Protecting Data In-Use from Firmware and Physical Attacks

Steve Weis

PrivateCore

About Me

Steve Weis
saweis.net
@sweis

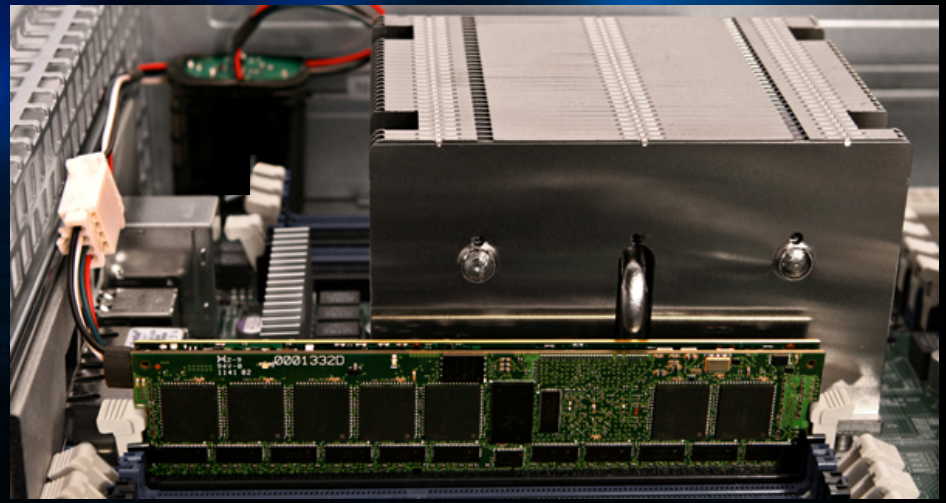
- Cryptography & Information Security
- Co-founder & CTO of PrivateCore
- Ex-Google Security
- PhD in crypto

Today's Talk


Luk
Kurmus
Müller
Fraser
Futral
Johnson
McKeen
Doorn
Felton
Khosla
Horchert
Martinez
Preneel
Shi
Feldman
Hermann
Johansson
Koltsidas
McCune
Schoen
Solihin
Clarke
Chen
Cornwell
Freiling
Hoekstra
Jakobsson
Newsome
Peterson
Scarlata
Soeder
Van
Champagne
Duc
Gasend
Heninger
Kaczmarek
Rihan
Robertson
Richardson
Sassatelli
Stewin
Yuyu
Blass
Bøegh
Elbaz
Fitzpatrick
Lal
Luksenberg
Paul
Maartmann-Moe
Schellekens
Tereshkin
Winter
Butler
Butterworth
Morin
Perrig
Shanbhogue
van
Walters
Berenzon
Bazhaniuk
Waldspurger
Sevinsky
Albin
Bardouillet
Bulygin
Lee
Keryell
Levillain
Potlapally
Triulzi
Wojtczuk
Anati
Arbaugh
Duflot
Kallenberg
Shafi
Torres
Zaddach
Alves
Appelbaum
Group
Hailfinger
Sunar
Calrino
Savagaonkar
Weis
Brossard
Brickell
Delugré
Goodspeed
Kovah
Rutkowska
Boileau
Guillemin
Witherden
Alexrovich
Camenisch
Dornseif
Herzog
Skochinsky
Vasudevan
Balzarotti
Bystrov
Gueron
Gebotys
Phegade
Perez
Tarnovsky
Weathers
Carrier
Chhabra
Clarkson
Economou
Heasman
Pappachan
Seshadri
Valadon
Del
Devadas
Francillon
Halderman
Mozak
Peiqiang
Permeh
Stöcker
Horovitz
Petroni
Suh
Dijk
Chifflier
Gazet
Hammouri
Loucaides
Rozas
Cuvillo
Dewald
Furtak
Gupta
Kleissner
McDaniel
Enck
Felten
Ionescu
Kursawe
Loukas
Pabel
Molina

black hat USA 2014

Spot the implants



NSA ANT

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

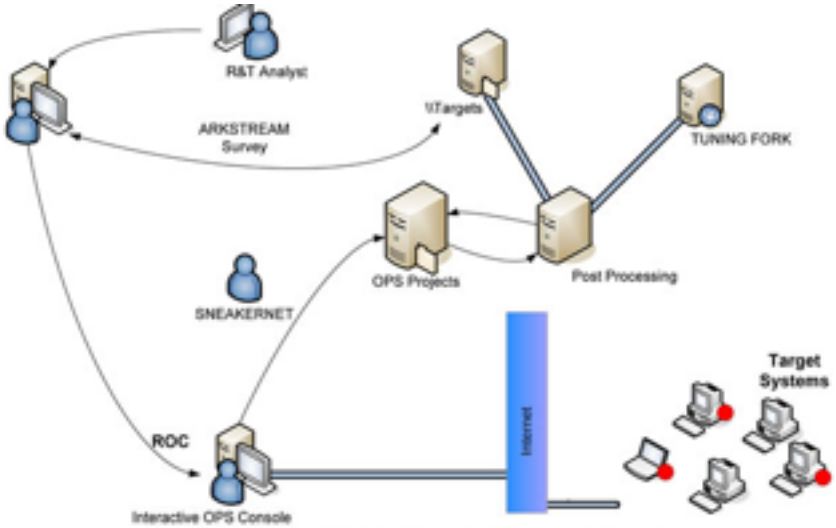
NSA Observer https://nsa-observer.laquadrature.net/

