TAG CYBER

DESIGN OF SECURE PC ENDPOINTS: AN INTRODUCTION TO HP WOLF SECURITY

EDWARD AMOROSO, TAG CYBER

HP WOLF SECURITY

TAG CYBER

DESIGN OF SECURE PC ENDPOINTS: AN INTRODUCTION TO HP WOLF SECURITY

EDWARD AMOROSO

Security capabilities integrated into the PC stack, below the OS, are shown to provide more robust endpoint protection. The HP Wolf Security offering exemplifies this approach for a modern zero trust endpoint computing environment.

INTRODUCTION

The enterprise community has begun to prioritize endpoint security to compliment zero trust approaches to networking. Previously it was feasible for endpoint PCs and other devices to simply be secured by perimeter controls such as firewalls. However modern approaches to work-from-home and virtualized access do not enjoy such blanket protection. Endpoints must therefore include embedded and integrated controls.

One aspect of endpoint security that has received less emphasis than anti-virus and other more familiar controls is the protection design of the underlying PC stack. This is surprising since early efforts to develop security designs included attention to developing a trusted hardware base as a fundamental aspect of the security model.

In this report, we re-introduce the reader to the foundational aspects of protecting PCs with emphasis on the underlying security functionality that can be integrated and embedded into the underlying hardware. We illustrate the discussion with HP Inc.'s Wolf Security commercial offering, which creates a highly secure PC environment for end-users.

WHAT IS A TRUSTED COMPUTING BASE?

The original concept of anchoring system security into an underlying trusted base was invented in the 1980's as part of the US government's research into secure system design. The goal was to find ways to ensure that the most important functions in a system (usually a small set of core capabilities such as rebooting) could be counted on to have high assurance. Such assurance would come from heightened scrutiny and economy of design.

As a result, the so-called trusted computing base (TCB) soon became part of the security lexicon and was an important aspect of secure system architecture. Closely related to the concept of a security kernel, the TCB as implemented in a layered design provides a trusted foundation on which to deploy additional functionality, including support for the highest application layer (see Figure 1).

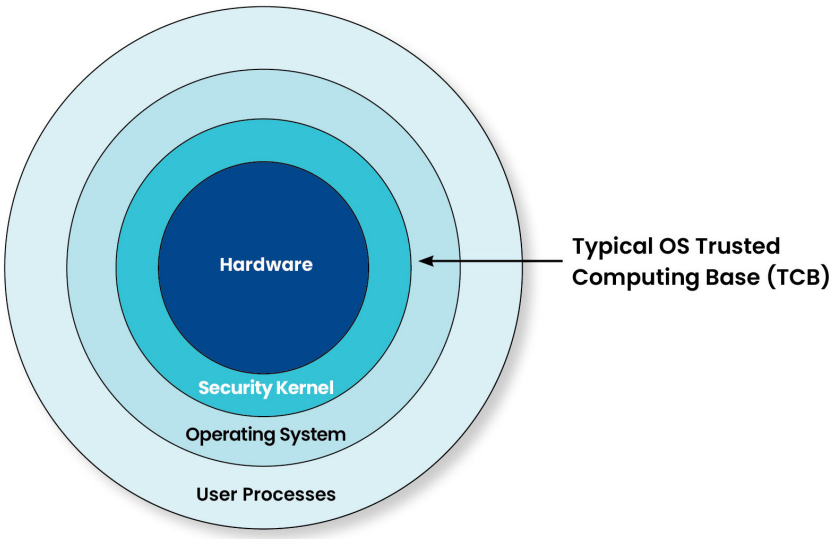

Figure 1. Typical Trusted Computing Base for Operating System

A key learning from the traditional TCB is that security is best established foundationally at the hardware level, and then exported upward to higher levels of firmware and software to reduce cyber risk. High assurance is established at the lower levels through verification methods that focus on software integrity measurements for computing activities such as rebooting, start-up, and other administrative and maintenance tasks.

- Hardware / Firmware - Offering high assurance that security policy controls will be enforced rigorously is best achieved at the lowest and deepest layers of the TCB – and for PCs, this implies hardware and firmware security. While assurance can never be perfect, users can maximize confidence in enforcement by demanding that controls be rooted in the underlying system hardware and firmware design and configuration. The basic concept is to establish a high integrity platform upon which the security stack can be built with confidence, with capabilities anchored in hardware to detect attacks at the deepest level, and to recover from successful integrity breaches. Typical capabilities in a modern PC should include hardware roots of trust for secure storage, certificates, reporting, firmware update, integrity breach detection, and recovery[12]. Hardware and firmware should also be designed for secure remote management at scale in a modern hybrid environment, enabling configuration integrity checks, hardware tamper controls, and secure logging facilities.

