black hat USA 2020

AUGUST 5–6, 2020

BRIEFINGS

When Lightning Strikes Thrice: Breaking Thunderbolt 3 Security

Björn Ruytenberg

Eindhoven University of Technology

@0Xiphorus • bjornweb.nl

Who Am I

Björn Ruytenberg
@0Xiphorus

Vulnerability researcher

Main interests: hardware and firmware security, sandboxing, input validation

More about me: https://bjornweb.nl

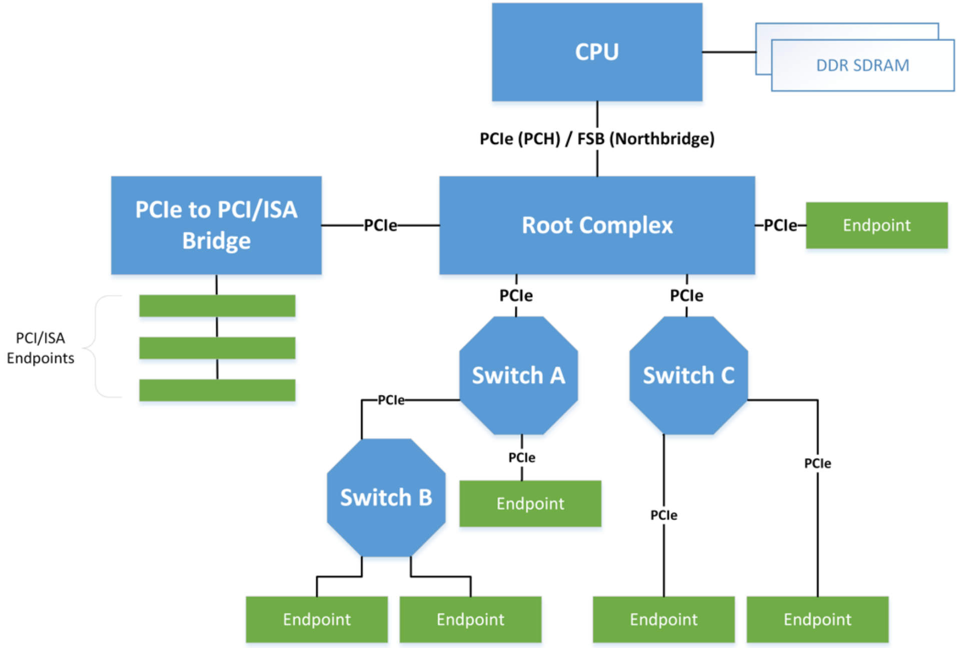
MSc student in Computer Science @ TUE

- This work part of master's thesis

TU/e EINDHOVEN UNIVERSITY OF TECHNOLOGY

PCI Express Basics – Quick Review

- A standardized interconnect for attaching hardware devices in a computer system
- Designed as CPU-architecture agnostic, internal I/O interconnect for low-latency, high-bandwidth
- Intended to overcome limitations of PCI, most notably:
  - Scalability: per-device configurable bandwidth, flexible link width
  - Networking: moves from *bus* to *packet switching*; allows for more flexible topology, QoS / congestion control
- Network topology: root complex, switch, endpoints, PCIe to legacy bridge (e.g. ISA/PCI/PCI-X)
- Direct Memory Access (DMA) primary CPU-peripheral mode of transport

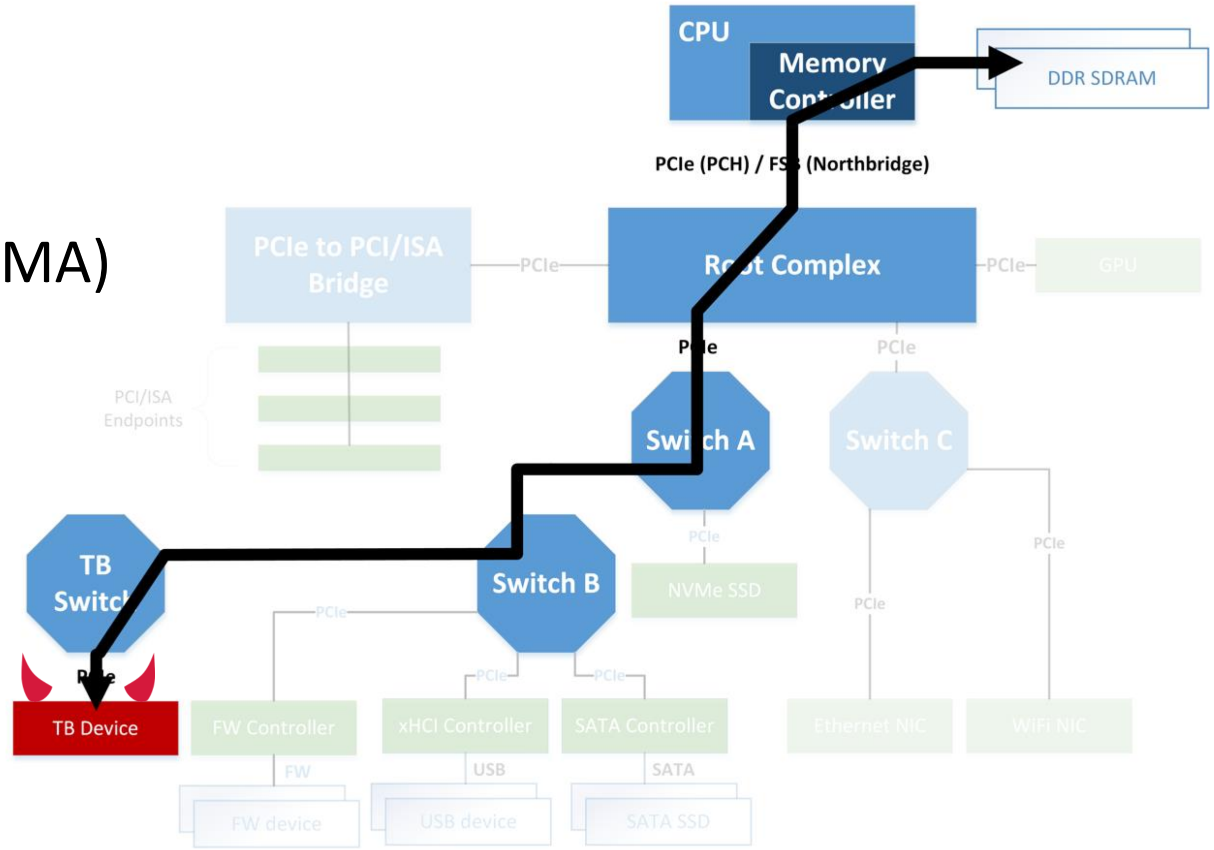


Thunderbolt: A PCIe-based Interconnect

- High-performance, proprietary I/O protocol developed by Intel and Apple
- PCIe-based, Direct Memory Access (DMA)-enabled I/O
- Use cases
  - External graphics, docking stations, 5K monitors, high-speed external storage, peer-to-peer networking
- Thunderbolt 1 (2011) and 2 (2013) mostly exclusive to Macs
  - Mini-DisplayPort form factor – multiplexes TB, native DP
- Thunderbolt 3 (2015) first version to be widely adopted
  - USB-C form factor – multiplexes TB, native DP and/or USB-C

DMA attacks

- **Thunderbolt 1**: no protection against physical attacks
- Plug in malicious device
  → Unrestricted R/W memory access (DMA)
- Access data from encrypted drives
- Persistent access possible, by e.g. installing rootkit



DMA attacks (selected)

- **Owned by an iPod [Dornseif 2004]**
  - First research to demonstrate practical DMA attack
  - Malicious FW device presents Serial Bus Protocol 2 (SPB-2) endpoint, which triggers host controller to allocate DMA channel for fast bulk data transfers
  - Several authors release exploitation tools [Boileau 2006] [Plegdon 2007]
  - Improved upon for memory forensics [Witherden 2010]
  - "Improved upon" in law enforcement spyware such as FinFireWire [Gamma 2011]
- **Subverting Windows 7 x64 kernel with DMA attacks [Aumaitre 2009]**
  - First PCI-based attack through custom PCI device with DMA engine
- **Inception [Maartmann-Moe 2014]**
  - Improves upon Witherden's `libforensic1394` by presenting virtual SBP-2 interface through ExpressCard, FW device + TB-to-FW adapter
- **PCILeech [Frisk 2016]**
  - Native PCIe attack
  - DMA attack using FPGA with PCIe PHY (full size, ExpressCard, miniPCIe, M.2-NVMe), optionally tunneled through Thunderbolt enclosure
  - Improved later with various functionality: e.g. dumping FDE keys, dumping UEFI memory regions, patching Windows lock screen process
- **Thunderclap [Markettos et al. 2019]**
  - Replaces PCIe endpoint in TB device with malicious one, then performs DMA attack
  - Does not break Security Levels access control, but relies on tricking user into authorizing malicious device

Threat Model

- Brief physical access to victim system, aka “evil maid attack”
- Example real-world scenarios:
  - Laptop locked or set to sleep; left unattended in hotel room, while victim is out for dinner
  - Desktop systems locked or set to sleep; left unattended outside office hours
  - Cleaning crew has unfettered access

Threat Model

Industry measures against opportunistic physical access

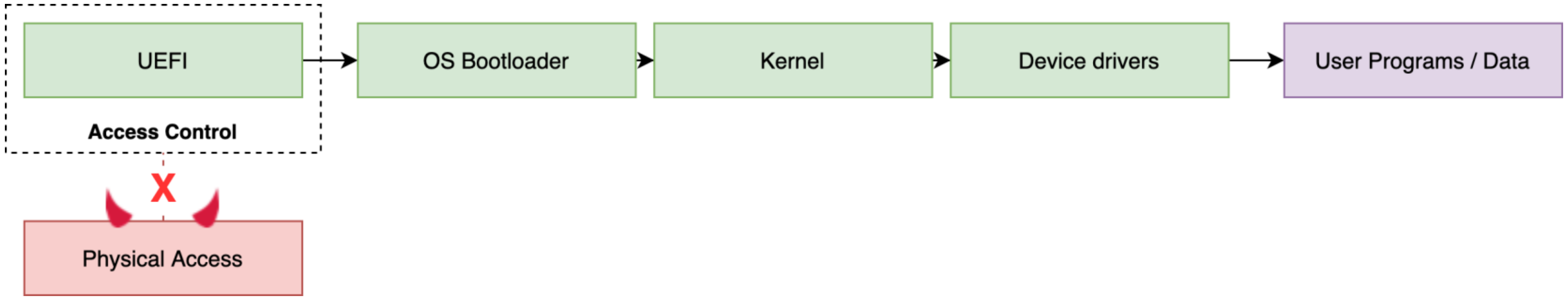
1. BIOS access control
2. Secure Boot
3. Boot Guard
4. Full Disk Encryption

…

Threat Model

Industry measures against opportunistic physical access

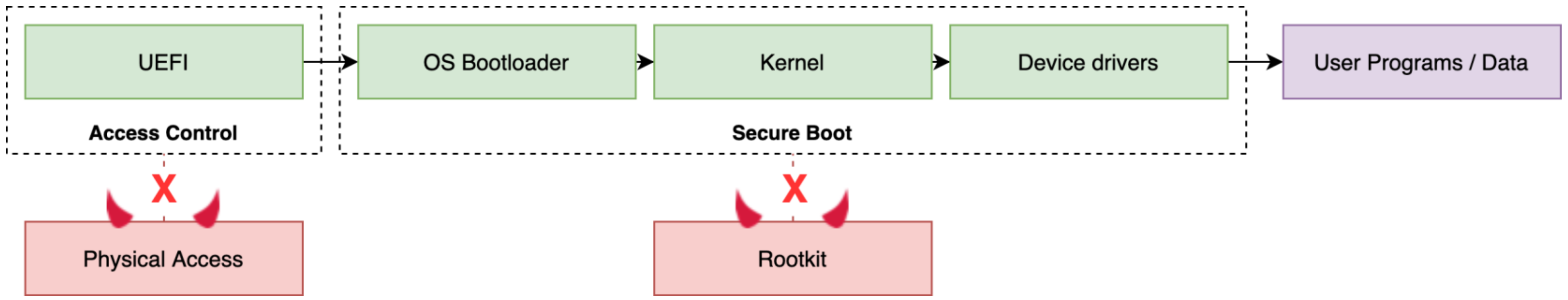
1. BIOS access control
   - Prevents unauthorized modification of system settings
   - E.g. require password on entering BIOS



Threat Model

Industry measures against opportunistic physical access

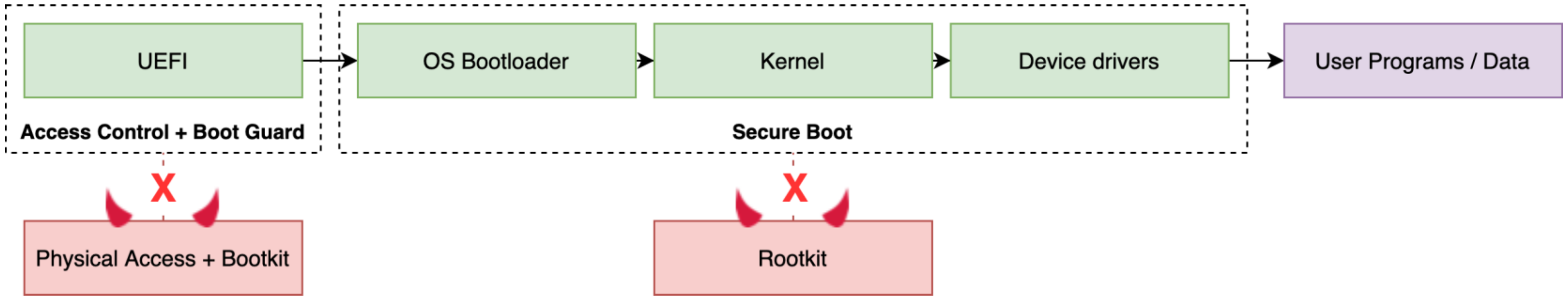
1. BIOS access control
2. Secure Boot
    - Protects against malicious, unsigned code early in boot process
    - Cryptographically verify boot chain: OS bootloader, kernel, drivers



