IOActive®

Research-fueled Security Services

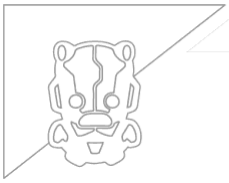
\ RESEARCH \

13th Generation Intel Core Attack Surface Study

Commissioned by Intel

March 2023

Contents



IOActive.

Background

Fundamentally, all the Intel vPro security technologies introduced through the 12th generation of Intel Core Processors exist to enforce trustworthy computing. Below is a high-level presentation of the landscape, with details provided in subsequent sections.

Intel security technologies such as CSME, TXT, DRTM, and SRTM guarantee that code leading up to and into the OS is all trusted. This presumes that SMM must be trusted. Time has shown that this presumption is not realistic.

Intel security technologies such as ISSR, ISRD, and IRBR guarantee both integrity and measurability of SMM while deprivileging SMM. These guarantees satisfy the previous dependence on trust in SMM.

Hardware-based virtualization can be leveraged to further offer capabilities to the OS so that trustworthy computing can be achieved at that level. VT-x allows for the entire OS to be virtualized and to build facilities such as trust levels and additional compartmentalization and isolation on top of the hypervisor.

In concert, these capabilities provide the necessary building blocks for an OS to deliver trustworthy computing. For this to be true, there must be no implementation issues such as buffer overflows, memory corruption, etc. Again, this presumption has proven unrealistic over time as there have been a never-ending stream of implementation issues that malicious actors have been able to exploit.

Intel hardware features such as NX and CET can strategically mitigate implementation issues. Combined with software-level mitigation capabilities offered by operating systems and compilers—such as hardened heap, ASLR, and CFG—Intel vPro security features effectively mitigate the exploitability of a huge swath of the colossal quantity of inevitable implementation issues.

A gap that has only recently been addressed is unauthorized direct memory access such as FireWire, Thunderbolt, SATA, and NVMe. Intel VT-d can restrict I/O is leveraged to protect the OS and enforce trustworthy computing.

Most lately, VT-rp addresses the residual susceptibility to data-only attacks or modifying page tables, addressing attacks that cannot be mitigated by CET and thus stopping most foreseeable end-runs around ROP/JOP/COP mitigations.

In addition to factors of which have yet to conceive, known areas of weakness that have yet to be covered include:

- JIT
- Logic issues
- Side channels
- Information leaks
- Hardware bugs

Intel Corporation (Intel) engaged IOActive, Inc. (IOActive) to conduct a quantitative improvement study of the hardware security features introduced in Intel's vPro platforms:

8th-9th Generation

- Intel® Runtime BIOS Resilience
- Intel® Trusted Execution Technology (Intel® TXT)
- Intel® System Security Report
- Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI)
- Intel® Secure Key
- Intel® BIOS Guard
- Intel® Platform Trust Technology (Intel® PTT)
- Intel® Threat Detection Technology (Intel® TDT) Accelerated Memory Scanning

10th Generation

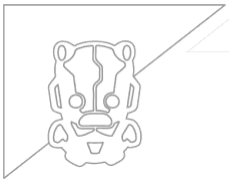
- Intel® System Resources Defense
- Intel® Transparent Supply Chain (Intel® TSC)
- Intel® TDT Cryptojacking Detection

11th Generation

- Intel® Control-flow Enforcement Technology (Intel® CET)
- Intel® Total Memory Encryption (Intel® TME)
- Intel® TDT ransomware detection
- Intel® Key Locker

12th - 13th Generation

- Intel® Total Memory Encryption - Multi-Key (Intel® TME-MK)
- Intel® Virtualization Technology - Redirect Protections (Intel® VT-rp)
- Intel® Firmware Guard (update/recovery)
- Tunable Replica Circuit - Fault Injection Detection
- Intel® TDT Anomalous Behavior Detection



Analysis

The deployment of Intel hardware security features is a complex process and its impact on security is difficult to quantify. The hardware security features offer robust protection against exploits but their deployment can take time as they require software support. To measure the security improvements from the hardware features, we have defined a metric called Potentially Addressable Mitigation Surface (PAMS). Please see Appendix B for methodology details. PAMS measures the reduction of the attack surface by the hardware mitigations based on their full deployment and theoretical effectiveness.

