THE ENTERPRISE HARDWARE ATTACK SURFACE AND HOW TO DEFEND IT

Attackers are increasingly targeting the largely unprotected hardware and firmware within all types of devices. Firmware vulnerabilities are common and difficult to manage, and once exploited, allow attackers to subvert traditional security and gain long-lasting persistence within a network. In this paper, we will explore the nature of the risk, why it has become a priority now, and how organizations can protect themselves today.

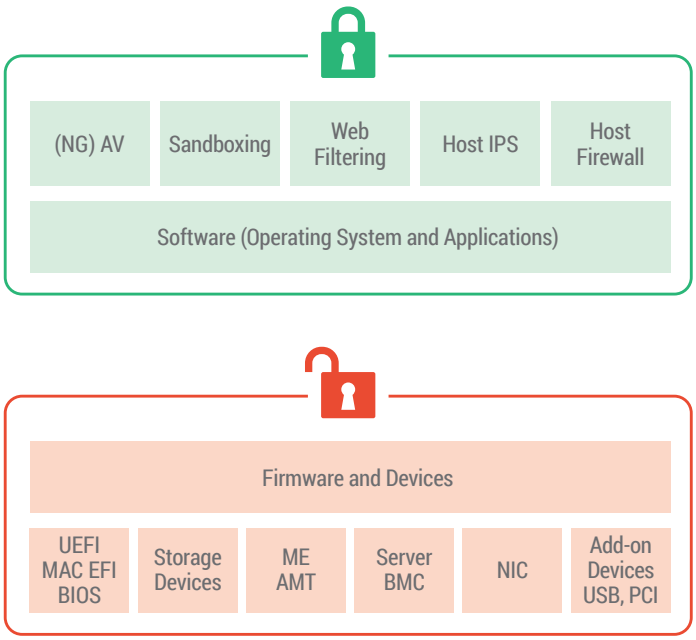
INTRODUCTION

All computing devices, from the most advanced servers and network devices to the lowliest USB drives, all function from the physical layer up. Internal logic on the motherboard, internal components, and the processors themselves provide the bedrock of computing that supports the operating system, which in turn supports applications, virtual hosts and services.

While this hierarchy is obvious and well-understood, it has not been incorporated into the security model for most organizations. In most cases, information security is addressed from the operating system up, with the hardware layer being ignored and assumed to be secure.

This assumption is proving to be a mistake, as real-world attackers are increasingly targeting the physical layer where devices remain largely undefended and unmonitored. Devices of all types within an enterprise depend on proprietary firmware code that is typically not audited, not verifiable, contains many vulnerabilities and is difficult to patch. Once compromised, attackers are free to subvert many of the carefully crafted security controls installed at the operating system and above.

While hardware-level vulnerabilities and attacks are not new, the landscape has changed and continues to evolve rapidly. What was once considered a largely academic pursuit has rapidly turned into one of the most active areas of conflict between attackers and defenders. In this paper we will look at the factors driving the change, the challenges to the traditional security model, and introduce a new layer of security going forward.



The unprotected hardware and firmware layer

HARDWARE GETS THE SPOTLIGHT

Firmware, BIOS, and chip-based logic has been around since the earliest days of computing. As such, it is fair to wonder why this attack surface would be overlooked for years and suddenly become a priority now.

While there are variety of factors at play, two issues seem to be taking priority. First, the barriers to analyzing firmware have been drastically reduced, meaning that the firmware layer is suddenly far more accessible to anyone in the security community. This means that now the code in firmware and other infrastructure is open to scrutiny in much the same way that traditional software has been for years.

Secondly, the industry has faced a major spike in the use of hardware and firmware implants by advanced actors in the wild. In short, advanced attackers have proven the value of attacking below the operating system, and less skilled attackers now have the tools to follow in their footsteps.

Hardware Vulnerabilities Go Mainstream

Vulnerabilities in the physical/firmware layers have always been present, but until recently they were very difficult to see. In the past, analyzing firmware and chip-level code required specialized and expensive tools. It was also much more time consuming for researchers to do an adequate analysis of firmware as opposed to traditional software. This meant that research was limited to a very small fraction of the security community.

