Trusted Computing Technology and Government Implants (Unclassified version)

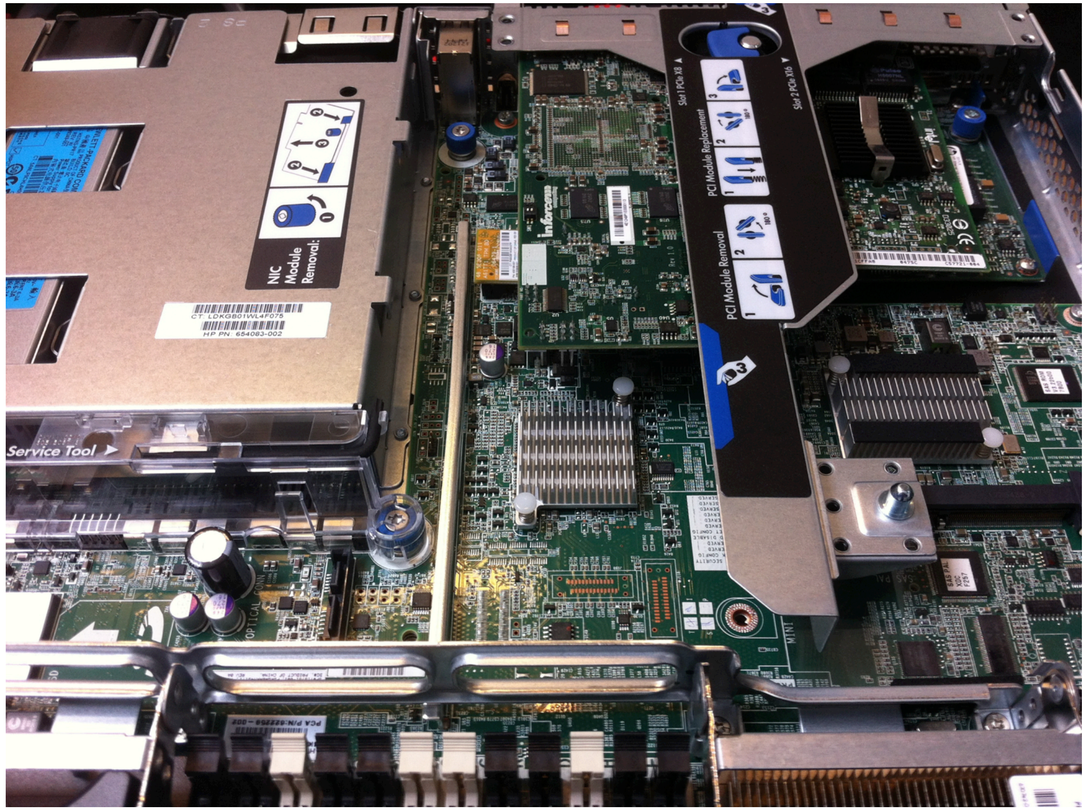
TrustyCon 2014

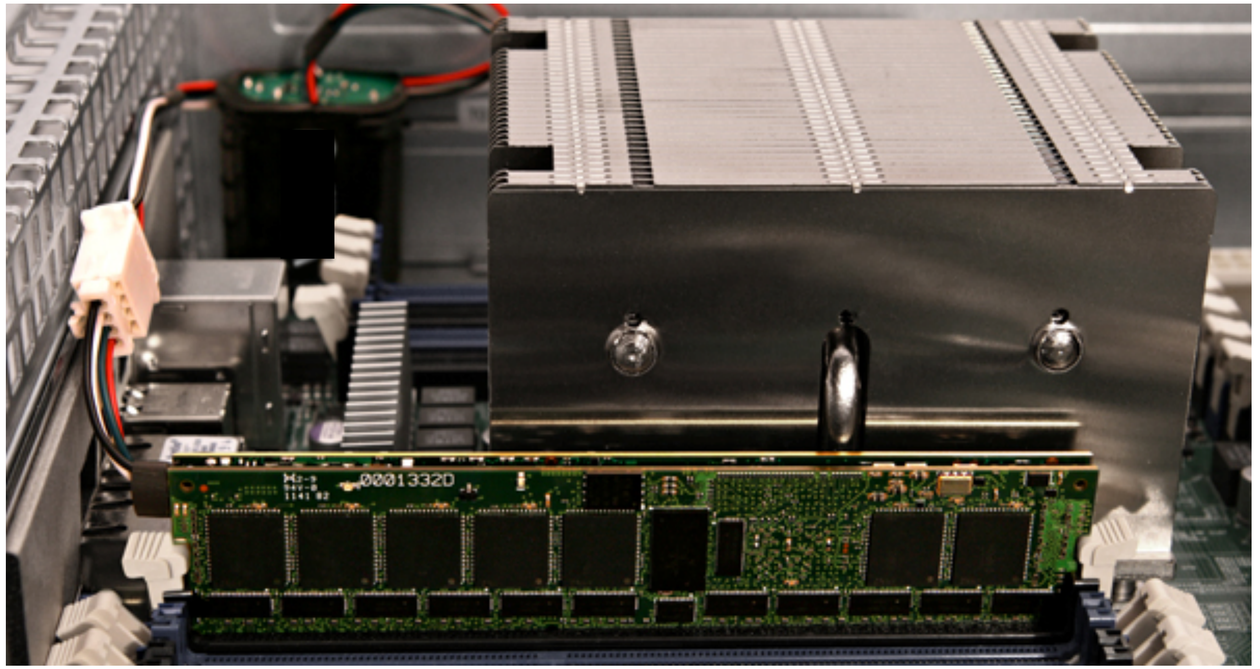
Steve Weis

Intro

- **Me:** Cryptographer, Co-founder & CTO PrivateCore,
  Google 2-factor, Keyczar, saweis.net, @sweis
- **Today's talk:**
  - Snapshot of government hardware, firmware, & software implants
  - "Trusted Computing": What is it? Can it help? Can we trust it?
  - Defensive technologies on the horizon

Can you spot the implants?