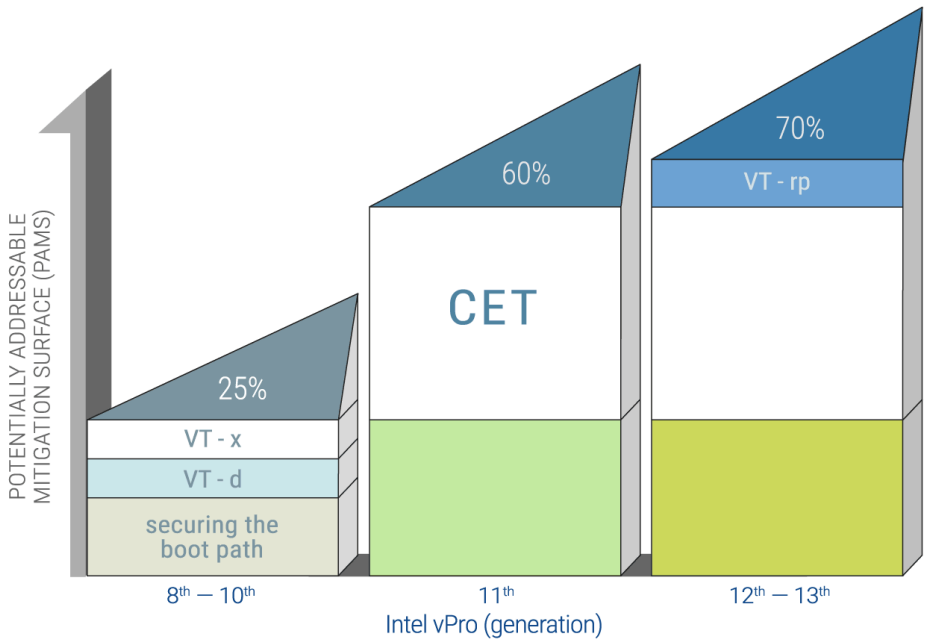
The lag between the release of hardware mitigations and their integration into different software systems further complicates the evaluation of their impact; however, PAMS offers an estimate of the percentage of attacks that the particular mitigation can stop when fully deployed with support in the OS and other relevant software. PAMS is a cumulative measurement of the improvements offered by the three waves of Intel® vPro security defenses and aims to provide a quantitative measure of the value added by these new capabilities.

> The two waves of Intel vPro are sets of hardware security measures aimed at improving the security of computing platforms. The first wave (8th, 9th, and 10th generations) focused on closing off the most vulnerable attack surfaces of the time by enhancing the integrity of BIOS functions, low-level hardware drivers, and virtualization. The second wave (11th,12th and 13th generations) focused on the integrity of the whole platform by adding anti-ROP/JOP/COP control flow verification, encrypted memory, and enhancing malware security scanning. The 13th generation Intel® architecture is the newest revision of vPro and is expected to leverage CET to significantly curtail the effectiveness of currently known methods of kernel exploits and VT-rp (HLAT) with TME-MK through an additional two-level isolation layer—from memory encryption and hypervisor-controlled page tables—between hypervisor entities that disallows virtualized tenant cross-visibility and hypervisor exploits.