Threat Model

Industry measures against opportunistic physical access

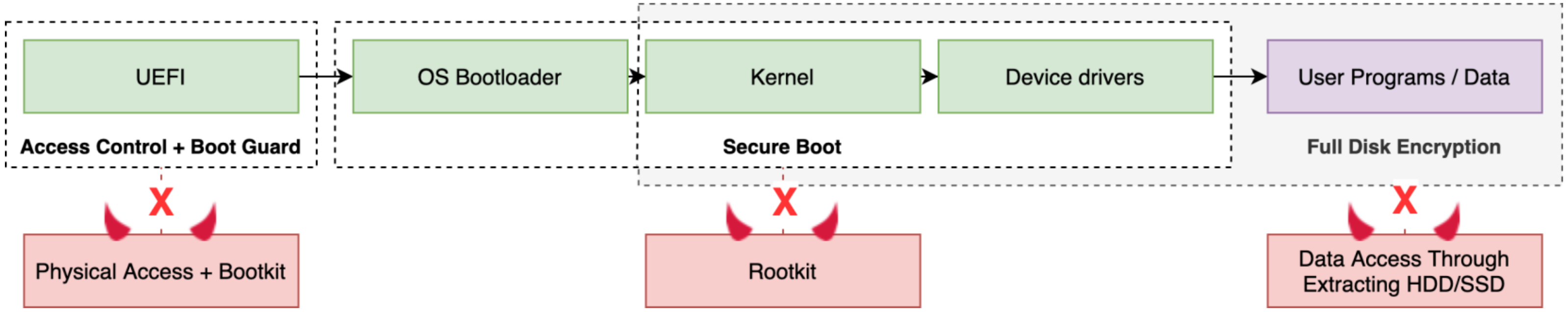
1. BIOS access control
2. Secure Boot
3. Boot Guard
   - Protects against malicious firmware implants
   - Cryptographically verifies BIOS integrity



Threat Model

Industry measures against opportunistic physical access

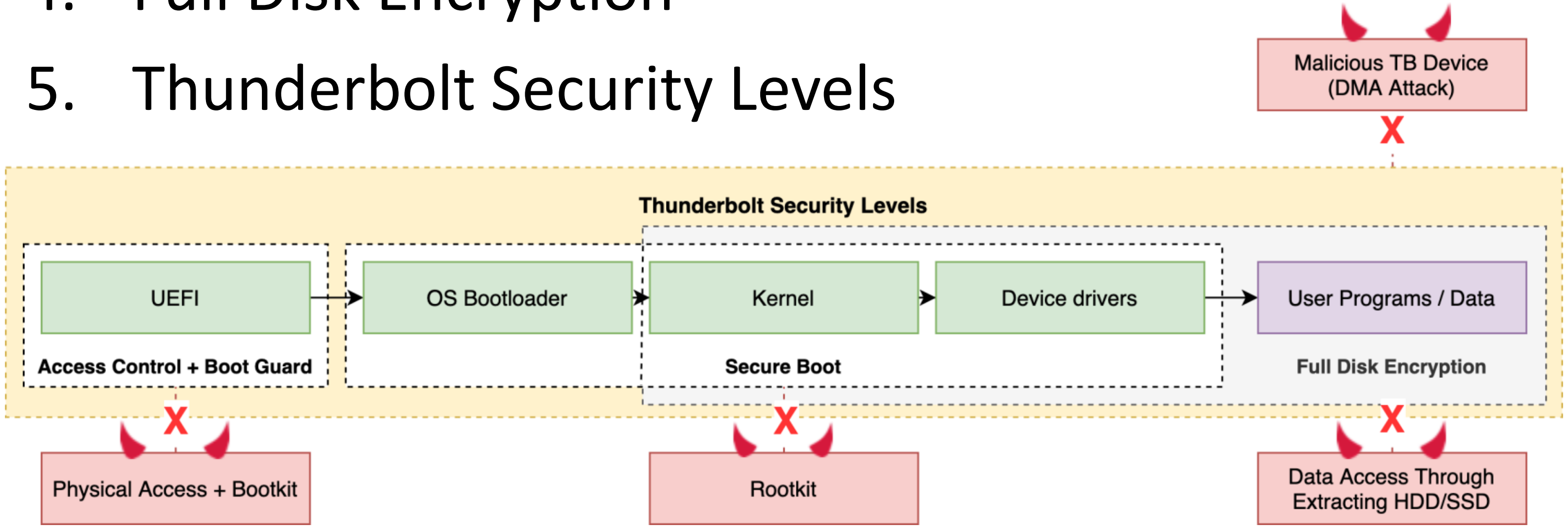
1. BIOS access control
2. Secure Boot
3. Boot Guard
4. Full Disk Encryption
   - Protects against physical data extraction
   - Encrypts user data + OS root (depending on FDE config)



Threat Model

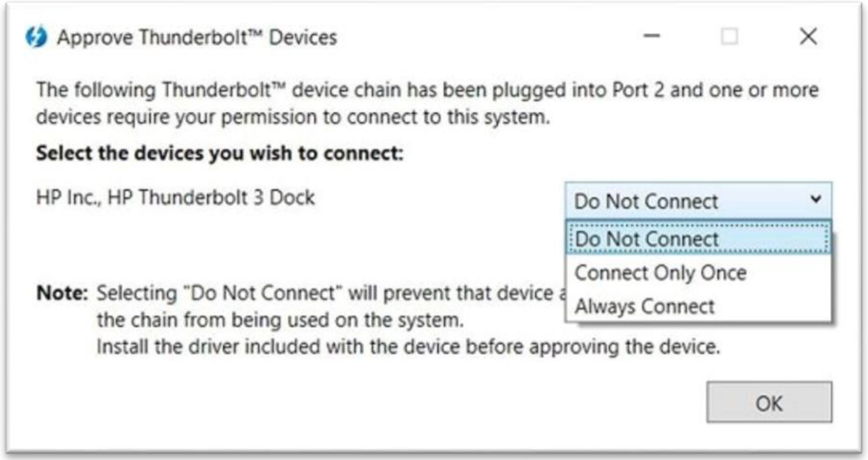
Industry measures against opportunistic physical access

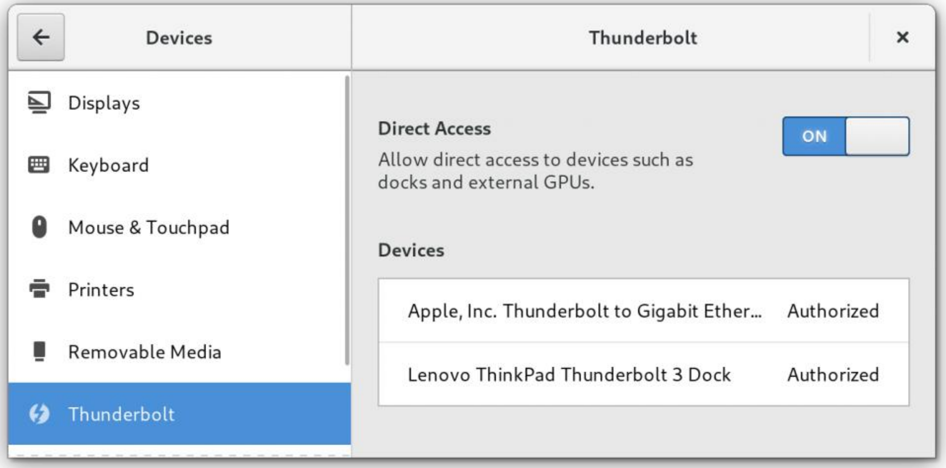
1. BIOS access control
2. Secure Boot
3. Boot Guard
4. Full Disk Encryption
5. Thunderbolt Security Levels



Thunderbolt Security Architecture

- **Security Levels** – access control system enabling users to authorize trusted device only
- Introduced in Thunderbolt 2
- No authorization = No PCIe tunneling

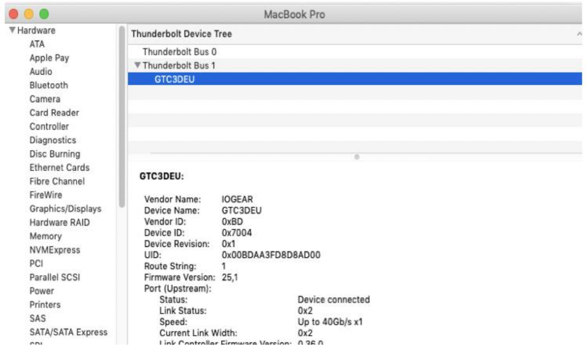


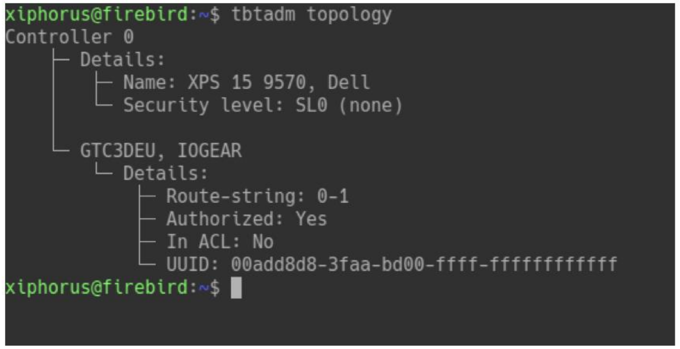


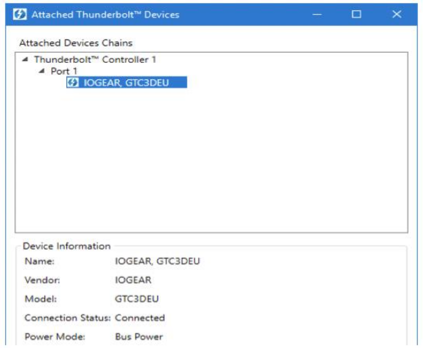
Thunderbolt Security Architecture

Thunderbolt devices authenticate to the host using the following metadata:

- **Device ID:** 16-bit device identifier
- **Device name:** ASCII string
- **Vendor ID:** 16-bit vendor identifier
- **Vendor name:** ASCII string
- **Universally Unique Identifier (UUID):** 64-bit number uniquely identifying device, fused in silicon







Source: Thunderbolt 3 and Security on Microsoft Windows 10 Operating System – Intel Corporation

black hat USA 2020

Thunderbolt Security Levels

	Definition
SL0 None	• No security (legacy mode)
SL1 User	• Device authorization ACL based on UUID • UUID fused in silicon • Default setting on all PCs
SL2 Secure	• Device authorization based on UUID (SL1), *plus* • Cryptographic device authentication (challenge-response)
SL3 No PCIe tunneling	• Disable all Thunderbolt connectivity • USB and/or DisplayPort tunneling only
SL4 Disable daisy-chaining	Terminate PCIe tunneling at first TB device (some Titan Ridge controllers only)
Pre-boot protection	PCIe tunneling enabled only if Thunderbolt device previously authorized by user

Security Levels prevent malicious TB devices from accessing PCIe domain, thereby protecting against:

- Device-to-host DMA attacks
- Device-to-device (P2P) DMA attacks
- PCI ID spoofing to target vulnerable device drivers
- TLP source ID spoofing

Source: Thunderbolt 3 and Security on Microsoft Windows 10 Operating System – Intel Corporation

Introduction to Thunderspy

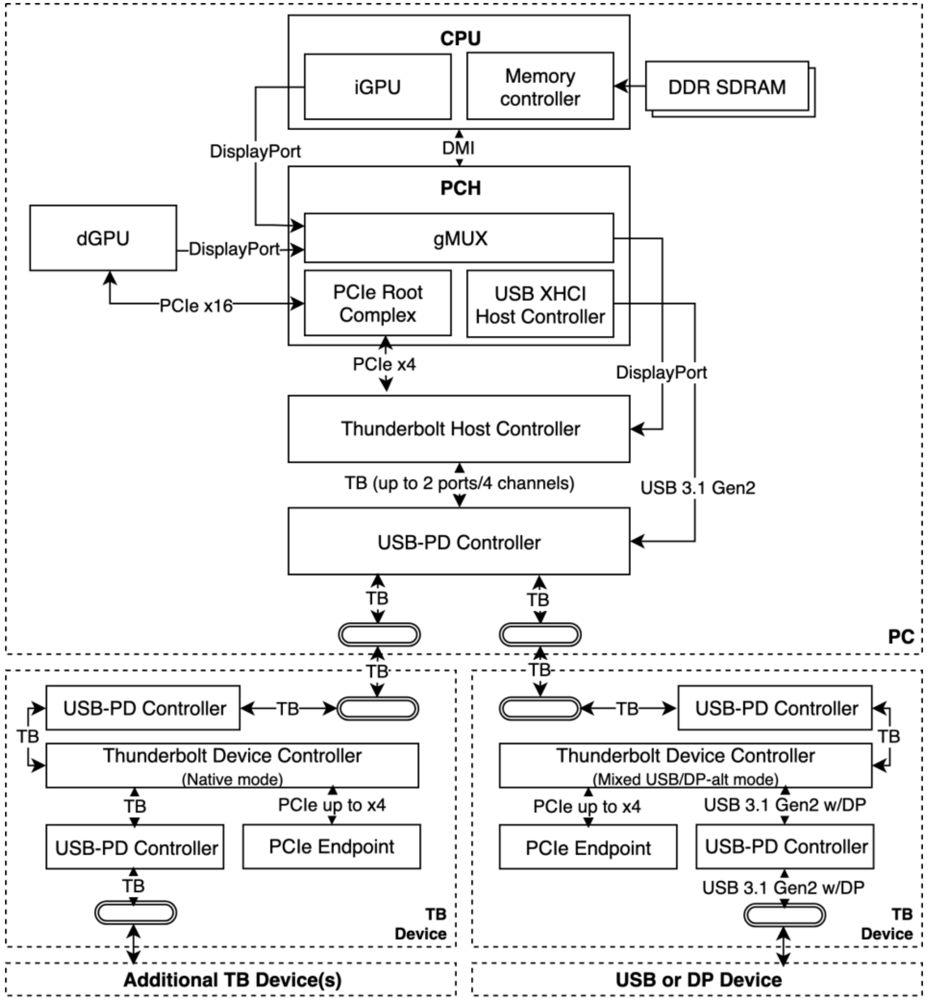
- Previous research:
  - Before Security Levels: attacks primarily focus on PCIe-level DMA attacks to compromise Thunderbolt security
  - After Security Levels: attacks require cooperation of user, i.e. inadvertently connecting malicious peripherals
- Thunderspy is a new class of vulnerabilities that breaks Thunderbolt protocol security
- First attack on Thunderbolt Security Levels
- 7 vulnerabilities and 9 practical exploitation scenarios