All of this has changed in the past few years. New tools have come to market that have lowered the costs of hardware analysis by an order of magnitude. Today researchers can insert a USB drive and begin analyzing a chip directly. With fewer barriers, the code in the hardware and firmware layer is suddenly fair game both for ethical researchers as well as attackers. While such exposure has been standard for traditional software, it is very new for hardware, where for years the code was assumed to be unreachable.

An Untended Garden of Vulnerabilities

Unfortunately with this new visibility, researchers have found the hardware layer to be inundated with flaws. Every device is inundated with proprietary code that is often vulnerable, hard to audit, and even harder to patch. The Spectre and Meltdown vulnerabilities illustrated that even the giants of the industry such as chip manufacturers are not immune to serious problems. However, the more unsettling prospect for security teams is that they likely represent the best case scenario of hardware vendors.

Whereas some larger manufacturers invest heavily in product security and research, many hardware providers do not. Given that very few researchers could look for hardware vulnerabilities in the past, the majority of the hardware supply chain has been driven by cost and not security. As a result, devices from servers, to PCs, to phones are packed with motherboards, disk drives, network cards and a variety of other hardware components that were chosen based on price and were never expected to be part of a security attack surface. That assumption is increasingly proving false, bringing large amounts of insecure code into the light of day.

Over the last few years the industry has seen a spike in the amount of critical vulnerabilities and implants that have been discovered including:

- UEFI, Mac EFI, and SMM firmware
  - » LoJax UEFI Rootkit
  - » Tianocore
  - » SMM firmware vulnerabilities
  - » ThinkPwn
  - » Mac firmware worms
  - » Multi-platform UEFI vulns
- "Lights out" management controllers
  - » HP iLO
  - » Supermicro BMC
  - » Intel Management Engine (ME/AMT)

- Computer components and peripherals
  - Hard drives
  - Wi-Fi chips
  - Embedded and keyboard controllers
  - Smart Battery System
  - BadUSB
- Hardware vulnerabilities and exploitation techniques
  - DRAM Rowhammer
  - Flip Feng Shui
  - CPU memory sinkhole
  - Firmware Secure Boot bypass
  - CPU Speculative Execution (Spectre and Meltdown)

Fixing problems can be a challenge even once they are found. Unlike traditional software vulnerabilities, firmware updates are far less frequent. In some cases a low-cost component provider may never get around to delivering an update, or it may go unaddressed for years. Even when firmware updates are available, many organizations lack programs to update the firmware on their devices [1, 2]. This means that not only are there many vulnerabilities in hardware, they tend to have particularly long tails as well.

This has led system manufacturers to build defenses into the hardware such as the recently revealed Google Titan chip. However, these hardware mitigations may not always be available and even when they are, these security chips have been found to contain vulnerabilities themselves. This was the case with vulnerable firmware inside Infineon Trusted Platform Module or inside AMD Platform Security Processor. The very devices intended to protect our systems at a hardware level can be compromised and host stealthy implants.

