TAG

WHY SUPPLY CHAIN SECURITY DEMANDS FOCUS ON HARDWARE: AN INTRODUCTION TO ECLYPSIUM

DR. EDWARD AMOROSO,
CEO, TAG INFOSPHERE[1]

WHY SUPPLY CHAIN SECURITY DEMANDS FOCUS ON HARDWARE: AN INTRODUCTION TO ECLYPSIUM

DR. EDWARD AMOROSO, CEO, TAG

This report explains how supply chain security in the context of endpoints must include foundational attention and focus on the underlying hardware. The concept is illustrated in the context of the commercial supply chain security platform from Eclypsium.

INTRODUCTION:

Enterprise teams have come to recognize the importance of supply chain security for their servers, laptops, network gear, and other systems supporting information technology (IT) and operational technology (OT) applications. This is accomplished typically through supply chain risk programs that provide a comprehensive view of the software, including open source, that is used to construct such systems.

This is a good practice, obviously, since the complexity of such endpoints systems and devices has grown to the point where the underlying components are not easily identified. This creates risk since the source of such components could be either malicious, negligent, or otherwise unsuited for use as a supplier to the using enterprise. Software Bill of Materials (SBOM) methods have emerged to help address this risk.

Our view, however, is that most enterprise users neglect the importance of addressing the security of their underlying hardware. This lack of attention might come from the incorrect belief that nothing can be done to address such risk, but it is more likely the case that addressing hardware risk, unlike software risk, is often viewed as outside the scope of the typical enterprise.

In this report, we make the case that supply chain security is not only in scope for enterprise security teams, but that it is an essential task. Furthermore, we demonstrate using the commercial platform from Eclypsium that supply chain attention to the hardware aspects of servers, PCs, laptops, and other devices is not only feasible, but can be conveniently performed in a cost-effective manner.

OVERVIEW OF SUPPLY CHAIN SECURITY

Supply chain security for servers, PCs, laptops, and devices has correctly focused on protecting these systems from vulnerabilities introduced through third-party suppliers. The applicable supply chains range from design and manufacturing to distribution and integration. Each stage presents potential risks, as malicious actors could introduce compromised components, counterfeit products, or software backdoors that could be exploited later.

Historically, the focus of supply chain security has been on software. This emphasis is due to the inherent complexity and visibility of software vulnerabilities. Software is easier to modify after deployment, making it a frequent target for supply chain attacks. Cybersecurity practitioners understand this and have prioritized software security – and we fully acknowledge the use-cases that drive such decisions.

For example, attackers will insert malicious code into software updates or tamper with source code during development. The infamous SolarWinds attack in 2020, as one prominent incident, highlighted how a compromised software supply chain could lead to widespread infiltration across government and private sectors. Security leaders across the globe used the SolarWinds case as a means for enhancing (sometimes starting) their supply chain security program.

IMPORTANCE OF HARDWARE SUPPLY CHAIN SECURITY

As suggested, hardware security has often been overlooked, despite the significant risks it poses. Hardware vulnerabilities are harder to detect and mitigate since they are embedded in the physical components of devices. Once compromised, malicious hardware can be nearly impossible to fix without complete replacement. This is especially challenging for enterprise teams, who rarely have much control over the hardware in use across their infrastructure.

Luckily, recent years have helped to reveal the importance of hardware security in the supply chain, particularly as concerns about nation-state actors compromising hardware during manufacturing have grown. But the supply chain for these devices is complex, involving multiple stages from design and manufacturing to distribution and deployment. Each stage presents vulnerabilities that bad actors could exploit to introduce compromised hardware or firmware.

Compromised hardware can serve as a persistent threat, allowing attackers to bypass software-level security measures, remain undetected, and maintain long-term access to sensitive systems. For example, malicious microchips or altered circuitry could be embedded in network devices, granting unauthorized access or control to an adversary. Such breaches can lead to data theft, sabotage, or the creation of backdoors, all of which are difficult to find after deployment.

Ensuring the security of hardware components is also vital for maintaining trust in the entire IT ecosystem. Businesses and government agencies rely on these devices to store and process sensitive data, control critical infrastructure, and enable secure communications. If the hardware foundation is compromised, the security of all dependent systems is jeopardized, leading to potentially catastrophic consequences.

