TAG CYBER

MAKING THE CASE FOR FIRMWARE IN THE CONTEXT OF ZERO TRUST SECURITY: AN OVERVIEW OF THE ECLYPSIUM PLATFORM

EDWARD AMOROSO, TAG CYBER

eclypsium®

TAG CYBER

MAKING THE CASE FOR FIRMWARE IN THE CONTEXT OF ZERO TRUST SECURITY: AN OVERVIEW OF THE ECLYPSIUM PLATFORM

EDWARD AMOROSO

Firmware connects and integrates the hardware and software on any computing device and thus represents a critically important aspect of any endpoint security implementation strategy. The commercial Eclypsium platform[1] is used in this report to illustrate this protection concept for enterprise endpoint devices.

INTRODUCTION

Enterprise teams have come to recognize that new solutions for cybersecurity are required in the context of work-from-home and de-perimeterized usecases. This has resulted in a rethinking of the protection features required for end-user devices, network infrastructure, cloud hosting services and software application environments. Each of these device types and their myriad supporting components must include protections that do not rely on a perimeter.

Endpoint security has been a major focus area for chief information security officers (CISOs), as well as their chief information officer (CIO) and IT operations partners. This emphasis and collaboration stems from the exposure that comes from de-perimeterization and the explosion of new devices (e.g., PC, laptop, tablet, mobile device, internet of things (IoT) device, smart TV, and so on) that need to access cloud-hosted workloads.

Such endpoint security focus has resulted in a massive portfolio of new commercial products, many of which replace traditional antivirus software products with new endpoint detection and response (EDR) offerings. This is good news for enterprise practitioners, because it introduces good implementation options for a variety of usecases, usually guided by the popular zero trust model for cybersecurity.

One aspect of this security equation that has received unusually light focus has been the firmware that underlies the design of all endpoint systems. It is the firmware that serves as the integration layer between the software and hardware on all PCs, mobile devices and other endpoint systems. As such, it represents a high-value target for threat actors, as well as an attractive means for security defenders to implement protections.

In this report, we make the case for increased focus on firmware in the context of zero trust security for endpoint protection. The target audience include the CISO, CIO and IT operations manager and practitioner, under the assumption that individuals within these groups will have a good understanding of zero trust, but relatively less familiarity with firmware. The firmware security concepts are illustrated in the context of the commercial Eclypsium platform.

A BRIEF OVERVIEW OF FIRMWARE

Firmware is a type of software that offers detailed, code-embedded instructions for how a hardware device should operate. Firmware provides the lowest level of software control in a computing device, and often the highest privileges, and is often changeable via rewrite or "reflashing" procedures. While the purpose of changeable firmware is maintenance and configuration control, such changeability introduces significant cybersecurity issues.[2] Importantly, these changes to firmware can often be initiated from the operating system layer, which is prone to compromise.

One of the most familiar types of firmware is the BIOS (basic input/output system) found on personal computers and other devices.[3] The BIOS has the responsibility to initialize hardware during the boot sequence and includes a variety of runtime services, such as testing and the setting of security and update controls. BIOS software is intimate with the hardware and is specifically designed to work with the hardware (e.g., motherboard) of the device.

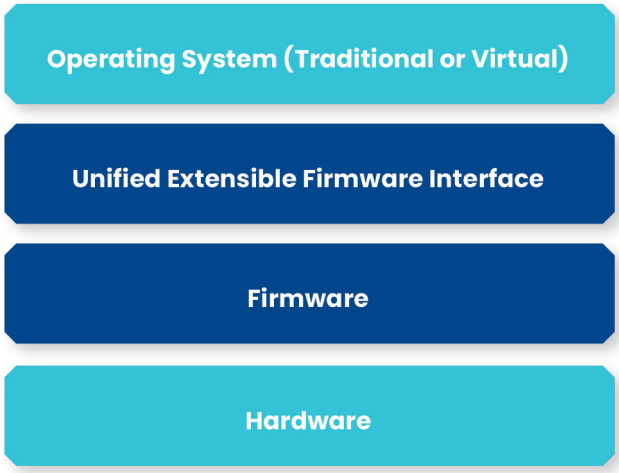

Figure 1. Component Firmware on a Modern Computing Device

To support the maintenance, diagnostics and update requirements of modern PC and device users, a technical standard known as Unified Extensible Firmware Interface (UEFI)[4] was developed as an improvement to traditional legacy BIOS. Companies such as Intel have played a major role in establishing and promoting the standard and its owner, the UEFI Forum.