Many Targets to Choose From

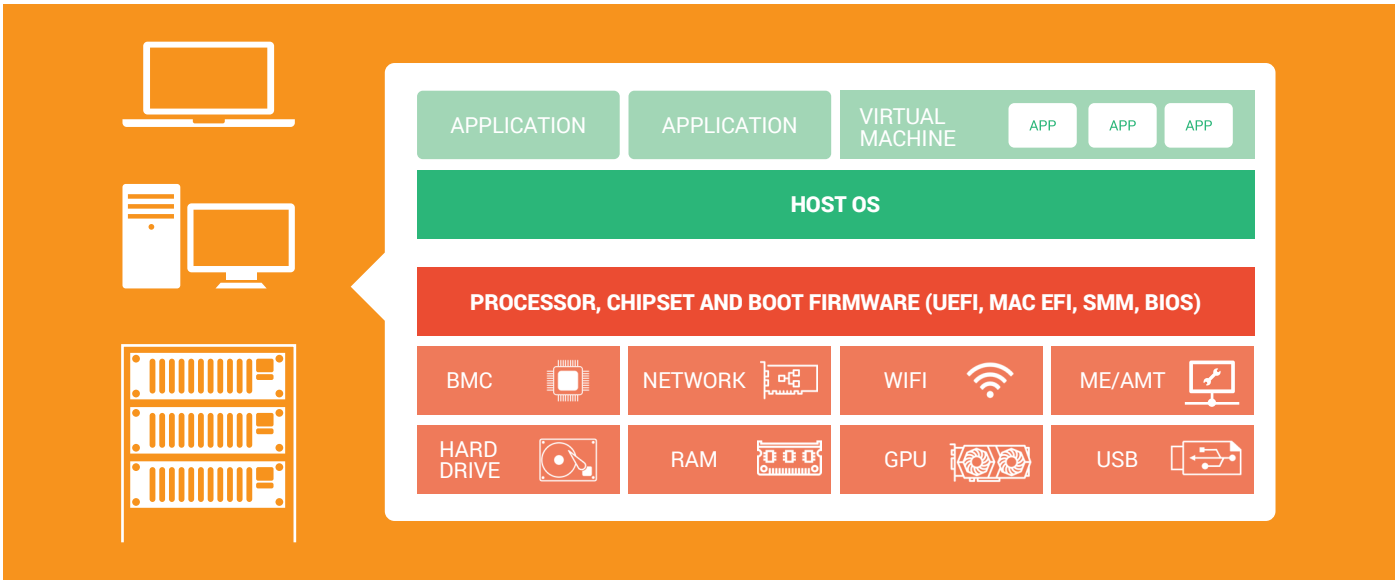
Attackers have many options when they target the hardware layer. Not only do all devices have firmware, many of system's individual components will have their own independent firmware. BIOS and the more modern UEFI or Mac EFI provide the gateway to the system firmware on a device's motherboard. Recent Eclypsium research demonstrated how UEFI can be attacked remotely and the discovery of LoJax UEFI rootkit in the wild demonstrated how attackers are using firmware attacks to subvert the host operating system and persist across system re-imaging and even hard drive replacement.

However, the problem extends well beyond the motherboard. Hard drives, network or WiFi cards, graphics cards, system-on-chip and variety of other components have their own internal controllers and firmware that drive their behavior. Compromising these devices provides an attacker with direct and fundamental access to the most sensitive information on the system.

> ...not only are there many vulnerabilities in hardware, they tend to have particularly long tails as well.

Within servers, baseboard management controllers (BMCs) and IPMI are used to deliver dedicated "lights out" management to servers using hardware and interfaces that are independent of the host operating system. However, out of band management is not limited only to servers. Intel Management Engine (ME) and Active Management Technology (AMT) provides the same functionality for traditional PCs as well. Backdoors have likewise been found within the firmware of network routers and firewalls, allowing attackers to not only backdoor the network, but the very security products charged with defending it. Even seemingly lowly USB peripherals contain their own internal controller code that can be compromised and used to subvert the operating system of a system it is connected to.

The sum total of all of these devices make for a complex ecosystem even on an individual host device. The problem gets vastly more complex when you begin to look at vulnerabilities at the organizational level. Enterprises often have a dizzying combination of corporate laptops, networking gear, white-box servers supporting virtual environments, and the list goes on. Simply trying to track a single known vulnerability in a chip or hardware component can be incredibly difficult in the best of circumstances.



Backdoors and Implants in the Wild

With the sudden accessibility of the hardware layer, it should be no surprise that attackers are starting to take notice. Many examples have been predictably associated with advanced actors intent on maintaining silent persistence within a target.

LoJax, one of the first UEFI rootkits seen in the wild, and the Black Energy attack against infrastructure in the Ukraine both bore the clear signs of nation-state actors. Likewise the disclosure of EFI and BIOS implants for Macs and PCs and the Equation Group implants targeting firewalls, networking gear, hard drives and other infrastructure confirmed that implants had made the jump to use in the wild.

