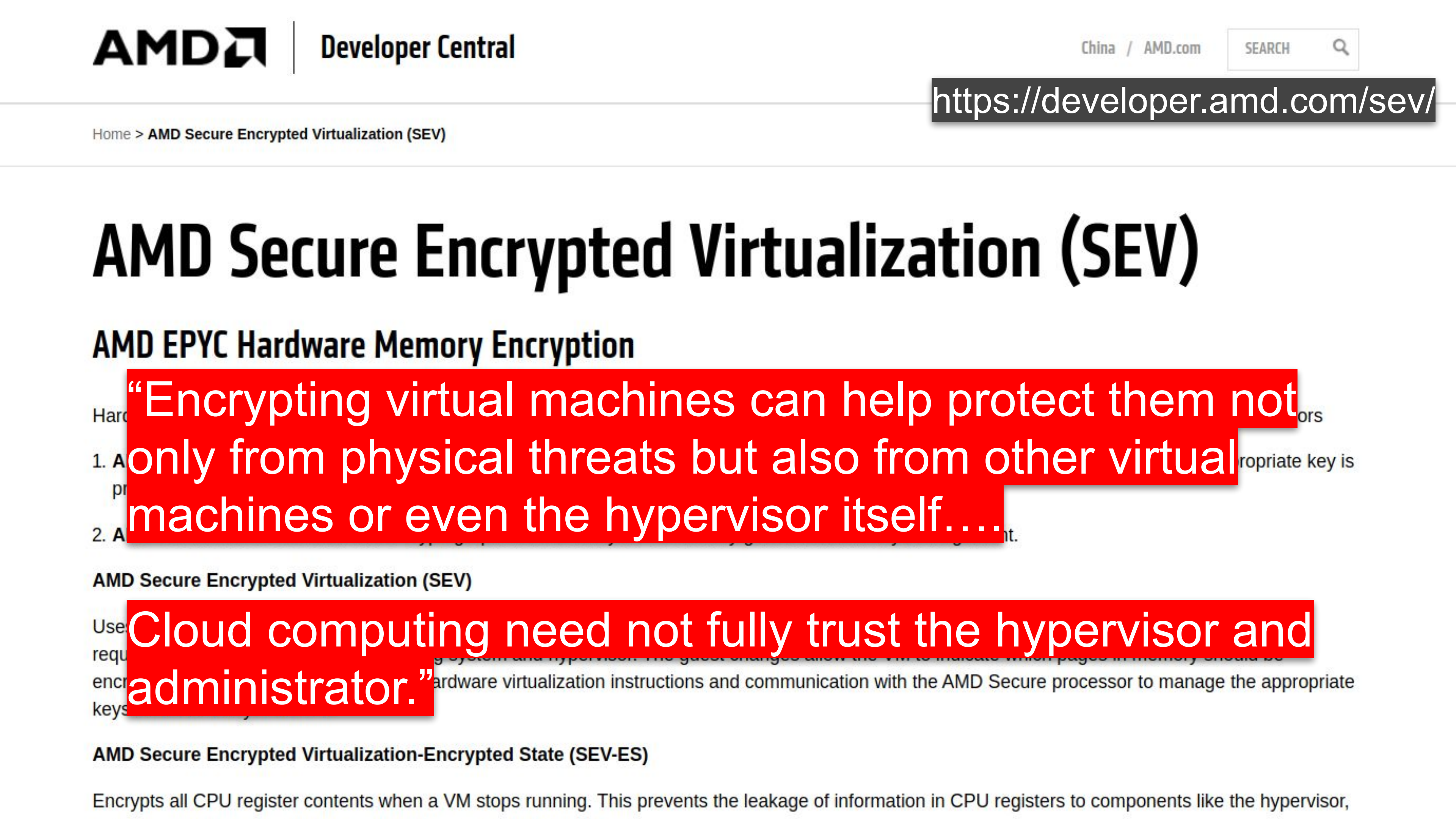
https://signal.org/blog/private-contact-discovery/

Technology preview: Private contact discovery for Signal

moxie0 on 26 Sep 2017

At Signal, we've been thinking about the difficulty of private contact discovery for a long time. We've been working on strategies to improve our current design, and today we've published a new private contact discovery service.

"The open source enclave code builds reproducibly, so anyone can verify that the published source code corresponds to the [attested hash] value of the remote enclave."



AMD | Developer Central

China / AMD.com SEARCH

https://developer.amd.com/sev/

Home > **AMD Secure Encrypted Virtualization (SEV)**

AMD Secure Encrypted Virtualization (SEV)

AMD EPYC Hardware Memory Encryption

“Encrypting virtual machines can help protect them not only from physical threats but also from other virtual machines or even the hypervisor itself….

Hard ... ors

1. A ... ropriate key is pr

2. A ... nt.

AMD Secure Encrypted Virtualization (SEV)

Cloud computing need not fully trust the hypervisor and administrator.”