With the massive proliferation of new devices connected to the internet comes a large deployment of firmware operating in many different contexts. In some cases, the firmware might be the only software running on a device. For example, some simple IoT devices might include only firmware to turn on and off its components or to control the device operation. Such ubiquity makes firmware a good place to rethink and optimize security strategies.

FIRMWARE SECURITY ISSUES

The firmware community has come to recognize the variety of cybersecurity issues that emerge in the context of protecting laptops, servers, IoT devices and many more computing systems that are vulnerable to low-level attacks. Several risk factors (listed below) make firmware attractive to offensive actors, while also making it more difficult for traditional cybersecurity solutions to detect and mitigate attacks.

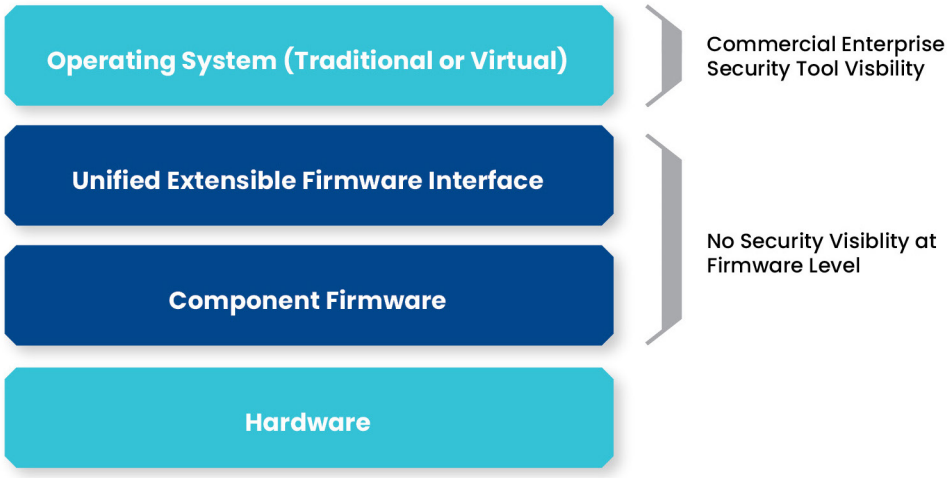

Figure 2. Firmware Resides Below the Visibility of Conventional Security Controls

Specifications
Device manufacturers do not always uniformly follow a common specification such as UEFI. Every security researcher knows that when specifications are loosely followed or not present, this introduces attack use cases for offenders. It allows scanning to detect varying responses, and it enables attacks that look for functionality that has been unaccounted for by the firmware designer.

Implementation and Updates
OEMs often ship weak configurations of firmware (for a variety of valid reasons). Unfortunately, these misconfigurations can be exploited by adversaries, rendering other security controls ineffective. Even patch updates meant to bring new functionality or to plug a security hole can end up reintroducing old vulnerabilities, or creating entirely new ones. This is similar to implementation mistakes and risks for OS and application layer updates. Firmware is simply more obscure.

Malware
Firmware is an excellent target for embedding malware into an endpoint. It provides a stable host environment for the malware, and with firmware update processes, it can even be manipulated and managed. Typical firmware-resident malware is injected via buffer overflow scenarios, or through malicious usecases such as system management mode (SMM) code injection by bad actors.

In recent years this has been especially true of ransomware, now tailored to focus on firmware-level toeholds. Examples include the Netwalker ransomware targeting Pulse Secure VPN vulnerabilities in firmware (CVE-2019-11510), Cl0p ransomware that took advantage of vulnerabilities in Accellion FTA products (see CISA alert AA21-055A), and attacks on Fortinet networking devices (see Eclypsium blog from November 2021).

Visibility
The use of firmware as a target for attack is attractive because its operation generally resides below the level at which most existing security platforms have visibility. This means that many security monitoring capabilities such as packet capture, security log analysis and behavioral analytics will not have the ability to observe anomalies or even known bad patterns in the underlying firmware execution.

For these reasons, it is imperative that enterprise teams implement controls at the firmware level to address specification, malware and visibility risks. This generally requires deliberate introduction of capabilities at the firmware level, because it is not convenient (or even feasible) to externally monitor firmware issues using conventional enterprise security systems such as the SIEM or SOAR.

ROLE OF FIRMWARE IN ENDPOINT SOLUTIONS

One of the more prominent security solutions deployed to consumer, business and government infrastructure is known as endpoint detection and response (EDR). Evolved from early antivirus software, most EDR deployments are intended to protect PCs, laptops and other user devices from becoming infected with malware carried inbound over email, web browsing or other services.