Network devices and servers have become a key target for advanced actors. The US Department of Homeland Security recently issued an alert for a large-scale state-sponsored attack targeting enterprise network devices such as routers, switches, and firewalls. Once compromised, attackers would modify the device firmware to gain near full visibility and control over the victim network. The VPNFilter malware also targeted networking devices and contained code to disable the device by overwriting its firmware. Research from Mandiant uncovered backdoors in Cisco routers dubbed SYNful knock that allowed an attacker to take control of the device using specially crafted TCP packets.

Additionally, devices can be compromised in the hardware supply chain even before they are unboxed by the eventual owner. NIST recently highlighted the importance of this style of risk by adding an entire Supply Chain Risk Management (SCRM) category to its Critical Infrastructure Cybersecurity framework.

While these examples exhibit the handiwork of advanced actors, they show that these threats are real, and are critical tools for attackers who want to maintain persistence in an environment without detection. And as we have seen in the past with malware and other threats, the disclosure of new techniques from advanced actors quickly spread to other targeted attack groups and ultimately the criminal ecosystem as well. With the breadth and depth of the attack surface and the widespread lack of controls at the hardware level, there is every reason to believe that this trend will continue.

SUBVERTING THE TRADITIONAL SECURITY MODEL

The ability for firmware implants and backdoors to subvert traditional security controls makes them almost invaluable to advanced attackers. By acting at the hardware level, attackers can bypass security controls running at the OS or container level, effectively hiding their malicious activity from detection. This provides attackers with long-term, nearly undetectable persistence while still retaining direct access to data on drives, in memory, or sent over the network. By nature, these attacks are often long-term, strategic, and can evolve over months and years to target or destroy an organization's most valuable assets.

Going Below the OS

Firmware, BIOS, and chip-based logic has been around since the earliest days of computing. As such, it is fair to wonder why this attack surface would be overlooked for years and suddenly become a priority now.

While there are variety of factors at play, two issues seem to be taking priority. First, the past few years have shown a major spike in the use of hardware and firmware implants by advanced actors in the wild. Secondly, the barriers to security research have been drastically reduced, meaning that the firmware layer is suddenly far more accessible to anyone in the security community.

This means that now the code in firmware and other infrastructure is open to scrutiny in much the same way that traditional software has been for years. In short the high-end attackers are leading the way, and the lower-end attackers now have the tools to emulate them.

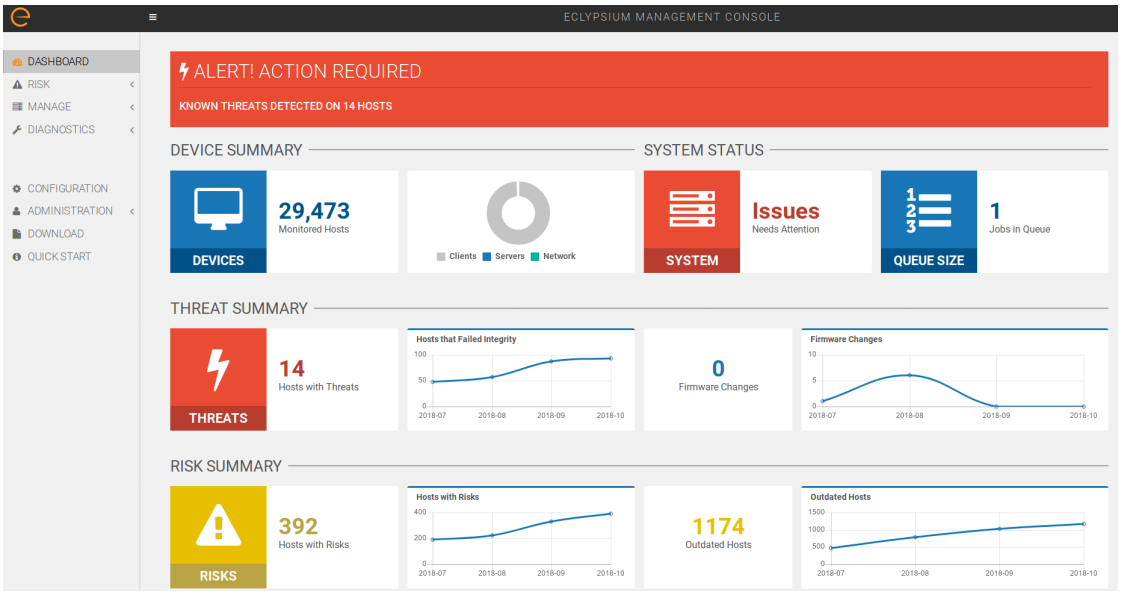
This is of particular relevance as the industry increasingly adopts more and more virtualization. While computing trends toward increasing layers of abstraction with apps and services running in VMs and containers, all of those virtual assets eventually depend on the hardware. Instead of trying to compromise the virtual environment, attackers could simply exploit the hardware that the virtual world rides upon.

