White Paper

**Platform Technology**
**Cybersecurity**

# 11th Gen Intel® Core™ Processor Security


## Authors

**Stephanie Domas**

Director of Strategic Security & Communications


## Introduction

Intel has a long history of providing increasingly capable and cost-effective processors with backward-compatible instruction set that preserves software capabilities over time. Intel silicon products provide an architecture the scales from the data center down to the device level. The Intel x86 and Instruction Set Architectures (ISA) enable a huge ecosystem across servers, PCs, mobile devices, embedded platforms, and virtualized systems. Intel also provides application and system developers with advanced tools and re-validated system components.

Intel has delivered remarkable advancements in hardware-based security, hardware-based manageability, hardware-based virtualization, and deterministic real-time compute/networking. Intel continues to increase its portfolio of hardware-based security solutions focused on three main areas: Foundational Security, Workload Protection, and Software Reliability.

### Built in Security

The fragmented chain of suppliers that build Devices (OEM > ODM>OSV> ISV>SI>Customer) choose their own preferred implementations of security capabilities, often implementing critical Root of Trust (RoT) functions in software or expensive discrete hardware security components.

It is often then left to the environment owner/operator to determine how to implement security. However, this can be too late as baseline security constructs must be enabled in the hardware in order to implement certain fundamental capabilities (e.g., RoT, boot integrity, identity storage, updateability). Intel implements such foundational security capabilities in the hardware, enabling the OEMs/ODMs to build on top of these functions, and allowing system integrators and service providers to expose them to the owner/operator.

A device must first and foremost help protect itself (including secrets, identities, keys, data) from attackers and build a chain of trust across the multiple stack layers that each present a unique attack surface. Hardware RoT capabilities provide unique isolation and seed ingredient capabilities that can be used to plug into each security layer to make the entire system or stack more secure.

### About this Paper

This paper is designed to inform security architects, engineers, developers and users, about the spectrum of Intel security solutions that can be found on the 11th gen Intel® Core™ Processor, which is sometimes referred to by its code name, Tiger Lake. Not every security feature covered in this paper is available on every 11th Gen Intel® Core™ processor SKU. Various SKUs have been optimized for different characteristics or use cases, and as a result may have a different subset of security capabilities.

## Table of Contents



### Intel® vPro Platform and Intel® Hardware Shield

Intel® Hardware Shield represents a set of security capabilities available on the Intel vPro® platform. These capabilities comprise of three swimlanes: Below-the-OS Security, Application & Data Protections, and Advanced Threat Protections. The Intel vPro platform with Hardware Shield is available on select 11th gen Intel Core Processor SKUs. Learn more about Intel Hardware Shield, including technical white papers on the three swimlanes.

### A Commitment to Security

System trust is rooted in security - if hardware isn't secure, then a system cannot be secure. At Intel, our goal is to build the most secure hardware on the planet, from world-class CPUs to XPUs and related technology, enabled by software. And we have sophisticated systems to find and address security vulnerabilities in our products.

Intel's commitment to security has never been stronger. We invest in unparalleled people, processes, and products, integrating security in the ways we work and everything we work on. As we relentlessly pursue the best solutions to protect customer systems and data, you can be confident Intel is committed to:

- **Unwavering Customer Focus.** We put customer needs first in our security decisions. We listen to their challenges and use this feedback to guide everything we research, architect, build, and release. Trust is rooted in transparency. We communicate security advisories and product updates to help customers stay informed and keep their systems protected.
- **Continuous Technology Innovation.** New threats will emerge, and vulnerabilities will be found, so Intel is committed to growing, adapting, and relentlessly advancing security. From accelerating cryptography and Confidential Computing, to safeguarding our supply chain and manufacturing operations, we never stop innovating.
- **Robust Incident Response.** We invest extensively in vulnerability management and offensive security research for the continuous improvement of our products. Our Bug Bounty program is a critical way we get outside perspectives, collaborating with researchers and leading academic institutions to find and address vulnerabilities. Intel role models best practices for incident response; when an issue is identified, we follow coordinated vulnerability disclosure practices to release findings and mitigations together.
- **Security by Design.** We follow rigorous policies and procedures spelled out in our Security Development Lifecycle (SDL) to integrate security principles and privacy tenets at every step of hardware and software development. Intel has dedicated experts driving a security-first mindset that starts with research and design and doesn't stop until products reach end of servicing.
- **Community Advocacy.** It's clear no single entity can solve complex security challenges alone. We work with technology partners, academic institutions, industry organizations, and governance bodies worldwide. These efforts support development of policies, industry guidelines, standards, and research to elevate shared security goals that benefit everyone.