Making matters more complex, the globalization of the technology and security industries means that hardware components are often sourced from various manufacturers worldwide. This global supply chain increases the risk of tampering or counterfeiting, necessitating rigorous vetting and verification processes by enterprise security teams to ensure that components are authentic and have not been altered.

ISSUE OF COMPLIANCE

Cybersecurity compliance demands for secure underlying hardware and firmware focus on ensuring that systems are resilient against attacks that target foundational components. Compliance standards often require the implementation of secure boot processes, firmware integrity checks, and hardware-based encryption. These measures prevent unauthorized access, tampering, and persistent threats that can compromise system integrity from the lowest levels.

For example, NIST SP 800-193 offers guidelines for "Platform Firmware Resiliency," emphasizing the importance of protecting firmware from unauthorized modifications, ensuring the ability to recover from firmware failures, and maintaining the integrity of firmware updates.[1] Organizations must comply with these standards to ensure that hardware and firmware components are secure, reducing the risk of attacks that could compromise the entire system.

UNDERSTANDING THE ECLYPSIUM PLATFORM

The commercial platform from Eclypsium serves as an excellent use-case for world-class, modern supply chain security focused on hardware. The company is focused on helping enterprise teams trust their technology at a much deeper level, by providing improved assurance that the components used to construct information technology (IT) infrastructure have sufficient integrity and security.

This is accomplished in the Eclypsium platform through scans of the hardware, firmware, and also software components in IT systems. The objective is to improve the depth of inventory, to identify vulnerabilities that could be exploited, and to detect threats. Integrating such scans into a continuous monitoring process and connecting them with hardening tasks results in an improved supply chain security ecosystem. Key platform functions include the following:

- **Integrity Verification** – A key objective is to provide a measure of integrity verification for the underlying hardware in servers, PCs, laptops, and other devices.
- **Zero Trust Support** – The promise of zero trust can only be achieved if the endpoints, no longer protected by a perimeter, have full supply chain trust.
- **Equipment Compromise** – Avoidance of this type of attack should be a concern to any practitioner running operational infrastructure.
* **Regulatory Compliance** – The growing need to demonstrate security and compliance for endpoint devices demands attention to the full supply chain stack.

The goal of such lower-level visibility into hardware and firmware is most powerful when combined with actionable decisions regarding patching and updating devices, fixing the vulnerabilities found in components, and including results of scans into compliance and regulatory reporting. The sections below provide an overview of how the product is actually used in a supply chain context.

ASSET INVENTORY

The Eclypsium platform provides a management console designed to provide insight into assets, organized into groups. The asset type is listed along with information about the specific device including vendor, IP address, MAC address, version, and other metadata. The console includes information about security configuration, known vulnerabilities for that device, software bill of materials (SBOM) data, and status of on-going scans. Figure 1 shows a snapshot of the console.

[1] *This important NIST special publication document on platform firmware guidelines and standards can be accessed here: https://csrc.nist.gov/pubs/sp/800/193/final.*