Government Implants

SPIEGEL ONLINE

Shopping for Spy Gear: Catalog Advertises NSA Toolbox

By Jacob Appelbaum, Judith Horchert and Christian Stöcker

WIRED

NSA Hackers Get the 'Ungettable' With Rich Catalog of Custom Tools

BY KIM ZETTER 12.30.13 4:11 PM

The New York Times

N.S.A. Devises Radio Pathway Into Computers

By DAVID E. SANGER and THOM SHANKER JAN. 14, 2014

NSA Observer Site contains US classified material

System Taxonomy Recap

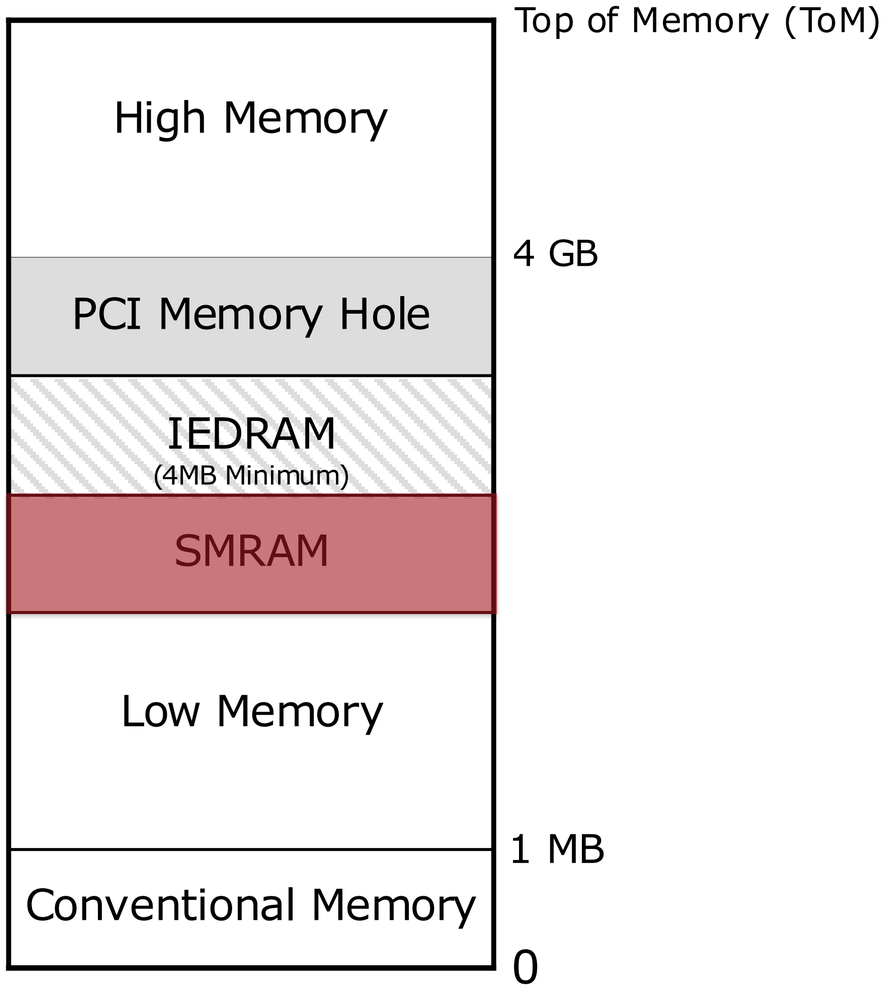
Software	**Hypervisor, Operating System, Applications**
Firmware	**BIOS, SMM, Option ROMs, SINIT ACMs**
Hardware	**Processor, Memory, Storage, Devices, Buses**

BIOS / SMM Attacks

- Exploit delivered via USB stick
- Target system BIOS
- Exploits system management mode (SMM)

Why attack BIOS and SMM?

- **Basic I/O System (BIOS)**: Persistent firmware that runs first before the OS.
- **System Management Mode (SMM)**: Special mode of operation that runs with highest privileges, which is installed by BIOS and invisible to OS.



Hard Drive Firmware Attacks

- Infect hard drive firmware
- Compromise master boot record (MBR)
- Provides software application persistence