- Security Kernel – Above the firmware, a security kernel is established to create the execution platform for applications. While this kernel can be created within the operating system, a more secure approach is to use a hypervisor, which has a smaller attack surface and facilitates more flexible and robust leverage of hardware-based security functions. As in data center or cloud application hosting, the hypervisor creates trust boundaries between applications, isolating malware from sensitive data running in parallel on the same platform. On modern endpoint PC architectures, hypervisors can also be used to contain threats from risky activities, or to provide protection of the highest-value applications and data even if other parts of the OS are compromised.

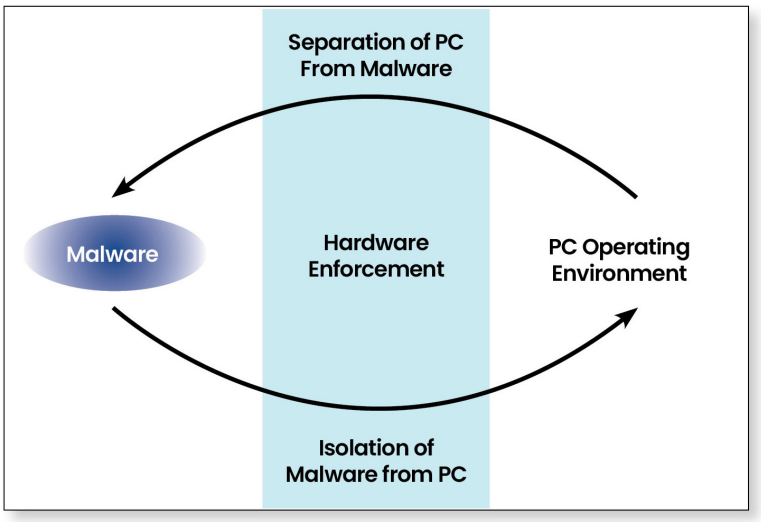

Figure 2. Foundational Architecture of a Secure PC

Perhaps the most powerful aspect of this foundational protection for a secure PC is that it ensures that higher-level investments in endpoint security software are not undermined by low-level hardware and firmware attacks. By some estimates, the market for endpoint security tools totaled $10B and growing,[3] so this goal to protect that financial investment is significant. In the next section, we show how the HP Wolf Security system accomplishes this goal in a commercial deployment.

CASE STUDY: HP WOLF SECURITY

With its long history in computing, HP Inc. serves as an illustrative case study on secure endpoint design. Over the years, HP has continuously led innovation in the security architecture of PCs at the hardware and firmware level, adding capabilities such as hardware-based cryptographic validation and system assurance. Most recently, HP's acquisition of Bromium added the ability to use virtualization at the higher layers of the endpoint stack to isolate malware from PC resources using strong hardware-based enforcement. The same technology is also used to isolate "known good" applications from attack.

One of the major tenets of the HP approach has been to apply zero trust security principles from the deepest level of a PC architecture, assuming perimeter and software protections are not sufficient to deliver PC security in the modern hybrid world. The balance of this report will describe the HP endpoint security stack, starting at the lowest level and working upwards.

HP'S ENDPOINT SECURITY STACK – A RESILIENT ARCHITECTURE FOR APPLICATION PROTECTION

The HP Endpoint Security Controller (0): This secure micro-controller is in control of the computer (even when the PC is off), providing a secure platform root of trust for the HP and customer security stack above it. This physically isolated and cryptographically

protected hardware microcontroller provides a hardware root of trust for detection, update, recovery, and manageability, all operating below the OS. This is in addition to the industry standard Trusted Platform Module (TPM) root of trust for storage and reporting. The HP Endpoint Security Controller is third-party certified and provides hardware-enforced security anchors to higher layer capabilities.

HP Sure Start (1): In its 6th generation, Sure Start is HP's integrity breach detection and self-healing capability for PC BIOS firmware and settings. When the PC is first powered on, HP Sure Start holds the CPU in reset, as HP believes the CPU should not execute the UEFI firmware until it has been validated. HP Sure Start validates the firmware and firmware settings are authentic and match the private copy, which has been electrically isolated from the CPU. If there is corruption, HP Sure Start will restore the correct firmware and settings from the private copy. HP has designed Sure Start to be anchored in the security of its Endpoint Security Controller, and to be fully manageable according to the organization's remediation policy.

HP Sure Admin (2): This introduces the use of strong public key cryptography instead of relying on static passwords for secure BIOS administration. In this scheme, BIOS passwords are replaced with a public key managed by the IT security team. Secure communication and remote management of BIOS firmware configuration can therefore be enforced without the risk of deploying and managing passwords. The solution also enables tech support and operators to authenticate to the BIOS at the local machine using a one-time authorization mechanism controlled cryptographically by the enterprise.

HP Sure Recover (3): This offers the ability for the hardware to securely install, re-install, or recover an entire OS, with built-in cryptographic integrity verification. Built using the Endpoint Security Controller, this capability can securely download a corporate image from the Cloud when OS recovery is required, ensuring the machine can always be recovered to a known good state. Alternatively, the recovery image can be pre-staged on secure embedded flash, enabling fast recovery regardless of network conditions. Sure Recover can be pre-configured at the factory and enables IT to lock hardware configuration for autonomous secure recovery by end-users regardless of their location.