We actively work to deliver security without sacrificing performance. Working with our customers and industry partners, we can achieve the levels of secure performance people expect and deliver technology they trust.

View our security first pledge

## Foundational Security

Critical protection to help verify trustworthiness of devices and data.

### ALUX

ALUX instructions refer to hardware accelerated instructions used in the modular exponentiation of asymmetric encryption such as RSA. While they are not exclusively cryptographic instructions, they perform commonly used primitives leveraged in public key (asymmetric) cryptography, including SSL, digital signature generation and verification, and key exchange algorithms.

ALUX collectively refences to 4 instructions (ADCX, ADOX, MULX, and RORX) which have been accelerated aiming to decrease the impact of these frequently used cryptographic functions. Acceleration is achieved through more efficient use of CPU resources and leveraging the flags registers for additional computational space. This improved performance opens up the potential for supporting higher encryption workloads on the system.

To benefit from ALUX instructions, code performing relevant crypto functions needs to explicitly utilize these instructions. This can take the shape of a software application incorporating them, or cryptographic libraries shifting the relevant computation to the corresponding accelerated instructions.

### Intel® AES New Instructions (Intel® AES-NI)

Intel® AES New Instructions (Intel® AES-NI) is an enhancement to core crypto performance to improve compute efficiency of the AES cryptographic algorithm. A vector form, Vector AES, is used to enable two (256-bit) and four (512-bit) lanes, increasing AES throughput.

AES is a heavily used symmetric cryptographic algorithm and spans a multitude of workload types and use cases. Some common cases being user operations such as web browsing, video streaming, email (SSL/TLS), and system operations such as full disk encryption. By more efficiently using system resources, accelerated AES, through AES-NI, has the potential to increase workload throughput on the system and reduce performance related impact to user experience.

To leverage Intel AES-NI, code performing the relevant AES computations needs to have been built with a supported compiler or leverage a crypto library which has been built with support.

### Intel® BIOS Guard

Intel® BIOS Guard is a BIOS Flash update hardening technology that creates a very small trust boundary for BIOS image updates to Flash. It removes from the trust boundary the System Management Interrupt (SMI) handler and nearly all of the power-on self-test (POST) BIOS, as well. This small trust boundary helps reduce the risk of Flash based attacks, including permanent subversion and/ or denial of service attacks. Attacks on platform BIOS can result in BIOS-based Rootkit, and platform denial of service. Intel BIOS Guard uses the Model State Register (MSR) to generate the Flash open/ close special cycles. This results in the Flash open/close only being writeable from BIOS Guard AC-RAM mode. 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.

Usage of BIOS Guard for flash updating is achieved through OEM and BIOS integration

## Intel® Boot Guard

Intel® Boot Guard provides protection against BIOS flash storage attacks, such as those that aim to install malicious, often persistent, drivers into the system (ex. Membroni, Lojax). Intel Boot Guard works by performing verification of the Initial Boot Block (IBB). By performing integrity checking, starting with the very first executable BIOS module, the IBB, Intel Boot Guard builds a Static Chain of Trust (SCoT) rooted in immutable hardware. The policies and keys used by Boot Guard are permanently burned into the chipset which makes them resistant to tampering. If a failure or breach is detected, then the system restores the BIOS back to a known good state. BIOS rootkits can result in persistent, high privilege level, presence on systems, that can be very difficult to detect by traditional software or remediate due to their privileges existence outside of the OS and software security solutions.