As suggested above, the visibility of EDR deployments will be primarily at the application level, with some visibility at the lower network levels. In all cases, however, EDR solutions are not designed to have visibility into the underlying firmware or hardware. Such attention is not consistent with data collection means for EDR and complicates the types of deployments that can be marketed and sold.

Figure 3. Augmenting Endpoint Security With Firmware Protection

This implies that for full coverage of endpoint security, organizations should complement their EDR solution and any other endpoint protections (e.g., antimalware software, device scanning, data encryption) with a security capability that addresses firmware threats. In the best case, this would be easily integrated into the EDR processing environment, with a common means for reporting identified anomalies or indicators.

While this approach would appear to be an obvious extension to modern endpoint security, it has not been a common solution for many enterprise teams. This might come from the relative lack of attention from popular security frameworks such as NIST CSF,[5] or it could be the result of having few commercial options. In the next section, we outline one vendor-provided firmware security platform that addresses this latter concern.

OVERVIEW OF ECLYPSIUM

Headquartered in Portland, Oregon, commercial security vendor Eclypsium is a privately held company that provides enterprise firmware and hardware cyberprotection. The Eclypsium solution addresses the challenges listed above in this report by offering an inventory of firmware and hardware security posture, scanning for vulnerabilities and required updates, and alerting when an assessment pinpoints risks requiring attention. Specific capabilities include the following:

- *Identify Device Firmware* — The Eclypsium solution supports discovery of firmware in devices to build an inventory. This is useful when performing initial triage on whether a reported firmware vulnerability is relevant to an enterprise. The firmware is fingerprinted and associated with a profile for endpoints and other types of devices.
- *Verify Firmware Security* — The platform also supports verification of firmware profiles against an Eclypsium database of vendors and configurations. This supports assessment of the firmware with suitable policies and allows enterprise teams to prioritize their endpoint and related device risk.
- *Fortify Enterprise Devices* — The solution supports proactive improvement and automated update to firmware on all endpoints and related devices. The goal is to ensure optimal configuration to avoid firmware exploitation of vulnerabilities and improper settings. A typical firmware reporting screen is shown in Figure 4.

Figure 4. Typical Eclypsium Firmware Security Dashboard

The advantages for enterprise teams using the Eclypsium platform include support for zero trust security goals that rely on secure endpoints, augmentation of vulnerability management programs that cannot update firmware, improvement of supply chain security through better tracking of firmware posture, support for work-from-home initiatives that depend on endpoint security, and augmentation of patching programs that have blind spots to endpoint firmware.

ACTION PLAN FOR ENTERPRISE

Any enterprise team that relies on endpoints — and this includes essentially all enterprise teams in every sector and of every size and scope — is advised to develop a plan for addressing firmware risk. This should include the following steps:

Step 1: Inventory
Enterprise teams should assess whether any existing solutions are in place to identify and verify their firmware, especially for endpoints. For most teams, this step will result in little or no existing support.

Step 2: Vendor Review
The enterprise should then perform an assessment of which vendors have offerings that can help secure firmware on endpoints. As suggested above, Eclypsium should be included in this process. TAG Cyber analysts[6] are always available to research as a service (RaaS) customers to assist in this step.

Step 3: Implementation Plan
The final step involves establishment of an implementation plan to move forward with a proof of concept (POC) and eventual deployment of a commercial solution such as Eclypsium's to the endpoints supporting the company. TAG Cyber's expert analysts can also assist in the development of such plans.

ABOUT TAG CYBER

TAG Cyber is a trusted cybersecurity research analyst firm, providing unbiased industry insights and recommendations to security solution providers and Fortune 100 enterprises. Founded in 2016 by Dr. Edward Amoroso, former SVP/CSO of AT&T, the company bucks the trend of pay-for-play research by offering in-depth research, market analysis, consulting and personalized content based on hundreds of engagements with clients and nonclients alike—all from a former practitioner perspective.

[1] *https://eclypsium.com/*

[2] *Many good internet resources exist for learning about firmware. Good support references are included, for example, in the Wikipedia entry for firmware at https://en.wikipedia.org/wiki/Firmware.*

[3] *https://whatis.techtarget.com/definition/BIOS-basic-input-output-system*

[4] *https://uefi.org/*

[5] *https://www.nist.gov/cyberframework*

[6] *https://www.tag-cyber.com/*