Before the introduction of vPro, the primary method used by attackers to exploit computers was through buffer overflow attacks. These vulnerabilities peaked at about 23% of reported issues in 2003 and began an accelerating decline[1].. There are over 10,000 vulnerabilities attributable to buffer overflows in the CVE database, with 23% of those considered "severe"[2]. The initial introduction of hardware-assisted Data Execution Prevention (DEP) reduced the available attack surface removing the simple buffer and heap overflow exploit techniques from the attacker's option list; however, this reduction in the attack surface was short-lived as

[1] https://cve.mitre.org/docs/vuln-trends/index.html
[2] https://info.dovermicrosystems.com/blog/2021-buffer-overflows

a new technique called Return-Oriented Programming (ROP) was published in 2008, which opened up the attack surface by utilizing existing code segments already marked as executable. Related techniques known as Jump-Oriented Programming (JOP) and Call-Oriented Programming (COP) arose around the same time.



BIOS attacks, also known as firmware attacks, were considered rare between 2008 and 2016 due to the technical skills required to execute them. As attackers became more sophisticated, the number of BIOS attacks increased and various types of BIOS malware emerged such as BIOS rootkits, LoJax, and BIOS-ransomware. Low-level BIOS protections were introduced to address the growing attack surface of UEFI BIOS functions, which became the most common form of low-level firmware for servers, PCs, and laptops by around 2010. Despite being important, BIOS vulnerabilities and attacks constitute a small portion of the attack landscape even though low-level BIOS protections play a significant role in preventing the attack surface from growing.

Device driver vulnerabilities were a significant threat in the cyber security landscape between 2010 and 2016. Exploits targeting device drivers allowed attackers to gain access to a system and execute arbitrary code, making them critical when an exploit path was discovered. In 2010, Intel introduced VT-x and VT-d hardware tools to provide software developers with effective hardware protection against these kernel DMA and memory access attacks; however, adoption of these defenses has been slow and incremental, with many drivers not yet updated to take advantage of the available mitigations. PAMS estimates a theoretical reduction in attack surface of via protecting the driver code corresponding to the percentage of windows code comprised of drivers.

The Second Wave of vPro refers to the 11th, 12th, and 13th generations of Intel's platform technology. One of the major concerns in the security of computer systems is the exploitation of memory-safety vulnerabilities. One such technique that has become widely used by attackers is ROP/JOP/COP. In ROP/JOP/COP, attackers use pieces of existing code, marked as executable, to build blocks for program functions and modify system components to compromise systems. The technique evolved from return-to-libc attacks in 2007 for the x86 architecture. ROP/JOP/COP techniques have been responsible for a large majority of serious vulnerabilities that have allowed remote code execution (RCE), with analysis suggesting that ROP/JOP/COP techniques were a part of 90% of all RCE techniques[3].

A more recent survey of exploit developers puts the critical use of ROP/JOP/COP techniques in 60-80% of critical code execution memory corruption vulnerability exploits[4]. ROP gadgets are made up of modifying function return values to these instruction fragments. The technique has become so dominant that toolsets have evolved to scan code and automatically build ROP gadget chains and programs. ROP is a major tool in the attacker's toolkit, particularly for code execution bugs in critical browser components and almost any system component, from OS kernels to embedded devices.

Despite efforts to mitigate ROP/JOP/COP attacks through software measures, such as Return Flow Guard and Control Flow Guard (RFG and CFG) and anti-ROP/JOP/COP measures in Anti-Virus (AV) products, these measures have been shown to be prone to bypasses[5]. Several reports, such as "Bypass Control Flow Guard comprehensively" [6]and "RPC Bypass CFG," describe methods of bypassing CFG to execute malicious code. A design flaw in Microsoft's CFG was discovered, allowing attackers to bypass the security mechanism completely, as described in the "Design Weakness in Microsoft CFG allows Complete Bypass" article.[7] ROP/JOP/COP continues to be a viable threat even in the presence of some software mitigations.

Intel® CET is the latest and most advanced mitigation technique to tackle the problems posed by ROP/JOP/COP attacks. CET supplements the software-based mitigations offered by CFG to address ROP/JOP/COP attacks and offer a higher level of security. Windows's implementation using the shadow stack elements of CET supplementing the capabilities of CFG[8] provides greater overall effectiveness compared to only utilizing CFG as CET leverages dedicated hardware resources.