In addition to building a SCoT Boot Guard can leverage chipset fuses to prevent BIOS rollbacks.

Boot Guard is enabled through BIOS vendors, and no additional action is required by end users, or IT staff to benefit from its protection.

For more in-depth information see Intel's white paper

## Intel Firmware Restart / Update

Intel Firmware Restart / Update is a collection of security capabilities focused on Firmware Update and Resiliency. The number of firmware attacks and vulnerabilities continues to rise and keeping system firmware up to date with the latest functional and security patches, plays a critical role in a systems security posture. Firmware guard aims to reduce some of the pain and risk points associated with firmware patch rollout: authenticity, resiliency, and telemetry.

Intel Firmware Restart / Update authenticity for in-field updates to BIOS, CSME, and IFWI, provides security assurance through using UEFI standard capsules verification to certify the patch is legitimate.

Resiliency focuses on firmware recovery which comes in two forms. The first is if a patch load is interrupted, then automatic and seamless recovery occurs without the need for end user's involvement. The second, which is available in Intel vPro platform, allows for real-time attack resilience, whereby the firmware will protect itself, and if required, recover the firmware to a known good state. The recovery capabilities work by leveraging other Intel security features: Intel Boot Guard, Intel BIOS Guard, and TopSwap. Firmware Version control helps protects machines from downgrading to out-of-date patches. Rollback to old, vulnerable, firmware versions is a technique hackers use to re-introduce known weakness into a system. Rollback protection is a way to reduce the potential of this class of attack.

Telemetry includes Firmware Version reporting that gathers firmware version information from different components on the system and publishes it for administrator/OEM review and analysis. This can help ensure all systems have the latest patch installed.

For a system to benefit from Intel Firmware Restart / Update's capabilities it must be enabled and supported through both the OSV and OEM.

## Intel® Converged Security and Management Engine (Intel® CSME)

Intel® Converged Security and Management Engine (Intel® CSME) is a hardware-based manageability and security controller that is purposefully isolated from the CPU. It provides a systems root of trust for components during the platform's silicon initialization. On startup it does a base initialization of the Platform Controller Hub (PCH), including configuration of clocks and GPIO. As boot continues, it performs authentication and loading of FW into HW engines integrated into the main CPU and PCH such as Power-Management controller (PMC), Audio, camera, Type C, and Sensor FW, and supports secure debugging capabilities of the PCH.

Intel CSME supports a range of both manageability and security features. The security focused features include support for: Intel® Platform Trust Technology (Intel® PTT), Intel Boot Guard, HW DRM, and secure loading and execution of Intel® Dynamic Application Loader (Intel® DAL) applets, secure firmware loading of platform-firmware components such as TBT (Thunderbolt), Type-C, Sensor Solution FW, and Intel® Active Management Technology (Intel® AMT) which allows for remote network access to systems that are in low power state or not functioning, enabling secure remote monitoring and management.

To benefit from Intel CSME support must be integrated into the operating system.

For additional information see Intel's white paper

## Protected Audio Video Path (PAVP)

Protected Audio Video Path (PAVP) produces an end-to-end protected path for data flowing through the graphics/audio pipeline to allow the platform to get access to high value premium media content. The platform uses an authentication scheme based off of ECDSA to allow an app/content-source to determine cryptographically whether it is talking to a PAVP-enabled platform, and therefore provides a way for the source to send encrypted video/audio content for processing in the hardware. Intel AES-NI is used to protect the data in memory as it flows through the various graphics and audio processing pipeline stages prior to being displayed. For full end to end protection the PAVP solution delivers the cryptographically protected content directly to the Display Engine, where it is delivered securely via High-Bandwidth Digital Content protection (HDCP) to the monitor.

To benefit from PAVP support must be integrated into the operating system.

