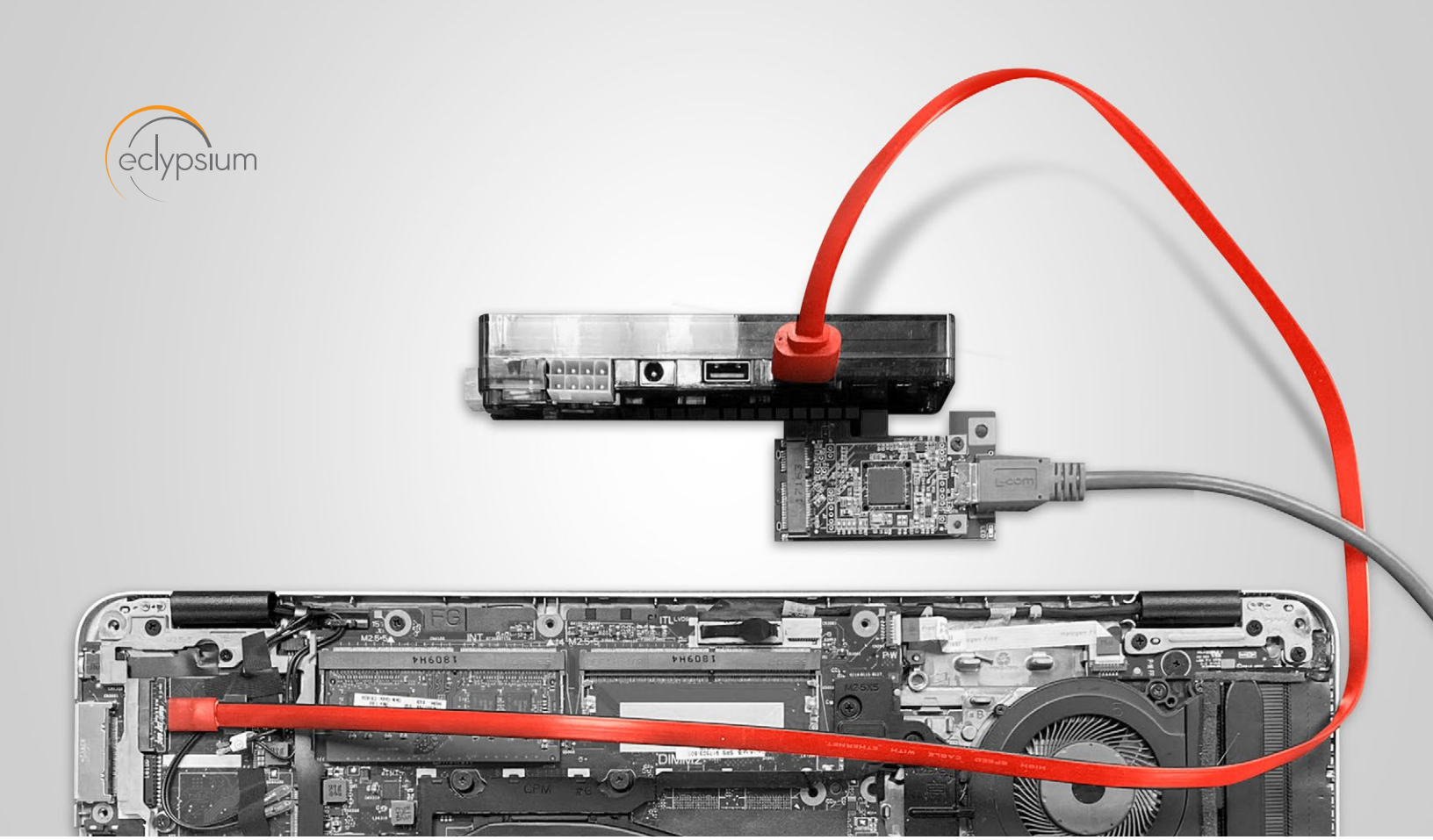


DIRECT MEMORY ACCESS ATTACKS

A WALK DOWN MEMORY LANE

HIGH-SPEED DMA ATTACKS BYPASS BUILT-IN HARDWARE PROTECTIONS ON ENTERPRISE DEVICES

Eclypsium's latest research shows that enterprise laptops, servers, and cloud environments continue to be vulnerable to powerful Direct Memory Access (DMA) attacks, even in the presence of protections such as UEFI Secure Boot, Intel Boot Guard, HP Sure Start, and Microsoft Virtualization-Based Security.