The Second Wave (11th, 12th, 13th generation) CPUs come with substantial attack surface reduction measures, and also add features for Endpoint Protection systems such as Windows Defender for Enterprise, CrowdStrike Falcon EDR, ESET, and Blackberry, which implement

---

[3] https://securityintelligence.com/anti-rop-a-moving-target-defense/
[4] https://twitter.com/dragosr/status/1615195037331226626
[5] https://eyalitkin.wordpress.com/2017/08/18/bypassing-return-flow-guard-rfg/
[6] https://www.blackhat.com/docs/us-15/materials/us-15-Zhang-Bypass-Control-Flow-Guard-Comprehensively-wp.pdf
[7] https://www.darkreading.com/vulnerabilities-threats/design-weakness-in-microsoft-cfg-allows-complete-bypass
[8] https://blog.maikxchd.com/control-flow-enforcement-on-windows-with-cfg-and-intel-cet

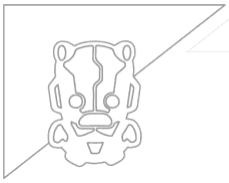
TDT acceleration. These CPUs come with hardware-level measures, such as CET and anti-ROP/JOP/COP measures, Hypervisor Isolation, memory encryption, and TDT, to provide a high level of security against cyber threats.

Intel® CET has been adopted by Microsoft in its Windows OS and is included in Windows 10 version 21H1 and later. CET support is also being developed for the Linux kernel, with patches being proposed and developed to support CET in the open-source kernel. In the browser world, CET is enabled for security-critical browser processes for Chrome and related browsers (Chromium, Edge) starting with release 90 on Windows. The implementation of CET is considered a major step towards eliminating the use of ROP and other control flow hijacking techniques. With CET, developers are given a much more robust protection system that has no performance penalties or bypass loopholes compared to preceding software ROP mitigation techniques. At some point, we expect browser vendors to expand this protection further to most processes including renderers.

> Intel® CET is an effective protection against ROP/JOP RCE exploits if fully implemented by OSes and application developers. Presuming that NX is being used, the PAMS model estimates that the widespread adoption of CET would result in a 35% reduction in attack surface for ROP/JOP exploits. This is based on a conservative estimate that 60% of serious attacks and vulnerability exploits rely on ROP/JOP in conjunction with memory corruption and that earlier software measures were 25% effective at blocking these exploits. Intel® CET is considered one of the most significant security improvements in the vPro architecture.

Windows Secured-core PCs are a new type of device introduced in conjunction with Microsoft designed to provide a high level of security for enterprise and government customers. The devices are built with a chain of trust that starts at the hardware level. Key features of Windows Secured-core PCs—Dynamic root of trust for measurement, memory access protection, SMM protection, Hypervisor code integrity—depend on corresponding features from Intel vPro: TXT, IRBR, ISSR, ISRD, VT-d, and VT-x. UEFI secure boot further allows Microsoft to specify that only Microsoft-signed bootloaders are authorized. These devices are also more resistant to attacks thanks to virtualization-based security and hypervisors. The Virtualization-Based Security (VBS) feature creates a secure partition for the OS and applications, isolated from the rest of the device, making it more difficult for attackers to access sensitive information or take control of the device. PAMS estimates that these non-virtualization measures to secure the boot path offer up to an additional 15% reduction and that VT-d and VT-x combine to offer up to a further 5% reduction each.

Intel TDT includes several features such as Accelerated Memory Scanning, Cryptojacking Detection, and Anomalous Behavior Detection. These features use hardware-based monitoring to detect and prevent malicious activity, such as malware and cryptocurrency mining, on a system. TDT is supported in Windows 10 and Windows Server systems through the Windows Defender Advanced Threat Protection (ATP) feature, which allows IT administrators to configure the settings. TDT is expected to be supported in Linux in the future.