THUNDERSPY

Identifying attack surfaces

- Thunderbolt is a proprietary standard
- Protocol specifications not publicly documented
- Hardware architecture not publicly documented
- Dissected various Thunderbolt devices and Thunderbolt-equipped systems

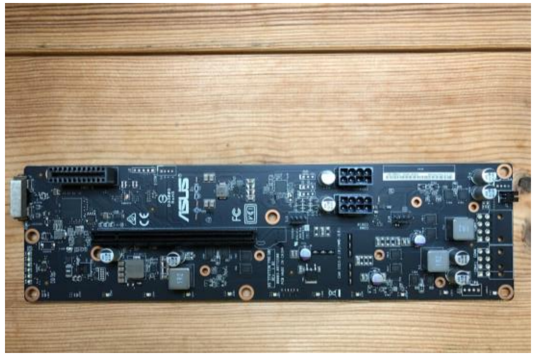
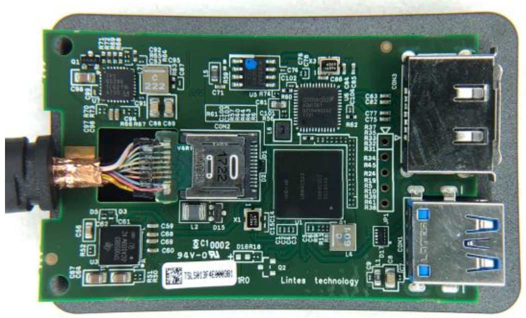
Our Analysis of TB Hardware Architecture



Identifying attack surfaces

- Thunderbolt is a proprietary standard
- Protocol specifications not publicly documented
- Hardware architecture not publicly documented
- Dissected various **Thunderbolt devices** and Thunderbolt-equipped systems

Thunderbolt Devices



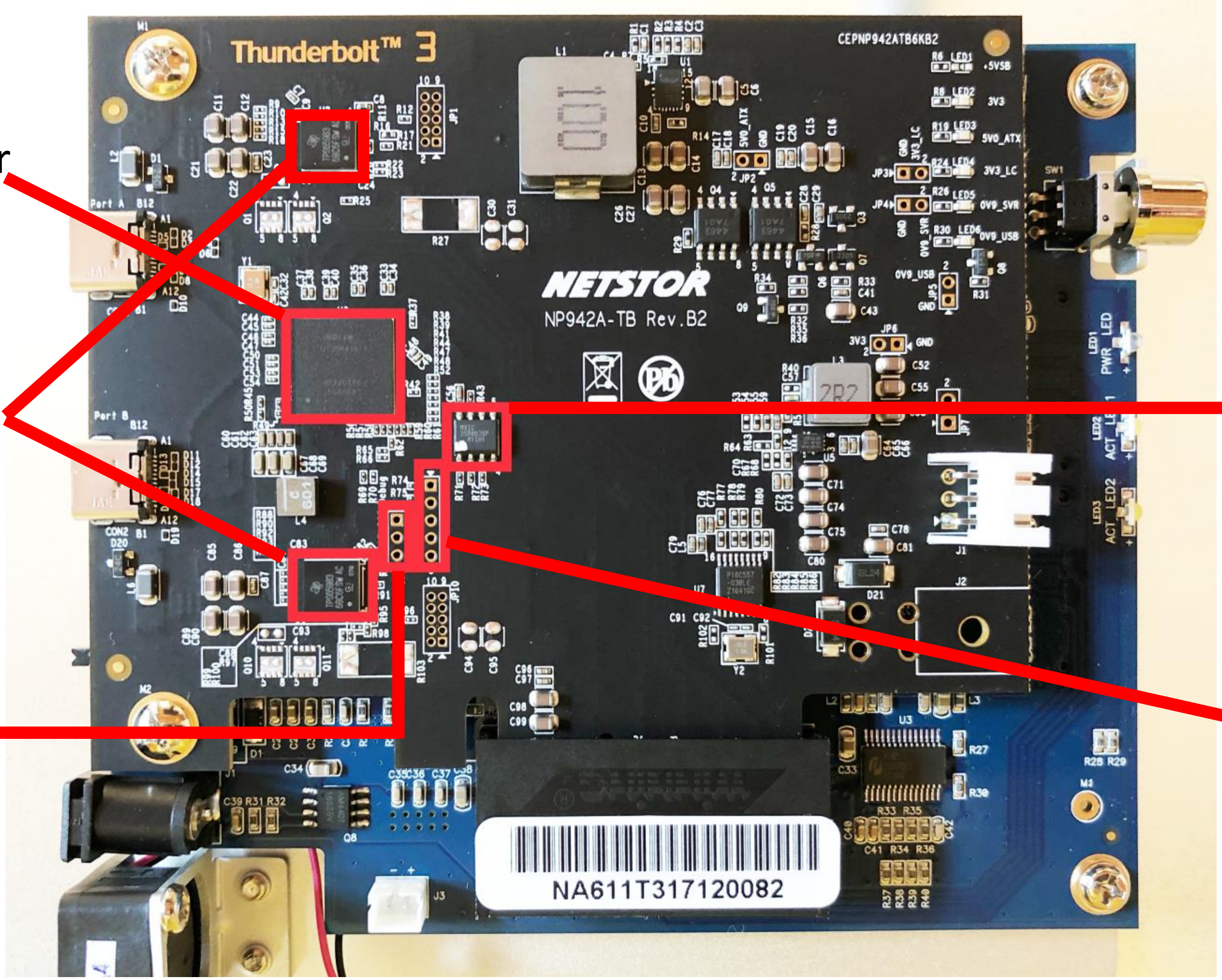




NetStor Thunderbolt NVMe Enclosure

Intel JHL6540
TB 3 host/device controller
4-channel, dual port

2* TPS65983
USB Type-C PD Controller
Power Switch
High-speed Multiplexer



I²C

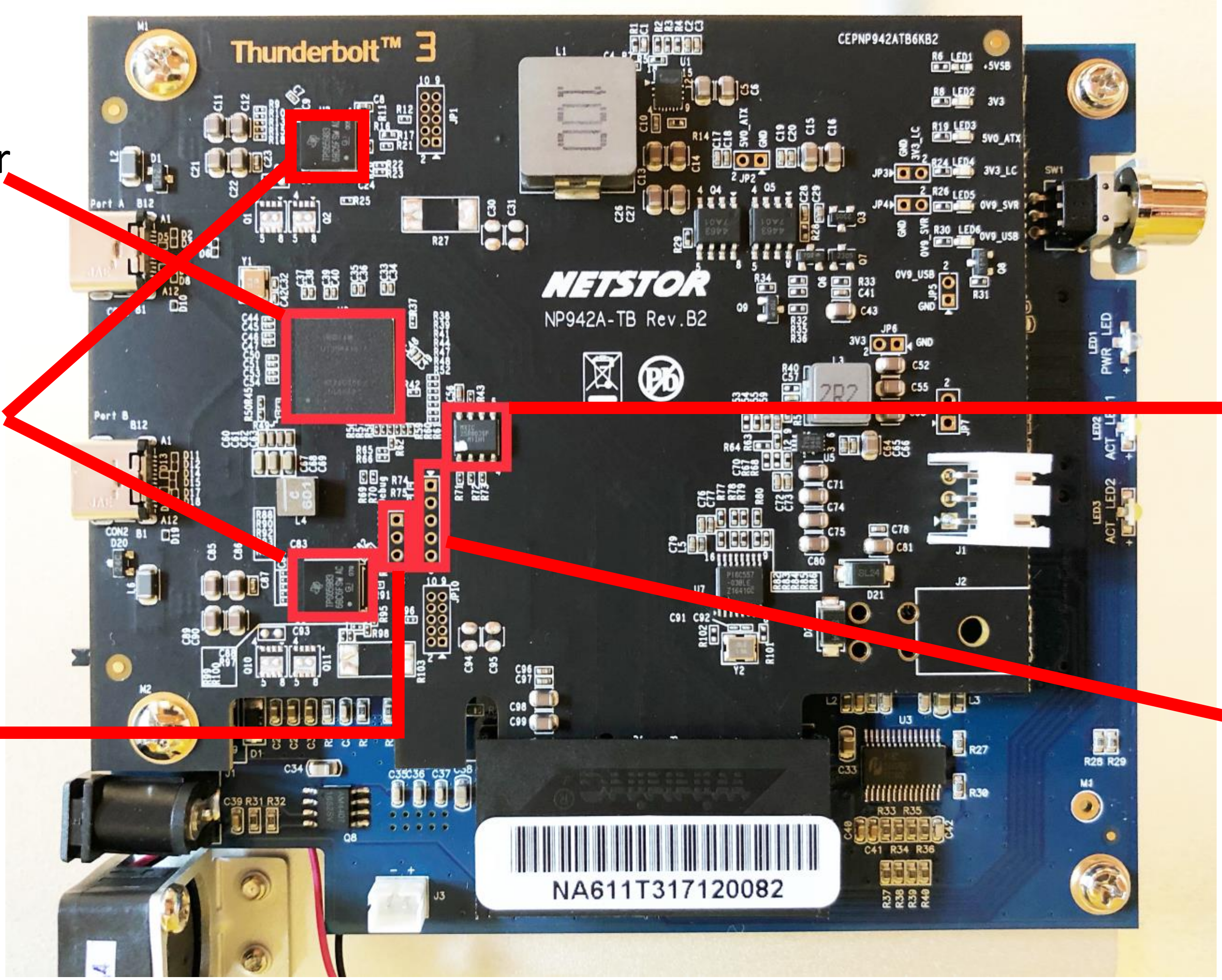
MX25R8035F
8 Mbit SPI Flash

JTAG ?

NetStor Thunderbolt NVMe Enclosure

Intel JHL6540
TB 3 host/device controller
4-channel, dual port

2* TPS65983
USB Type-C PD Controller
Power Switch
High-speed Multiplexer

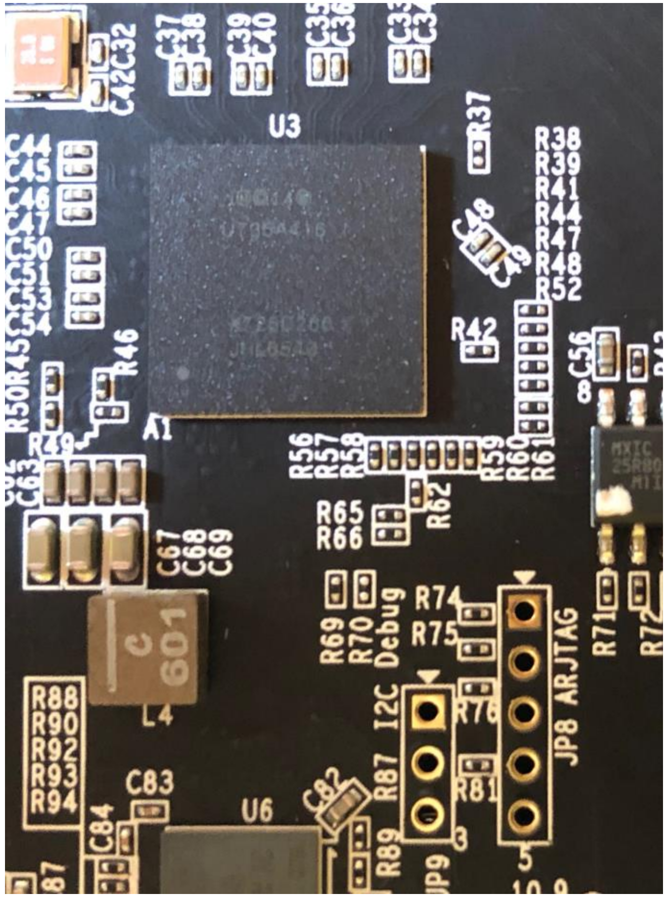


MX25R8035F
8 Mbit SPI Flash

~~JTAG ?~~ ☹

I²C

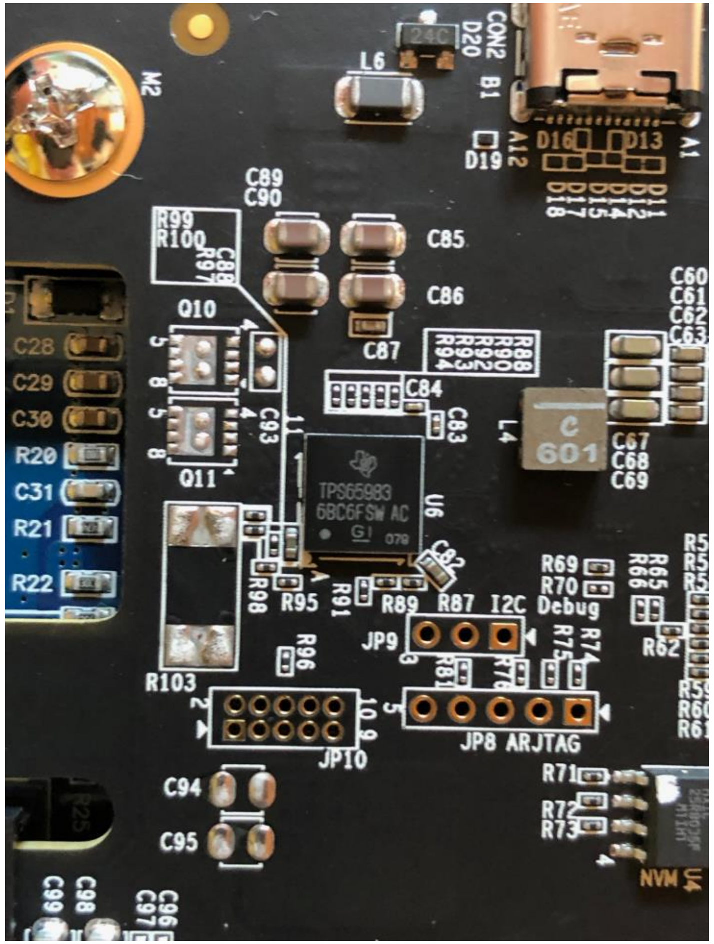
Intel JHL6540 Thunderbolt Controller



- 4 channel, dual-port Thunderbolt 3 controller
- Up to 20 Gbit per channel
- Supports Host and Endpoint mode
- “Alpine Ridge” generation:
    - DisplayPort 1.2
    - Integrated HDMI 2.0 LSPcon
    - USB 3.1 passthrough
    - USB-PD + 100W charging