Use ... requ ... encr ... ardware virtualization instructions and communication with the AMD Secure processor to manage the appropriate keys

AMD Secure Encrypted Virtualization-Encrypted State (SEV-ES)

Encrypts all CPU register contents when a VM stops running. This prevents the leakage of information in CPU registers to components like the hypervisor,

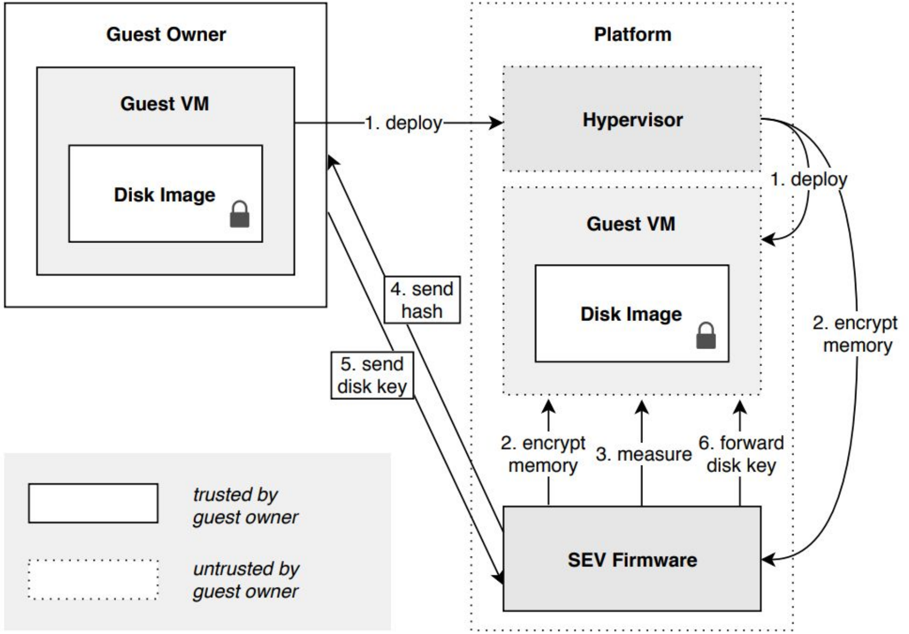


Figure 3: Initial deployment of a guest virtual machine in an SEV scenario.

Buhren et al, “Analyzing AMD SEV’s Remote Attestation”