TDT improves the performance of Endpoint Detection and Response (EDR) solutions by offloading functions to hardware metrics or auxiliary GPU processors, reducing the resource impact of EDR. The EDR market is growing due to the need to protect against advanced threats and secure sensitive data, and TDT can further accelerate the adoption of EDR by making it less resource-intensive. TDT makes EDR faster, but it does not significantly reduce the attack surface beyond the initial attack surface reduction from deploying EDR, for the purposes of this analysis. The attack surface reduction effect of TDT may be overshadowed by the security impact of memory encryption and CET, particularly the latter which has the potential to be a fundamental ground shift in information security.

Intel® TME is a hardware-based security feature that encrypts all system memory in DRAM, including OS and application data. This helps protect against physical memory attacks where an attacker gains access to the memory and extracts sensitive information, reducing the chances of many forms of information leak exploits. TME-MK is an extension of TME that allows virtual containers/machines to use multiple keys for encrypting different memory regions, providing an additional layer of security through individual data isolation. This technology is expected to play a key role in assembling hardware level integrity for virtualized systems with the release of Intel 13th generation systems and future versions of Microsoft Windows OS.

Kernel information leaks refer to vulnerabilities in the OS kernel that allow attackers to access sensitive information stored in memory. Although kernel information leaks are relatively uncommon compared to other vulnerabilities, they can have a significant impact when they occur because they provide attackers with high-level access to the system. The attack surface reduction contribution of TME and TME-MK may be overshadowed by other hardware mitigations, but they are considered the building blocks for a more significant defensive structure in future processor generations.

The accumulated security measures in the 13th generation of Intel® vPro hardware aims to reduce the attack surface through the implementation of several hardware attack countermeasures. Microsoft has implemented several security measures for the Windows kernel based on the intel hardware security building block Intel has provided, such as Hyper-V Isolation, Virtual Secure Mode (VSM), Virtualization-Based Security (VBS), Hypervisor Code Integrity (HVCI), and Windows Hypervisor Platform. These features use hardware-assisted virtualization to isolate and protect the Windows kernel from malicious code and other security threats. Intel® CET protected software from ROP exploits, but attackers were still looking at data-only attacks or modifying page tables to achieve code execution. Intel® VT-rp with its hypervisor page table HLAT protection will significantly shrink that vulnerability gap.

> The combination of these security measures with full multi-key memory encryption, which isolates memory between VMs and VMs from the hypervisor, will make it difficult for attackers to target OS kernels, both inside VMs and in virtualized hypervisors from host OSes. When fully supported by the OS, CET could stop ROP code execution in OS kernels, foiling privilege escalation and credential exfiltration, and making attack pivoting more difficult. VT-rp, HLAT, and OS virtualization support

stop known end runs to anti-ROP protection, and TME-MK offers memory encryption as a final wall of defense against hypervisor escape. PAMS projects a reduction of up to 10% from VT-rp.

CET protected software from ROP exploits (which was the most significant technique for real-world exploits on the OS kernel after CFG and the other mitigations were put in place) and after the deployment of CET attackers were looking at data-only attacks or to modify page tables to achieve code execution, simply because it was the only attack vector that still available in the kernel. Intel® VT-rp and HLAT protection will close that vulnerability gap, which means that attackers will potentially only have hardware attacks left as a method to get into the kernel.

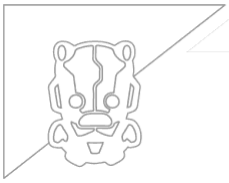
- Andrea Allievi, Senior Windows Core OS Developer at Microsoft

---

With the totality of protection features accrued through vPro hardware security advances severely restricting Windows, Linux, and other OS kernel exploit techniques, full software support should allow strong hardware-level VM isolation when completely leveraged by OS vendors. This latest architecture release from Intel may have reached a level of security robustness such that virtualized workloads will be able to run with the same or even greater security integrity guarantees compared to dedicated hardware. Complete utilization of vPro hardware security capabilities—between CET, TME-MK, VT-rp, and security technologies from previous generations—can potentially mitigate a massive subset of software-based attacks against the kernel by enabling robust code-execution memory-manipulation countermeasures and OS kernel security guarantees. The total Potientally Addressable Mitigation Surface provided by latest-generation vPro hardware security capabilities can be expressed as follows:

- **Securing the boot path: 15%**
- **Virtualization:**
  - VT-x: 5%
  - VT-d: 5%
  - VT-rp: 10%
- **CET: 35%**

Accumulating all of these reductions yields a maximum PAMS of 70% from the latest generation of vPro security features.