Attacks targeting BMCs and IPMI make this concern even more troubling. These interfaces are designed to ensure servers are remotely manageable even when the host OS isn't running. By controlling this management infrastructure within the server, an attacker could modify the virtual environment and even change the operating system itself. With security solutions not monitoring software and firmware running on the BMCs and most organizations not monitoring BMC management network, attackers are able control the management network of data centers while staying hidden in the organization's infrastructure.

It is important to note that this same idea applies to traditional user PCs as well. Intel's Management Engine (ME/AMT) provide out of band management for PCs in much the same way that IPMI is used by servers. This likewise means that it is possible to attack a laptop even when it is powered off.

Remediation Avoidance

The problem persists even when we consider security remediation. When a security team suspects a device is compromised, one of the standard responses is to simply reimage the machine. However, simply reinstalling the operating system will have no effect on a device compromised at the firmware level. Not only is the firmware not replaced during a fresh install, it also runs before the OS. The firmware controls how the operating system is loaded or communicates with the hardware, and thus has incredible power over the machine and how it will run.



Vulnerabilities and Patching

While the hardware attack surface has suddenly been thrust into the spotlight, most organizations have almost nothing to help them manage vulnerabilities. First of all, firmware updates are often very few and far between. Known vulnerabilities can persist for years. Hardware vendors who are largely focused on providing stable hardware are often unable to keep up with advanced attackers in a race to constantly update firmware for products that are already released and introduce mitigations to rapidly changing exploitation techniques which general purpose operating systems have.

Secondly, updating firmware can be tricky. It can be difficult to even find devices that are vulnerable due to a lack vulnerability scanning at the hardware level. And unlike software updates, which are highly automated, firmware updates are often complicated and require significant time and manual effort for administrators. Recent examples with process firmware updates causing instability and unexpected reboots in servers further discourage security teams from deploying firmware updates in their critical infrastructure.

The result is that organizations often lack the tools to know where they are vulnerable, to address known vulnerabilities, and to detect and mitigate any active compromises. Let's take a look at new model that can address these challenges.