https://arxiv.org/pdf/1908.11680.pdf

PSP INSIDE

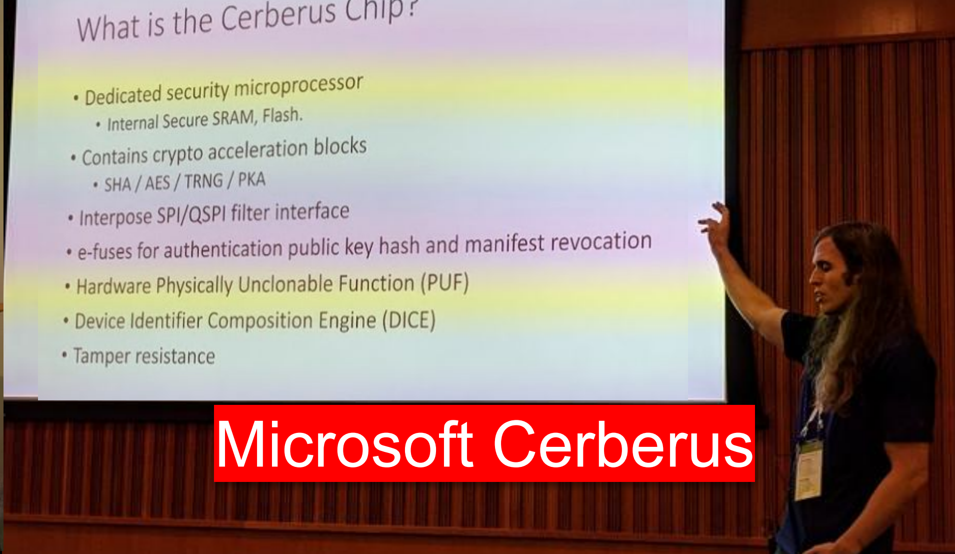
Google Security Chip H1

A member of the Titan family

Chrome OS Use Case

vbendeb@google.com

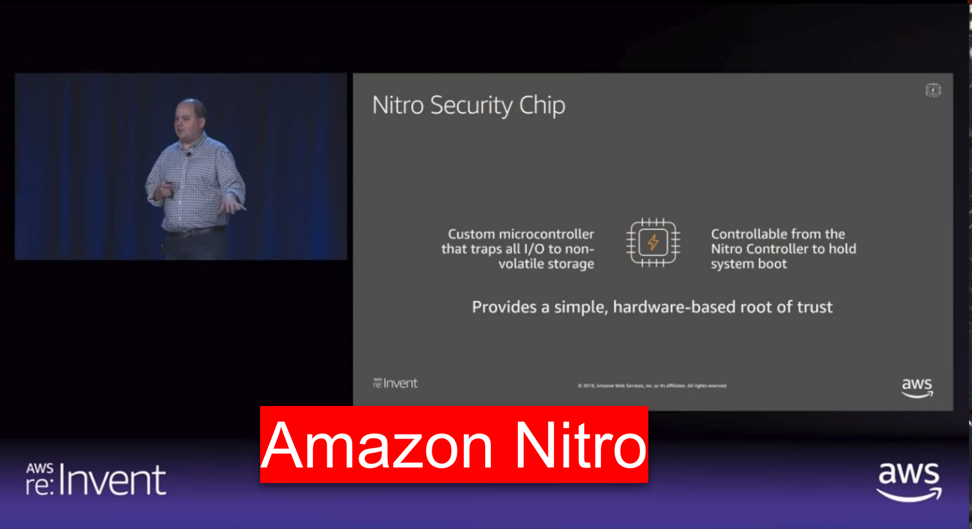
Google Titan



What is the Cerberus Chip?

- Dedicated security microprocessor
  - Internal Secure SRAM, Flash.
- Contains crypto acceleration blocks
  - SHA / AES / TRNG / PKA
- Interpose SPI/QSPI filter interface