Appendix A: Overview of Intel® vPro Security Features

This report reviews critical security features spanning the 8th through 13th generation of Intel CPUs and the corresponding security claims for each generation. Following an enumeration of specific hardware and firmware features that enable these claims, we present a quantitative analysis of the maturity and effectiveness of the controls in the context of each claim.

All security features (even features before the 8th generation) are cumulative. Nth generation CPUs benefit from security features in N-1, N-2, etc., typically with extensions and enhancements. These features are also holistic: they should not be considered in isolation, but rather as a whole package larger than the sum of its parts.

Quantitative analysis of these kinds of claims is not easy, and it is often not practical to get hard data on exactly how many attacks are or could have been prevented—hard science quantitative analysis—without extensive empirical work. When available, IOActive uses such data. In most cases, however, IOActive has relied on soft science quantitative analysis and qualitative research. This means that while there might not be exact numbers for all of these security claims, credible sources have been consulted, analyzed, referenced, and quoted.

Table 1. Intel® Core Processor Generations[9]

Generation	Codename	Introduction
1	Nehalem	November 2008
2	Sandy Bridge	January 2011
3	Ivy Bridge	April 2012
4	Haswell	June 2013
5	Broadwell	September 2014
6	Skylake	August 2016
7	Kaby Lake	August 2016
8	Coffee Lake	October 2017
9	Comet Lake	April 2020
10	Tiger Lake	September 2020
11	Rocket Lake	March 2021
12	Alder Lake	October 2021
13	Raptor Lake	October 2022

[9] Source: https://en.wikipedia.org/wiki/Intel_Core

The Two Waves of vPro:

- First Wave (8th, 9th, and 10th Generation): The first set of vPro featured focused on closing off the most obviously important and vulnerable attack surface of the time, the integrity of the BIOS functions, low-level hardware drivers, and virtualizations.
- Second Wave (11th, 12th, 13th Generation): The second major set of features focused on the integrity of the whole platform, beyond the integrity of the low-level BIOS and drivers that the first wave specialized on. Adding anti-ROP/JOP control flow verification to stop most kernel and many applications attacks, encryption memory to put up a new barrier between virtualized environments, so the hypervisor can be fully bidirectionally isolated from the host memory space, and further enhancing the TDT GPU based security scanning and hardware security metrics and anomaly detection into some vertical detection user segments, as well as some interesting new features for "secured cores" to be resistant to even hardware tampering techniques like glitching.

Appendix B: Methodology for Assessing Quantitative Improvement

As we see from the timelines of the deployment and support for the Intel hardware mitigations, the task of quantifying any practical improvements from hardware security features is complex. The features occasionally have been found to be able to be bypassed, as there were a spate of such research findings in the 2017-18 time period as researchers verified the implementation details of these new mitigations. The major complicating factor is that the release of the hardware features precedes robust software support.

To that end, to quantify the security improvements available from the hardware feature set we define a metric called Potentially Addressable Mitigation Surface (PAMS). The Intel hardware security features offer robust, difficult-to-bypass exploit defenses that have a low performance impact—if they are enabled and supported by the OS, drivers and applications software.

We have seen the slow march of deployment of many of these features incrementally rolling out over real world applications as support is gradually baked into the OSes, then drivers, and eventually all the way up to user software level, but this is always a process that takes some non-zero finite amount of time as developers learn about how to implement the new features and roll them out to their exiting codebases in new updates.

