White Paper

Information Technology
Cybersecurity

Intel® Hardware Shield – Below-the-OS Security

Intel Business Client Platform Security Marketing

Introduction

This document covers security features in Intel® Hardware Shield on the Intel vPro® platform and how they provide foundational security in the hardware and firmware layers below the operating system. It covers both software and hardware security capabilities.

Intel® Hardware Shield Overview

The Intel vPro platform delivers hardware-enhanced security features that help protect all layers in the computing stack. Intel Hardware Shield, exclusive to the Intel vPro platform, helps reduce the attack surface of the system by locking down system critical resources to help prevent malicious code injection from compromising the OS, helping to ensure the OS runs on known hardware, and delivering hardware-to-OS security reporting to enable the OS to enforce a more comprehensive security policy. In addition, Intel Hardware Shield offers advanced threat protection features that can perform active memory scanning to help improve the detection of advanced threats while reducing false positives and minimizing performance impact.

Intel Hardware Shield comes ready out of the box with every Intel vPro platform. Not only does Hardware Shield come ready on every vPro platform, these technologies are designed to work with the first system power on. No ISV application is needed to enable or make use of these technologies. Intel Hardware Shield has three main components: advanced threat protections, application and data protections, and below-the-OS security.

Advanced Threat Protections:

This security feature is hardware-powered and provides AI-enabled threat detection without noticeable performance degradation for the user. Advanced threat protection features provide proactive scanning for hard-to-detect threats, like ransomware and cryptojacking.

Application and Data Protections:

This is hardware-powered virtualization-based security for applications and the operating system. In addition to protecting data, this feature also provides performance enhancements.

Below-the-OS Security:

Intel Hardware Shield can lock down memory in the BIOS against firmware attacks and enforces a secure boot at the hardware level. These below-the-OS security features are set-up by the PC manufacturer, so IT departments and users can take advantage of them right out of the box.

Why Intel Hardware Shield?

Malware is a consistent and growing threat to IT. While the mechanisms of malware vary, they all seek to corrupt systems and disrupt business, steal data, or usurp control of platforms. As companies adopt more Bring Your Own Device (BYOD), plus virtualized, shared, and multi-tenant infrastructure models, the perimeter of the traditional network infrastructure is more dispersed and exposed to vulnerabilities. Similarly, traditional approaches of looking for "known bad" elements (the approach of most anti-virus or anti-malware programs) are only partially effective at coping with the increasing volume and sophistication of attacks today.

Enterprise businesses need integrated software and hardware solutions, and that is where Intel Hardware Shield comes in, Intel Hardware Shield, available exclusively on the Intel vPro platform, provides enterprise-class security all businesses require.

Current endpoint detection & response (EDR) solutions can help protect against attacks that happen at the software application and operating system (OS) level, but hackers continue to evolve their techniques and move increasingly towards the hardware infrastructure. Organizations of all sizes need to invest in better technology: hardware, BIOS/ firmware, hypervisor, VMs, OS and applications.

Hackers have begun targeting firmware, below what the OS or security software running on the OS can see and monitor. A compromised PC can offer up access identity, encryption keys, and passwords, in addition to sensitive data. Highlighting the scope of that threat, VentureBeat reported in December 2019. *"Over the last three years, the number of firmware vulnerabilities has grown nearly five-fold, according to the NIST National Vulnerability Database. Mobile and remote workers on public networks may be especially exposed; same with those using non-company devices. Unfortunately, these firmware incursions can be undetectable by traditional antivirus programs, security practices, and threat systems models The stakes are high: Much critical corporate data resides on unprotected desktops and laptops; some 61% of data breaches involve stolen credentials or phishing."*[1]

Security starts with Intel Hardware Shield. Businesses can focus on what is important, knowing that they are better able to defend themselves against emerging threats. The security improvements with Intel Hardware Shield extend to improving protections against malware targeting the BIOS on the way to a data breach.

What are Below-the-OS Security Technologies?

The category of Intel Hardware Shield below-the-OS technologies is comprised of several security features. These include Intel® BIOS Guard, Intel® Boot Guard, Intel Firmware Restart / Recovery, Intel® Platform Trust Technology (Intel® PTT), Intel® Runtime BIOS Resilience, Intel® System Security Report, Intel® System Resources Defense, and Intel® Trusted Execution Technology (Intel® TXT).