SECRET//COMINT//REL TO USA, FVEY

DEITYBOUNCE

ANT Product Data

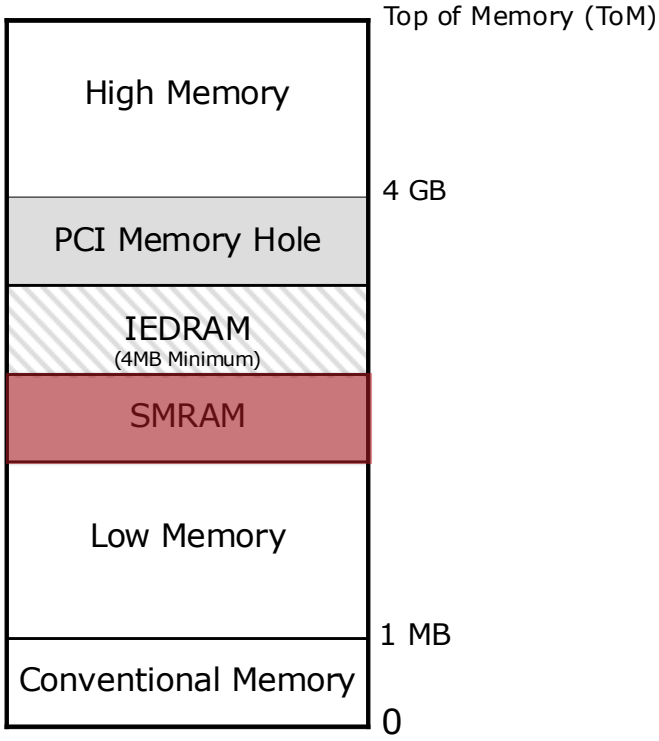
- Targets the BIOS firmware
- BIOS exploits system management mode (SMM)
- Infection through a USB stick



(TS//SI//REL) DEITYBOUNCE Extended Concept of Operations

System Management Mode

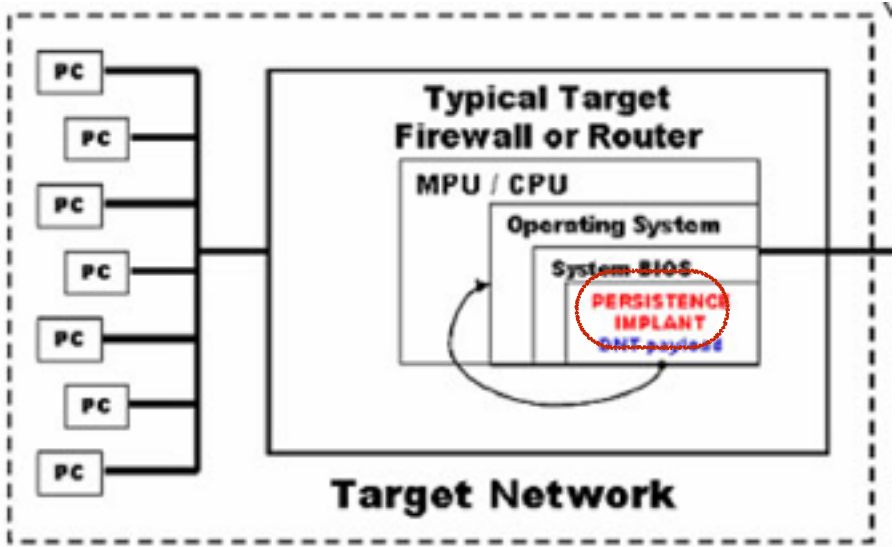
- “Ring -2”: Highest level of privilege
- Installed by BIOS
- SMRAM is not accessible to OS
- Non-maskable interrupts (SMIs)



GOURMETTROUGH

ANT Product Data

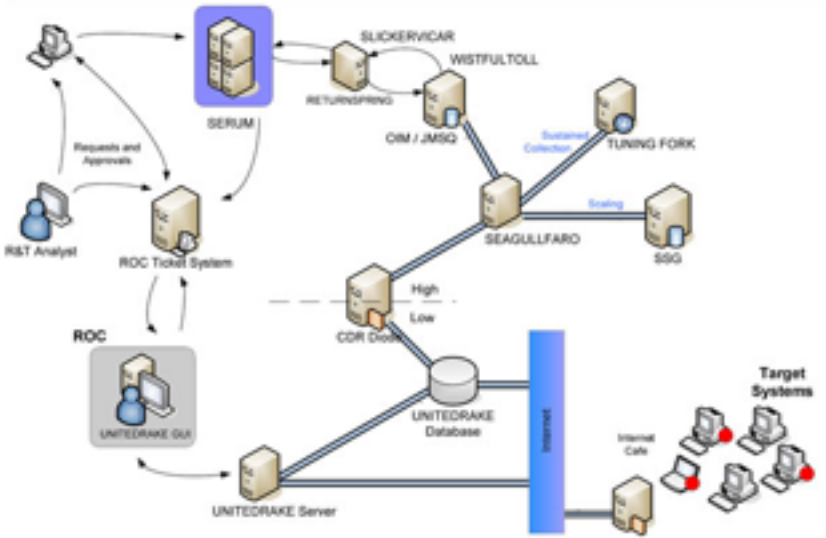
- Infects Juniper firewalls
- Again, targets the BIOS & SMM
- Since 2008 & unit cost: $0
- Other attacks on Cisco & Huawei