## Intel® Download and Execute (Intel® DnX)

Intel® Download and Execute (Intel® DnX) allows platforms to recover from an unbootable state caused by corruption of the BIOS and Firmware. Intel DnX restores the BIOS and Firmware image to known good and signed OEM configuration. The capability also provides support for secure debug capabilities which can aid in after-sales support services.

Intel DnX requires OEM integration and potentially BIOS support, and additional infrastructure integration if leveraging the debug capabilities.

### Intel® Platform Trust Technology (Intel® PTT)

Intel® Platform Trust Technology (Intel® PTT) is an integrated on-chip hardware Trusted Platform Module (TPM) that support Trusted Computing Group (TCG) TPM 2.0 standard and supports FIPS 140-2 certification L2. A TPM which provides the secure storage of keys/credentials, platform configuration registry values, and boot block measurements. Intel PTT provides attestation locally for runtime integrity protections or remotely to third party providers looking to ensure the device software stack is verified to a known value. The attestation reports communicate unauthorized modifications to device management systems. Intel PTT's integrated nature removes the necessity for a discrete TPM freeing up board space.

Intel PTT is implemented in firmware running on a coprocessor and Intel Converged Security and Management Engine, and then leveraged by the operating system.

### Intel® Runtime BIOS Resilience

Intel® Runtime BIOS Resilience reduces the risk of malware injected into the SMM environment at runtime. It achieves this by setting up the strict page table properties that greatly reduce the attack surface of malicious code able to get code execution below the OS. Page tables overseeing BIOS SMM, SMI Handlers, BIOS owned Non-SMM memory, and MMIO are locked down to only the minimum necessary permissions (such as read-only, no-execute). Additionaly, OS memory is removed entirely from mapping, such that it's not accessible from SMM at all. These policies make it challenging for an attacker to access OS memory space or make malicious changes to the below-OS environment.

For a system to benefit from Intel Runtime BIOS resilience, it must be integrated at the BIOS level.

### Intel® Secure Hash Algorithm Extensions (Intel® SHA Extensions)

Intel® Secure Hash Algorithm Extensions (Intel® SHA Extensions) is a family of instructions designed to accelerate the cryptographic Secure Hash Algorithm Extensions (SHA Extensions) variants SHA-1 and SHA-2 256. SHA is a heavily used cryptographic algorithm often leveraged to support verification of data integrity, provide a mechanism for authentication of secure communications, and identifying data duplication.

This improved performance opens up the potential for supporting higher encryption workloads on the system while reducing potential performance related user impact.

To leverage Intel SHA Extensions, code performing the eligible SHA computations needs to have been built with a supported compiler or leverage a crypto library which has been built with support.

### Security Protocol with Independent Recovery Algorithm (SPIRAL)

Security Protocol with Independent Recovery Algorithm (SPIRAL) is an extension and security enhancement to Intel Boot Guard. It establishes an end-to-end secure channel between the CPU and the Intel Converged Security and Management Engine with mutual authentication and session key agreement, for protecting Boot Guard data traveling between the CPU and CSME on the DMI bus. SPIRAL aims at mitigating man-in-the-middle attacks against Intel Boot Guard. As SPIRAL is a component of Intel Boot Guard, for a system to utilize it, Intel Boot Guard must be integrated by the OEM, and the system must have a supporting PCH and CPU.

### 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 handlers historically run at a privileged access level on the system, due to being a part of System Management Mode (SMM). This makes them desirable targets for exploitation, as a means to have gain near full control of the system.

Intel System Resources Defense provides 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.

To leverage Intel System Resources Defense it must be integrated into the BIOS.

### Intel® System Security Report

Intel® System Security Report provides an attestation of SMM policies on the system, when the Intel® TXT is used to launch the OS or hypervisor. A crypto verification is performed of entry code, and then the policy structure is evaluated resulting in a report that describes the policies to the OS. This security report is created towards the beginning of the OS Boot. This allows the OS to evaluate at runtime whether the trusted computing base of the OS has been isolated from the platform's SMM, allowing the OS to make more informed security policy decisions. Which aids in preventing attacks that would attempt to corrupt SMI handlers.