This situation is also further complicated when it comes to measuring the impact of these hardware security mitigations because in almost every case, the hardware enforcement of the security defenses was preceded by some software variant of the same attempted countermeasure in some sort of software implementation of the defensive techniques. In every case the hardware implementation is far more optimal, effective, and less vulnerable to malicious manipulation than the preceding software attempts to try the same attack interdiction.

On both the attacker side and the defender side, there is a substantial time window between when the new mitigation equipped hardware is released and the new protections are integrated into many diverse code areas and systems—just as the attackers show a substantial delay between when vulnerabilities are discovered, and or disclosed and when wide scale exploitation is observed. Figure 1 is a chart of traffic spikes on Google's Virus Total service for major vulnerabilities disclosed in 2020 and 2021. It shows that exploitation lags discovery of vulnerabilities by as much as a year, while from the timelines to Intel vPro mitigation adoption above we can see that full support of defensive attack mitigations can sometimes take several years. The graph spikes correspond to attacker activity (and VirusTotal lookups) using that vulnerability; the major spikes are always many months after the initial vulnerability disclosure/discovery.

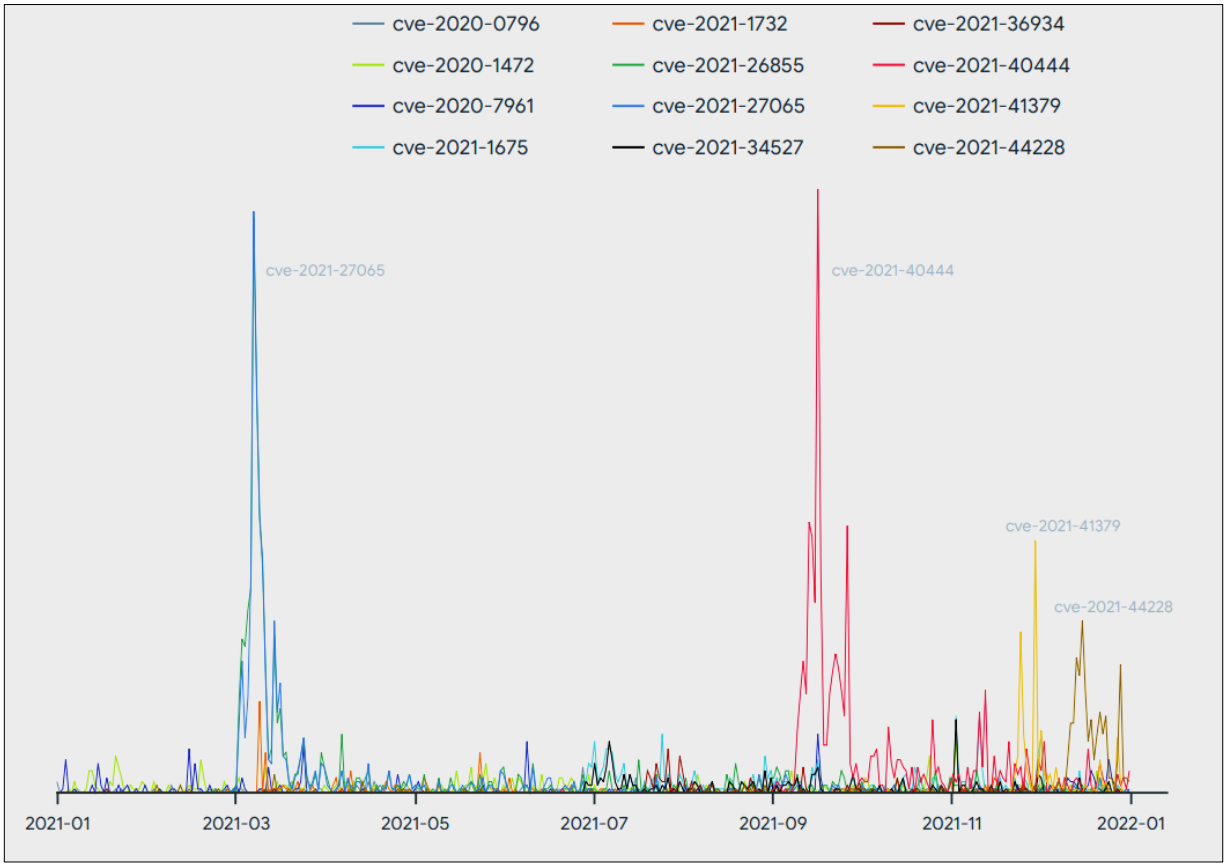
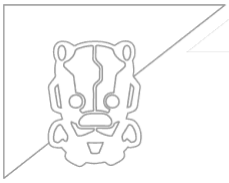