IRATEMONK

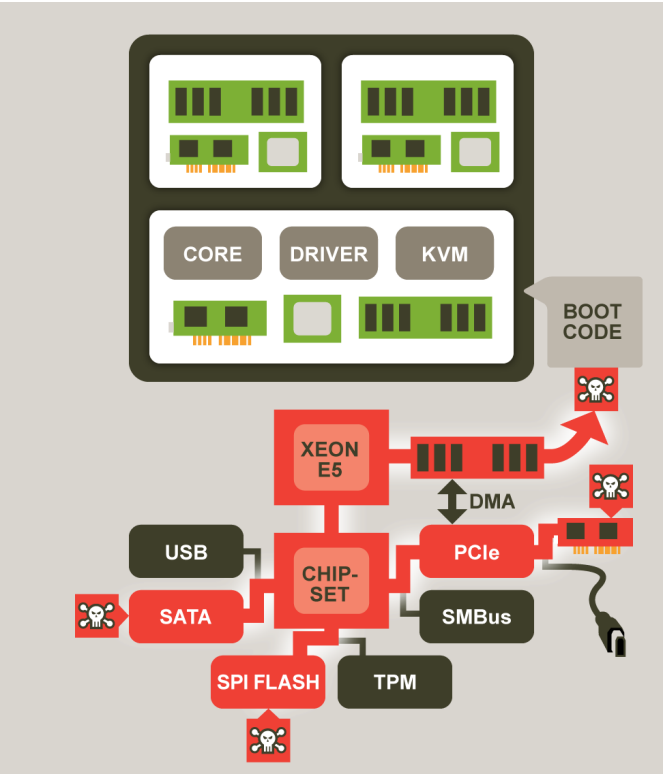
ANT Product Data

- Targets hard drive firmware
- Corrupted firmware modifies the disk master boot record (MBR)
- Since 2008 & unit cost: $0



(TS//SI//REL) IRATEMONK Extended Concept of Operations

Boot Integrity Attacks

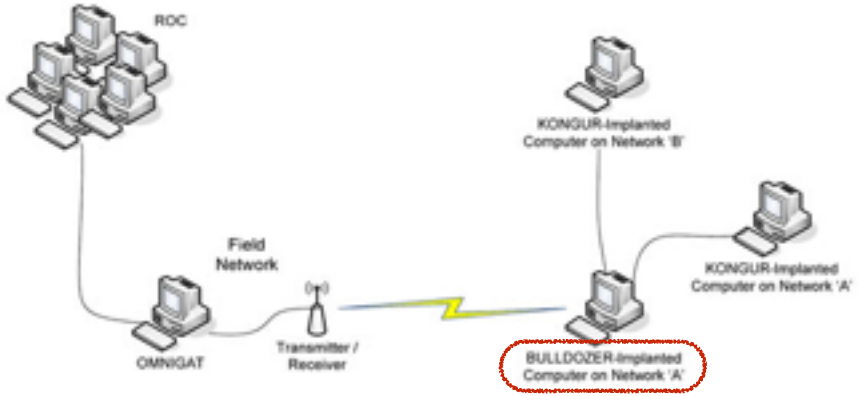


- BIOS / EFI
- Device firmware / Option ROMs
- Master boot records
- Keyboard controllers
- Management engines and controllers