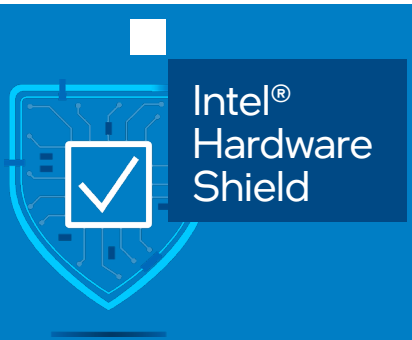
Intel BIOS Guard

Intel BIOS Guard is a BIOS Flash update hardening technology that creates a very small trust boundary for the BIOS image updates to Flash, eliminating the System Management Interrupt (SMI) handler and nearly all of the POST BIOS as well. It is related to Intel Boot Guard in as much as it provides a very strong update mechanism for the Initial Boot Block (IBB), (as well as the rest of the BIOS), which Intel Boot Guard verifies.

This small trust boundary reduces the risk of Flash based attacks in Intel vPro platforms, including permanent subversion and/or denial of service attacks. Attacks on platform BIOS could result in security problems including BIOS based Rootkits, denying bring-up of the system, and persistent platform denial of service. Furthermore, while some platform components can perform a cryptographic signature check on firmware as it is loaded from Flash, the BIOS typically does not. Therefore, it is possible that a wide variety of security problems can be introduced into the platform if the BIOS Flash gets maliciously overwritten.

While the Flash update process is still done in System Management Mode (SMM), it restricts the privileges of SMM to protect Flash update authentication and write. In other words, SMM is required to perform a role in the update process, but it cannot interfere with the actual update.

In client computers, a Model-Specific Register (MSR) is used to control write and erase operations to the BIOS Flash. This feature constrains Flash programmability to the BIOS System Management Interrupt (SMI) handler. When an update operation is complete, a MSR write by the SMI handler causes the PCH to inhibit Flash write and erase operations. Update authentication is performed by the SMI handler. From a security perspective, this means Flash protection is no Intel BIOS Guard uses a similar approach to control SPI Flash write



Below-the-OS Security
Provided by BIOS & Boot Flow Protection Technology

- **Intel® Bios Guard**
- **Intel® Boot Guard**
- **Intel® Firmware Guard**
- **Intel Firmware Update/ Recovery**
- **Intel® Platform Trust Technology (Intel® PTT)**
- **Intel® Runtime BIOS Resilience**
- **Intel® System Resources Defense**
- **Intel® Trusted Execution Technology (Intel® TXT)**
- **Intel® System Security Report**
- **Intel® Tunable Replica Circuit – Fault Injection Detection**

and erase capability. However, instead of binding Flash updates to SMM, with Intel BIOS Guard, the MSR used to generate the Flash open/close special cycles is only writeable from an Intel-signed (and hardware-verified) BIOS Guard Authenticated Code Module (ACM). Update authentication is also performed by the Intel BIOS Guard module. This yields a much smaller attack surface and a much more defensible environment from which to perform Flash operations. Furthermore, an Intel BIOS Guard enabled system does not allow host Flash writes from any other environment.

Intel Boot Guard

Intel Boot Guard provides a key element of hardware-based boot integrity that meets the Microsoft Windows requirements for UEFI Secure Boot to mitigate unauthorized BIOS boot block modifications.

Intel Boot Guard doesn't prevent access, or even writes to the Initial Boot Block (IBB), rather it verifies the correctness of this code before the CPU runs the IBB. The related keys and policies reside in fuses. Intel Boot Guard, as shown in Figure 1, only reads on the BIOS Boot Block. It fortifies the Root of Trust. Attacks on the root are thus stopped.

When booting with Intel Boot Guard enabled, the boot integrity is unalterable since it is anchored in hardware fuses. Intel Boot Guard becomes a hardware root of trust adding robustness to the chain of trust process where UEFI boot process cryptographically verifies and/or measures each software module before executing it. The result of the Intel Boot Guard process is a reduction in a chance of malware exploiting the hardware or software components on the platform.

Intel Boot Guard establishes a strong, hardware-based Static Root of Trust for Verification and Measurement. Both roots are established before control is passed to the reset vector (before executing a single BIOS instruction). This is accomplished in Intel Boot Guard by cryptographically verifying /measuring the first portion of BIOS code executed out of reset.

The policies of Intel Boot Guard are rooted in Field Programmable Fuses, making them unalterable for the lifetime of a platform. Once provisioned, Intel Boot Guard cannot be disabled, and provisioned policies cannot be spoofed.

Intel Boot Guard excludes the Serial Peripheral Interface (SPI) bus from the Trusted Computing Base, helping to detect corruption of the BIOS image in a Flash update or during transfer.