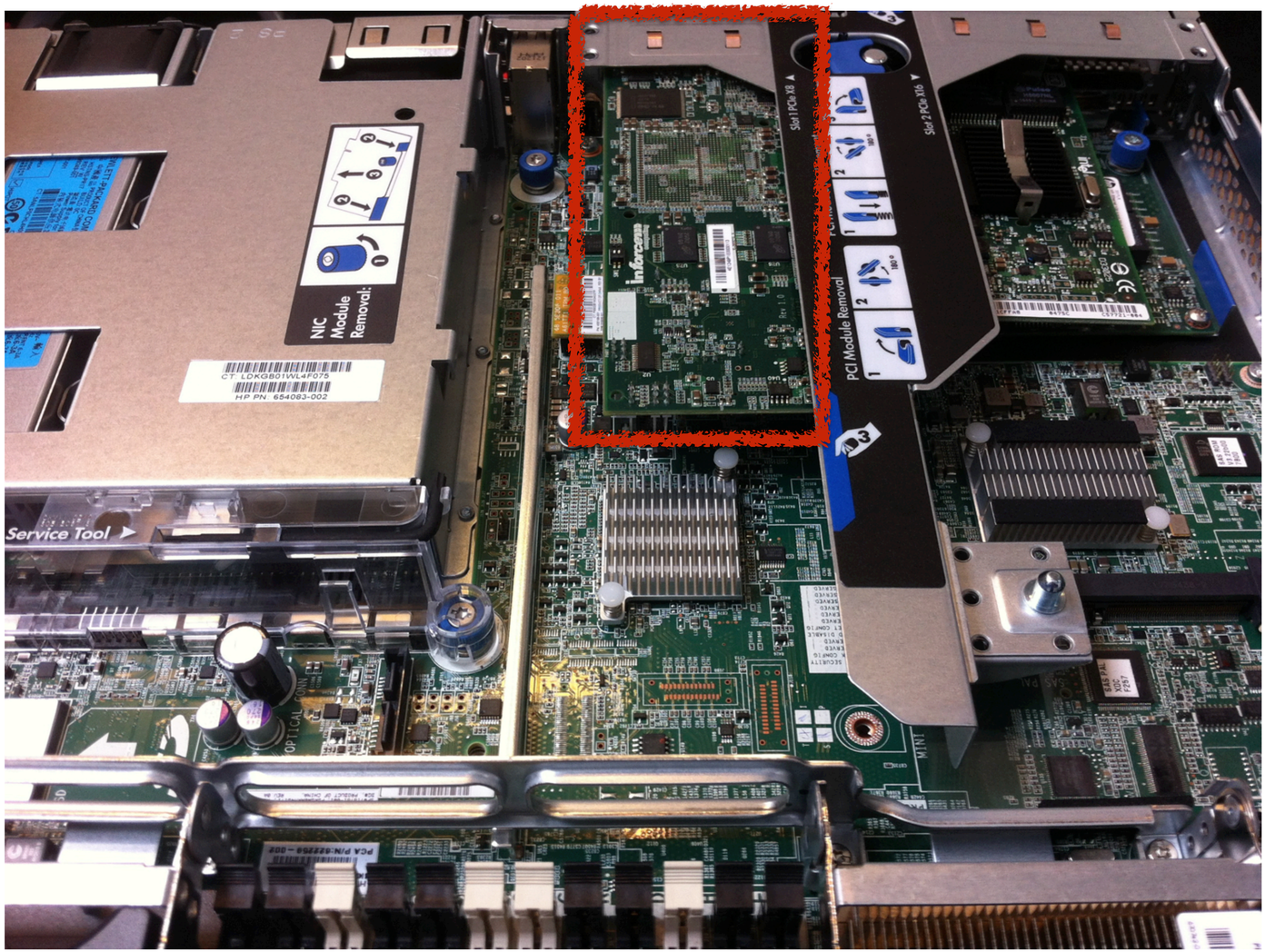
Potential Hardware Implants

- Two-way radios for communicating with SMM payloads