GINSU

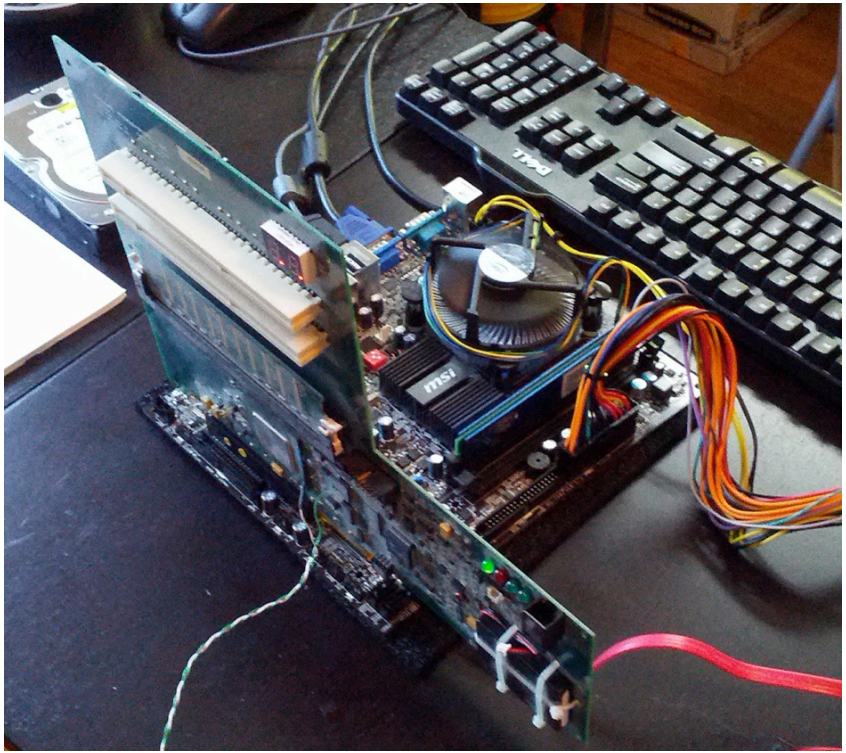
ANT Product Data

- Combined software, firmware, and hardware exploits.
- Paired with PCI implant device.
- Persists across OS reinstalls



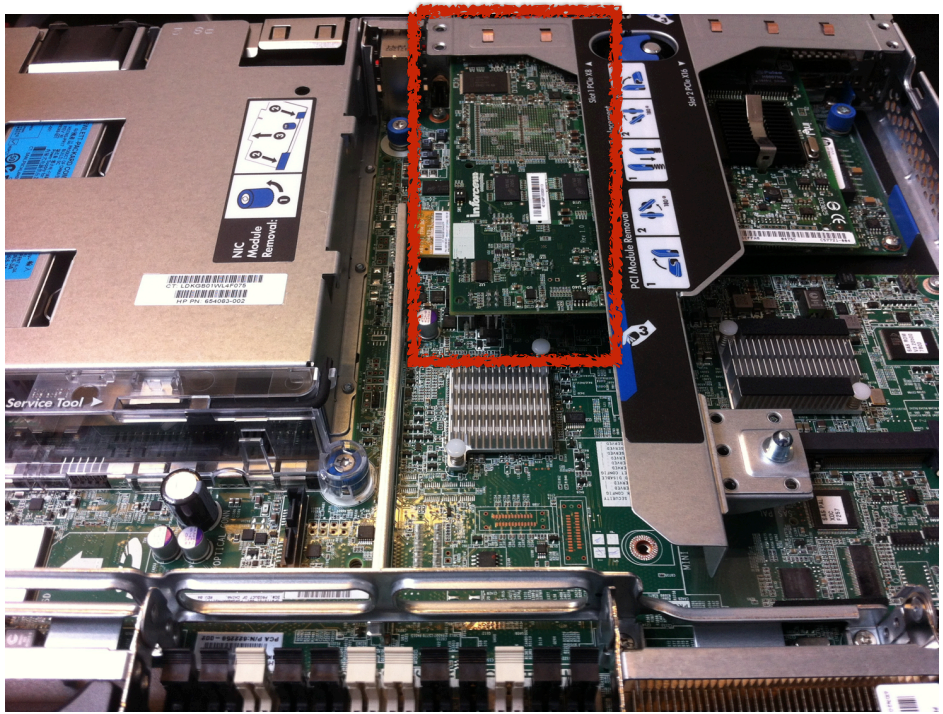
(TS//SI//REL) GINSU Extended Concept of Operations

