Solution Brief

Thunderbolt™ Security – Helps Keep Your Computer Ports More Secure

As part of Intel's Security-First Pledge, we are committed to continuously improving security over the Thunderbolt™ port.

Summary

Intel® Virtualization Technology for Directed I/O (VT-d), specialized hardware capabilities built into Intel processors is the foundation for DMA protection on Thunderbolt ports that helps prevent physical DMA attacks. These solutions block peripheral devices from unauthorized access to system memory.

Leading operating systems such as Windows, MacOS, and Linux have already implemented DMA protection using Intel VT-d technology.

Intel's Thunderbolt 4 certification requires VT-d based DMA protection. It is strongly recommended on computers with Thunderbolt 3 ports and has been enabled on PCs, where supported, since 2019.

Intel recommends standard security practices to reduce the risk of physical attacks. Such practices include using only trusted peripherals and preventing unauthorized physical access to computers. Hard disk drive encryption and a BIOS password can provide additional protection.

In Detail

With USB-C connector-based computer ports that provide PCI Express (PCIe) protocol, users can connect PCIe devices to the computer just as if they were installed internally. Such devices include portable and desktop storage, external graphics, memory card readers, ethernet adapters and other PCIe-based devices.

PCIe devices are unique because they are capable of Direct Memory Access (DMA), which enables fast and efficient access to the system memory without involving the processor. However shared memory between all the different devices in the system including those that are externally connected via the USB-C port may present a security risk if not properly protected.

Security for Thunderbolt computer ports is hardware-based and built on Intel's Virtualization Technology for Directed I/O (Intel VT-d), an Intel processor technology that provides IO virtualization (often referred to as IO Memory Management Unit or IOMMU). One of VT-d technology's features is DMA remapping (DMA-r) which is used for DMA protection by operating systems and BIOS. DMA-r helps protect the system memory by providing

an isolated memory region for each device connecting to the system. This way a device will only have access to its assigned memory and cannot read or write to other memory areas outside its own.

The following operating systems versions have VT-d and DMA-r based protection against DMA attacks on Thunderbolt™ computer ports:

- Windows OS implementation, known as Kernel DMA Protection, exists on all Windows 10 versions starting with 1803 (RedStone 4) and is enabled by default on systems that support it. To read more about Windows Kernel DMA protection please refer to this article.
- Mac OS VT-d based security has been supported since version 10.8.2 (2012). To read more click on this link.
- On Linux VT-d based security has been supported since Kernel version 4.21.

Operating system implementation helps protect the system during run time. In order to help protect against DMA attacks before the system boots and until the transition to the operating system, Intel has implemented UEFI firmware (BIOS) support for DMA-r based security that helps block devices from unauthorized access to system memory.

Although physical attacks may be hard to perform and require that an attacker possess your PC, nonetheless, Intel recommends standard security practices to reduce the risk of physical attacks. Such practices include using only trusted peripherals and preventing unauthorized physical access to computers. Hard disk drive encryption and a BIOS password can provide additional protection.

Disclaimers

- Intel technologies may require enabled hardware, software or service activation.
- No product or component can be absolutely secured.
- Your results may vary.