Protecting Data In-Use from Firmware and Physical Attacks

Steve Weis
PrivateCore
About Me

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

Steve Weis
saweis.net
@sweis
Today’s Talk
Spot the implants
NSA ANT

NSA Observer

https://nsa-observer.laquadrature.net/
• Targets the BIOS firmware
• BIOS exploits system management mode (SMM)
• Infection through a USB stick
System Management Mode

- “Ring -2”: Highest level of privilege
- Installed by BIOS
- SMRAM is not accessible to OS
- Non-maskable interrupts (SMIs)
• Infects Juniper firewalls
• Again, targets the BIOS & SMM
• Since 2008 & unit cost: $0
• Other attacks on Cisco & Huawei
• Targets hard drive firmware
• Corrupted firmware modifies the disk master boot record (MBR)
• Since 2008 & unit cost: $0
Boot Integrity Attacks

- BIOS / EFI
- Device firmware / Option ROMs
- Master boot records
- Keyboard controllers
- Management engines and controllers
• Combined software, firmware, and hardware exploits.
• Paired with PCI implant device.
• Persists across OS reinstalls
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](http://flashrom.org)

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

BIOS
Option ROMs
Platform Config
SINIT
Kernel
OS Config

CPU

TPM
TXT Attack Vectors

- Provenance
- BIOS
- Option ROMs
- Platform Config
- SINIT
- Kernel
- OS Config
- Forge?
- Overflow
- Hash Collision?
- Spoof CPU
- Extract Keys
- TPM
- Spoof Bus
- Paperclip
- Current
- Past
- Hypothetical
IOMMU

- Intel VT-D: Virtualization Tech for Directed I/O
- Protects against DMA
- Not universally enabled
<table>
<thead>
<tr>
<th>Software Cryptoprocessor</th>
<th>Registers</th>
<th>L3 Cache</th>
<th>Memory</th>
<th>Disk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software Cryptoprocessor</td>
<td>Pinned</td>
<td></td>
<td>Encrypted</td>
<td></td>
</tr>
<tr>
<td>CARMA</td>
<td>Pinned</td>
<td>Disabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Frozen Cache</td>
<td>No Fill</td>
<td>Exposed</td>
<td></td>
<td>Encrypted</td>
</tr>
<tr>
<td>Tresor</td>
<td>Exposed</td>
<td></td>
<td></td>
<td>Encrypted</td>
</tr>
<tr>
<td>Cryptkeeper</td>
<td></td>
<td></td>
<td></td>
<td>Encrypted</td>
</tr>
<tr>
<td>Status quo</td>
<td></td>
<td></td>
<td></td>
<td>Encrypted</td>
</tr>
</tbody>
</table>
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