The Notorious Tribble

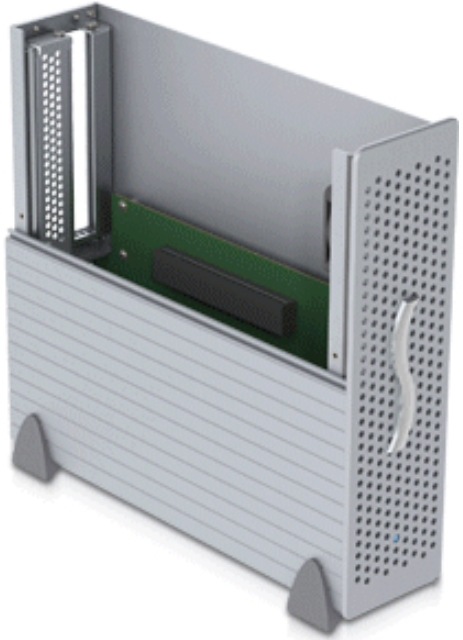


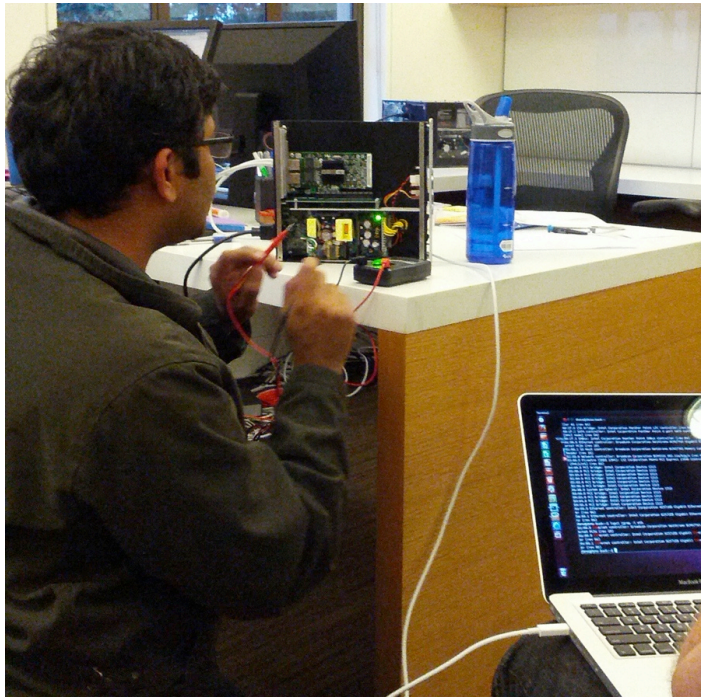
Do-it-Yourself PCIe Attack

- Intelligent Network Adapter
- Boots independently of host
- Exfiltrates data over network