- e-fuses for authentication public key hash and manifest revocation
- Hardware Physically Unclonable Function (PUF)
- Device Identifier Composition Engine (DICE)
- Tamper resistance

Microsoft Cerberus



Nitro Security Chip

Custom microcontroller that traps all I/O to non-volatile storage

Controllable from the Nitro Controller to hold system boot

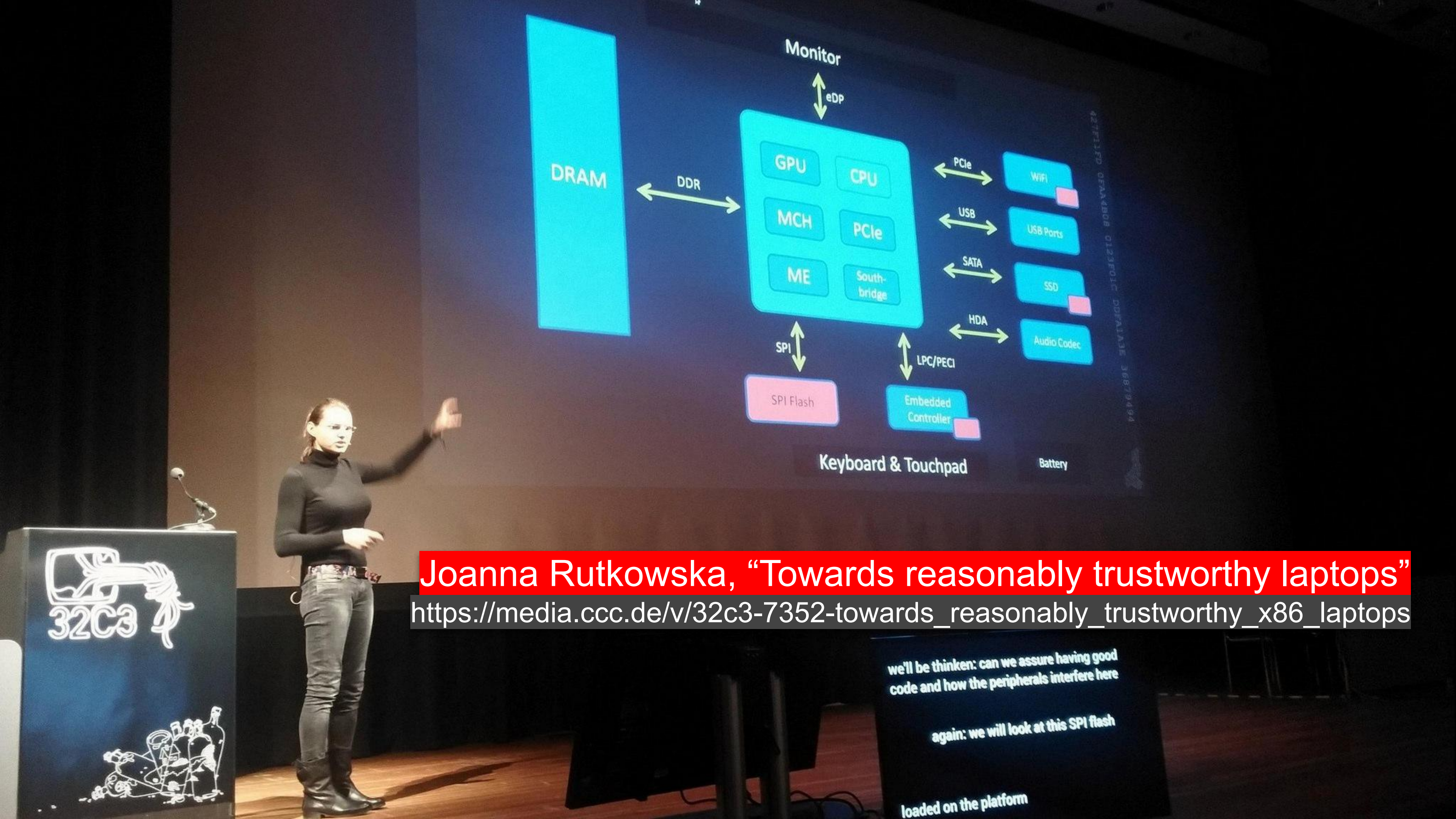
Provides a simple, hardware-based root of trust