Intel® Trusted Platform Module 2.0 (Intel® TPM) is supported by Intel Boot Guard as part of a measured boot. When performing a measured boot, Intel Boot Guard can execute first measurement from Intel TPM locality 3 thus providing the attester with an unspoofable indication of a strong, hardware- rooted, Static Root of Trust Measurement.

Recently, Intel Boot Guard was updated with SPIRAL. SPIRAL stands for "Security Protocol with Independent Recovery Algorithm". It is a protocol between the CPU and the Intel® Converged Security and Management Engine (Intel® CSME). The SPIRAL-protected Intel Boot Guard significantly increases difficulty of compromising Intel Boot Guard, even for attackers with advanced skills and tools.

Intel Firmware Guard

Hackers often exploit firmware vulnerabilities to bypass antivirus software. Rapid and resilient firmware updates can help protect platforms from these threats. But integration and validation costs can delay OEM response to firmware vulnerabilities, and customers may resist updating firmware out of fear of crashing their systems. To address that, Intel Firmware Guard facilitates OEMs in delivery of critical, recoverable firmware updates to their customers, as quickly as possible.

Intel Firmware Guard provides the ability to update the firmware on an end user's system and also recover from a firmware failure. Firmware updates are signed by OEM Intel, deployed by the PC manufacturer as a UEFI Capsule and applied in a fault-tolerant manner on the end user system. In case of a failure from power interruption during the update, the system automatically boots to a last known good state and restarts the firmware update process, all without user intervention. Along with fault-tolerant updates, Intel Firmware Guard also features post firmware update recovery and rollback. Upon detection of an update failure, the UEFI BIOS triggers a seamless recovery from a copy of the firmware. On the next power-up, boot-up happens from the recovery firmware that reads the status of the previous failure and restores the system to a good state.

Intel Platform Trust Technology

Intel PTT is a form of a Trusted Platform Module (TPM). This feature of Intel Hardware Shield includes the capabilities of a TPM 2.0 within Intel vPro platforms for storing keys, passwords, and digital certificates. Intel PTT is a credential storage and key management solution to meet Windows OS hardware requirements. It is optimized for low power consumption in the S0iX environment. Intel PTT supports the Trusted Computing Group 2.0 standard and FIPS 140-2 certifications.

Intel PTT is implemented in firmware running on a coprocessor such as the Intel CSME in the Intel vPro platform. The Intel CSME provides an isolated, platform trusted execution environment which is required to support several basic security services including secure boot, attestation, and content protection.

BitLocker is supported by Intel PTT for storage drive encryption. Intel PTT also supports Microsoft Windows OS requirements for TPM 2.0. To the Windows OS and application software, Intel PTT looks and acts like a TPM 2.0. Because Intel PTT is integrated into Intel CSME, it has direct access to certain fuses and resources without having to go over a potentially attackable user-accessible bus.

Intel Runtime BIOS Resilience

Intel Runtime BIOS Resilience is a unique feature of Intel Hardware Shield that helps PC manufacturers enforce a below-the-OS policy. Intel Runtime BIOS Resilience key value is to reduce the risk that malware can be injected into the SMM environment at runtime. It does so by setting up the page table with a policy that uses the security properties of paging and then locks the page table so it cannot be modified later during runtime. End users benefit because the platform is more secure against attacks launched from SMM.

If the platform implements a policy such that memory that is used by the OS is not mapped in the SMM page table along with Intel Runtime BIOS Resilience, Intel Runtime BIOS Resilience will 'lock' such a policy. The entry point and all the code within SMM becomes locked down. In addition, the memory map and page properties get locked down. The OS memory then becomes not accessible from SMM at all. This makes it challenging for an attacker to attempt at runtime to modify the page table to map memory that is used by the OS.

Prior to this technology, any code running in SMM could dynamically allocate memory as needed. This means if an attacker got into SMM, they could potentially allocate memory, gain visibility into the OS, and inject malware.

Intel System Resources Defense

Intel System Resources Defense extends the ability to enforce resource access policies for System Management Interrupt (SMI) handler firmware beyond memory resources covered by Intel Runtime BIOS Resilience.

SMI handers, historically, are in the trusted compute base of the OS. This means that any bug or vulnerability in SMI handlers could potentially be used to mount an attack on the OS. By default, the SMI handler has full read/write access to all hardware resources in the system, but what the SMI handler actually needs is far less. Malware writers looking for a way to mount a privilege escalation attack could use the excess privilege of the SMI handler.