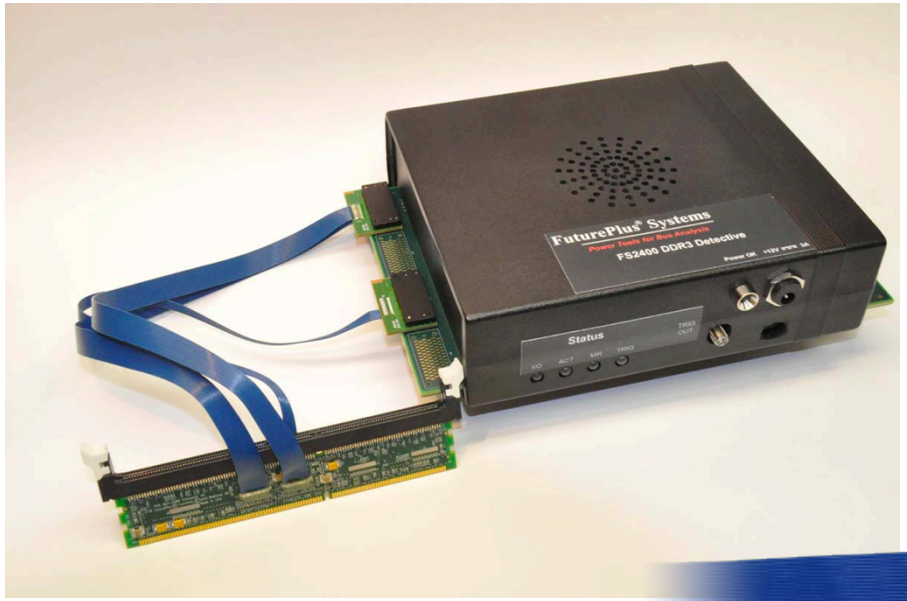


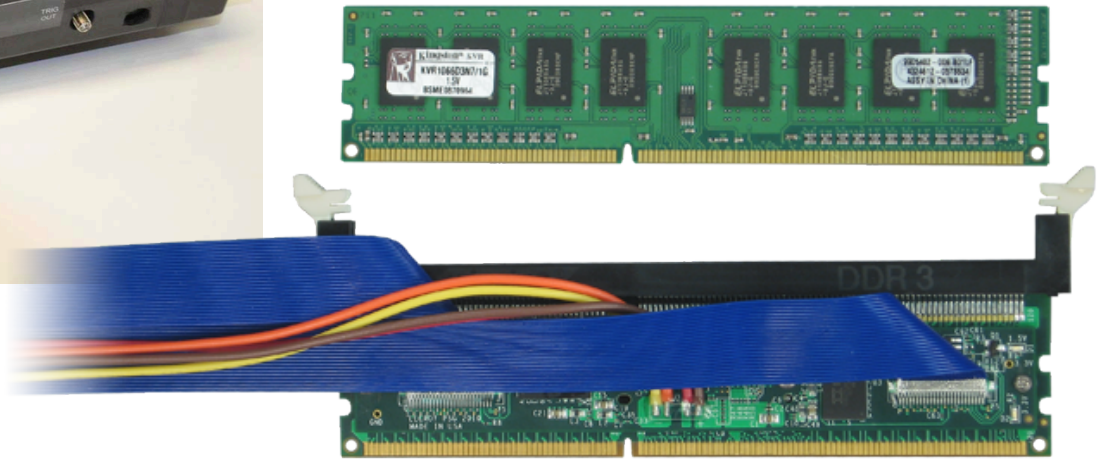
Firewire & Thunderbolt



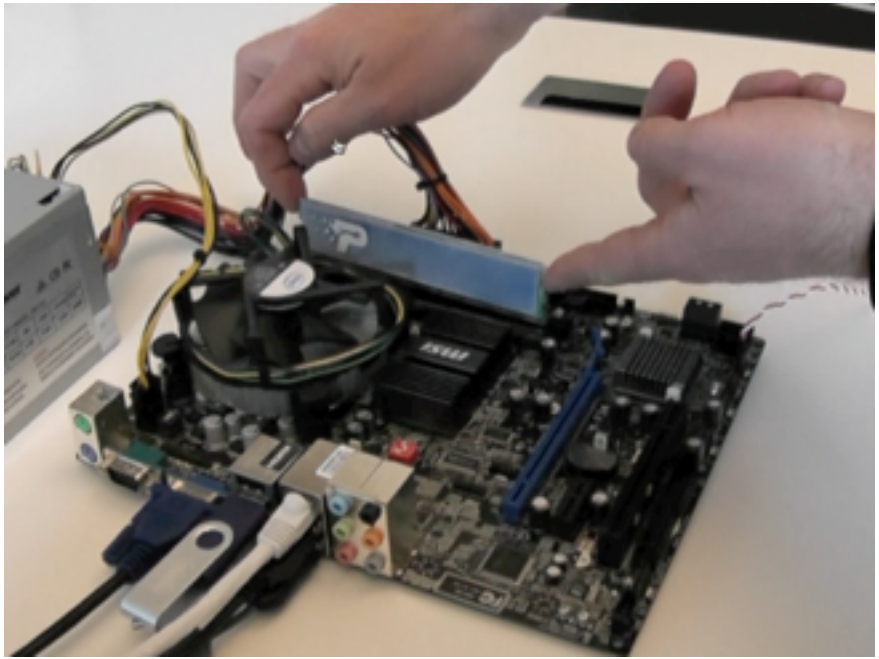


Memory Bus Analyzers



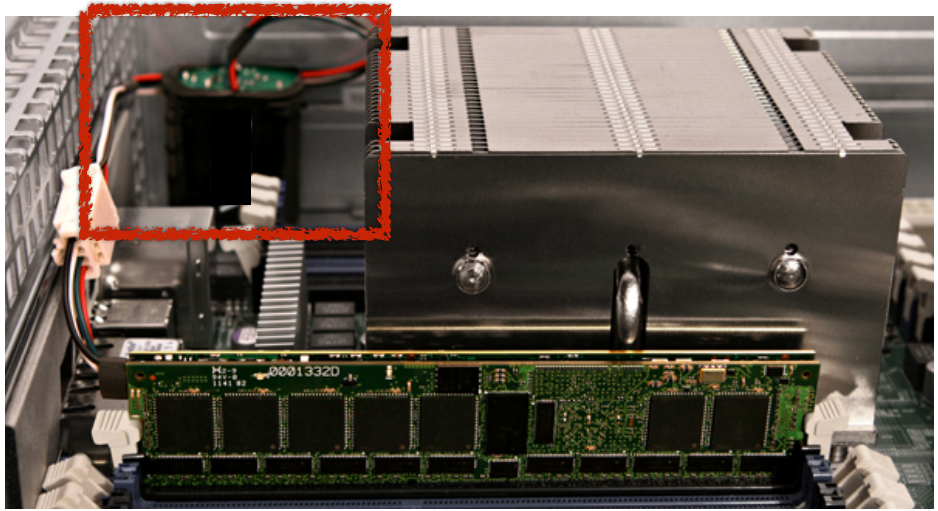


Cold Boot Attack



Non-Volatile RAM

- Contents are saved to flash memory on power loss
- Easily capture crypto keys
- Multiple persistent technologies in the pipeline



Defenses and Mitigations

Diagnostics Tools

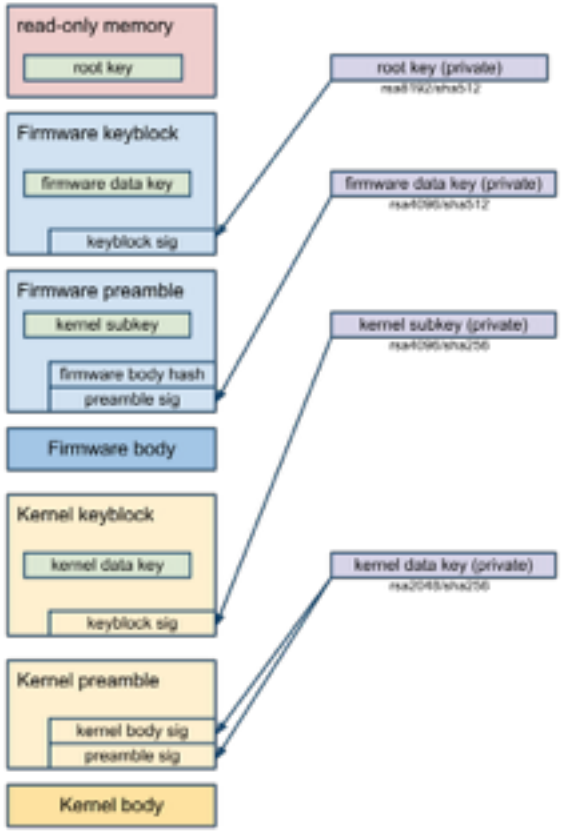
- **Flashrom**: General purpose tool to read firmware
  http://flashrom.org