For a system to support it must be integrated into the BIOS, then utilization of the report must be supported by the OS.

### Intel® Total Memory Encryption (Intel® TME)

Intel® Total Memory Encryption (Intel® TME) technology encrypts the platform's entire memory with a single key. Intel TME, when enabled via BIOS configuration, helps ensure that all memory accessed from the Intel CPU is encrypted, including customer credentials, encryption keys, and other IP or sensitive information on the external memory bus. The key used for memory encryption is generated using a hardened random number generator in the CPU that is never exposed to software. Data in-memory and on the external memory buses is encrypted and is only in plain text while inside the CPU. This allows existing software to run unmodified while protecting memory using Intel TME.

Intel TME prevents unauthorized sources from extracting information out of the DRAM/NVRAM that is outside of the SOC, in the event a device may have been lost or stolen.

### Intel® Transparent Supply Chain (Intel® TSC)

Intel® Transparent Supply Chain (Intel® TSC), is a part of Compute Lifecycle Assurance (CLA) and provides the capability for auditing that components on a platform are authentic. This service enables visibility and traceability of selected hardware components, firmware, and software for OEM and ODM partners. Intel TSC leverages the Intel Key Generation Facility (IKGF) to sign the Intel TSC data files

containing the platform-level component information. Additionally, Intel TSC provides an End User Web Portal where they will be able to download their signed system files along with the TSC AutoVerify Tool. TSC AutoVerify Tool provides the ability to verify the authenticity of selected hardware components and selected firmware of signed systems.

Usage of TSC is incorporated at the OEM and ODM level.

### Intel® Trusted Execution Technology (Intel® TXT)

Intel® Trusted Execution Technology (Intel® TXT) works by launching a Measured Launch Environment (MLE) with a central objective to provide its accurate measurement. This in turn enables a comparison of obtained measurement of all the critical MLE elements against a known good value and provides enforcement mechanisms to block launch of code. The process starts from a Dynamic Root of Trust for Measurement (D-RTM) established at OS loader time (early launch) or OS runtime (late launch) and continues by measuring key components executed during launch of the trusted OS kernel or VMM. Established trusted environment is able to check the consistency in behaviors and launched configuration against a "known good" sequence. Using this verified benchmark, the system can quickly assess whether any attempt to alter or tamper with the launch time environment have been made. Intel TXT supports both Intel TPM 1.2 and 2.0 and Intel PTT as a part of dynamic MLE.

Intel TXT additionally supports Launch Control Policy (LCP) – a verification engine enforcing the platform manufacturers and platform owners' policies over allowed platforms configurations and components to be executed during launch.

In order to use Intel TXT, the system needs a Intel TXT supportive OS, BIOS, and VMM. Then Intel TXT can be enabled via the BIOS.

### UEFI Secure Boot

UEFI Secure Boot is a key component of the hardware root-of-trust. It implements UEFI 2.3.1 standards and meets the associated NIST security requirements. UEFI Secure boot is complemented by hardware roots of trust, such as Intel Boot Guard, which ensures that the UEFI implementation is authentic. Similarly, UEFI Secure Boot is complemented by the Intel Trusted Platform Module Measured Boot, where the evidence of the boot, including the secure booth authorities can allow for attestation. This allows for detection of tampering by validating ditigal sigantures of to boot loaders, key operating system files, and unauthorized option ROMs.

To leverage UEFI Secure Boot, it must be integrated by the OEM and supported by the OS.