Intel System Resources Defense is a mechanism that can enforce policy on what system resources can be accessed by firmware SMI handlers from within SMM by establishing a ring 0 and ring 3 privilege separation with regard to hardware access from SMI handlers. When Intel System Resources Defense is implemented with policy that reduces SMI handlers' access to hardware resources such as policy with minimal required access to keep the platform running, it can help to harden the platform by reducing the attack surface in SMM.

When Intel System Resources Defense and Intel Runtime BIOS Resilience are implemented with a policy that does not allow SMI handlers to access resources that could potentially affect OS secrets, then the security of the OS is improved by isolating the trusted compute base of the OS from the SMI handlers. In simpler terms, this means that it reduces the risk that a bug or vulnerability in the SMI handler could be used to launch an attack on the OS.

Intel Trusted Execution Technology

Intel Trusted Execution Technology (Intel TXT) is the technology that the OS or hypervisor could use to initiate a measured and controlled launch of system software called the Measured Launch Environment (MLE). OS or hypervisor uses Intel TXT to establish the MLE generally at OS boot time. This MLE is a protected environment for itself and anything that may run within this environment.

Intel TXT measures key components executed during launch of MLE and allows the OS to check the consistency in behaviors and launch time configurations against a "known good" sequence. Using this verified benchmark, the system can quickly assess whether any attempts have been made to alter or tamper with the launch time environment.

The measurement of this environment is the dynamic root of trust for measurement. It is a simpler measurement because firmware responsible for booting up the platform is excluded from the environment. The smaller the trusted computing base is, the stronger its trust will be. Software residing in a small trusted computing base can be more easily examined and tested.

Intel TXT supports Intel TPM 2.0. It also supports the Intel Platform Trust Technology which is a form of Intel TPM 2.0. Intel TXT can work with a discrete Intel TPM or with Intel Platform Trust Technology. In addition, Intel TXT with Intel TPM enables attestation of the authenticity of the operating system.

Intel System Security Report

Launching the OS and a hypervisor with an Intel Trusted Execution Technology (Intel TXT) launch, on an Intel vPro platform, enables the OS to use Intel System Security Report. Intel System Security Report is a patented, trusted hardware-to-software channel to gain below-the-OS security visibility. In coordination with Intel TXT, Intel System Security Report communicates policies to the OS in a trusted manner at runtime.

Intel System Security Report gives an OS utilizing Intel TXT visibility of the platform resource access policy for SMM that has been put in place with Intel Runtime BIOS Resilience and Intel System Resources Defense. This also makes it possible for the OS to evaluate at runtime whether the trusted computing base of the OS has been isolated from the platform's SMM. This information enables the OS to make more informed security policy decisions if the OS chooses.

Intel System Security Report provides a one-time report at the time of the Intel TXT launch. This typically happens towards the beginning of the OS boot. Intel System Security Report works with Intel TXT to provide this information in a trusted manner. Without this capability, the OS's hypervisor or Measured Launch Environment (MLE) does not have any visibility into what system hardware or resources may be accessible from firmware SMI handlers.

Intel Tunable Replica Circuit – Fault Injection Detection

Fault injection attacks seek to physically disrupt the behavior of integrated circuits, causing devices such as the Intel CSME security processor to behave incorrectly. The most common attacks drive invalid voltage on the device pins. Speeding-up the clock source to the CSME is another form of fault-injection attack. The most common goal of a fault-injection attack is to cause the CSME to skip critical code paths, leaving the platform vulnerable to the execution of malicious code, exfiltration of secrets and other exploits. Intel developed and calibrated the Intel Tunable Replica Circuit – Fault Injection Detection (Intel TRC-FID) to detect and help mitigate these attacks in the CSME security processor starting with 12th Gen Intel Core processor-based business client platforms.

Intel TRC-FID helps protect against fault-injection attacks that use voltage glitching, clock glitching or electro-magnetic radiation. The Intel TRC-FID detects timing variation in circuits and is calibrated to a point where timing violations could only be the result of an attack. The Intel TRC-FID consists of a launch flip-flop (FF), a scan-configurable tunable delay chain, and a capture FF, allowing the Intel TRC-FID to detect such timing violations. When the Intel TRC-FID detects a glitch, in order to prevent further execution, Intel CSME hardware isolates the MinuteIA Core, preventing any further interaction of firmware code with hardware.

Below-the-OS Security Summary

Firmware vulnerabilities have increased five-fold over the last few years, according to the National Institute of Standards and Technology's National Vulnerability Database. Malware can modify firmware to gain access to the operating system and other software. Malicious software can manipulate unsecured firmware and gain access to critical data. It can even render the end user computer completely inoperable.