- USB interfaces with WiFi adapters built in
- Malicious PCI boards

Do-it-Yourself Implants

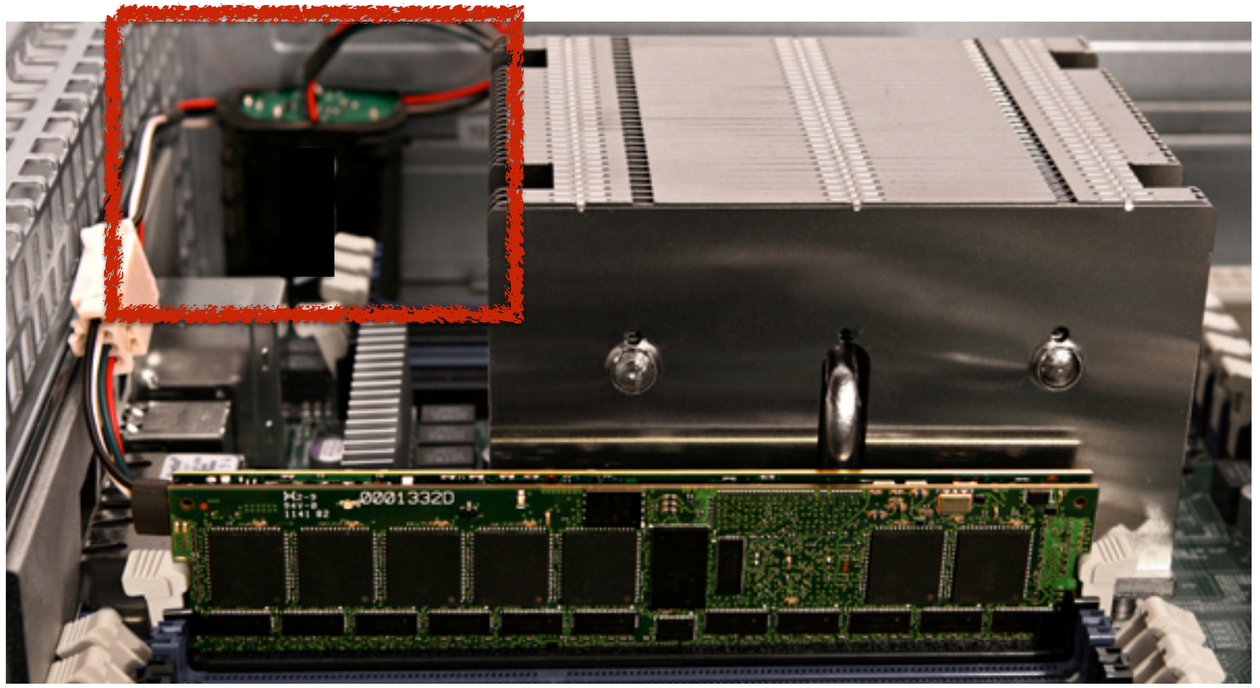
Can you spot the implant?

