Trust, Lies and Attestation

Trammell Hudson
Lower Layer Labs
@qrs@twitter.com   @qrs@mastodon.social
How do we prevent unauthorized code?

Simple: Turn on Verified Boot
CPU Reset

FW Signature Check

Valid → Run firmware validates OS, validates apps

Invalid → Halt

Verified Boot

Validates OS, validates apps
Thanks for coming to my talk!
Have a wonderful Day 2
At Hardwear.io
Freedom

Signing keys

Documentation
“Root of Trust for Update”

CC-BY-SA Jared Benedict
Lenovo 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.

Why open source firmware is important

Jessie Frazelle - @jessfraz

“Vendors can rarely debug firmware issues...”

https://devopsdays.org/events/2019-chicago/program/jessie-frazelle/
Replace Your Exploit-Ridden Firmware with Linux
Ronald Minnich, Google

https://www.youtube.com/watch?v=iffTJ1vPCSo
Freedom

Signing keys

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

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

(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: S32221, [redacted]
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 armv5tel GNU/Linux
/  # whoami
root
/  #
Modchips of the state

Technical feasibility of the Bloomberg/Supermicro hardware implants

Trammell Hudson, Two Sigma
@qrs
adversary: nation state (NSA!!!!!)

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?

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

Signature Valid?

Run firmware

Halt

Verified Boot
Ultra-high touch
• 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
Zero touch

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’s Utah Data Center.jpg
Philosophy

“Tools, not policy”

- 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; rep provisioning hardware with your own keys.

- Have tools for: Boots, Not Bricks.
  - Scary Screen?
Turning Linux engineers into firmware engineers

David Hendricks Firmware Engineer/Facebook
Andrea Barberio Production Engineer/Facebook

https://2018ocpregionalsummit.sched.com/event/F8ax/
Recovery from attacks is hard
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 is replaced.

By Lucian Constantin | Follow
Romania Correspondent, IDG News Service
Jul 14, 2015 6:56 AM PT

Safeguarding rootkits: Intel BootGuard

Alexander Ermolov

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.
Yigal Edery, Program Manager Azure Security

BMC - Typically unsecure
- No protect, no detect, no recovery
- No reliable attestations
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 it "easier to identify" users on the World Wide Web.

"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."

The group's target is all sorts of commerce and personal privacy.

The boycott was prompted by the group's hope that a number generator could make encryption of personal data problematic.
“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.”
TPM Usage

Introduction

Chrome OS uses the TPM for these tasks:

- Preventing software and firmware version rollback
- Maintaining information to detect transitions between 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
- 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.
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?

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; job
/
# 2.451809] clocksourced

https://trmm.net/Tpmtotp
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?
- How do I know my system is properly configured?

“We are building a system that has to be able to provide this information, and we will publicly release 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 to the integrity of the environment, and we will publicly release this measurement. This architecture will greatly diminish the worry of users.”
Open source server firmware future:

- u-bmc (ARM)
- coreboot (x86)

DEVELOP & DELIVER MORE SECURE SOLUTIONS

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

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
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.
Encrypting virtual machines can help protect them not only from physical threats but also from other virtual machines or even the hypervisor itself. Cloud computing need not fully trust the hypervisor and administrator.
Figure 3: Initial deployment of a guest virtual machine in an SEV scenario.
Google Security Chip H1
A member of the Titan family
Chrome OS Use Case
vbendeb@google.com

Microsoft Cerberus
- 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

Amazon Nitro
- 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

Apple T2
Joanna Rutkowska, “Towards reasonably trustworthy laptops”
https://media.ccc.de/v/32c3-7352-towards_reasonably_trustworthy_x86_laptops
hot take: laptops are embedded devices

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

FTDI FT232RL: Real vs Fake (CC-BY Zeptobars)
TPM Genie
https://github.com/nccgroup/TPMGenie
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
CPU Reset

Run firmware

Halt

Signature

Valid?

Freedom!

Resilience!

Attestation!

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