- BGA package
- No public datasheets
- Not much we can do without more invasive techniques

TPS65983 USB-PD Controller



Texas Instruments **TPS65983**

SLVSD93A – OCTOBER 2015 – REVISED APRIL 2016

TPS65983 USB Type-C and USB PD Controller, Power Switch, and High Speed Multiplexer

1 Features

- USB Power Delivery (PD) Controller
  - Mode Configuration for Source (Host), Sink (Device), or Source-Sink
  - Bi-Phase Marked Encoding/Decoding (BMC)
  - Physical Layer (PHY) Protocol
  - Policy Engine
  - Configurable at Boot and Host-Controlled
- USB Type-C Specification Compliant
  - Detect USB Cable Plug Attach
  - Cable Orientation and Role Detection
  - Assign CC and VCONN Pins
  - Advertise Default, 1.5 A or 3 A for Type-C Power
- Port Power Switch
  - 5-V, 3-A Switch to VBUS for Type-C Power
  - 5-V to 20-V, 3-A Bidirectional Switch to or from VBUS for USB PD Power
  - 5-V, 600-mA Switches for VCONN
  - Overcurrent Limiter, Overvoltage Protector
  - Slew Rate Control
  - Hard Reset Support
- Port Data Multiplexer
  - USB 2.0 HS Data, UART Data, and Low Speed Endpoint
  - Sideband Use Data for Alternate Modes (DisplayPort and Thunderbolt™)
- Power Management
  - Gate Control and Current Sense for External 5-V to 20-V, 5-A Bidirectional Switch (Back-to-Back NFETs)
  - Power Supply from 3.3-V or VBUS Source
  - 3.3-V LDO Output for Dead Battery Support
- BGA MicroStar Junior Package
  - 0.5-mm Pitch
  - Through-Hole Via Compatible for All Pins

2 Applications

- Thunderbolt 3 Devices

3 Description

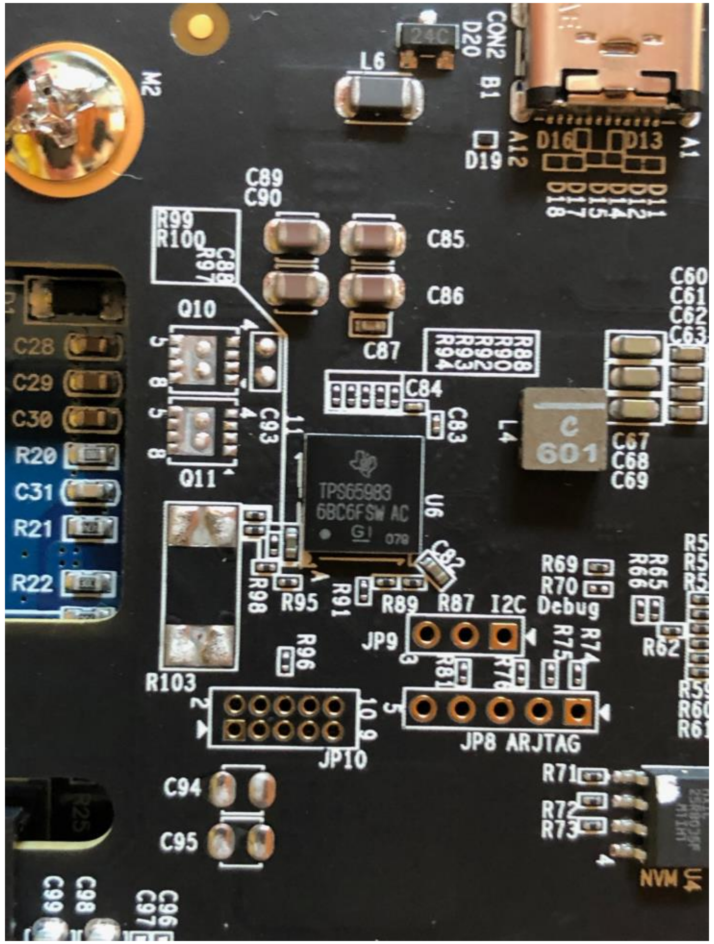
The TPS65983 is a stand-alone USB Type-C and Power Delivery (PD) controller providing cable plug and orientation detection at the USB Type-C connector. Upon cable detection, the TPS65983 communicates on the CC wire using the USB PD protocol. When cable detection and USB PD negotiation are complete, the TPS65983 enables the appropriate power path and configures alternate mode settings for internal and (optional) external multiplexers.

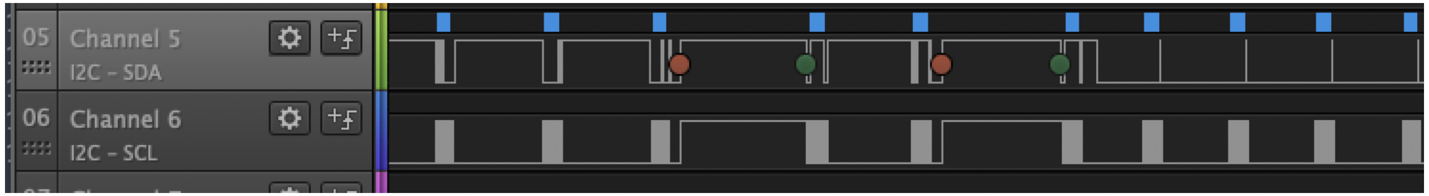
Device Information(1)

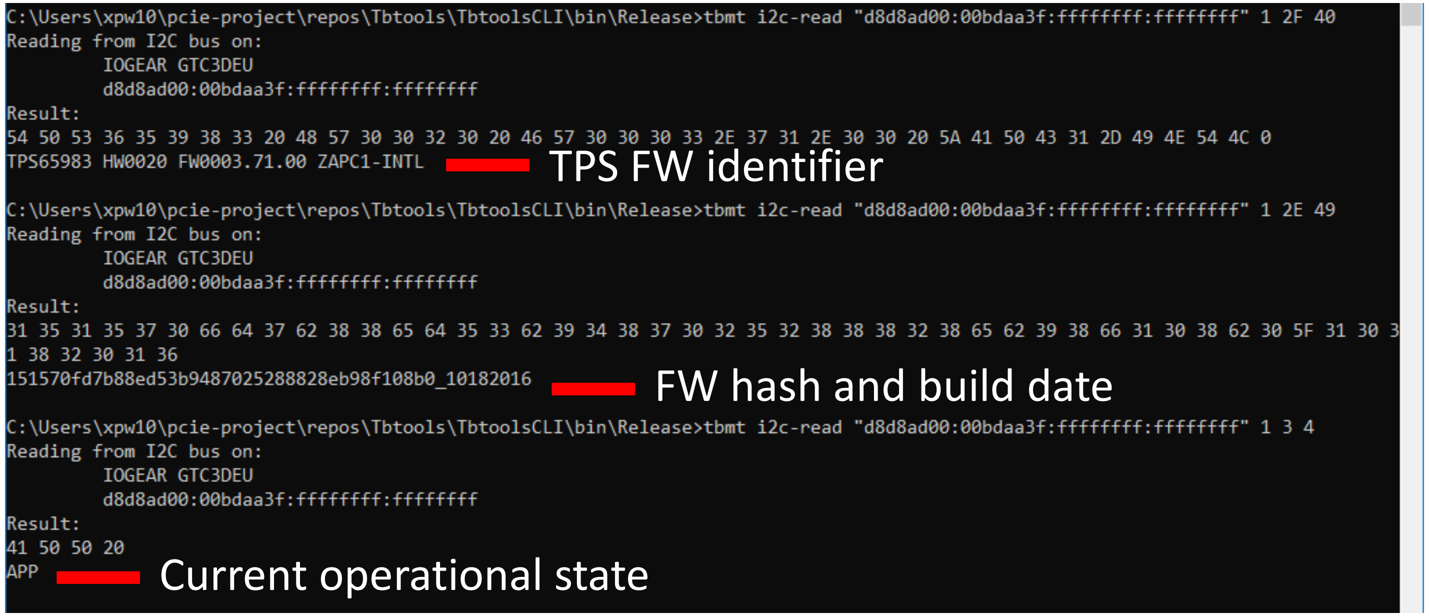
PART NUMBER	PACKAGE	BODY SIZE (NOM)
TPS65983	BGA MICROSTAR JUNIOR (96)	6.00 mm × 6.00 mm

(1) For all available packages, see the orderable addendum at the end of the data sheet.

TPS65983 USB-PD Controller





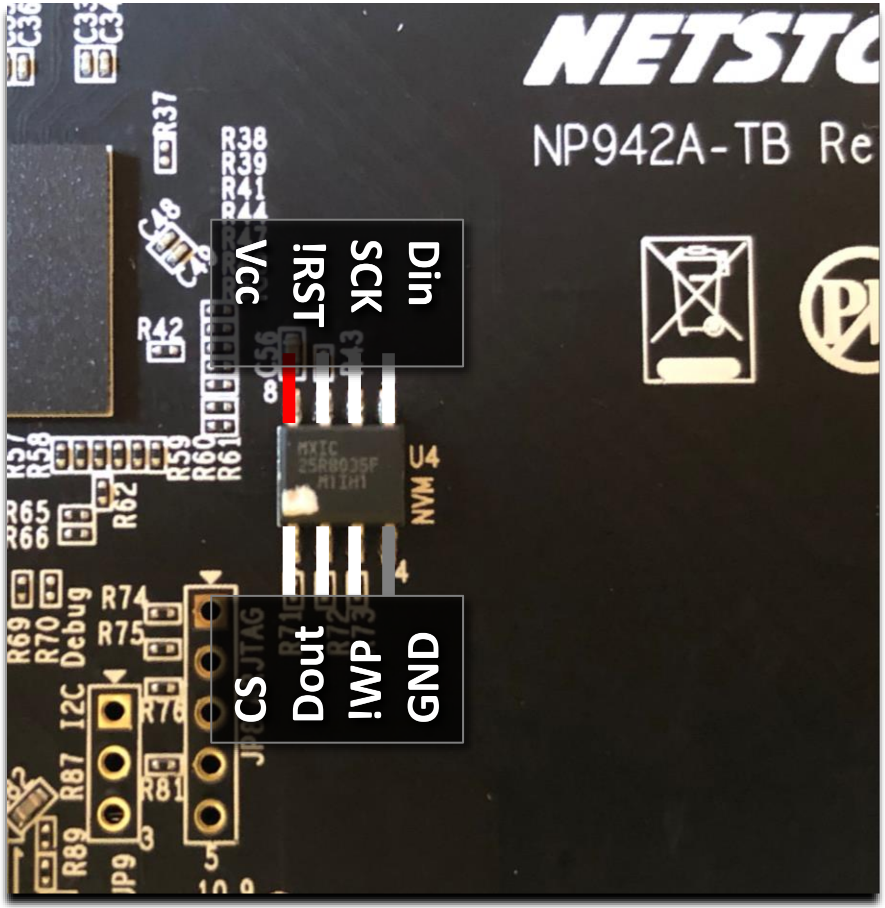


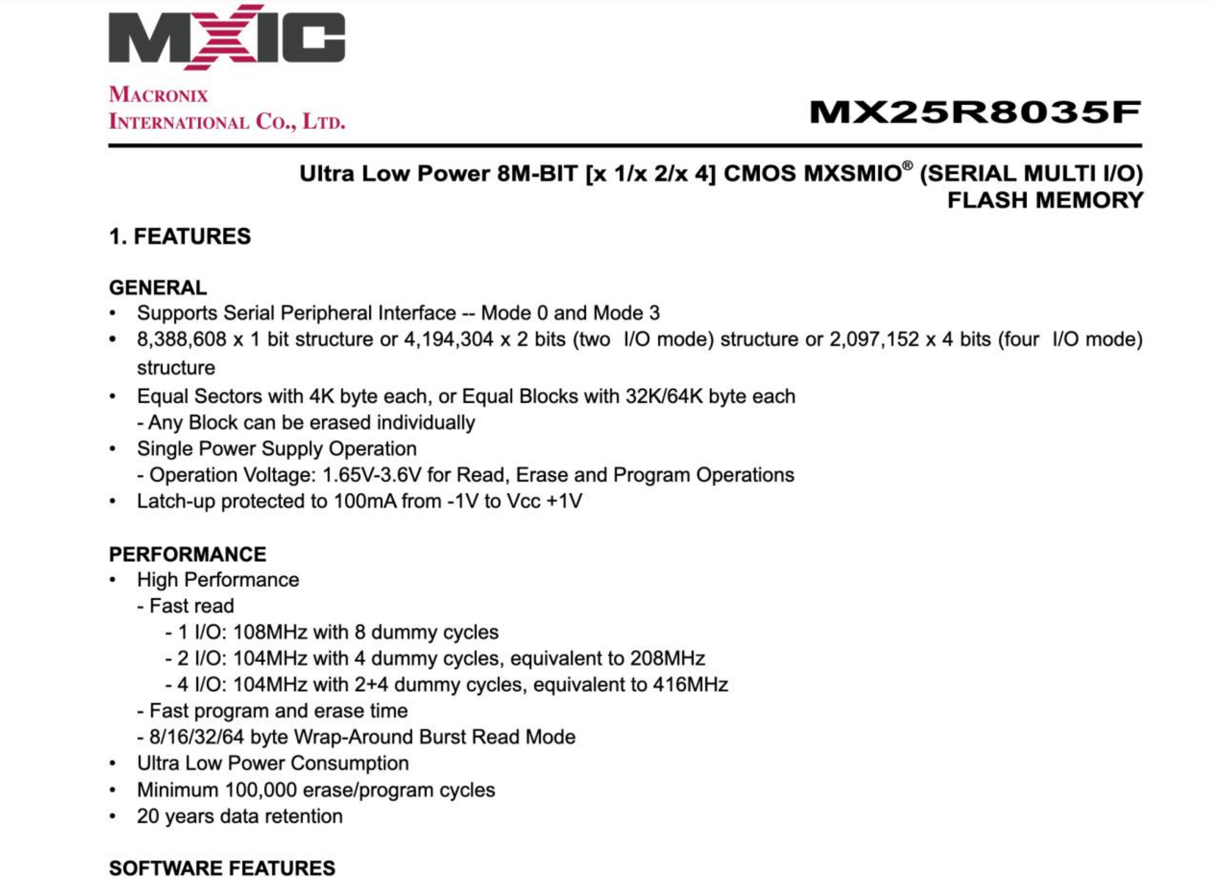
```
C:\Users\xpw10\pcie-project\repos\Tbtools\TbtoolsCLI\bin\Release>tbmt i2c-read "d8d8ad00:00bdaa3f:ffffffff:ffffffff" 1 2F 40
Reading from I2C bus on:
        IOGEAR GTC3DEU
        d8d8ad00:00bdaa3f:ffffffff:ffffffff
Result:
54 50 53 36 35 39 38 33 20 48 57 30 30 32 30 20 46 57 30 30 30 33 2E 37 31 2E 30 30 20 5A 41 50 43 31 2D 49 4E 54 4C 0
TPS65983 HW0020 FW0003.71.00 ZAPC1-INTL

C:\Users\xpw10\pcie-project\repos\Tbtools\TbtoolsCLI\bin\Release>tbmt i2c-read "d8d8ad00:00bdaa3f:ffffffff:ffffffff" 1 2E 49
Reading from I2C bus on:
        IOGEAR GTC3DEU
        d8d8ad00:00bdaa3f:ffffffff:ffffffff
Result:
31 35 31 35 37 30 66 64 37 62 38 38 65 64 35 33 62 39 34 38 37 30 32 35 32 38 38 38 32 38 65 62 39 38 66 31 30 38 62 30 5F 31 30 3
1 38 32 30 31 36
151570fd7b88ed53b9487025288828eb98f108b0_10182016

C:\Users\xpw10\pcie-project\repos\Tbtools\TbtoolsCLI\bin\Release>tbmt i2c-read "d8d8ad00:00bdaa3f:ffffffff:ffffffff" 1 3 4
Reading from I2C bus on:
        IOGEAR GTC3DEU
        d8d8ad00:00bdaa3f:ffffffff:ffffffff
Result:
41 50 50 20
APP
```

Macronix MX25R8035F





MXIC

MACRONIX INTERNATIONAL CO., LTD.