For more information see Intel's white paper

### VPMADD52

VPMADD52 is a new set of instructions that provide hardware based crypto accelerator for integer fused multiply accumulated operations. This type of the large exponentiation multiplication takes place as a part of the RSA algorithm. By leveraging the EVEX encoding (AVX512) which allows support for up to 512 bits registers, the processor is able to do multiple 52-bit unsigned integer multiplication, to generate eight 104-bit products, and accumulate their low high halves into 64-bit containers. This has the additional effect of reducing the instructions needed to perform 8 multiplications down to only 2. Usage of VPMADD52 requires heavy power usages and may result in machine's lowering of frequency. Due to this VPMADD52 is primarily impactful when used with multibuffered RSA operations, i.e. when numerous RSA operations are bundled together to execute in batch. The software stack will unite all the handshakes together, and then invoke the VPMADD52 functionality to execute in batch.

RSA is often used in key exchanges, for example, being used during a TLS handshake. High usage RSA use cases would be servers, which negotiate numerous handshakes per second with users. In situations requiring limited usage of RSA, such as end user systems, we recommend using ALUX acceleration capabilities to avoid the potential system frequency alteration, which is sometimes required with VPMADD52.

Usage of VPMADD52 is achieved through usage of a software library that supports multibuffered RSA operations and VPMADD52.

For more in-depth information see Intel's white paper

## Workload Protection

Trusted execution for hardware-isolated data protection.

### Intel® Secure Key Digital Random Number Generator (DNRG)

Intel® Secure Key Digital Random Number Generator (DNRG), is a HW-based random number generator supporting 128-bit security, and NIST SP 800-90 A, B and C compliant functionality, making it suitable for FIPS 140-2 and FIPS 140-3 certified products. Random numbers are frequently used as a seed in encryption algorithms, and the higher entropy (true randomness) a seed can provide, the stronger the resulting cryptographic usage will be. The alternative to hardware based random number generators is software based pseudo-random number generators (PRNG). PRNGs however can be slower, with lower entropy, which can make resulting use of them not as cryptographically strong. A robust true random number generator, such as Intel's DNRG, is especially valuable in virtualized environments, which are highly deterministic in nature potentially making software-based generators struggle to provide high entropy results.

The DRNG is accessible through supporting software cryptography libraries, and directly through the RDRAND and RDSEED instructions.

### Mode Based Execution (MBE) Control

Mode Based Execution (MBE) Control provides finer grain control on execute permissions to help protect the integrity of the system code from malicious changes. It provides additional refinement within the Extended Page Tables (EPT) by turning the Execute Enable (X) permission bit into two options:

- XU – eXecute permission for User pages
- XS - eXecute permission for Supervisor pages

The CPU selects one or the other based on permission of the guest page and enforce supervisor-executable with additional permissions. A benefit of this feature is that a hypervisor can more reliably verify and enforce the integrity of kernel-level code that is running in the Operating system (OS). The value

of the XU/XS bits is delivered through the hypervisor, so hypervisor integration support is required.

### Intel® OS Guard

Intel® OS Guard consists of a collection of technologies: Supervisor Mode Access Protection (SMAP), Supervisor Mode Execution Protection (SMEP), and SMM External Call Trap (ETC).

SMAP prevents supervisor data accesses to pages that are accessible in user mode. Attempted access results in page-fault exceptions. For this attack pattern a malicious actor leverages an OS vulnerability to get elevated privileges, then either attempts to read malicious data from user space or write malicious data into user space. SMAP helps provide platform security protection against this attack pattern, that attempts to leverage writing or reading data residing in user space, from within the kernel space

SMEP prevents instruction execution from user memory pages while the CPU is in supervisor mode. This is an attack pattern used in some privilege escalation attacks where an OS vulnerability is leveraged to gain elevated privileges. The attacker then jumps back into user space (often malicious) code, now running at elevated privileges.

SMM External Call Trap will trap System Management Mode (SMM) code that makes a call to code outside of its Trusted Computing Base (TCB), which is SMM code. This allows not only runtime detection of potentially hijacked SMM handlers, but also design and development debugging to quickly isolate incorrectly implemented SMM handlers. Due to SMM's elevated privilege level on the system and black box operation, exploitation of SMM is highly sought after, and difficult for traditional means (e.g. anti-virus) to detect and recover from.