Intel Hardware Shield, a component of the Intel vPro platform, is designed to improve the security of the device The Intel Hardware Shield technologies, when used with a minimum access policy, help to harden the platforms. And when used with a policy that does not allow access to resources that could affect the OS, can help reduce the risk that vulnerabilities in BIOS could be used to launch an attack on the OS.

Intel Boot Guard enables a hardware based static root of trust for measurement and verification of boot integrity before the OS boots up.

Intel Firmware Restart / Recovery focuses on firmware failures and BIOS updates, so end-customer systems are helped to be more up-to-date and more secure with timely, resilient updates.

Intel PTT acts as a TPM, and stores keys, passwords, and digital certificates.

Intel vPro platforms with Intel System Resources Defense and Intel Runtime BIOS Resilience together deliver state of the art platform security, addressing the data security concerns of the SMM while preserving the required platform utility SMM provides.

Using Intel System Security Report feature, the OS can enforce a more comprehensive security policy that includes hardware, firmware and software, including the SMM policy being enforced by Intel IRBR and Intel ISRD. Intel System Security Report provides visibility to the OS that the OS can use to make decisions on its security policy.

Finally, Intel TXT attests to the platform environment against the desired launch configurations defined.

Below-the-OS Security

Deployment & Use

New on 12th Gen Intel® vPro platforms

Intel Feature	Generation Introduced	Consumer SKU?	Mobile SKU?	Intel vPro® req't?	Intel vPro Enterprise?	Intel vPro Essentials?	Additional HW requirement? (Companion module, extra HW needed)	BIOS integration req't?	On by default?	OS enabling req't?	HW capability mapped to OS feature?	Secured core PC req't?	ISV solution needed?
Intel® Trusted Execution Technology (Intel® TXT)	legacy (10+ yrs)	N	Y	Y	Y	Y	N	Y	N (OEM option)	Y	System Guard Secure Launch	Y	N
Intel® BIOS Guard	4th Gen	Y	Y	Y	Y	Y	N	Y	Y	N	N/A	N	N
Intel® Boot Guard	4th Gen	Y	Y	Y	Y	Y	N	Y	Y	Y	Secure Boot	Y	N
Intel® Runtime BIOS Resilience	8th Gen	N	Y	Y	Y	Y	N	Y	Y	N		Y	N
Intel® System Security Report	8th Gen & 9th Gen refresh in 2019	N	Y	Y	Y	Y	N	Y	N	Y	SMM security config to System Guard	Y	N
Intel® System Resource Defense	10th Gen	N	Y	Y	Y	Y	N	Y	Y	N		Y	N
TPM 2.0 (Intel® Platform Trust Technology; discrete TPM)	11th Gen	Y (Intel® PTT)	Y (Intel PTT)	Y	Y	Y	Y, dTPM N, Intel PTT	Y	Y	Y	e.g. Credential Guard	Y	N
Intel® Firmware Update / Resilience	11th Gen	Y	Y	Y	Y	Y	Y, larger flash chip	Y	Y	N*	*Windows update TBD	N	N
Intel® Firmware Guard	12th Gen	Y	Y	Y	Y	Y	Y, larger flash chip	Y	Y	N*	*Windows update TBD	N	N
Turnable Replica Circuit - Fault Injection Detection	12th Gen	Y	Y	Y	Y	Y	ROW WIP	N	Y	N	N	N	N

Table 1. As components of Intel Hardware Shield, these technologies are straightforward to deploy and use.

Additional Resources

Intel vPro® Platform

Intel.com/vPro

Intel.com/HardwareShield

Intel.com/support Intel vPro Expert Center

Intel vPro

Intel.com/vPro Platform Support

[1] https://venturebeat.com/2019/12/04/fight-back-against-firmware-attacks/

All versions of the Intel vPro® platform require an eligible Intel® Core™ processor, a supported operating system, Intel LAN and/or WLAN silicon, firmware enhancements, and other hardware and software necessary to deliver the manageability use cases, security features, system performance and stability that define the platform. See intel.com/performance-vpro for details. Intel technologies may require enabled hardware, software or service activation.

All information provided here is subject to change without notice. Contact your Intel representative to obtain the latest Intel product specifications and roadmaps. Performance varies by use, configuration and other factors. Learn more at www.Intel.com/PerformanceIndex.

Performance results are based on testing as of dates shown in configurations and may not reflect all publicly available updates. See Performance Index for configuration details. Intel provides these materials as-is, with no express or implied warranties.

No product or component can be absolutely secure. Your costs and results may vary.

1122/MZ/DCC/PDF