MX25R8035F

Ultra Low Power 8M-BIT [x 1/x 2/x 4] CMOS MXSMIO® (SERIAL MULTI I/O) FLASH MEMORY

1. FEATURES

GENERAL

- Supports Serial Peripheral Interface -- Mode 0 and Mode 3
- 8,388,608 x 1 bit structure or 4,194,304 x 2 bits (two I/O mode) structure or 2,097,152 x 4 bits (four I/O mode) structure
- Equal Sectors with 4K byte each, or Equal Blocks with 32K/64K byte each
  - Any Block can be erased individually
- Single Power Supply Operation
  - Operation Voltage: 1.65V-3.6V for Read, Erase and Program Operations
- Latch-up protected to 100mA from -1V to Vcc +1V

PERFORMANCE

- High Performance
  - Fast read
    - 1 I/O: 108MHz with 8 dummy cycles
    - 2 I/O: 104MHz with 4 dummy cycles, equivalent to 208MHz
    - 4 I/O: 104MHz with 2+4 dummy cycles, equivalent to 416MHz
  - Fast program and erase time
  - 8/16/32/64 byte Wrap-Around Burst Read Mode
- Ultra Low Power Consumption
- Minimum 100,000 erase/program cycles
- 20 years data retention

SOFTWARE FEATURES

Thunderbolt 3 Controller Firmware

```
0x004196 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
0x0041AD FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
0x0041C4 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
0x0041DB FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
0x0041F2 FF FF FF FF FF FF FF FF FF FF FF FF FF FF 44 52 4F 4D 20 20 20 20 FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿDROM    ÿ
0x004209 FF FF FF FF FF FF FF 7F 00 00 00 00 00 00 58 00 D8 7D 45 3F 01 5C 00  ÿÿÿÿÿÿÿ.......X.Ø}E?.\.
0x004220 58 00 1C 61 01 01 08 81 80 02 80 00 00 00 08 82 90 01 80 00 00 00 08  X. a..................
0x004237 83 80 04 80 01 00 00 08 84 90 03 80 01 00 00 02 C5 0B 86 20 01 00 DC  ................Å . ..Ü
0x00424E 00 00 00 00 00 03 87 80 05 88 50 00 00 02 C9 02 CA 05 8B 50 00 00 0A  ..........P...É.Ê..P..
0x004265 01 4E 65 74 53 74 6F 72 00 0B 02 4E 41 36 31 31 54 42 33 00 00 00 00  .NetStor. .NA611TB3....
0x00427C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .......................
0x004293 00 00 00 00 00 00 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ......ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
0x0042AA FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
0x0042C1 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
0x0042D8 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
0x0042EF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
0x004306 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
```

```c
struct tb_drom_header {
        /* BYTE 0 */
        u8 uid_crc8; /* checksum for uid */
        /* BYTES 1-8 */
        u64 uid;
        /* BYTES 9-12 */
        u32 data_crc32; /* checksum for data_len bytes starting at byte 13 */
        /* BYTE 13 */
        u8 device_rom_revision; /* should be <= 1 */
        u16 data_len:10;
        u8 __unknown1:6;
        /* BYTES 16-21 */
        u16 vendor_id;
        u16 model_id;
        u8 model_rev;
        u8 eeprom_rev;
} __packed;
```

- Device ROM stores Thunderbolt device identity
  - Device name
  - Device ID
  - Vendor name
  - Vendor ID
  - UUID? **Yes, but only 2 out of 8 bytes**

Thunderbolt 3 Controller Firmware

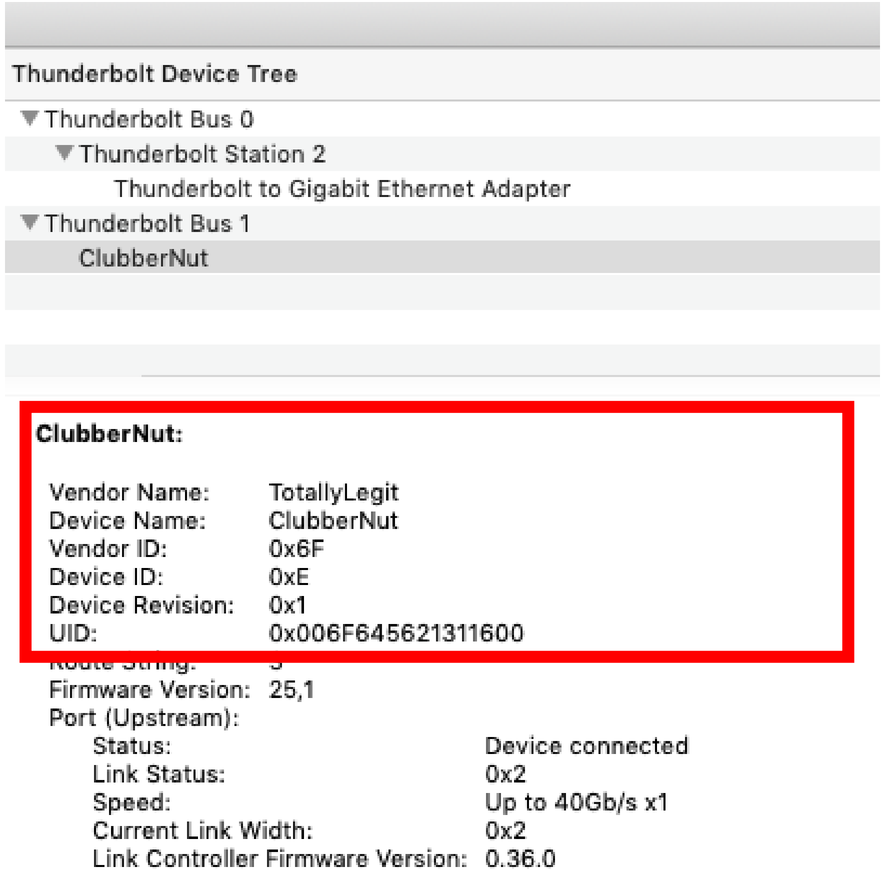
```
0x0375F3 FF FF FF FF FF FF FF FF FF FF FF FF FF 52 53 41 2B 45 58 50 20 FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿRSA+EXP ÿÿ
0x03760A FF FF FF FF FF FF 41 00 00 00 45 7F B9 8B 84 DF 8E E5 DE 3C 44 A9 0B  ÿÿÿÿÿÿA...E.¹..ß.åÞ<D©
0x037621 62 C4 8F 54 1D A8 94 24 F4 B4 8D 57 00 2B B9 1B FE 9C 4A 14 72 81 A8  bÄ.T ¨.$ô´.W.+¹.þ.J.r.¨
0x037638 2A C2 59 49 8E A0 86 86 BE 55 12 29 79 06 91 34 DD 2F 52 69 42 BE CE  *ÂYI. ..¾U.)y..4Ý/RiB¾Î
0x03764F A3 BC 4E B4 BF F2 A1 F3 C9 7C EE B7 B3 51 71 62 E1 C6 12 48 56 F8 20  £¼N´¿ò¡óÉ|î·³QqbáÆ.HVø
0x037666 BC 39 3D 3B 00 52 36 C2 DF 9A 39 C8 22 9A 5A 00 79 F2 11 5F 1F 35 90  ¼9=;.R6Âß.9È".Z.yò._ 5.
0x03767D 6F 65 1A ED 0E 6D 74 5F 29 4D 02 2C FA 7B 69 97 50 63 CB 05 B1 D8 C0  oe.í.mt_)M.,ú{i.PcË.±ØÀ
0x037694 2F D9 82 F1 09 4F B9 69 5E C9 A7 7F 53 97 9C 95 F8 C2 88 69 C2 46 A1  /Ù.ñ O¹i^É§.S...øÂ.iÂF¡
0x0376AB C8 68 AF EB 12 B0 A2 F4 11 5B 68 10 B4 08 24 D2 B7 3A C1 28 89 7C 85  Èh¯ë.°¢ô.[h.´.$Ò·:Á(.|.
0x0376C2 04 D4 24 14 9C 34 A1 68 D1 7E 41 35 F8 7A 67 FD 8A D8 C2 F4 C9 F7 DF  .Ô$..4¡hÑ~A5øzgý.ØÂôÉ÷ß
0x0376D9 A0 28 E8 69 9B 34 AE B4 A0 FB 17 0C FC 50 B4 02 0A 8D FF 5C 9C 9E 78   (èi.4®´ û. üP´. .ÿ\..x
0x0376F0 BB EB 1C D6 0F A5 F7 A9 7D 2B FA B5 20 4B ED CD 63 4C 97 13 EA 88 73  »ë Ö.¥÷©}+úµ KíÍcL..ê.s
0x037707 F0 FB 31 8B 27 46 3B 6F 54 B6 09 69 A9 01 00 01 00 FF FF FF FF FF FF  ðû1.'F;oT¶ i©....ÿÿÿÿÿÿ
```

```
0x036FC9 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
0x036FE2 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
0x036FFB FF FF FF FF FF 53 45 43 20 44 47 53 54 FF FF FF FF FF FF FF FF 40 00 00 00  ÿÿÿÿÿSEC DGSTÿÿÿÿÿÿÿÿ@...
0x037014 13 F0 28 69 CA AF B5 5F 9F 00 4D C3 65 6E 81 15 D4 4A 3B A6 C0 40 84 6A C2  .ð(iÊ¯µ_..MÃen..ÔJ;¦À@.jÂ
0x03702D 50 68 78 BC 26 30 59 D6 C9 94 B5 87 00 51 3D B3 B9 DE 81 95 88 22 9B 20 0C  Phx¼&0YÖÉ.µ..Q=³¹Þ...". 
0x037046 F7 A9 16 06 D2 1E DF 68 94 81 61 FD BE 57 21 54 27 CF 5E 45 57 EA C3 E2 1D  ÷©..Ò ßh..aý¾W!T'Ï^EWêÃâ
0x03705F 25 31 3F 61 07 D4 18 87 52 88 89 A4 6D C7 0D 71 F9 CE B9 19 E6 09 71 82 68  %1?a.Ô..R..¤mÇ qùÎ¹.æ q.h
0x037078 70 28 DE 8E 71 FC 56 2E FD 96 23 B5 D9 BB 57 57 AF AE D2 26 7C 9A 2C 71 2F  p(Þ.qüV.ý.#µÙ»WW¯®Ò&|.,q/
0x037091 02 21 6C 0A 4B C0 66 D0 CC A5 77 4F 17 4F CF 66 13 A7 81 37 BB 0F 8B 79 00  .!l KÀfÐÌ¥wO.OÏf.§.7»..y.
0x0370AA 0E F0 B8 AD 9B C9 9B B9 7C 86 39 C9 EE 9F 91 D2 D3 FA 41 BB 57 E0 B1 A2 C1  .ð¸..É.¹|.9Éî..ÒÓúA»Wà±¢Á
0x0370C3 15 0D E3 20 6F C0 5E CC BD 63 C6 85 34 A4 2D DF CB F7 83 37 6E 6D 5F 2F 13  . ã oÀ^Ì½cÆ.4¤-ßË÷.7nm_/.
0x0370DC 27 A5 C1 E6 B2 F6 46 06 0D A4 4F 6F D7 6E 18 73 10 B3 EA E1 8E 91 AB 55 73  '¥Áæ²öF. ¤Ooxn.s.³êá..«Us
0x0370F5 C2 54 D2 F4 97 CE A6 15 0A 75 80 F9 76 C9 42 FA FA 26 C8 C0 31 F3 CC A1 68  ÂTÒô.Î¦. u.ùvÉBúú&ÈÀ1óÌ¡h
0x03710E 08 4A 00 80 25 21 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  .J..%!ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
```

- Embedded in firmware
    - Public key (fingerprint likely stored in silicon)
    - Signed digest
- Device ROM stores Thunderbolt device identity
    - Device name
    - Device ID
    - Vendor name
    - Vendor ID
    - UUID (partial)
- **What is covered by the signature?**

Thunderspy: Vulnerability 1 + 2

- What is covered by the signature?
  - Not the DROM…
- **Vulnerability 1: Inadequate firmware verification schemes**
  - Firmware authenticated when updating from host, but not adequately upon connecting device, during boot, or resuming from sleep
  - Signature verification does not cover Thunderbolt device identity
- **Vulnerability 2: Weak device authentication scheme**
  - None of the identifiers linked to Thunderbolt PHY or each other, cryptographically or otherwise
  - E.g. can spoof arbitrary vendor ID that doesn't match vendor name



Thunderbolt 3 Controller Firmware

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.