SMAP and SMEP are automatically operational if the system is running a supporting OS, and SMM ECT is enabled by OEM's through the BIOS.

### Intel Virtualization Technology (Intel® VT-x)

Intel Virtualization Technology (VT-x) is a portfolio of technologies that empower virtualization through reduction in performance overhead and improvements to security. Intel VT-x abstracts hardware to allow multiple workloads to share a common set of resources. Virtualization provides a mechanism to isolate secure workloads from the main OS creating a separation between malicious code and actors in either the VM or host from impacting each other.

Support for Intel VT-x is incorporated by Virtual Machine Vendors (VMVs).

### Intel® Virtualization for Directed I/O (Intel® VT-d)

Intel® Virtualization for Directed I/O (Intel® VT-d) is a hardware technology within the general Intel Virtualization Technology suite. Intel VT-d provides hardware support for virtualizing and isolating devices requests (such as memory access and interrupts) to resources within the intended software created domains. VT-d achieves this through several capabilities: Flexible I/O device assignment to domains (VMs), DMA address translation, Interrupt Remapping and Virtualization, error reporting to system software, and support for technologies such as Single Root I/O Virtualization (SR-IOV) and Scalable I/O Virtualization (S-IOV) on devices to facilitate sharing of such devices directly by multiple VM's. Support for Intel VT-d is incorporated by Operating Systems Vendors (OSVs) and Virtual Machine Vendors (VMVs).

### Virtualized Trusted I/O

Virtualized Trusted I/O works in conjunction with a hypervisor and trusted I/O drivers running in a secure virtual machine VM to isolate and protect I/O data via VT EPT-based memory views. Virtualized Trusted I/O leverages Intel VT-x and Intel VT-d for virtualization, as well as USB and MIPI dual command challenge, to allow concurrent use of secure and non-secure cameras and biometric authentication. Support for Virtualized Trusted I/O is incorporated into the Hypervisor.

### Execute Disable Bit ( (XD-Bit)

Execute Disable Bit (XD-Bit) is a hardware-enforced memory page protection attribute, which enables pages to be set as data only (Readable and/or writeable). Attempts to execute from a page with the XD-Bit set will result in a page fault exception. This helps provide protection against code injection attacks, which often to execute code placed into a data buffer.

The XD-Bit support is built into the BIOs, OS, or hypervisor.

## Software Reliability

Platforms that help protect against a range of cybersecurity threats.

### Intel® Control-flow Enforcement Technology (Intel® CET)

Intel® Control-flow Enforcement Technology (Intel® CET) helps code owners defend against control-flow hijacking malware. Control-flow hijacking attacks are commonly used, and are routinely targeting OSs, browsers, and general software applications.

Such attacks are hard to detect and prevent because they leverage existing code running from executable memory, in order to manipulate a programs behavior. Return Oriented Programming (ROP), Jump Oriented Programming (JOP), and Call Oriented Programming (COP) are all forms of control-flow hijacking attacks. These attacks emerged and quickly rose in popularity as security controls that prevent traditional buffer overflows became more common.

In ROP attacks, an unauthorized attacker modifies the application's return addresses, located on the stack. When the application completes a function and the processor retrieves the return address, instead of returning to the authentic caller, it returns to the attacker's modified location.

JOB and COP rely on similar techniques in which destinations for indirect branch instructions such as Call and Jump are modified to point to an attacker desired location.

Intel CET consists of two core capabilities, the first is Indirect Branch Tracking (IBT). IBT helps defend against JOP/COP attacks through locking down available target locations for indirect jump and call instructions. Traditional control flow would allow for code execution to start at any executable address, IBT locks this down to only addresses that have been predetermined at compile time, to be legitimate. An indirect

jump or call to an illegitimate target address ends in the processor signaling the "Control Protection" exception.

The second is a shadow stack, to defend against ROP attacks. The shadow stack maintains a copy of the authentic call stack, as the program executes. When a return operation is encountered, the destination on the main stack is compared against the shadow stack. If the two return addresses don't match, the processor signals the "Control Protection" exception.