DMA attacks are a particularly powerful class of attacks for any adversary who has compromised firmware locally or remotely on peripheral hardware such as network cards, or who has physical access to a system. As the name suggests, DMA attacks enable a potential attacker to read and write memory off a victim system directly, bypassing the main CPU and OS. By overwriting memory, attackers can gain control over kernel execution to perform virtually any manner of malicious activity. We collectively refer to these as Memory Lane attacks.

While we will look at a few specific examples here, it is important to note this is an industry-wide issue. Previously, successful DMA attacks have been demonstrated against Intel NUC and Lenovo laptops, and these vulnerabilities apply equally to servers as well as laptops. While device vendors, chip vendors, and operating system vendors have all developed new controls to defend against these threats, our research shows that many devices with built-in hardware protections continue to be vulnerable.

For our research, we selected two representative laptops from leading manufacturers, HP and Dell, with enterprise-class hardware and software protections, and endeavored to determine whether they were susceptible to DMA attacks. We uncovered two different DMA vulnerabilities in the Dell and HP laptops, detailed below. Such attacks provide real-world examples of how weaknesses and threats at the hardware and firmware level can quickly subvert not only hardware protections, but also defenses at the operating system and software layers. They serve as a reminder to organizations that all security has limits, and vulnerabilities will be discovered. Hardware-based root of trust and chain of trust schemes are necessary but not sufficient protection. A layered, defense-in-depth approach should extend these technologies to detect and respond to new threats and vulnerabilities.

A DMA ATTACK PRIMER

Direct Memory Access is a capability designed into modern devices to provide components or peripheral devices with direct high-speed access to the system's memory. For example, a network adapter or Firewire device may need to read and write information quickly. Passing this traffic up to the OS and back down again is slow and inefficient. Instead, DMA allows devices to directly communicate with the system's memory without passing through the operating system.

While efficient, this capability also can provide attackers with direct access to information and kernel privileges. Tools such as Ulf Frisk's PCILeech provide a concrete example of how DMA attacks can work in the wild. PCIe devices come in many forms, with Thunderbolt ports being some of the most common. By connecting PCILeech to a system, an attacker can directly read and write to system memory, and extend control over the execution of the kernel itself. This can allow an attacker to execute kernel code on the system, insert a wide variety of kernel implants, and perform a host of additional activity such as spawning system shells or removing password requirements.

While many DMA attacks require physical access to the device, some can also be mounted remotely. For example, software that has already compromised a system can modify firmware to gain privileges within the system via DMA. Remote DMA attacks have also been demonstrated across a network. Physical DMA attacks can be closed-chassis or open-chassis. In a closed-chassis attack, DMA is accessed via an externally available port such as Thunderbolt, while the device remains closed. Conversely, an open-chassis attack requires an attacker to physically open the case to gain access to the internal hardware of a device, raising the difficulty and risk of detection for such an attack.

Over the last decade, chipset and hardware vendors have introduced new technologies aimed at stopping DMA-based threats, but the necessary firmware and operating system support has only recently started to reach customers. For example, Intel and AMD have introduced input output memory management unit (IOMMU) technologies, which aim to provide additional security between physical IO devices and memory. Intel's Virtualization Technology for Directed I/O, (VT-d), inserts logic in the chipset that can create protection domains between DMA-capable devices and the computer's physical memory. In order to fully close the pre-boot DMA gap, both UEFI firmware and the OS need to support the DMA protection using IOMMU (VT-d) hardware. If the firmware leaves the DMA protection on while it transfers control to the OS bootloader, but the OS does not update the DMA remapping controls as needed, normal system functionality will be broken due to incorrectly blocked DMA operations. Firmware support to protect against these attacks did not exist in the UEFI reference code until 2017 and the first devices with this support became available to customers only in 2019. On the OS side, Windows 10 1803 released in the Spring of 2018 was the first version that supported leaving DMA protection on while the OS boots. However, as we will demonstrate, the mere presence of technologies like IOMMU does not necessarily keep a device safe from DMA attacks.

Let's take a look at a few examples, including two new vulnerabilities discovered by the Eclypsium team and mitigated by the affected vendors.

CLOSED-CHASSIS DMA ATTACK - DELL XPS 13

As part of our ongoing research into firmware attacks, we tested a relatively new device from Dell, the XPS 13 7390 2-in-1. Released in October 2019, the 7390 2-in-1 is the convertible follow-on to Dell's highly popular XPS 13 laptop. The device we tested was based on Intel's 10th generation Ice Lake processor.

We quickly found that the XPS 13 7390 was susceptible to pre-boot DMA attacks. We were able to perform DMA code injection directly over Thunderbolt during the boot process. This closed-chassis DMA attack can be performed considerably faster and with less risk than an open-chassis attack, as an attacker could simply connect to the exposed port of the device without otherwise having to modify the device.

