Thunderbolt™ 3 and Security on Microsoft Windows® 10 Operating system

September 2018

Scope

This document provides information on the Intel® Thunderbolt™ 3 controller security features on Microsoft* Windows 10 operating system. It focuses on the PCI express I/O related security features.

Targeted audience

This document is intended for Thunderbolt™ 3 users who may have questions or concerns regarding Thunderbolt™ security and would like more information.

Background

The Thunderbolt™ controller is a PCIe device, which means that it has Direct Memory Access (DMA) IO (via PCIe), and exposes the PCIe protocol externally through USB-C ports for a range of usages. This potentially allows access to system memory from a physical IO device that is being connected and utilizing the PCIe protocol. In order to mitigate potential malicious access to system memory from an external PCIe device, there is security protection with Thunderbolt™ 3 that prevents unauthorized Thunderbolt™ PCIe-based devices from connecting without user authorization. For instance, this will prevent unauthorized access when the system is locked. This is achieved by the following set of capabilities:

- **Software based authorization of Thunderbolt™ 3 Ports:** Thunderbolt™ 3 ports are controlled by a utility software and driver provided by Intel, that allows the user to decide whether a device's PCIe data path can connect to the system or not.
- **Policy management** (also referred to as **Security Levels**): This capability allow the user to decide between multiple levels of restricting policies such as disabling the Thunderbolt™ 3 port, allowing it but only with explicit approval of the user each time a device is connected, allowing only devices with cryptographic authentication or allowing it in a Display Port or USB only mode (more details below)
- **Pre-boot protection** Thunderbolt™ devices are allowed to be enumerated and connected during boot time only if they have been approved by the user before.

In this paper we will discuss in further detail the various security features that help protect[†] the PC from potential known Thunderbolt™ 3 related PCIe IO vulnerabilities.

Thunderbolt™ 3 Security Features details and definitions

Authenticating newly attached device

Firmware and software supported feature that requires user approval before allowing a PCIe capable Thunderbolt™ connection for the first time, supported on Thunderbolt™ starting in 2013

Cryptographic Authentication

Cryptographic authentication of connection to help prevent a peripheral device to be spoofed to masquerade as an "approved" device to the user (authentication of the connection), supported from Thunderbolt™ 2 products onward, starting in 2014

Separating Thunderbolt™ data stream

Separating Thunderbolt™ data stream from display tunneling to help prevent walk-up access of PCIe unless it is specifically allowed.

Unique ID number

Every Thunderbolt™ 3 Controller has a unique ID fused in silicon during production, this allows to identify a specific device

ACL - Accepted Components List

A list of Thunderbolt™ devices ("components") that the user has already approved to enumerate and can connect automatically

Security Levels (SLx)

Thunderbolt™ enables implementation of different security policies.

These modes apply to PCIe protocol, while DisplayPort connects by default as it has no DMA capability exposure

SL 0: No limitations, everything enumerates and connects (2011 and newer)

SL 1: Ask for permission to connect device (2013 and newer) – **the default mode**

Require (admin level) user permission to add new PCIe enabled devices (SL1 security)

The Thunderbolt™ software on the PC maintains a list of the Unique IDs for every Thunderbolt™ peripheral that has received user permission to "always connect." (Access Control List)

If the Unique ID of the Thunderbolt™ peripheral is not on the ACL, the PCIe connection is not allowed until the user responds to a connection prompt, typically with the following options:

(1) Connect one time, (2) Always connect, (3) Do not connect

Connection permissions are managed per PC, and not per user login.

SL 2: Only devices with HW cryptographic authentication are added (2014 and newer)

Hardware based challenge / response - The first time a Thunderbolt™ peripheral's Unique ID is granted "always connect" PCIe access, a key is written to the peripheral controller's non-volatile memory and added to the host PC's ACL list. Each time a peripheral's Unique ID is found on the ACL, the PC's controller sends a security challenge. The response from the peripheral is then verified before the PCIe connection is allowed. If the response is not valid, the user receives a connection permission prompt.

Beyond the new hardware cryptographic authentication the user experience is the same as SL1

SL 3: TBT mode is set to "Display Port only and will not tunnel or transmit PCIe data. (2013 and newer)

† No computer system is absolute secure