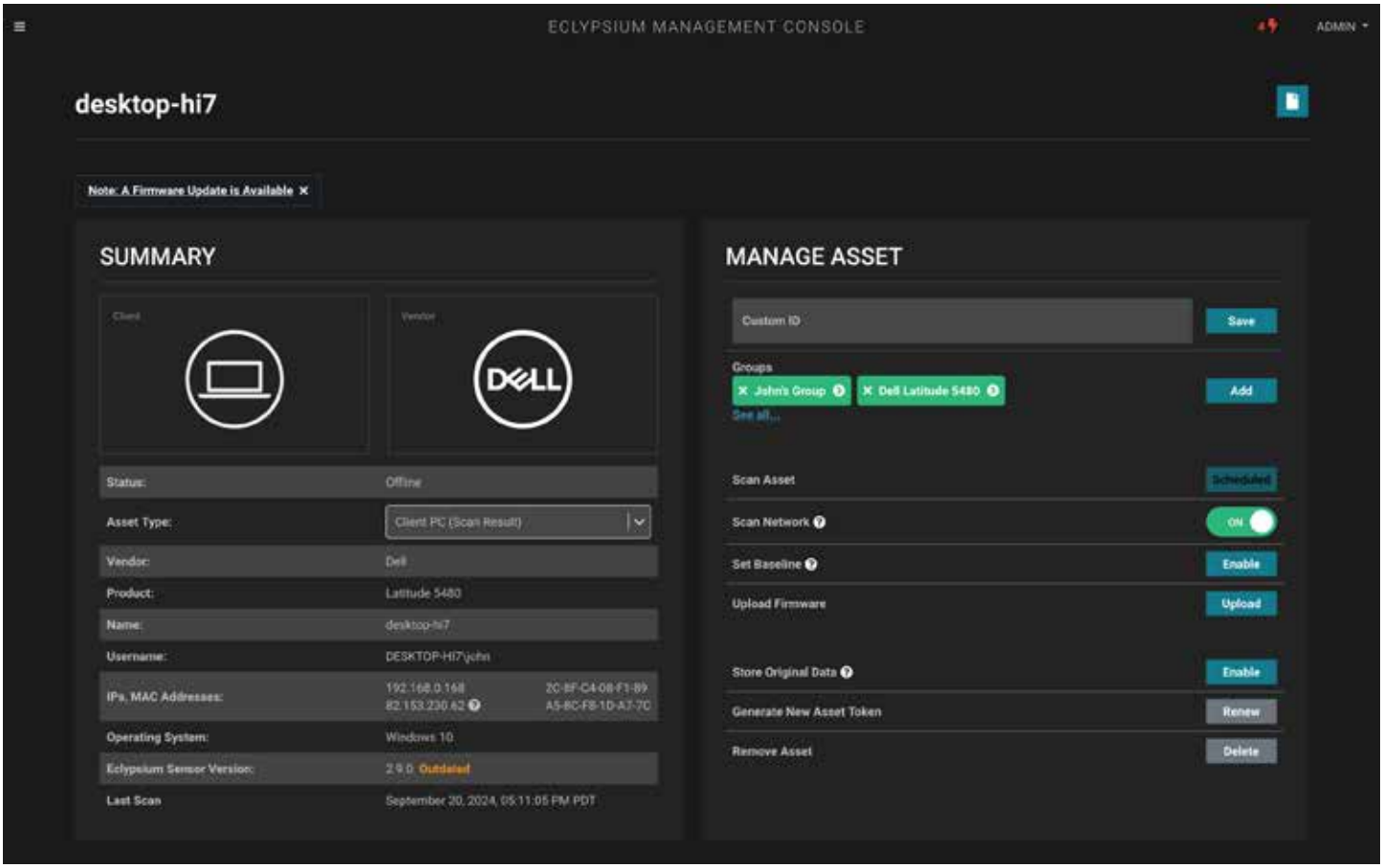

Figure 1. Snapshot View of the Console

The console snapshot in Figure 1 demonstrates the inventory focus of the platform, which should be familiar to any IT security practitioner. A common issue that emerges today in audits, assessments, and customer demands is that the local security team must provide evidence of an accurate inventory of assets. This emphasis has traditionally not included an inventory view of the hardware components, but this can be rectified with the Eclypsium solution.

CASE STUDY: FOREIGN ATTACK ON COMMERCIAL HARDWARE

To illustrate the point, consider that over a five-year period, Sophos, a well-known UK-based cybersecurity firm, engaged in a complex battle against Chinese hackers who persistently targeted its firewall products.[2] The attackers, who were ultimately traced to Chengdu, China, and linked to groups like APT41 and APT31, employed sophisticated techniques to exploit vulnerabilities in Sophos' devices.

What happened was that the hackers scanned the Internet for Sophos firewall devices with exposed management interfaces. Upon identifying vulnerable systems, they exploited unpatched firmware to gain unauthorized access. Once inside, they deployed a UEFI implant, used on test systems as well as a firmware backdoor that allowed them to maintain persistent access, even surviving firmware updates and device reboots.

The malware operated at a low level, intercepting system processes and concealing its presence from standard security tools. Sophos' investigation revealed that the malware communicated with command-and-control servers, enabling the attackers to exfiltrate data and potentially manipulate network traffic. The sophistication of the malware indicated a high level of expertise and resources, suggesting state-sponsored involvement.