- **Intel CHIPSEC:** Platform security assessment framework
  https://github.com/chipsec/chipsec

- **MITRE Copernicus**: Extracts BIOS and checks if modifiable

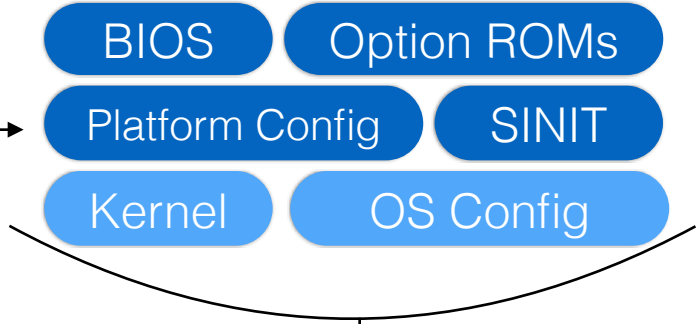
Verified Boot

- Root of trust in read-only firmware
- Each step verifies signatures on the next step
- Modifying any part of the boot process invalidates the chain.



Trusted Execution Technology

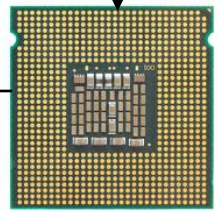
Firmware and software needed to boot



Remote Attest

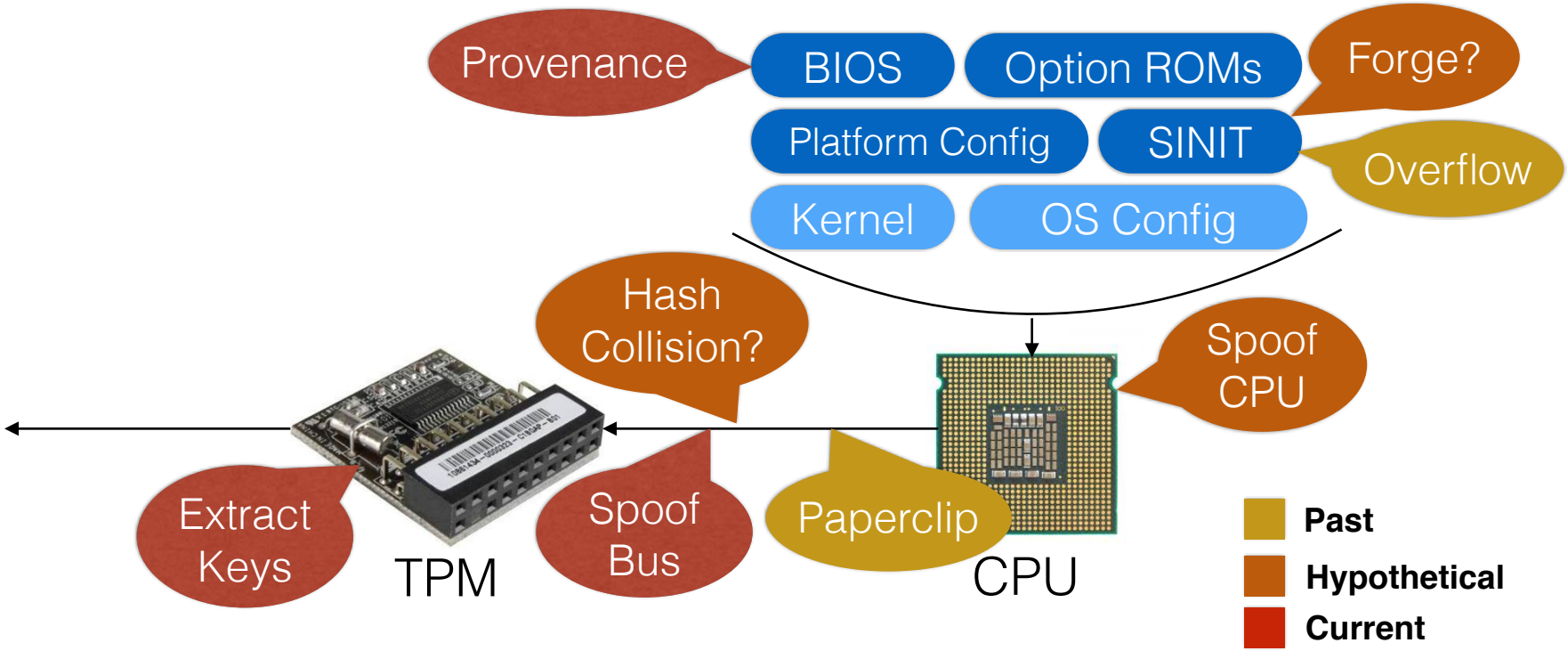
TPM

Measure



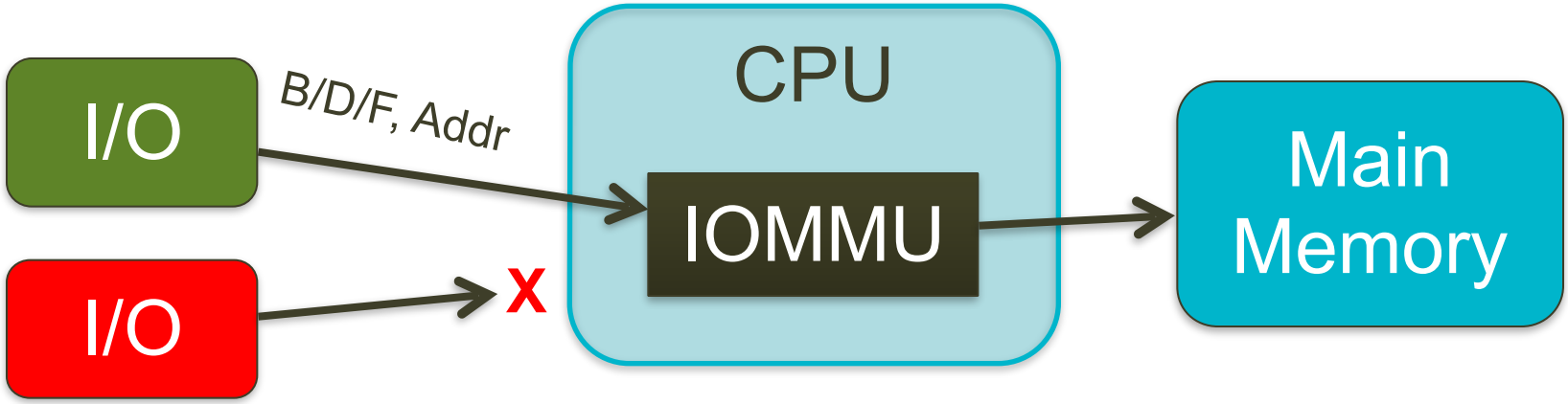
CPU

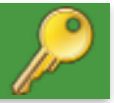
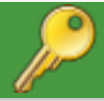
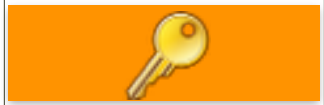
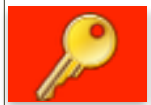
TXT Attack Vectors



IOMMU

- Intel VT-D: Virtualization Tech for Directed I/O
- Protects against DMA
- Not universally enabled



	Registers	L3 Cache	Memory	Disk
Software Cryptoprocessor		Pinned 	Encrypted	
CARMA		Pinned	Disabled	
Frozen Cache		No Fill 	Exposed	Encrypted
Tresor			Exposed	Encrypted