- PCI attack device
- Implemented with off-the-shelf hardware
- Boots independently of host
- Exfiltrates data over the network



Can you spot the implant?

- Non-volatile RAM (NV-RAM)
- RAM contents are saved to flash memory on power loss.
- Attackers can capture crypto keys from preserved memory contents
- Several non-volatile memory technologies are in the pipeline



Trusted Computing

Ensure _____’s software is running on _____’s computer.

Trusted Computing for DRM

Ensure a content owner's software is running on your computer.

Trusted Computing for You

Ensure your software is running on your computer.

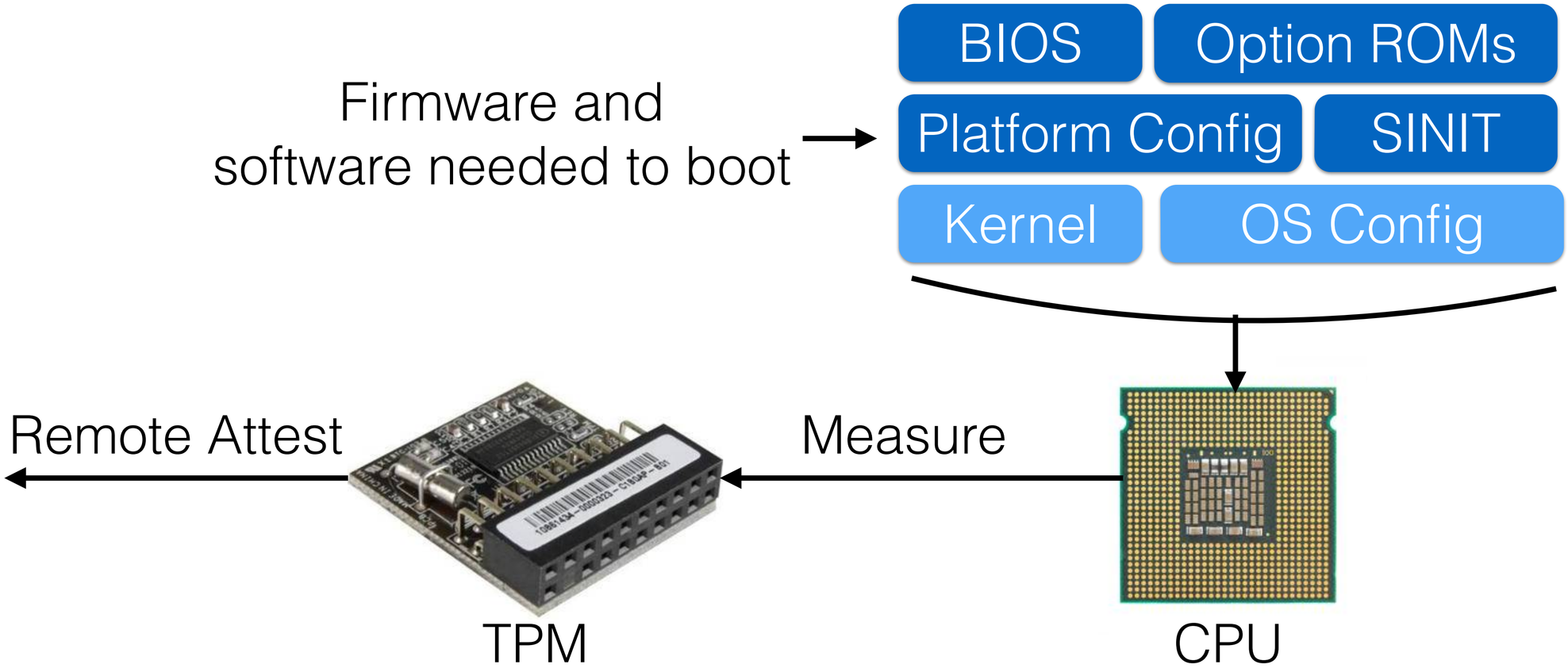
Trusted Platform Module

The Coming Civil War on General Purpose Computing:
"*A TPM is a nub of stable certainty: If it's there, it can reliably inform you about the code on your computer.*"

- Cory Doctorow

- Public-key encryption and signatures
- Random number generation
- Persistent key storage
- Special "Platform Configuration Registers" (PCRs)