re:Invent
© 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.
aws
AWS re:Invent
aws

Amazon Nitro

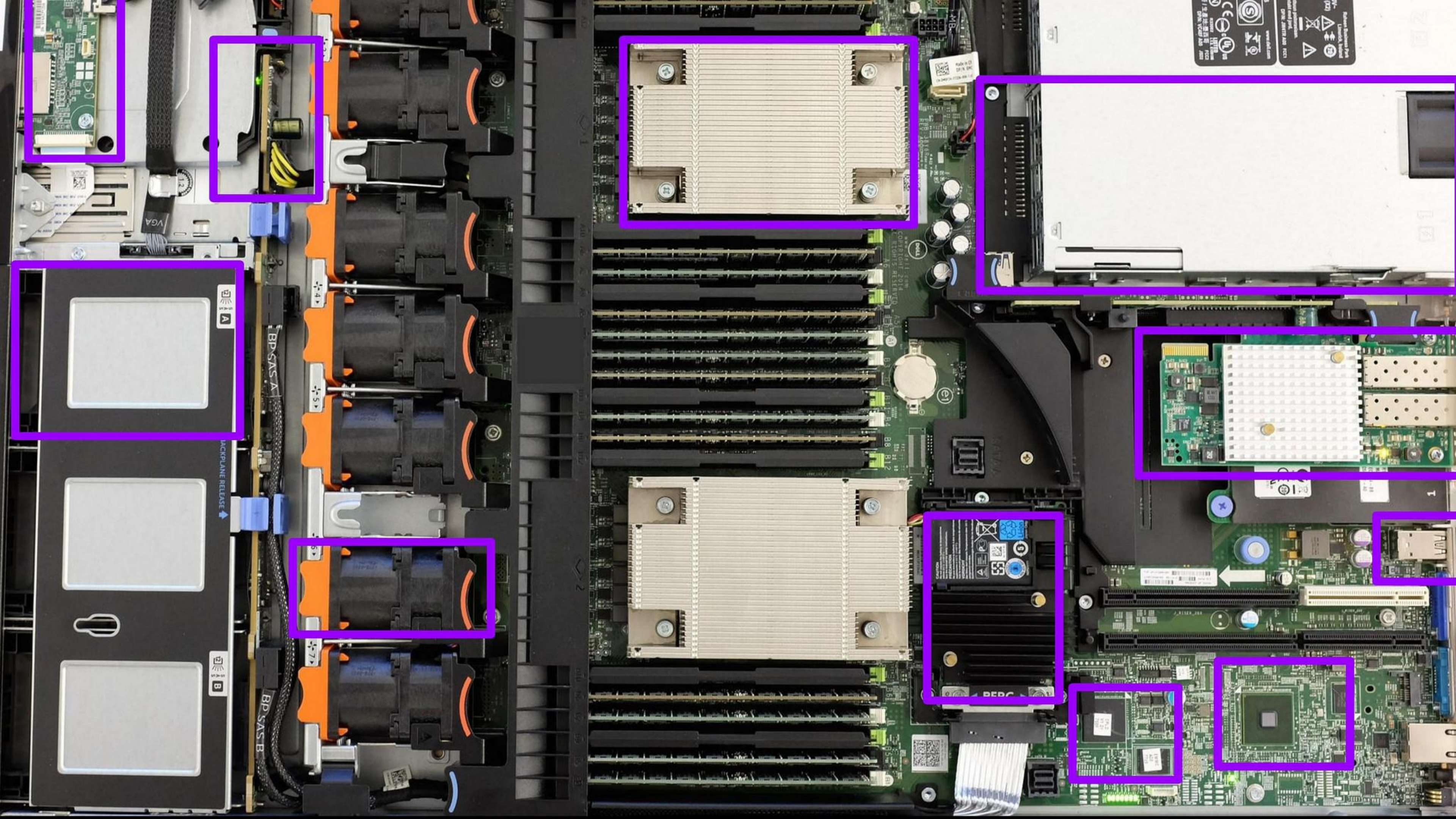
Apple T2

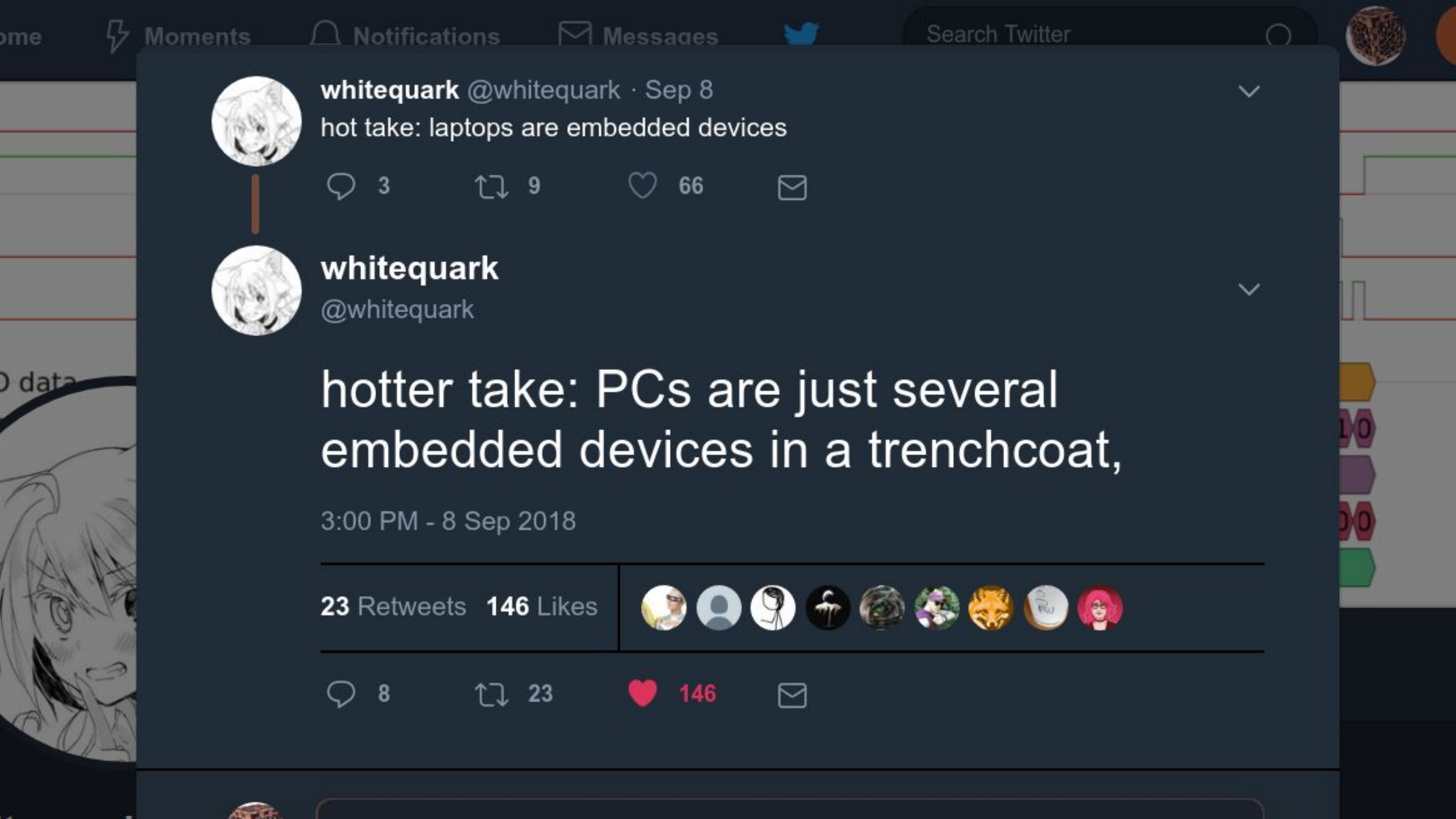
CC-BY-NC
https://www.ifixit.com/Guide/Image/meta/rfh6gOxsLWInTGKc



Joanna Rutkowska, “Towards reasonably trustworthy laptops”