HP Sure Click (4): Application Isolation Using Micro-Virtualization

The HP Sure Click Enterprise platform involves use of disposable virtual machines that are created on demand to isolate risky tasks, such as opening email attachments and clicking on links and downloads. The task is contained, hence if it turns out to be malicious the attacker cannot corrupt the PC, exfiltrate data or perform lateral movement. The isolation is enforced by the CPU hardware, making it very resilient to software-based circumvention. The result is a high-security processing environment that enforces separation.

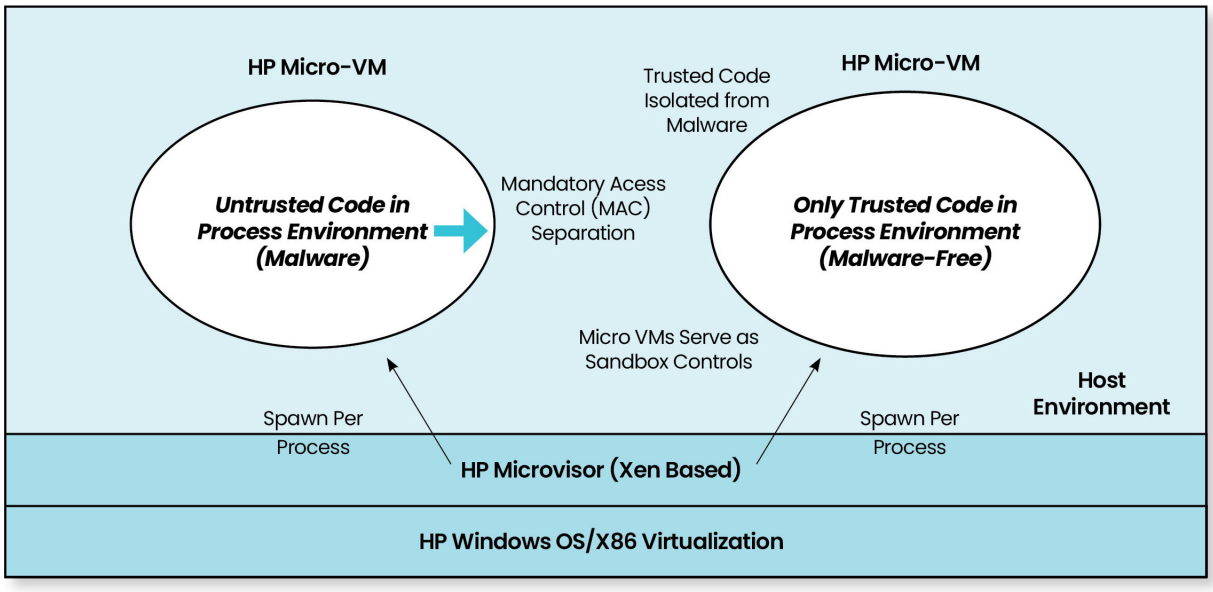

Figure 3. Isolation Using Micro-VM

Micro-VMs are spawned by the HP host environment on a per-task basis. If malware is present in a micro-VM, perhaps as a result of a user clicking on a bad link, this malicious code is isolated from the host environment by the mandatory access control (MAC)-based isolation enforced by the hypervisor. Trusted code is thus separated from untrusted code, which allows safe co-existence on the same system. When the task is completed, the micro-VM is destroyed, taking the malware with it.

A parallel HP offering known as Sure Access Enterprise uses the same virtualization technology to protect "known good" remote access applications from everything else on the PC. Remote IT administration for example creates an ideal point of attack for PC malware: It can easily leverage the remote access connection to move laterally, plant code for persistence, and exfiltrate data. SAE isolates these remote access sessions from the rest of the PC stack and applications, so that they cannot be exploited. This provides a powerful compensating control for securing privileged user activity.

Ultimately, HP Wolf Security is designed to reduce the overall attack surface of the endpoint, primarily through low level functionality rooted in trusted hardware. This provides a powerful complement to any additionally deployed endpoint security tools.

REFERENCES

https://press.hp.com/us/en/press-releases/2021/launch-hp-wolf-security.html

https://www.forbes.com/sites/adrianbridgwater/2015/07/14/what-is-micro-virtualization-and-why-is-it-good-for-windows-10/?sh=41ac4c1c4a14

ABOUT TAG CYBER

TAG Cyber is a trusted cyber security 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 non-clients alike—all from a former practitioner perspective.

[1] *The Trusted Computing Group defines the Trusted Platform Module hardware root of trust and associated trusted computing architecture*

[2] *See NIST guidance on hardware design for firmware resilience and roots of trust for update, detection and recovery at https://csrc.nist.gov/publications/detail/sp/800-193/final*

[3] *See https://www.statista.com/statistics/497965/endpoint-security-market/*

4AA8-1318ENW