PROTECTION FROM THE HARDWARE UP

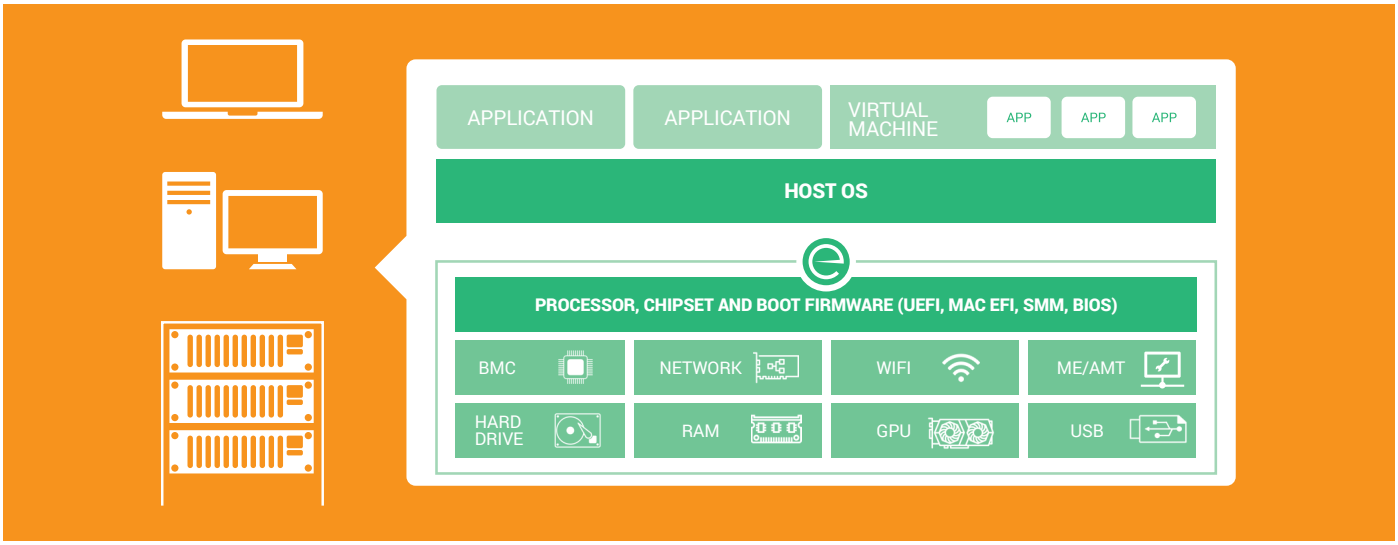
Eclypsium introduces a new layer of security dedicated to protecting enterprises at the hardware and firmware level. The technology allows organizations to find vulnerabilities in their devices, detect known implants active in systems of an organization or tampering with the firmware, and actively isolate any affected systems. Key features and capabilities are summarized below:

1. Attack Surface Management

- Risk analysis of all monitored hosts—Analysis of firmware versions, and known vulnerabilities in the hardware and firmware. Analysis of hardware components, configuration and hardware protections supported by the system
- Firmware update management—Centralized management of system firmware updates, and other firmware components.

2. Detection and Containment of Threats

- Firmware integrity monitoring and implant detection
  - Detection of implants in system firmware, hardware components (motherboards, network interface cards, baseboard management controllers, graphics cards, HDD and SSD storage devices, etc) as well as OS boot level implants.



- Runtime behavior monitoring—Analysis of device, firmware, and OS behavior to identify signs of compromise or stealthy implant behavior.
- Remediation—Reliable containment for any affected systems via hardware based mechanisms.

The Eclypsium user interface makes it easy to quickly check the overall posture of your environment, find any active threats, and drill down into details for any threat or host. Administrators can see information about firmware and hardware available on any monitored host including release dates of firmware components, and even check for the availability of updates from the vendor. Users can then verify the integrity of all firmware components, run on-demand assessments or scans, monitor runtime heuristics of the device, and review any identified threats.

Summary

Firmware is in every device in the modern enterprise from user devices like mobile phones and laptops to the servers, switches, and networking gear that define our data centers and the network itself. While the code and logic within this layer has been largely ignored for many years, a wave of new attacks has shown that organizations can no longer afford to rely on "security by obscurity" when it comes to their hardware. Vulnerabilities in the hardware layer are common, remain unpatched for long periods of time, and provide attackers with incredible power and ongoing stealth.

As with all types of information security, it is not enough to simply hope for our assets to defend themselves. For example, while operating systems are packed with security features, it is no substitute for layers of dedicated security. This is increasingly true of security at the hardware level as well. Even as hardware vendors begin to focus more on security, organizations need the independent visibility into their hardware attack surface with the ability to proactively detect and respond to threats. Eclypsium provides this critical layer of security. While this paper introduces many of the key concepts behind the solution, it is by no means exhaustive. We hope that you will be inspired to learn more on the subject, and we look forward to discussing how Eclypsium can help to protect the hardware layer of your organization.