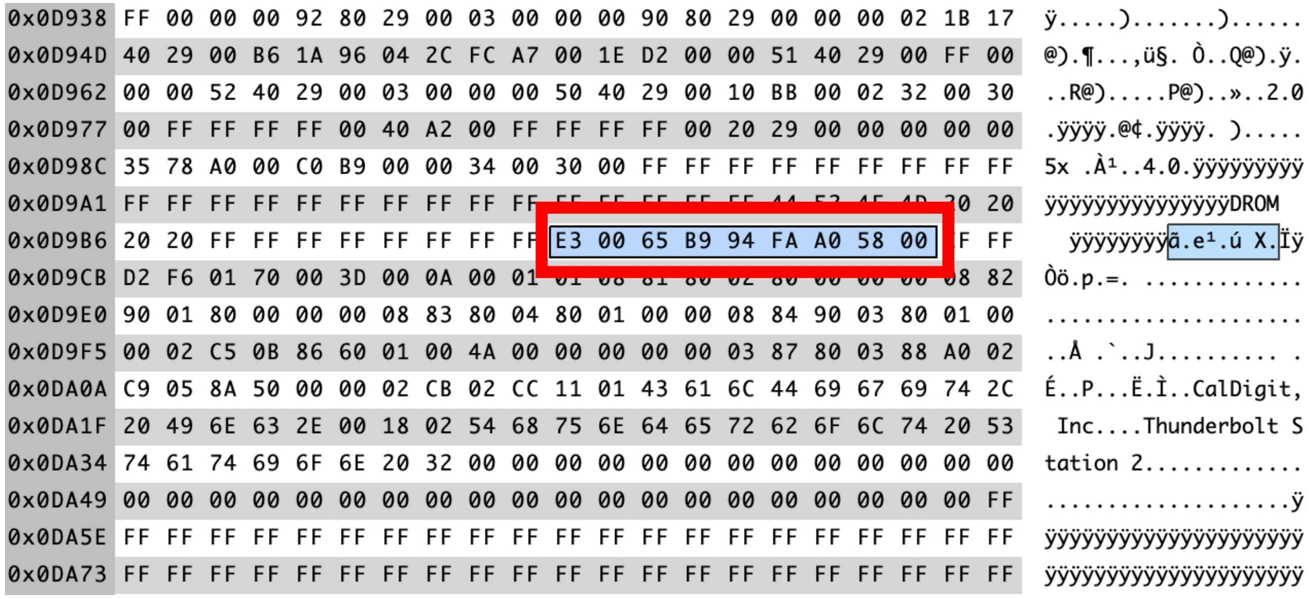
Unique ID number

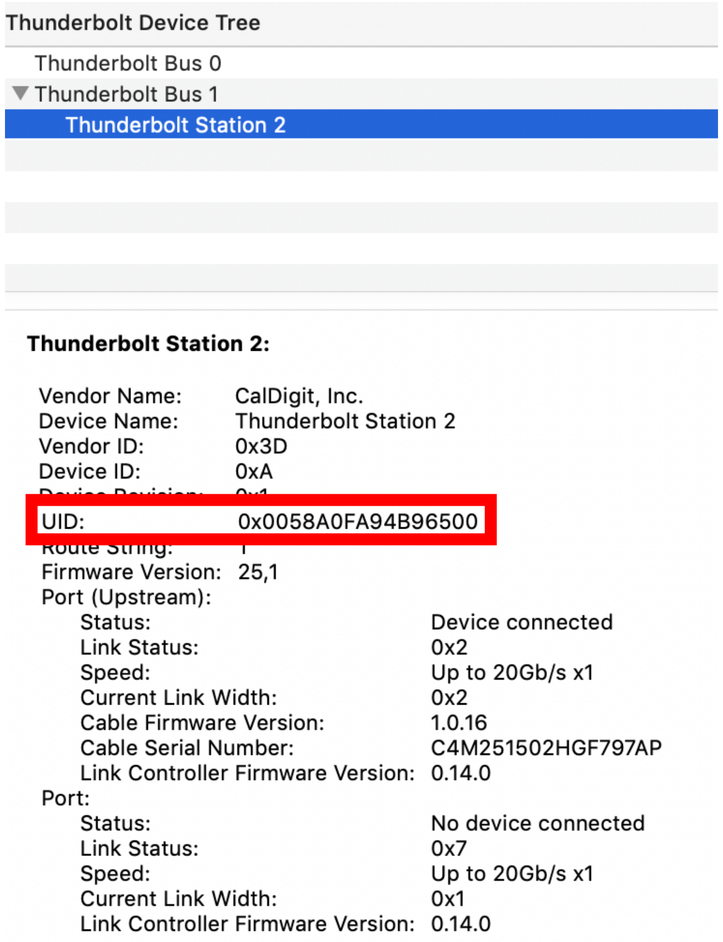
Statement inaccurate, but interesting emphasis on TB3

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

Source: Thunderbolt 3 and Security on Microsoft Windows 10 Operating System – Intel Corporation

Thunderbolt 2 Controller Firmware

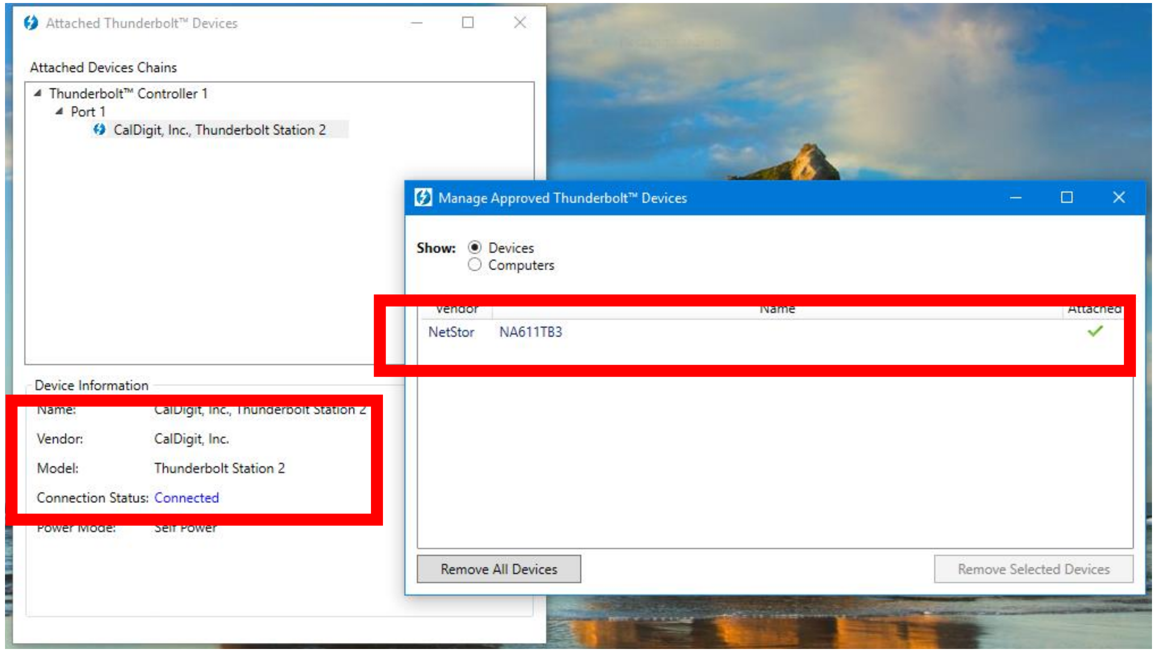




- UUID stored in plaintext, not covered by any signatures

Thunderbolt 2 Controller Firmware

- UUID stored in plaintext, not covered by any signatures
- TB2 device can spoof TB3 devices
- Device identified as previously authorized = profit!



Thunderspy: Vulnerability 3 + 4

- **Vulnerability 3: Use of unauthenticated device metadata**
  - DROM not cryptographically verified
  - When combined with vulnerability 1 + 2, enables arbitrary identities and cloning user-authorized devices
- **Vulnerability 4: Downgrade attack**
  - Backwards compatibility with subjects Thunderbolt 3 systems to vulnerability introduced by Thunderbolt 2 hardware

- **Exploitation scenarios**
  - 3.1.1 – 3.1.3: Cloning victim devices with and without physical device access
  - Demonstrates spoofing victim device identity on arbitrary attacker device

Device Controller Firmware Outline

Jump address
- Host mode: 0x00 *
- **EP mode:** 0x4000

Secure key dictionary
- Maps 8-byte host UUID to 32-byte key

PHY config
- PtoSPtoQWake
- EE_CIO

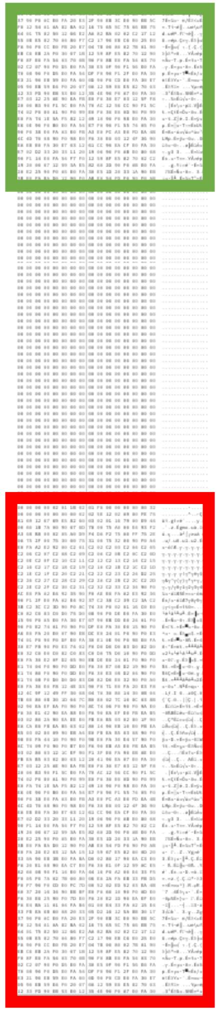
DROM (0x4000)
- Device identity

PHY config (continued)
- EE_PCIE
- EE_DMA
- EE_USB_PA / PB
- EE_PCIE_PHI
- EE_DP
- PATCHES
- DP_IN_UCODE
- …

“RSA+EXP” public key

Signed digest

TPS USB-PD FW



TPS USB-PD FW (continued)

Temporary FW update buffer for host-initiated updates

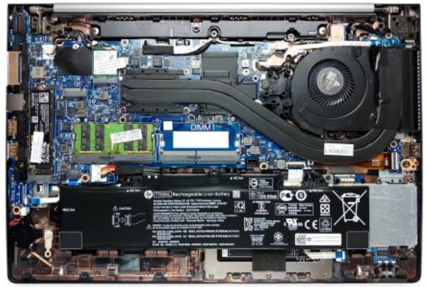
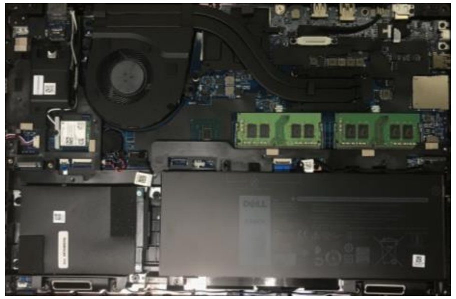
*Offset varies by controller model, FW revision, and presence of secure key dictionary

Identifying attack surfaces

- Thunderbolt is a proprietary standard
- Protocol specifications not publicly documented
- Hardware architecture not publicly documented
- Dissected various Thunderbolt devices and **Thunderbolt-equipped systems**

Thunderbolt-Equipped Systems

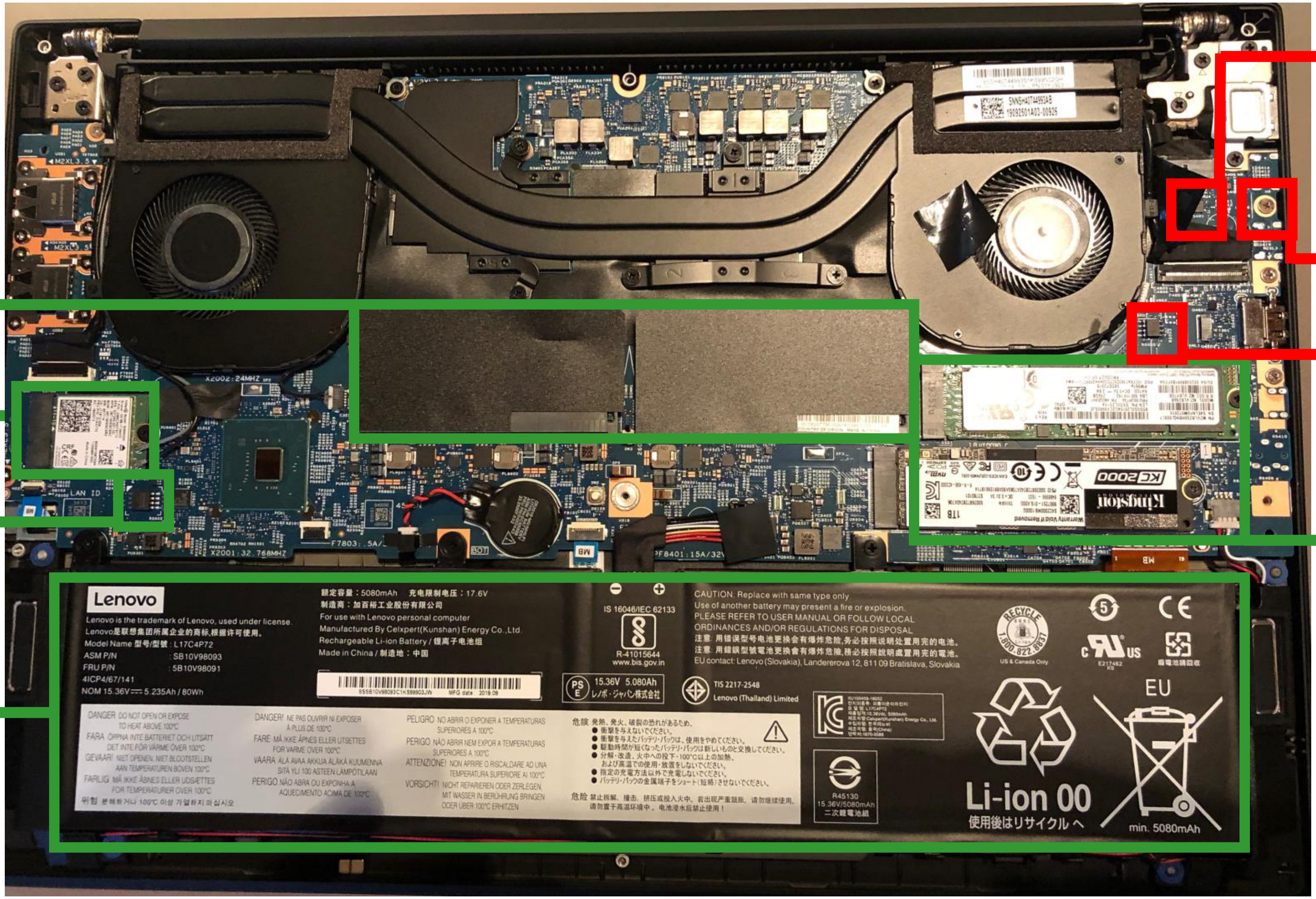


- **Five vendors, seven generations of systems:**
  Intel, Lenovo, HP, Dell, Apple (2013 – 2020)
- **Five generations of Thunderbolt controllers:**
  Falcon Ridge (TB2), Alpine Ridge-2015, Alpine Ridge-2016, Titan Ridge, Ice Lake (TB3)