This issue in the firmware settings of the device was due to an insecure default BIOS configuration in the XPS 13 7390, which was set to "Enable Thunderbolt (and PCIe behind TBT) pre-boot modules". We notified Dell of this issue and recommended that this setting be set to "off" by default.

VENDOR MITIGATIONS

Dell has published a security advisory to address this issue at https://www.dell.com/support/article/SLN319808 and has confirmed that all other platforms supporting Thunderbolt have this setting turned off by default.

OPEN-CHASSIS DMA ATTACK - HP PROBOOK 640 G4 WITH HP SURE START GEN4

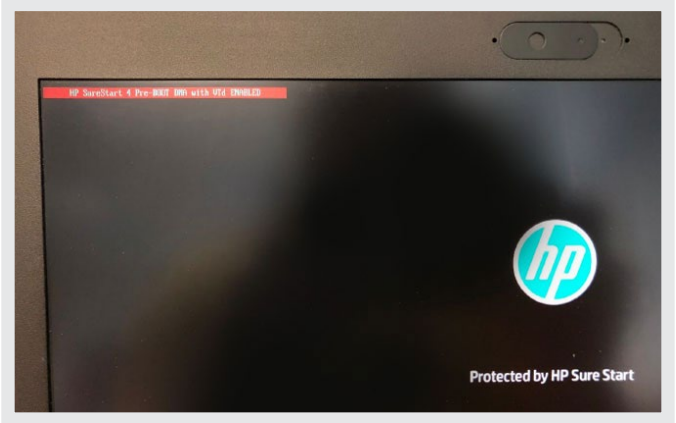
As part of this same research project, we acquired an HP ProBook 640 G4, designed with enterprise-grade performance, security, and manageability, including HP Sure Start Gen4. Among other capabilities, HP Sure Start incorporates an embedded controller designed to verify the integrity of the BIOS before the CPU executes its first line of code. Although this device was not vulnerable to closed-chassis attacks, we discovered that, even though the system was protected by HP Sure Start and VT-d was enabled, the platform was still susceptible to an open-chassis pre-boot DMA attack. Pre-Boot DMA attacks target the system UEFI and disrupt the chain of trust that ensures a secure boot process.

To defend against such an attack a system must ensure that unauthorized code is not allowed to execute from the beginning of the boot process until after the hand off to the operating system. A pre-boot DMA attack

works at this critical time, and has the potential to completely compromise a system, even when other code integrity protections (like HP Sure Start, Intel Boot Guard, or Microsoft Virtualization Based Security with Device Guard) are employed. Extending these protections to also cover DMA attacks is possible, but not necessarily in place on systems already in use.

While the overall process was relatively straightforward, the attack **did require us to open the case of the device**. As noted earlier, such an open-chassis DMA attack would raise the risk from an attacker's perspective, but would still remain plausible for a dedicated adversary.

Once the device was opened, we simply replaced the M.2 wireless card in the system with a Xilinx SP605 FPGA development platform. The FPGA was then connected to our attacking machine and tested the system against a well-known, public DMA attack technique. We were able to successfully attack the system and gain control over the device. By using DMA to modify the system RAM during the boot process, we gained arbitrary code execution, thus bypassing the HP Sure Start protections that verify BIOS code integrity before CPU execution starts.



While we specifically tested against the HP ProBook 640 G4 - a new model, available for purchase online still today - it is likely that other laptops are also similarly vulnerable. In fact, pre-boot processes are an area of weakness across all laptops and servers from many manufacturers. In the case of HP, while the machine was not susceptible to a closed-case attack, the version of HP Sure Start in the mode we tested was insufficient to protect against our type of attack. There are many components, from hardware to firmware to the operating system, that all need to work together to prevent pre-boot DMA attacks.

VENDOR MITIGATIONS

HP Sure Start Gen4 and earlier generations of devices didn't include DMA attacks in the threat model. HP Sure Start Gen5 added IOMMU based protection for closed-chassis DMA attacks via Thunderbolt, and in response to our research, HP decided to extend the HP Sure Start Gen5 threat model to now include and protect against open-chassis DMA attacks.

HP released an updated version of the BIOS on January 20, 2020.