[2] *See https://www.wired.com/story/sophos-chengdu-china-five-year-hacker-war/ for an excellent description of this hacking incident and its implication for hardware-level security.*

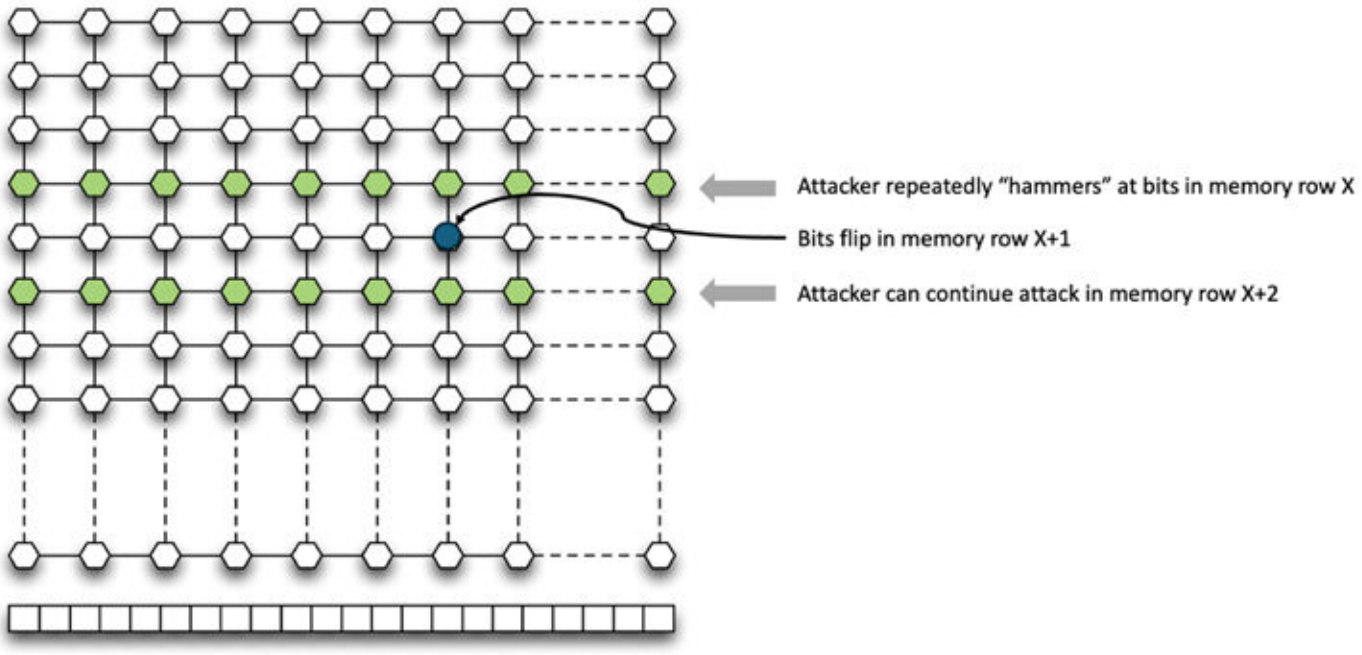

Figure 2. Rowhammer Hardware Cyber Attack

This prolonged attack underscores the critical need for robust hardware and firmware security measures. Traditional security solutions often focus on software-level threats, leaving hardware and firmware layers vulnerable. Attackers exploiting these lower layers can achieve deep system control, establish persistent footholds, and evade detection by conventional security tools. Firmware-level malware can survive system reboots and even reinstallation of operating systems, making remediation challenging.

ROLE OF ECLYPSIUM IN PREVENTING SIMILAR INCIDENTS

As suggested above, Eclypsium offers solutions designed to detect and mitigate threats at these critical layers. Their platform provides comprehensive visibility into firmware components, enabling organizations to identify vulnerabilities and unauthorized modifications. By continuously monitoring firmware integrity, Eclypsium can detect anomalies indicative of malicious activity, such as the presence of bootkits or other firmware-level malware.

Additionally, Eclypsium's solutions facilitate timely firmware updates and patch management, reducing the window of opportunity for attackers to exploit known vulnerabilities. Implementing such specialized security measures is crucial for organizations to protect against advanced persistent threats targeting hardware and firmware components.

NEXT STEPS

The advice here is that enterprise and government teams should revisit their supply chain security process to determine how additional focus on hardware might become an improved feature. For the reasons explained above, the benefits of such attention should be obvious. We thus strongly recommend that security teams take the next step today toward such supply chain enhancement – and our view is that Eclypsium offers an effective platform to support such goal.

ABOUT TAG

Recognized by Fast Company, TAG is a trusted next generation research and advisory company that utilizes an AI-powered SaaS platform to deliver on-demand insights, guidance, and recommendations to enterprise teams, government agencies, and commercial vendors in cybersecurity, artificial intelligence, and climate science/sustainability.