AXIADO

Cybersecurity and Ransomware Protection Starts with Hardware & AI

Gopi Sirineni, President & CEO
Axiado Corporation

AXIADO.COM

SEPTEMBER 2023

In the dynamic landscape of cybersecurity, the relentless battle against ransomware is a testament to the evolving nature of cyber threats. Ransomware attacks have undergone a metamorphosis, emerging as highly sophisticated adversaries that excel in the art of stealth and evasion. In 2022 it is reported that an AVG malicious ransomware attack eluded detection for an astounding 324 days, with an additional 91 required to regain control. The protracted concealment of such an attack can spell calamity for organizations, underscoring the imperative for swifter and more intelligent detection mechanisms.

The scale of the ransomware issue is staggering, with an estimated 4,000 attacks occurring daily. This statistic is conservative as it only accounts for reported incidents, leaving countless others unrecorded. Notorious ransomware attacks such as WannaCry, NotPetya, Sodinokibi, SamSam, the Colonial Pipeline Ransomware Attack and Kronos have etched their names in the annals of cybersecurity history.

What exactly is ransomware in layman's terms? Picture an unauthorized actor gaining access to your system, implanting malicious software that ruthlessly denies you access to your device and encrypts your invaluable data. The outcomes can range from rendering your system inaccessible to outright data theft or deletion. In nightmarish scenarios, these malevolent actors take superuser or admin privileges, seizing complete control of your system and demanding a ransom for its release. Victims often have no choice but to pay the ransom in desperation.

However, ransomware has evolved far beyond mere file encryption and Bitcoin demands. Modern ransomware tactics have embraced harassment and introduced double and triple extortion schemes.. These multifaceted approaches leave conventional counsel, such as maintaining secure backups, woefully inadequate in the face of rapidly evolving threats.

Let's delve into the intricate web of shortcomings and far-reaching consequences wrought by ransomware attacks:

- **Delayed Patching:** Even after a ransomware attack becomes headline news, it can take months for cybersecurity experts, including the chief information security officer (CISO) or chief security officer (CSO), to ascertain if their own systems are susceptible to a similar assault. This time lag leaves enterprises vulnerable to potential copycat or follow-up attacks.
- **Recovery Challenges:** Once a ransomware attack has unfolded, victims often find themselves with no recourse other than acceding to the ransom demands, especially if critical data is at stake.
- **Forensics Conundrum:** Ransomware attacks are executed with meticulous precision, often leaving behind no discernible traces. This meticulous erasure of digital footprints renders forensic analysis a futile endeavor, leaving victims in the dark regarding the perpetrator's identity and methodologies. Furthermore, there is no guarantee that the malevolent actors will refrain from returning or disseminating their tactics to other nefarious entities after receiving the ransom.
- **Productivity Loss and Replacement Expenses:** Even after the ransom is paid, compromised systems remain tainted and often unusable. This predicament necessitates the migration of data to fresh systems, incurring both productivity losses and replacement costs.
- **No Safe Disposal/Decommissioning Methods:** The specter of threat actors gaining access to discarded systems looms large, potentially providing them with the keys to the kingdom through traced IDs or credentials for future attacks on enterprise systems.

MALICIOUS ACCESS TO THE SYSTEM

How do these malevolent actors insinuate themselves into systems in the first place? The most prevalent method is through phishing emails. Victims frequently and unwittingly succumb to the bait presented in these deceptive emails, either by clicking on malicious links or falling prey to drive-by downloads while visiting compromised websites. This seemingly innocuous lapse in judgment serves as the gateway for the introduction of the ransomware variant into their device, setting the stage for an impending catastrophe.

In some instances, cybercriminals resort to physical breaches to execute inside-out assaults, further compounding the complexity of the security landscape. In all these scenarios, the adversary gains ingress into the system through some form of credential compromise, whether it is through the act of clicking on malicious links or the loss of credentials.

These vulnerabilities, often referred to as "ports of entry," can manifest in various system components, encompassing software applications, drivers, kernel code, operating system code or firmware code. Cybercriminals adeptly exploit these entry points, establishing themselves as administrators and subsequently setting their sights on the "money chest" – the repository of invaluable content ensconced within the hardware platform, akin to a bank thief targeting the vault.

SOFTWARE-ONLY ZERO-TRUST SOLUTIONS

While many existing software-only solutions strive to exert control over these potential ports of entry, cybercriminals continually adapt and circumvent these defenses. Many of these solutions purportedly adhere to the zero-trust model, relying on the sanctity of the hardware root of trust (ROT). However, there have been distressing instances where even the ROT itself has been compromised, casting doubt upon the efficacy of these defenses.

This evolving threat landscape has engendered a burgeoning demand for innovative solutions that complement existing software-based defenses. These novel solutions need to offer a more robust layer of protection against ransomware attacks by operating directly within the hardware.

TODAY'S DATA CENTER HARDWARE SECURITY

How does the security of hardware currently stand? Within the realm of datacenter infrastructure solutions, a pivotal component known as the "control and management" platform assumes the responsibility of ensuring system integrity during the boot process. Additionally, it manages identity keys that facilitate attestation and authentication of runtime applications. Although this architectural paradigm has demonstrated its effectiveness over the course of 25 years, it now faces new and formidable challenges.