Lenovo ThinkPad P1 (2019)



RAM

WiFi

Winbond W25Q128V (BIOS)

Battery

Intel JHL7540
TB3 host controller
4-channel, dual port
(other side)

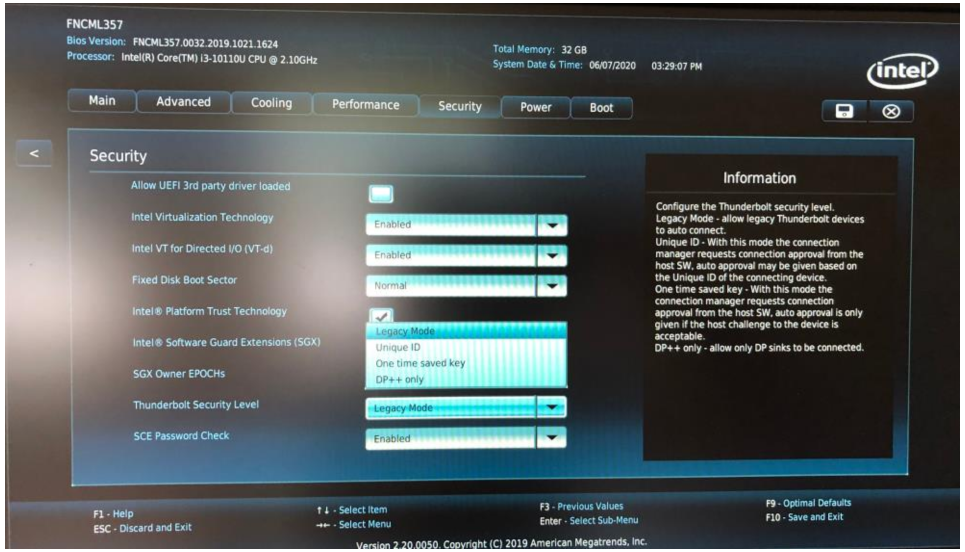
TPS65982 USB-PD
(other side)

Winbond W25Q80.V
TB3 host controller
FW

NVMe
storage

Host Controller: Key Questions

- UEFI enables user switching Thunderbolt Security Levels
  - DXE programs TB controller upon setting SL, so UEFI stores SL state?
- SL1+2 require storing device UUIDs
  - Device ACL?



Host Controller Firmware Outline

Jump address
- **Host mode:** 0x00 *
- EP mode: 0x4000

No secure key dictionary
(stored on OS disk; pre-boot auth appears based on UUID only)

PHY config
- PtoSPtoQWake
- EE_CIO

Device ACL (UUIDs)

Host Security Level configuration

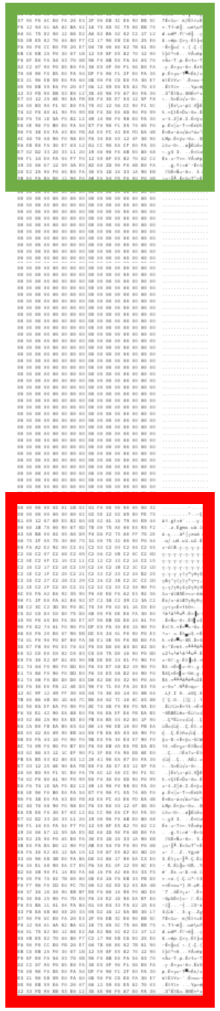
DROM (0x4000)
- Host identity

PHY config (continued)
- EE_PCIE
- EE_DMA
- EE_USB_PA / PB
- EE_PCIE_PHI
- EE_DP
- PATCHES
- DP_IN_UCODE
- …

“RSA+EXP” public key

Signed digest

TPS USB-PD FW



TPS USB-PD FW (continued)

Temporary FW update buffer for host-initiated updates

*Offset varies by controller model, FW revision, and currently active Security Level

Thunderspy: vulnerability 5

- **Vulnerability 5: Use of unauthenticated controller configurations**
  - Two state machines: UEFI and host controller FW maintain SL state
  - Host controller FW overrides UEFI state
  - FW signature does not cover security configuration

- **Exploitation scenario**
  - 3.2.1: Disabling Thunderbolt security (SL1/SL2), or restoring Thunderbolt connectivity when disabled (SL3)
    - Demonstrates attacking host controller firmware: patch SL to 0 (no security)
    - Works against every Security Level
    - Enables restoring TB connectivity, even user disabled it (SL3)

SPI Flash: Write Protection

W25Q80DV/DL

winbond

7.1.6 **Complement Protect (CMP)**

The Complement Protect bit (CMP) is a non-volatile read/write bit in the status register (S14). It is used in conjunction with SEC, TB, BP2, BP1 and BP0 bits to provide more flexibility for the array protection. Once CMP is set to 1, previous array protection set by SEC, TB, BP2, BP1 and BP0 will be reversed. For instance, when CMP=0, a top 4KB sector can be protected while the rest of the array is not; when CMP=1, the top 4KB sector will become unprotected while the rest of the array become read-only. Please refer to the Status Register Memory Protection table for details. The default setting is CMP=0.

7.1.7 **Status Register Protect (SRP1, SRP0)**

The Status Register Protect bits (SRP1 and SRP0) are non-volatile read/write bits in the status register (S8 and S7). The SRP bits control the method of write protection: software protection, hardware protection, power supply lock-down or one time programmable (OTP) protection.

SRP1	SRP0	/WP	Status Register	Description
0	0	X	Software Protection	/WP pin has no control. The Status register can be written to after a Write Enable instruction, WEL=1. [Factory Default]
0	1	0	Hardware Protected	When /WP pin is low the Status Register locked and can not be written to.
0	1	1	Hardware Unprotected	When /WP pin is high the Status register is unlocked and can be written to after a Write Enable instruction, WEL=1.
1	0	X	Power Supply Lock-Down	Status Register is protected and can not be written to again until the next power-down, power-up cycle.(1)
1	1	X	One Time Program(2)	Status Register is permanently protected and can not be written to.

Note:

1. When SRP1, SRP0 = (1, 0), a power-down, power-up cycle will change SRP1, SRP0 to (0, 0) state.
2. This feature is available upon special order. Please contact Winbond for details.

Special order, yet some TB controller flash samples appear to ship support

Thunderspy: vulnerability 6

- **Vulnerability 6: SPI flash interface deficiencies**
  - Host controller FW maintains SL state (vulnerability 5)
  - SPI flash write protection allows preventing user to change SL
    - On supported flash, irrevocable OTP write protection turns it into ROM

- **Exploitation scenarios**
  - 3.3.1 – 3.1.3: Rendering SL0 permanent and blocking future firmware updates
  - Demonstrates ability to patch SL to 0 (vuln 5), then render it permanent (vuln 6)
  - Shown in demo 1

Summary: Thunderspy Attack Methods (selected)

Attack method 1 *Exploitation scenarios:* 3.2.1, 3.3.1, 3.3.2, 3.3.3	Attack Thunderbolt host controller firmware to disable Thunderbolt security. System will accept any arbitrary attacker devices. • Requires brief access to laptop (~ 5 min) and reprogramming host controller firmware • Does not require access to victim's Thunderbolt devices
Attack method 2 *Exploitation scenarios:* 3.1.1, 3.1.3	Clone user-authorized Thunderbolt device identity to an arbitrary attacker device. System will accept attacker device as being legitimate, user-authorized device. • Does not require reprogramming host controller firmware • Requires brief access to one of victim's Thunderbolt devices (~ 5 min)
Impact (both)	• Unrestricted read and write access to system memory (DMA) • Access data from encrypted drives • Persistent access possible, by e.g. (i) exploiting Thunderspy vulnerability 6, or (ii) installing rootkit to ensure continued access without requiring Thunderspy

For additional exploitation scenarios, please refer to the vulnerability report.

Demo – Unlocking Windows PC in 5 minutes using attack method 1

Edited to fit Black Hat session. Please refer to our YouTube recording for the complete real-time footage.

Thunderbolt Security Levels – Revisited

	Definition
SL0 None	• No security (legacy mode)
SL1 User	• Device authorization ACL based on UUID • UUID fused in silicon • Default setting on all PCs
SL2 Secure	• Device authorization based on UUID (SL1), *plus* • Cryptographic device authentication (challenge-response)
SL3 No PCIe tunneling	• Disable all Thunderbolt connectivity • USB and/or DisplayPort tunneling only
SL4 Disable daisy-chaining	Terminate PCIe tunneling at first TB device (some Titan Ridge controllers only)
Pre-boot protection	PCIe tunneling enabled only if Thunderbolt device previously authorized by user

Thunderbolt Security Levels – Revisited

	Definition	What we found it to mean
SL0 None	• No security (legacy mode)	
SL1 User	• Device authorization ACL based on UUID • UUID fused in silicon • Default setting on all PCs	• UUID not so unique – can be spoofed • UUID not fused in silicon
SL2 Secure	• Device authorization based on UUID (SL1), *plus* • Cryptographic device authentication (challenge-response)	Keys stored in plaintext on device SPI flash – can be cloned
SL3 No PCIe tunneling	• Disable all Thunderbolt connectivity • USB and/or DisplayPort tunneling only	…until the attacker reprograms the controller firmware to SL0 (no security)
SL4 Disable daisy-chaining	Terminate PCIe tunneling at first TB device (some Titan Ridge controllers only)	To connect malicious device, simply unplug existing device or pick another TB port
Pre-boot protection	PCIe tunneling enabled only if Thunderbolt device previously authorized by user	All security levels broken, so has no effect

Thunderspy PoC Tools

Thunderbolt Controller Firmware Patcher

https://github.com/BjornRuytenberg/tcfp

```
0xiphorus@xplptp:/Volumes/Data/PCIe-project/repos/tcfp$ python3 tcfp.py parse samples/intel-nuc8i3beh-M45PE80-nvm33-user.bin
Vendor ID : 0x8086
PCI ID : 0x15da
PCI Device Name : JHL6340 Thunderbolt 3 Bridge (C step) [Alpine Ridge 2C 2016]
Model ID : 0x6357
NVM version : 1 (0x1)
Vendor : Intel Corporation
Device : NUC8BEB
Security Level : SL1

0xiphorus@xplptp:/Volumes/Data/PCIe-project/repos/tcfp$ python3 tcfp.py parse samples/hp-zbook-studio-g4-W25Q80.V-nvm41-secure.bin
Vendor ID : 0xf0
PCI ID : 0x15d3
PCI Device Name : JHL6540 Thunderbolt 3 Bridge (C step) [Alpine Ridge 4C 2016]
Model ID : 0x826b
NVM version : 1 (0x1)
Vendor : HP, Inc.
Device : HP ZBook Studio G4
Security Level : SL2

0xiphorus@xplptp:/Volumes/Data/PCIe-project/repos/tcfp$ python3 tcfp.py parse samples/lenovo-p1-new-MX25L8005-nvm36-dp-usb.bin
Vendor ID : 0x109
PCI ID : 0x15ea
PCI Device Name : JHL7540 Thunderbolt 3 Bridge [Titan Ridge 4C 2018]
Model ID : 0x1711
NVM version : 36 (0x24)
Vendor : Lenovo
Device : ThinkPad P1
Security Level : SL3
```

```
0xiphorus@xplptp:/Volumes/Data/PCIe-project/repos/tcfp$ python3 tcfp.py patch lenovo-p1-new-MX25L8005-nvm36-dp-usb.bin
Vendor ID : 0x109
PCI ID : 0x15ea
PCI Device Name : JHL7540 Thunderbolt 3 Bridge [Titan Ridge 4C 2018]
Model ID : 0x1711
NVM version : 36 (0x24)
Vendor : Lenovo
Device : ThinkPad P1
Security Level : SL3

Image patched succesfully.
0xiphorus@xplptp:/Volumes/Data/PCIe-project/repos/tcfp$ python3 tcfp.py parse lenovo-p1-new-MX25L8005-nvm36-dp-usb.bin
Vendor ID : 0x109
PCI ID : 0x15ea
PCI Device Name : JHL7540 Thunderbolt 3 Bridge [Titan Ridge 4C 2018]
Model ID : 0x1711
NVM version : 36 (0x24)
Vendor : Lenovo
Device : ThinkPad P1
Security Level : SL0

0xiphorus@xplptp:/Volumes/Data/PCIe-project/repos/tcfp$
```