https://media.ccc.de/v/32c3-7352-towards_reasonably_trustworthy_x86_laptops


VGA
BP SAS A
BACKPLANE RELEASE
BP SAS B
PERC



whitequark @whitequark · Sep 8

hot take: laptops are embedded devices

3 9 66

whitequark

@whitequark

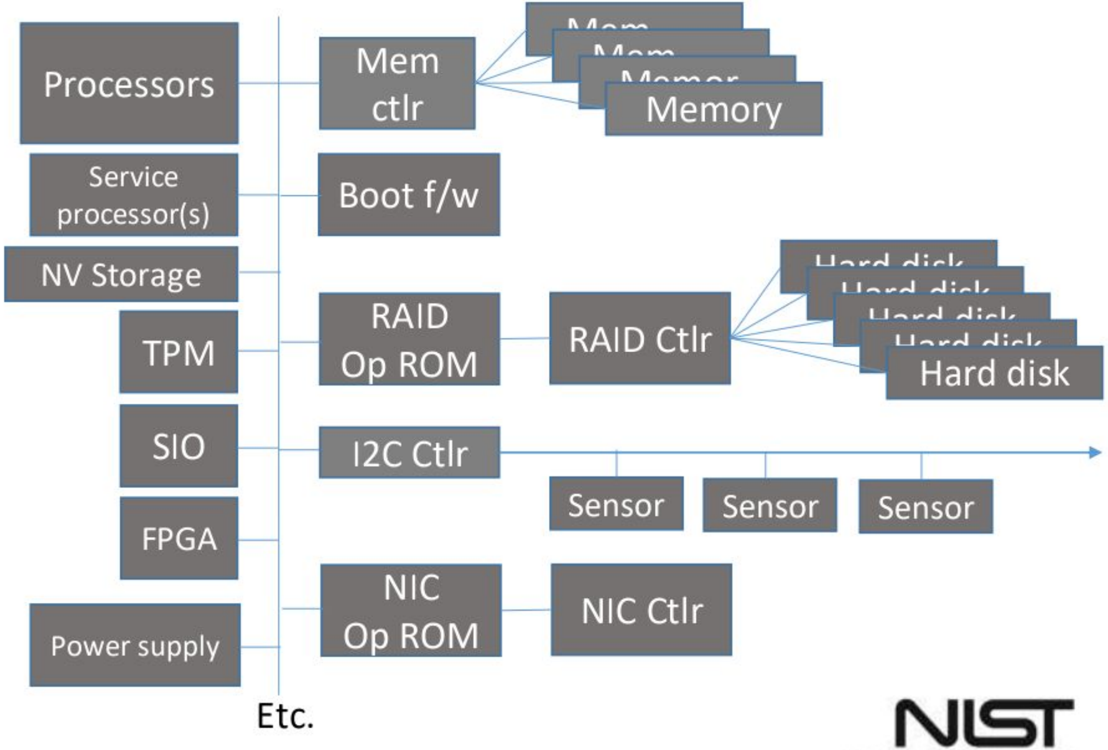
hotter take: PCs are just several embedded devices in a trenchcoat,

3:00 PM - 8 Sep 2018

23 Retweets **146** Likes

8 23 146

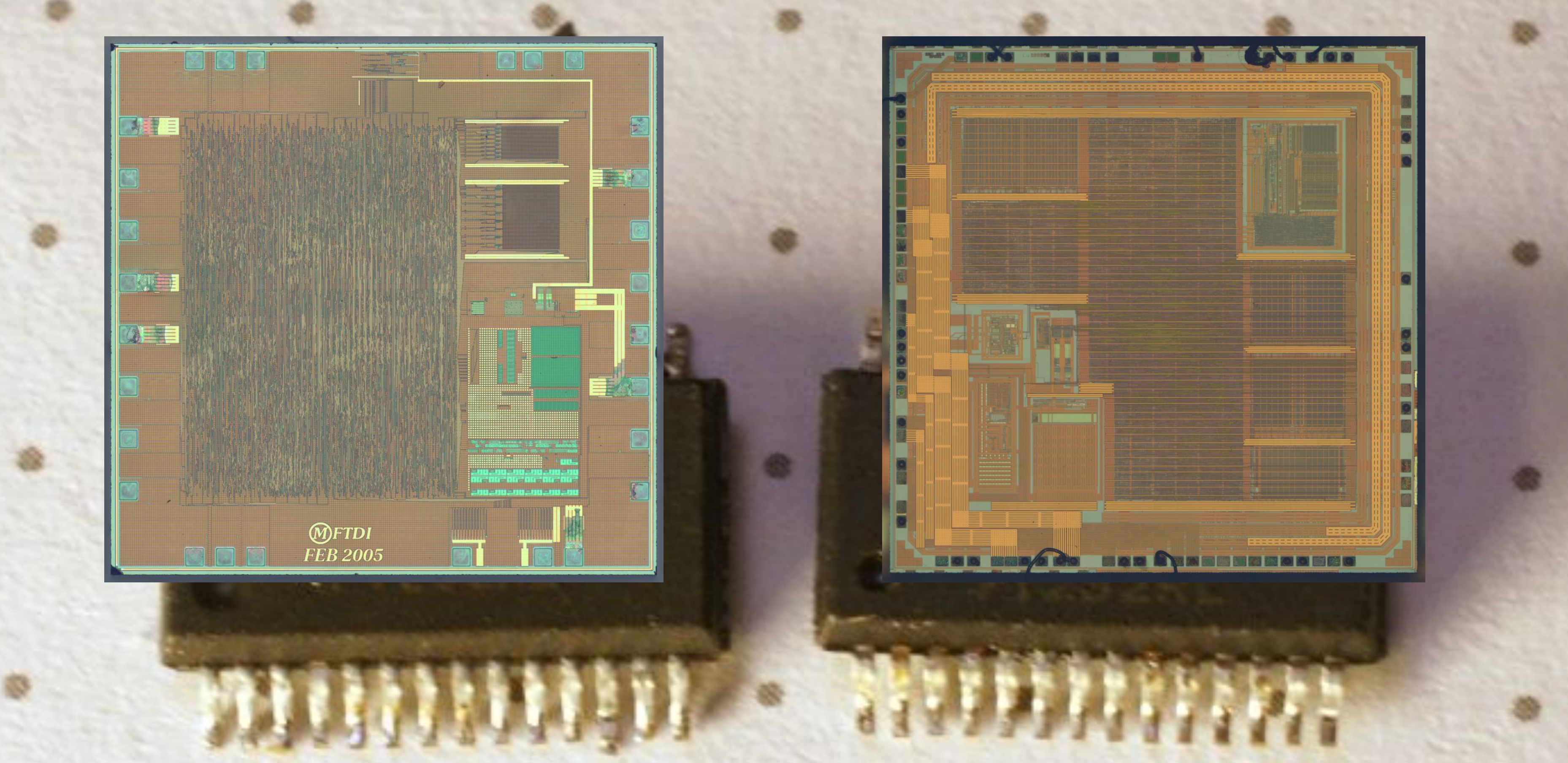
NIST Special Publication 800-193
Platform Firmware Resiliency Guidelines