HP has provided Eclypsium with an HP EliteBook 840 G6 that includes the most recent generation of HP Sure Start (Gen 5) and the latest version of BIOS (01.04.02 released on January 20th 2020). The device with this latest version of BIOS successfully protects against our attempts at open-chassis DMA attacks. We performed a number of tests with this latest version of the HP firmware and with the "pre-boot DMA protection" option set to "Thunderbolt only", we were able to reliably get arbitrary code execution during the boot process via DMA using the PCI Leech through the NVME M.2 card slot. However, after setting this option to "Thunderbolt and PCIe expansion card", we made multiple attempts to initiate DMA transactions with the PCI Leech and all attempted DMA read operations failed. When enabled, these new protections appear to mitigate the pre-boot DMA attack or minimize the window so that we weren't able to perform the attack.

SOFTWARE AND REMOTE DMA ATTACKS

It is important to note that DMA is a powerful technique that does not necessarily require the attacker to have physical access to the device. In fact, data centers and cloud environments can be at the greatest risk for remotely enabled DMA attacks.

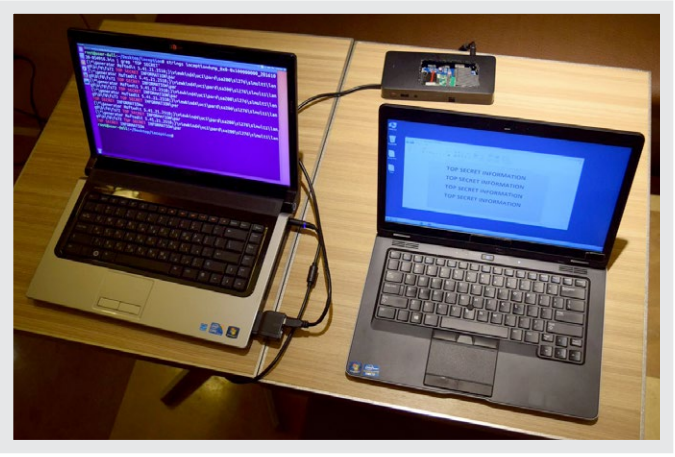
Parallel computing clusters often need to share large volumes of information between systems with extremely low latency. In the same way that DMA allows fast direct access between peripherals and system memory on a device, Remote DMA or RDMA provides similar direct access to memory between devices over Ethernet and other network interconnects. And once again, this direct access to memory can provide an avenue for attack. The Throwhammer exploit developed by VUSec provides a perfect example. In the case of Throwhammer, the VUSec team notes that:

"...an attacker can trigger and exploit Rowhammer bit flips directly from a remote machine by only sending network packets. This is made possible by increasingly fast, RDMA-enabled networks, which are in wide use in clouds and data centers. To demonstrate the new threat, we show how a malicious client can exploit Rowhammer bit flips to gain code execution on a remote key-value server application."

DMA attacks can also be used by traditional malware-based attacks as a way of gaining additional privileges and control over a compromised host. For example, malware on a device could use a vulnerable driver to implant malicious firmware to a DMA capable device such as a NIC. That malicious code could then DMA back into memory during boot to get arbitrary code injection during the boot process. The fundamental ability of DMA attacks to shim attacker code into the boot process makes it useful for almost any type of attacker goal.

WIGIG EXAMPLE

Earlier, the Intel Advanced Threat Research team demonstrated performing a DMA attack over the air by modifying a WiGig dock to compromise a Dell laptop wirelessly connected to the dock. The network architecture of WiGig uses PCIe tunneled inside of wireless network packets, and we were able to use the DMA capabilities of this functionality to dump secrets out of the laptop remotely over the air. In this example the laptop was never touched by the attacker or physically connected to any device, but was compromised remotely via DMA.



Source: https://twitter.com/c7zero/status/792860835706130433

SUMMARY - TRUST, BUT VERIFY

This research demonstrates that despite increasing manufacturer attempts at firmware and hardware protection, DMA attacks are still a problem. While manufacturers have started to add protections against closed-chassis DMA attacks over Thunderbolt, these protections are not always sufficient or enabled by default, leaving unsuspecting enterprises to think they are protected when they are not. Furthermore, these closed-chassis mitigations have failed to address open-chassis attacks using WiFi or WWAN card slots. Protections such as HP Sure Start previously did not include DMA attacks in their threat model until the latest generation of hardware and firmware. DMA attacks can be devastating to the integrity of a system. With the ability to read and write data and gain control of the kernel, attackers are limited only by their imagination in their use and abuse of this capability.

The escalating threat from firmware and hardware attacks has begun to be recognized by the industry, motivating new efforts such as the Secured-core PC initiative, introduced last October by Microsoft for some new Windows-based laptops. We are very supportive of the work PC OEMs and OS vendors are doing to design in more hardware protection. We will continue to research the effectiveness of these new protection initiatives to identify the gaps firmware attacks can exploit. We also recommend enterprise security leaders continue to adopt a policy of trust, but verify.