Thunderspy PoC Tools

SPIblock

https://github.com/BjornRuytenberg/spiblock

```
0xiphorus@xplptp:/Volumes/Data/PCIe-project/repos/spiblock$ python3 spiblock.py -p
Manufacturer ID: 0xC2
Device ID: 0x2017
Device: MACRONIX_MX25L6405
0xiphorus@xplptp:/Volumes/Data/PCIe-project/repos/spiblock$ python3 spiblock.py -s
Status Register : 0x40
Write Enable Latch WEL : Disabled
Status Register Protect SRP0 : Disabled
Block Protection BPx : Disabled
0xiphorus@xplptp:/Volumes/Data/PCIe-project/repos/spiblock$ python3 spiblock.py -p
Manufacturer ID: 0xEF
Device ID: 0x4014
Device: WINBOND_NEX_W25Q80_V
0xiphorus@xplptp:/Volumes/Data/PCIe-project/repos/spiblock$ python3 spiblock.py -s
Status Register : 0x0
Write Enable Latch WEL : Disabled
Status Register Protect SRP0 : Disabled
Block Protection BPx : Disabled
0xiphorus@xplptp:/Volumes/Data/PCIe-project/repos/spiblock$ python3 spiblock.py -p
root: WARNING: Enabling block protection for SPI device unsupported (flashrom status: 'TEST_UNTESTED').
Manufacturer ID: 0x20
Device ID: 0x4014
Device: ST_M45PE80
0xiphorus@xplptp:/Volumes/Data/PCIe-project/repos/spiblock$ python3 spiblock.py -s
root: WARNING: Enabling block protection for SPI device unsupported (flashrom status: 'TEST_UNTESTED').
Status Register : 0x0
Write Enable Latch WEL : Disabled
Status Register Protect SRP0 : Disabled
Block Protection BPx : Disabled
0xiphorus@xplptp:/Volumes/Data/PCIe-project/repos/spiblock$
```

```
0xiphorus@xplptp:/Volumes/Data/PCIe-project/repos/spiblock$ python3 spiblock.py -p
Manufacturer ID: 0xEF
Device ID: 0x4014
Device: WINBOND_NEX_W25Q80_V
0xiphorus@xplptp:/Volumes/Data/PCIe-project/repos/spiblock$ python3 spiblock.py -s
Status Register : 0x0
Write Enable Latch WEL : Disabled
Status Register Protect SRP0 : Disabled
Block Protection BPx : Disabled
0xiphorus@xplptp:/Volumes/Data/PCIe-project/repos/spiblock$ python3 spiblock.py -b 1
Succesfully enabled block protection.
0xiphorus@xplptp:/Volumes/Data/PCIe-project/repos/spiblock$ python3 spiblock.py -s
Status Register : 0x1c
Write Enable Latch WEL : Disabled
Status Register Protect SRP0 : Disabled
Block Protection BPx : Enabled (3)
0xiphorus@xplptp:/Volumes/Data/PCIe-project/repos/spiblock$ python3 spiblock.py -w 1
Succesfully enabled WP pin control.
0xiphorus@xplptp:/Volumes/Data/PCIe-project/repos/spiblock$ python3 spiblock.py -s
Status Register : 0x9c
Write Enable Latch WEL : Disabled
Status Register Protect SRP0 : Enabled
Block Protection BPx : Enabled (3)
0xiphorus@xplptp:/Volumes/Data/PCIe-project/repos/spiblock$ python3 spiblock.py -w 0
Error: Device does not allow changing status registers. De-assert WP pin first.
0xiphorus@xplptp:/Volumes/Data/PCIe-project/repos/spiblock$ python3 spiblock.py -b 0
root: WARNING: WP pin control enabled. Make sure to de-assert WP pin, otherwise this action will fail.
root: WARNING: If successful, this action will disable WP pin control.
Error: Device does not allow changing status registers. Disable WP pin control (SRP) first.
0xiphorus@xplptp:/Volumes/Data/PCIe-project/repos/spiblock$
```

Thunderspy: Affected systems

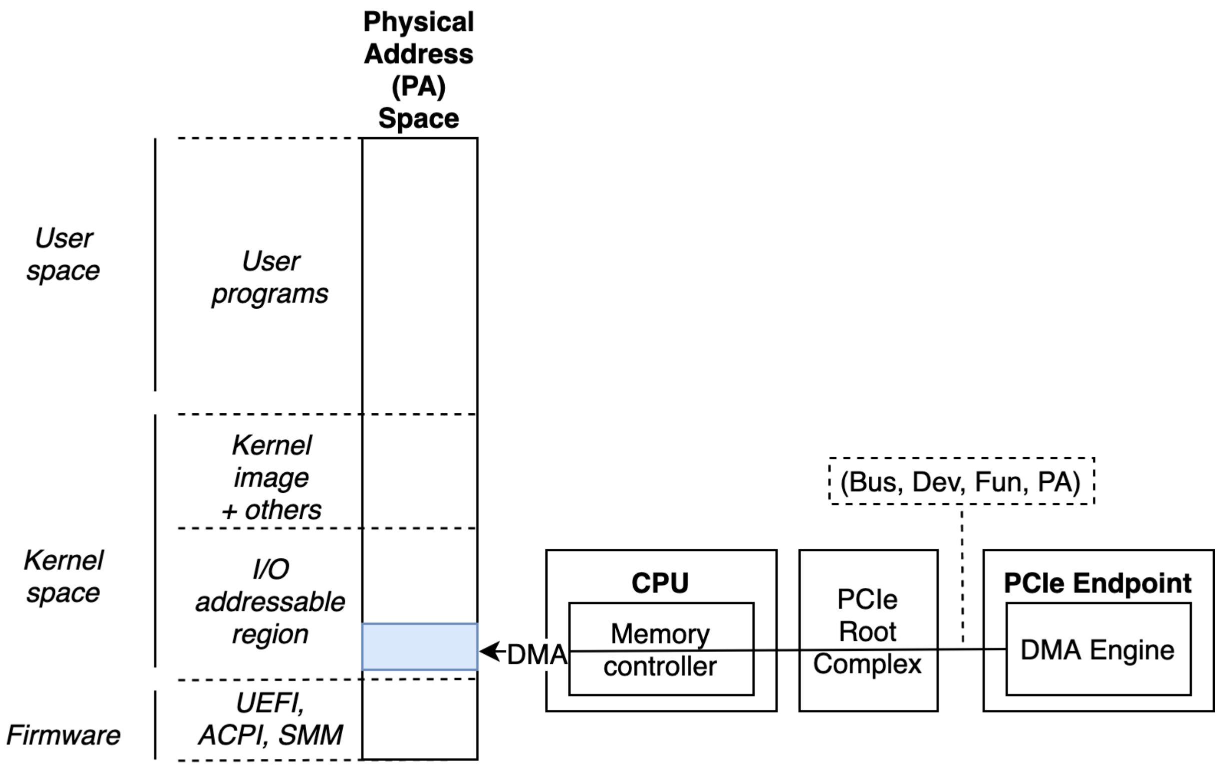
- **All Thunderbolt-equipped systems shipped between 2011-2020**
  - All PCs released between 2011-2018 fully vulnerable
  - All Macs running Windows and Linux (Boot Camp) fully vulnerable
  - Some systems providing Kernel DMA Protection, shipping since 2019, partially vulnerable: https://thunderspy.io/#kernel-dma-protection
  - MacOS partially vulnerable: https://thunderspy.io/#affected-apple-systems
- **Spycheck**
  - Free and open-source tool to determine if your system is vulnerable: https://thunderspy.io
  - Alternatively, follow manual verification steps on website

Thunderspy: Intel’s response

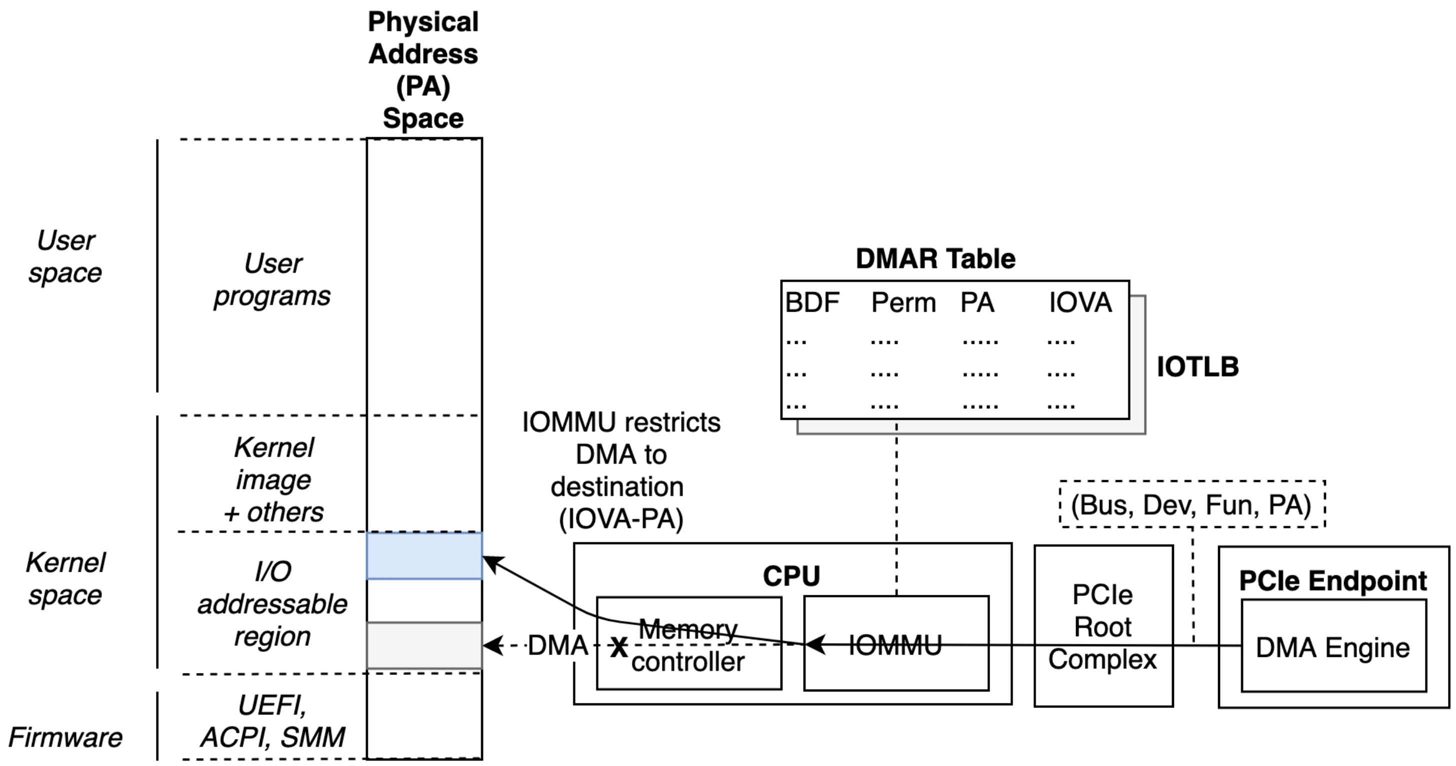
Kernel DMA Protection

- Intel-suggested mitigation to Thunderspy
- Opt-in DMA remapping for Thunderbolt devices
- Requires Windows 10 >= 1803, Linux kernel >= 5.0

Device-to-Host DMA



Device-to-Host DMA with IOMMU



Thunderspy: Intel's response

Kernel DMA Protection

- Intel-suggested mitigation to Thunderspy
- Opt-in DMA remapping for Thunderbolt devices
- Requires Windows 10 >= 1803, Linux kernel >= 5.0

However,

- Partial mitigation only
  - Mitigates only vulnerabilities 4-6
  - Prevents impact via DMA, but remaining vulnerabilities 1-3 expose system to BadUSB-style attacks
- Requires IOMMU and UEFI (BIOS) support
- UEFI support exclusively available on some >= 2019 systems
- **Not available on systems < 2019**

Thunderspy 2

- All Thunderbolt-equipped systems released 2011-2018, and several >= 2019, remain unpatched against Thunderspy
- Starting with Haswell (2013), a lot of Intel consumer systems feature an IOMMU, thus technically capable of supporting DMA remapping
- **Thunderspy 2:** OS-agnostic ACPI table upgrade patch
  - Brings Kernel DMA Protection to roughly 6 years worth of systems
    - Includes Thunderbolt 2!
  - Experimental OS-agnostic UEFI extension
    - Works with Windows 10 1803+ and Linux kernel 5.0+
    - Note: ACPI patching could also be turned into attack, i.e. disabling Kernel DMA Protection on supported systems. Recommended to self-sign TS2 extension and use measured boot (next slide)
  - Protection level similar to officially supported systems at OS runtime
    - Does not protect against boot time attacks, but screenlocking + sleep mode are covered ☺

Thunderspy 2: Mitigations on Linux

- We are working with the Linux kernel hardware security team to develop kernel-level mitigations
  - Work around ACPI to enable Kernel DMA Protection on unsupported Thunderbolt systems
- Meanwhile, Linux users can use TS2 UEFI extension
  - Secure Boot: sign using your own keys
  - Combine with measured boot (e.g. TPM-enabled GRUB) for additional security

Demo 2 – **Kernel DMA Protection patched onto unsupported machine**

What's Next?

The future of Thunderbolt-based interconnects

- What issues currently remain unaddressed?
  1. **Thunderspy vulnerabilities 1–3**: No means to distinguish between forged and legitimate DROMs. Devices that look legitimate physically could still be malicious.
  2. **Narrow scope of Kernel DMA Protection vs. Security Levels:** Enables PCIe tunneling without user interaction. Does not protect against malicious devices that
     - spoof arbitrary PCI IDs to target vulnerable device drivers
     - spoof TLP source IDs to hijack transactions
- How may these issues affect USB 4 and Thunderbolt 4?
  - To mitigate Thunderspy, Thunderbolt 4 now requires Kernel DMA Protection as part of vendor product certification
  - Backwards compatibility likely means susceptibility to (1), while (2) remains unaddressed

What's Next?

The future of Thunderbolt-based interconnects

- What are potential avenues on mitigating these remaining issues?
  - **Thunderspy vulnerabilities 1–3**:
    Firmware embeds public key + digest; may allow to verify authenticity on host (driver, DXE) if Intel publishes digest scope
  - **Narrow scope of Kernel DMA Protection vs. Security Levels:**
    (1) Allow all DMA devices on boot. OS runtime: initially, "null-route" all new DMA devices using IOMMU. Require screen unlocking and explicit user authorization, then have IOMMU assign I/O memory range.
    (2) Virtualization-based security (VBS) may help prevent kernel memory safety issues
    (3) TB controller-assisted TLP source ID verification (similar to PCIe ACS)
  - **USB 4:**
    Implement UEFI toggle that controls Thunderbolt signaling (… and maintain state in UEFI only, please!)

Takeaway

- **Thunderspy:** a new class of vulnerabilities breaking Thunderbolt security
  - No fix from Intel for vulnerable systems released in 2011-2020; Kernel DMA Protection available only on some >= 2019 systems
  - Check if your system is vulnerable – use Spycheck or verify manually
  - Full vulnerability report: https://thunderspy.io
- **Thunderspy 2:** experimental, OS-agnostic mitigation to Thunderspy
  - Brings Kernel DMA Protection to all vulnerable systems with IOMMU
- **The future is PCI Express**
  - Thunderbolt is a powerful external interconnect enabling high-bandwidth, low-latency use cases previously not possible
  - USB 4 and Thunderbolt 4 upcoming, but adequate protection schemes remain absent (for now?)

Thank You

Questions?

Björn Ruytenberg

@0Xiphorus

https://bjornweb.nl