Andrew Regenscheid
Computer Security Division
Information Technology Laboratory

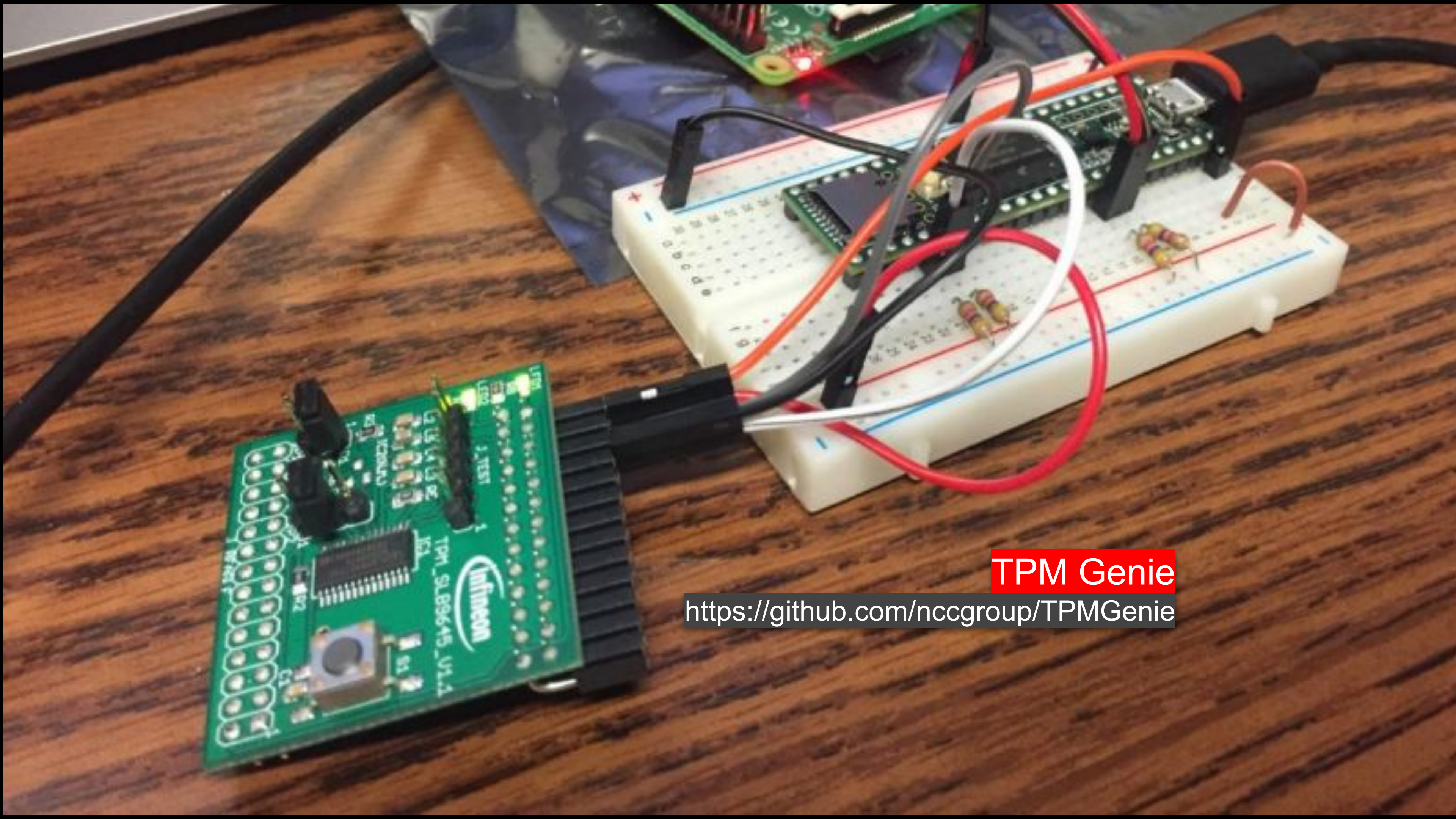
https://doi.org/10.6028/NIST.SP.800-193

National Institute of Standards and Technology
U.S. Department of Commerce



FTDI FT232RL: Real vs Fake (CC-BY Zeptobars)