Figure 1. Exploitation Timeline for Serious Vulnerabilities Introduced in 2020 and 2021 (Source: Virus Total 2021 Malware Summary)

This implementation lag complicates estimates of the addressable attack surface reduction that these vPro hardware defenses offer. To try to get some true measure of the merit of the hardware mitigations in terms of a quantifiable measure, we will use an attack surface reduction metric dubbed PAMS. PAMS is a measurement of the attack surface reduction potential of the hardware mitigations based on theoretical, fully effective deployment of the features. The Intel hardware security features are robust—they just take some time to deploy and build into the software. Each of these Intel features offers software developers chances to shut some important doors that exploits use to corrupt memory, control program flow, and execute malicious functions, and PAMS is an estimated measure of the percentage of attacks that the particular mitigation could stop when fully deployed with support in the OS and other relevant software, by estimating the importance of the attack technique in question in the modern mix of exploits and attacks seen in the real world.

PAMS will be measured in percentage of exploit capability reduction. Each of these mitigations whittles away at the available attack surface for exploits. As empirical results accumulate, we will analyze the cumulative improvements offered by the three waves of Intel® vPro security defenses to establish more robust quantitative measures of the value added by these new vPro capabilities over the history of the Intel CPU line.



Appendix C: Acronyms

Acronym	Definition
ABD	Anomalous Behavior Detection
AES-NI	Advanced Encryption Standard New Instructions
APT	Advanced Platform Telemetry
ASLR	Address Space Layout Randomization
ATP	Advanced Threat Protection
AV	Anti-Virus
AVX-512	Advanced Vector eXtensions 512
CET	Control-flow Enforcement Technology
CFG	Control Flow Guard
DEP	Data Execution Prevention
EDR	Endpoint Detection and Response
EPT	Extended Page Tables
HLAT	Hypervisor-managed Linear Address Translation
IBT	Indirect Branch Tracking
iGPU	Integrated Graphics Processing Unit
IRBR	Intel® Run-Time BIOS Resilience
ISRD	Intel® System Resource Defense
ISSR	Intel® System Security Report
ITSC	Intel® Transparent Supply Chain
IVT	Intel® Virtualization Technology
JOP	Jump Oriented Programming
MPX	Memory Protection eXtensions
NX	No eXecute
OS	Operating System
PAMS	Potentially Addressable Mitigation Surface
PTT	Platform Trust Technology
RCE	Remote Code Execution
ROP	Return Oriented Programming
SHSTK	Shadow Stack
SRD	System Resource Defense
TDT	Threat Detection Technology
TME	Total Memory Encryption
TME-MK	Total Memory Encryption – Multi-Key
TRRC	Tunable Recovery Replica Circuit
TXT	Trusted Execution Technology
VBS	Virtualization-Based Security
VBS-Ci	Virtualization-Based Security of Code integrity
VDI	Virtual Desktop Infrastructure
VM	Virtual Machine
VMM	Virtual Machine Monitor

Acronym	Definition
VSM	Virtual Secure Mode
VT-d	Virtualization Technology - directed I/O
VT-rp	Virtualization Technology - redirect protections
VT-x	Virtualization Technology - x86
XD	eXecute Disable