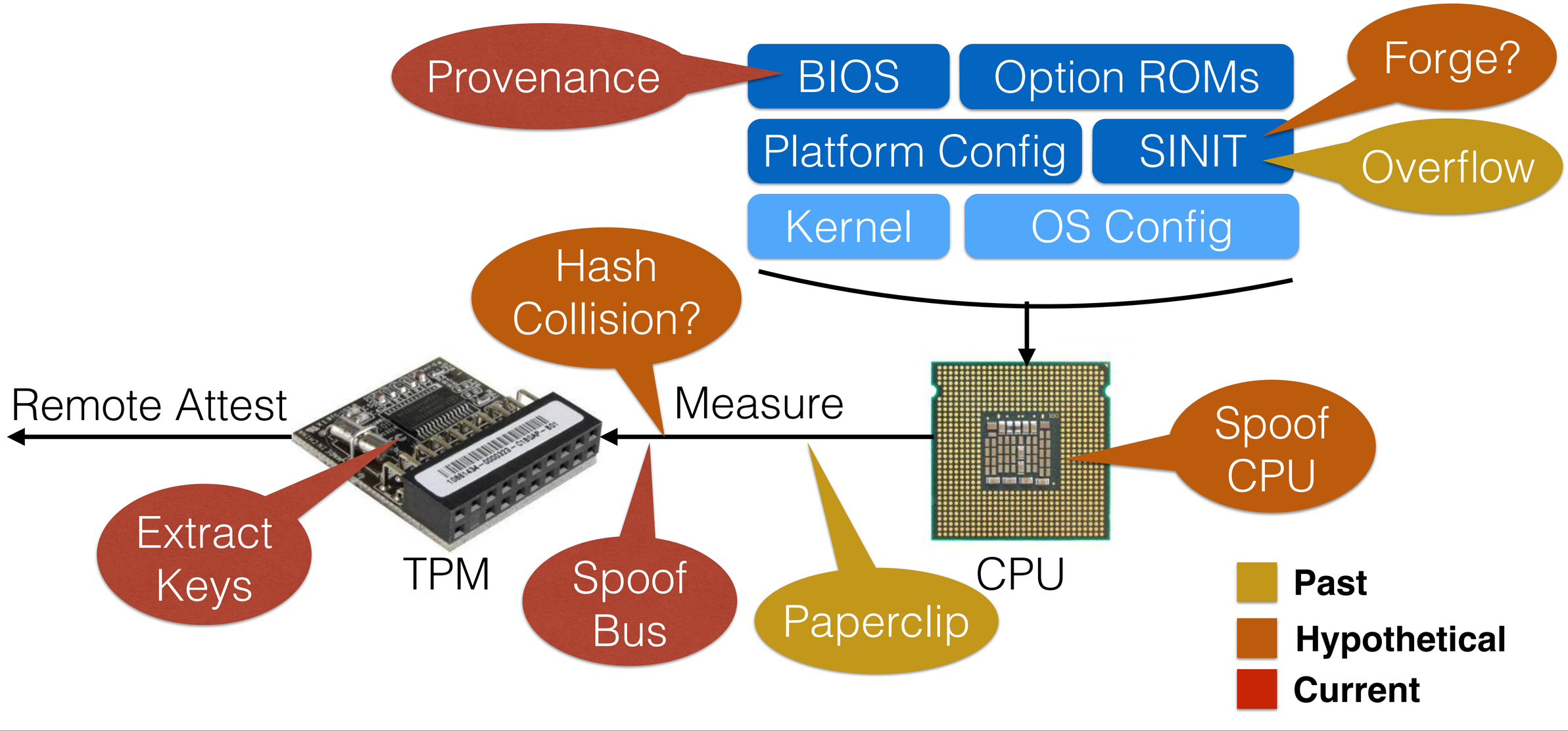
Trusted Execution Technology



Suspension of Disbelief

- What about physical attacks and hardware implants?
- Why do we trust the TPM? Where did it come from?
- Why do we trust the CPU for that matter?

Attack Vectors



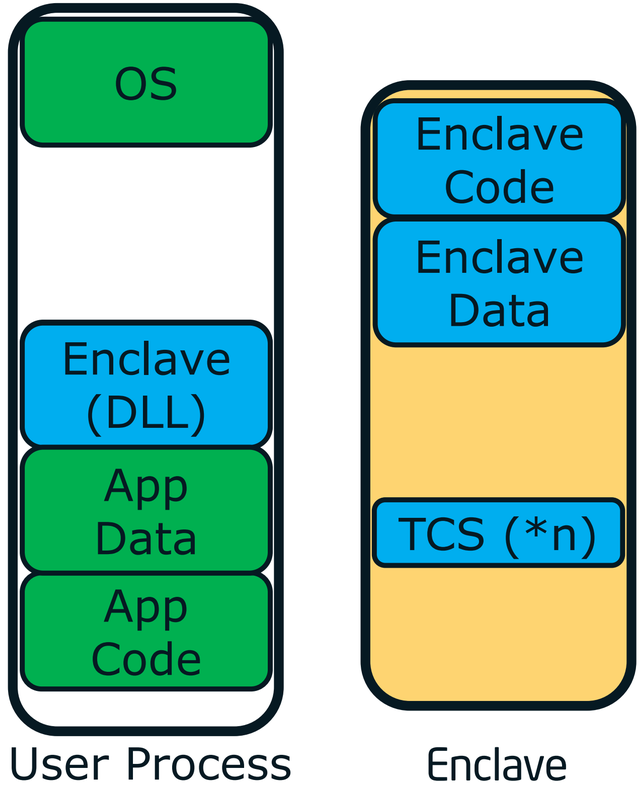
Where does this leave us?

- State-sponsored actors can circumvent trusted computing.
- Trusted computing still offers protection, although we ultimately have to trust the CPU and TPM.
- In the next 1-3 years: New hardware and platform security features
- Beyond: Practical applications of cryptographic protocols for security computation, e.g. fully homomorphic encryption.

Upcoming Technologies

Software Guard Extensions (SGX)

- Secure “enclaves” protected from other code.
- Enclaves are attested and won’t run if modified.
- Enclaves are backed by fully-encrypted memory.
- Potentially could make DRM hard to circumvent.



Enhanced Privacy ID (EPID)

- Provides ability for CPU to anonymously sign data.
- Could authenticate CPUs as real, without leaking identity.
- Caveat: Rooted in globally unique key material in CPU hardware.

Trusted Platform Module 2.0

- TPM 1.2 is deprecated and banned in several countries.
- TPM 2.0
  - More algorithms and functionality
  - Support for alternate cryptographic suites
  - Better management
  - Easier on-boarding

Summary

- Government implants target software, firmware, and hardware.
- Trusted computing helps against firmware and software attacks, but not against state sponsors.
- New technologies like SGX and EPID can work for us or against us.


Thank you!