In both capabilities the action taken in the event of a discrepancy depends on the OS's implementation of Intel CET.

Utilizing Intel CET requires the code to have been built with a Intel CET supporting compiler, and then executed in a CET supporting OS. Intel CET can protect application software, as well as drivers, and the operating system itself.

Code built with Intel CET have full backwards compatibility and run seamlessly on non-Intel CET kernels and processors. Languages currently supported are C/C++ and Fortran.

### Intel® Threat Detection Technology (Intel® TDT)

Intel® Threat Detection Technology (Intel® TDT) is a suite of hardware-assisted security technologies that detects prevalent malware attacks and accelerates common security workloads. Through the use of CPU Telemetry and advanced ML algorithms, Intel TDT can help identify complex threats, like ransomware and cryptojacking, based on their distinctive computation behaviors. Intel TDT also offloads performance intensive security workloads, such as memory scanning and machine learning inferences, to Intel Graphic Processing Unit (GPU) to reduce their performance overheads. Usage of Intel TDT is achieved through incorporation by ISV's into security solutions, such as anti-virus or end point protection, to enhance detection of these advanced cyber threats and exploits.

By pairing CPU telemetry and GPU acceleration, Intel® TDT helps to make Endpoint security products more effective and more efficient on Intel platforms.

### User Mode Instruction Prevention (UMIP)

User Mode Instruction Prevention (UMIP) restricts a set of user space instructions (SGDT, SIDT, SLDT, SMSW, and STR) which can be used by malicious actors to reveal information about certain OS structures. UMIP removes these instructions from user space.

Support for UMIP is incorporated into the operating system and enabled in the CPU via a CR4 bit.

**Table 1.** Glossary

| | |
|---|---|
| AES | Advanced Encryption Standard |
| AMT | Active Management Technology |
| CET | Control-Flow Enforcement Technology |
| CLA | Compute Lifecycle Assurance |
| COP | Call Oriented Programming |
| CPU | Central Processing Unit |
| DAL | Dynamic Application Loader |
| DNRG | Digital Random Number Generator |
| DnX | Download and Execute |
| D-RTM | Dynamic Root of Trust |
| FIPS | Federal Information Processing Standards |
| GPU | Graphics Processing Unit |
| HDCP | High-Bandwidth Digital Content Protection |
| HW | Hardware |
| IBB | Initial Boot Block |
| IKGF | Intel Key Generation Facility |
| ISRD | Intel System Resources Defense |
| ISSR | Intel System Security Report |
| MBE | Mode Based Execution Control |
| MIPI | Mobile Industry Processor Interface |
| MMIO | Memory Mapped I/O |
| NIST | National Institute of Standards and Technology |
| OS | Operating System |
| OSV | Operating System Vendor |
| PAVP | Protected Audio Video Path |
| PCH | Platform Controller Hub |
| PMC | Power-Management Controller |
| POST | Power on Self-Test |
| PTM | Trusted Platform Module |
| PTT | Platform Trust Technology |
| RAM | Random Access Memory |
| RSA | Encryption Algorithm (Ron Rivest, Adi Shamir, Leonard Adleman) |
| SCoT | Static Chain of Trust |
| SHA | Secure Hash Algorithm |
| SMI | System Management Interrupt |
| SMM | System Management Mode |
| SPIRAL | Security Protocol with Independent Recovery Algorithm |
| TBT | Thunderbolt |
| TCG | Trusted Computing Group |
| TDT | Thread Detection Technology |
| TPM | Trusted Platform Module |
| TSC | Transparent Supply Chain |
| TXT | Trusted Execution Technology |
| UEFI | Unified Extensible Firmware Interface |
| USB | Universal Serial Bus |
| VMV | Virtual Machine Vendors |
| VT-d | Virtualization for Directed I/O |
| VTIO | Virtualized Trusted I/O |