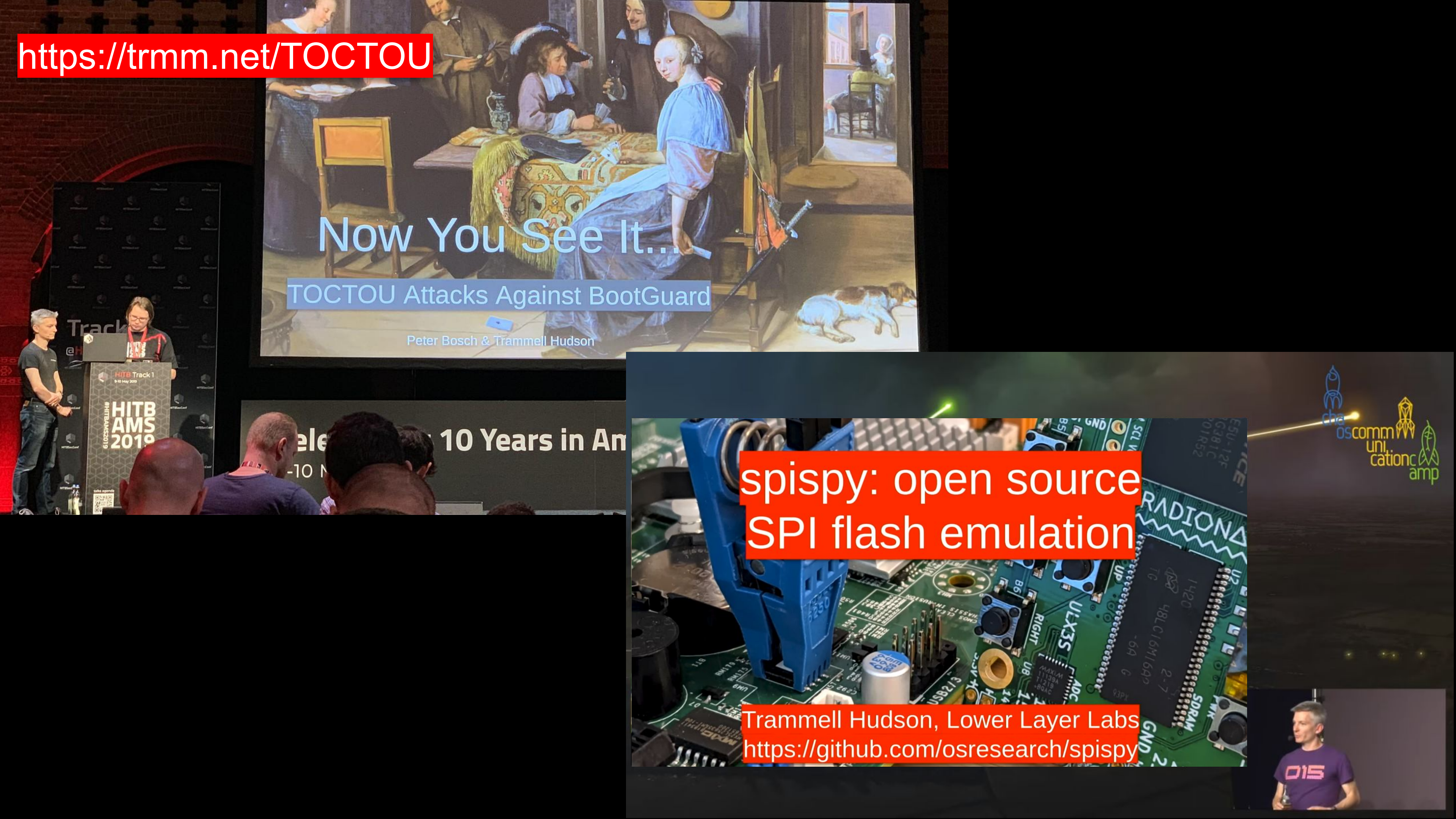
https://zeptobars.com/en/read/FTDI-FT232RL-real-vs-fake-supereal



TPM Genie

https://github.com/nccgroup/TPMGenie

https://trmm.net/TOCTOU



Now You See It...

TOCTOU Attacks Against BootGuard

Peter Bosch & Trammell Hudson

spispy: open source SPI flash emulation

Trammell Hudson, Lower Layer Labs
https://github.com/osresearch/spispy

Freedom!

Resilience!

Attestation!

http://slack.u-root.com/
#linuxboot