Within the ecosystem of a data center server system, two distinct categories of network ports coexist: "data ports" and "control and management" ports. The former, which engage in external communications, are typically fortified by firewalls. These firewalls, while efficacious as perimeter security, primarily scrutinize packet headers, deploying packet header analysis as their primary means to defend against potential threats. However, the crux of malicious activity often remains ensconced within the payload of these packets, eluding the prying eyes of conventional security measures.

EMERGENCE OF DATA PROCESSING UNITS

The introduction of data processing units (DPUs) has proven revolutionary over the past decade. Companies such as Nvidia, Broadcom, Marvell and Fungible have pioneered DPUs that excel at conducting deep packet inspections. This innovative approach significantly enhances security by meticulously filtering out malware. However, as IT professionals transition to the cloud and necessitate remote access to these crucial "master key" ports, they frequently encounter these ports ensconced behind the same or similar firewalls. Solely relying on traditional firewall technology to shield these vital "control and management" ports is precarious, given the inherent limitations of such an approach.

A NEW APPROACH: SECURE, AI-DRIVEN HARDWARE

In this rapidly evolving threat landscape, Axiado saw an opportunity to provide a new approach and embarked on a mission to conceive a solution that would fortify the existing security framework. This solution aspired to be reliable, self-learning, self-defending, AI-driven, and fundamentally anchored within the hardware. This ambitious vision ultimately gave birth to the concept of Trusted Compute/Control Units (TCUs), a meticulously crafted solution designed from inception to deliver comprehensive security for data center control and management ports.

TCUs harness the power of intelligent, on-chip AI to thoroughly scrutinize access sessions, detect anomalies, and monitor the boot process for potential side-channel attacks. These side-channel attacks encompass subtleties like voltage glitches and thermal anomalies. TCUs respond promptly to identify and neutralize these insidious threats. Furthermore, TCUs have been trained to recognize behavior patterns that are emblematic of known ransomware attacks, a capability honed through the analysis of hardware traces. This pattern recognition enables TCUs to promptly detect and thwart ransomware attacks in real-time, mitigating the potential damage.

PHYSICAL PORT AND SESSION PROTECTION

TCUs perform continuous and vigilant monitoring of physical ports, user sessions and application interactions. They assimilate contextual information to discern any behaviors indicative of a potential threat. This robust defense mechanism is adept at analyzing, detecting and thwarting a wide spectrum of threats, thereby safeguarding critical infrastructure against not only side channel attacks but also insider threats.

However, TCUs do not stop at merely fortifying against ransomware and other threats; they offer a panoply of value-added features that confer tangible benefits for various stakeholders, including cloud service providers (CSPs), colocation data centers (colos), OEMs and enterprises.

HARDWARE-BASED FORENSICS

TCUs capture hardware-based forensics data spanning from the boot phase to runtime. This trove of invaluable data assumes paramount significance, particularly in the aftermath of an attack. It serves as a critical resource for post-incident analysis, shedding light on the nature of the attack and the tactics employed by the attackers, while fortifying defenses for future endeavors.

ANOMALY AND RANSOMWARE DETECTION

TCUs excel in the detection of anomalies within the control and management facets of the system. They serve as early warning systems capable of identifying patterns indicative of potential ransomware attacks. Thanks to their advanced artificial intelligence, TCUs promptly flag irregularities, alerting administrators to potential threats. These units compare detected anomalies to known and trained vulnerabilities, enabling them to discern and halt attacks before they can inflict damage.

DETECT AND ISOLATE

TCUs have the unique capability to detect and isolate compromised systems with a granular level of control. This extends to applications, containers or virtual machines when abnormal behavior is detected. This granular control empowers IT professionals with the agency to decide whether to permit these entities to continue their operations or to intervene proactively to mitigate potential risks. This security feature not only enhances safety but also fosters efficient and effective system management.

HARDWARE OWNERSHIP MANAGEMENT, COMMISSIONING/DECOMMISSIONING

TCUs introduce a transformative functionality by facilitating hardware-based ownership transfers through Physical Unclonable Function (PUF) engines. This feature assumes pivotal importance in ensuring the security of the commissioning and decommissioning processes throughout the platform's lifecycle. It furnishes a comprehensive solution for the secure management of hardware assets, addressing concerns pertinent to data integrity and changes in ownership.

EMPOWERING ORGANIZATIONS WITH A HOLISTIC DEFENSE STRATEGY

Axiado's TCUs provide a formidable arsenal of advanced features that collectively augment the security, visibility and control of systems for a diverse array of stakeholders, encompassing CSPs, colos, OEMs and enterprises. These features encompass hardware-level forensic data monitoring, the early detection of anomalies, granular control over system components and secure hardware ownership transfers. This holistic ensemble of capabilities constitutes a robust and intelligent security solution tailor-made for the demands of modern data center infrastructure.

In the swiftly evolving arena of cybersecurity, Axiado's TCUs assume the mantle of innovation and resilience. These units do not merely protect systems and data; they empower organizations with a multifaceted defense strategy that converges cutting-edge hardware-level monitoring, anomaly detection, granular control and secure ownership management.