Cryptkeeper				Encrypted
Status quo				Encrypted

Upcoming Technologies

Software-Based Attestation

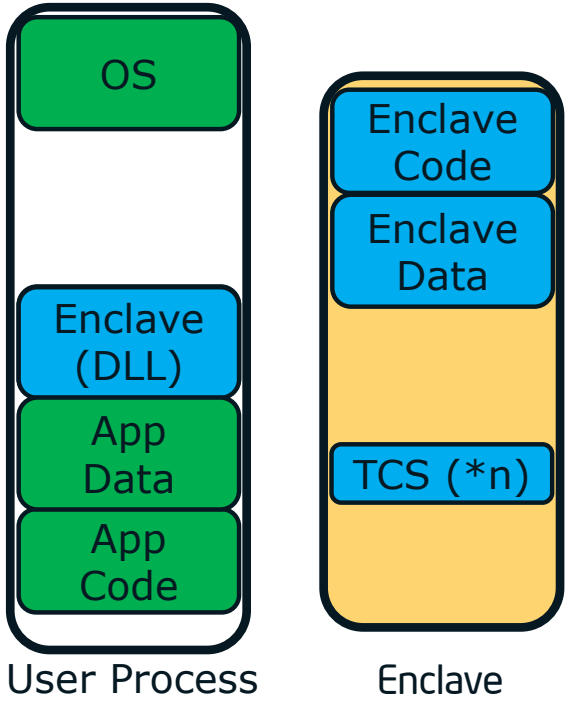
- Typical approach is to measure a performance metric
- Changes in expected code cause measurable difference
- Need to assure device is not being simulated
- One approach is to use HW-rooted key material in device…

Enhanced Privacy ID (EPID)

- Successor to Direct Anonymous Attestation (DAA)
- Provides ability for CPU to anonymously sign data.
- Could authenticate CPUs as real, without leaking identity.
- Rooted in globally unique key material in CPU hardware.

Software Guard Extensions (SGX)

- Small, user-mode “secure enclaves”
- Fully attested by CPU-based keys
- Backed by fully-encrypted memory.
- Could be great for DRM



My Wishlist

- A mature SMM transfer monitor (STM) or some other means of isolating the SMM.
- Extended support for hardware-based memory encryption
- A way to provision my own keys into a CPU root of trust
- Finer L3 cache controls, e.g. line locking, coloring, etc.

Thank you