



# When Lightning Strikes Thrice: Breaking Thunderbolt 3 Security

BJÖRN RUYTENBERG, MSC  
EINDHOVEN UNIVERSITY OF TECHNOLOGY

[@ØXIPHORUS](#) • [BJORNWEB.NL](#)

# Thunderbolt: A PCIe-based Interconnect

- High-performance, proprietary I/O protocol developed by Intel and Apple
- PCI Express (PCIe)-based, Direct Memory Access (DMA)-enabled connectivity
- **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
- **USB4 (2019)** extends TB3 to additional market segments
  - While not spec-mandated, virtually all USB4-compliant host controllers to date support TB3 signaling
  - Beyond x86: first TB version to be adopted on ARM

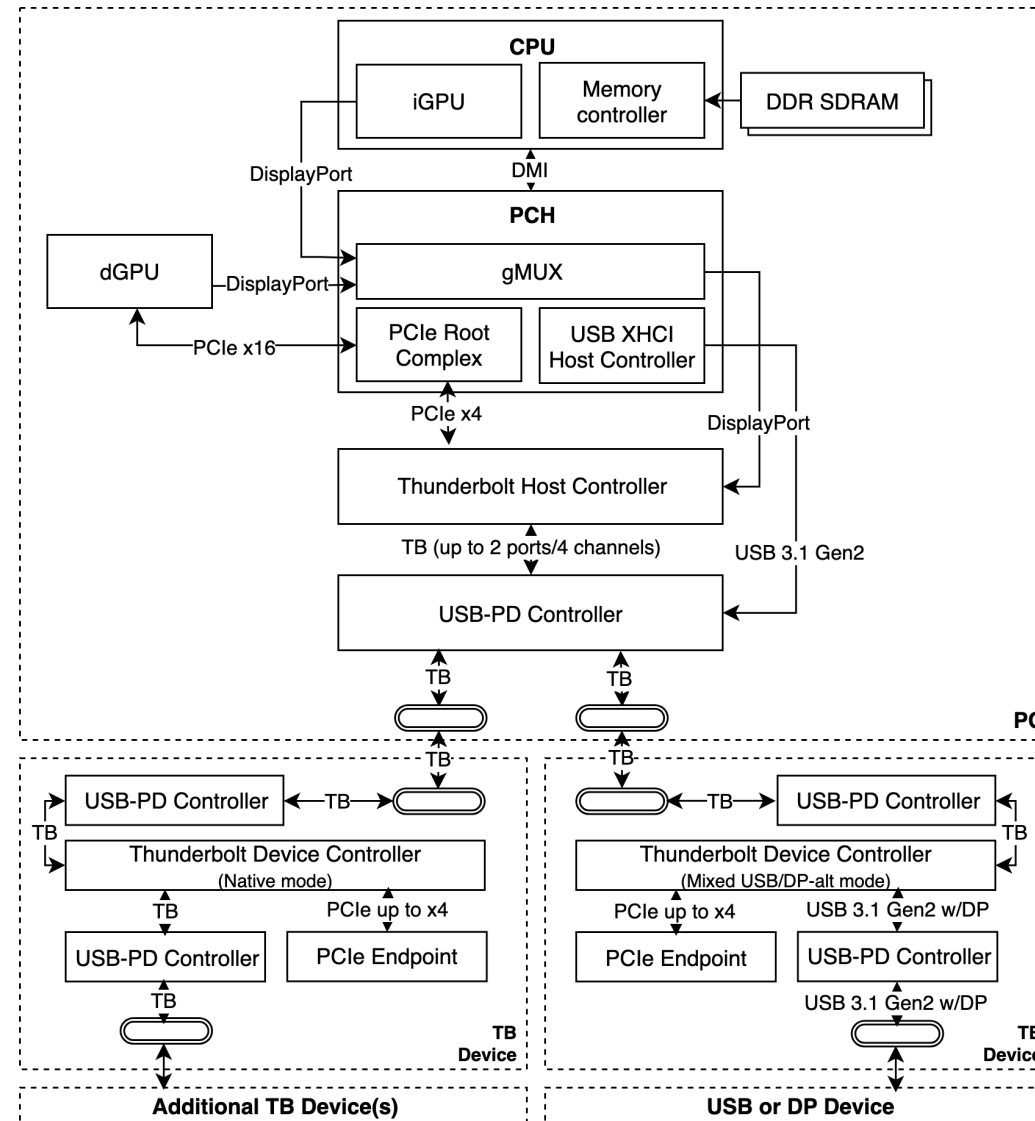


# Reverse Engineering Thunderbolt

- Thunderbolt is a proprietary standard
- Protocol specifications not publicly documented
- Hardware architecture not publicly documented

# Reverse Engineering Thunderbolt

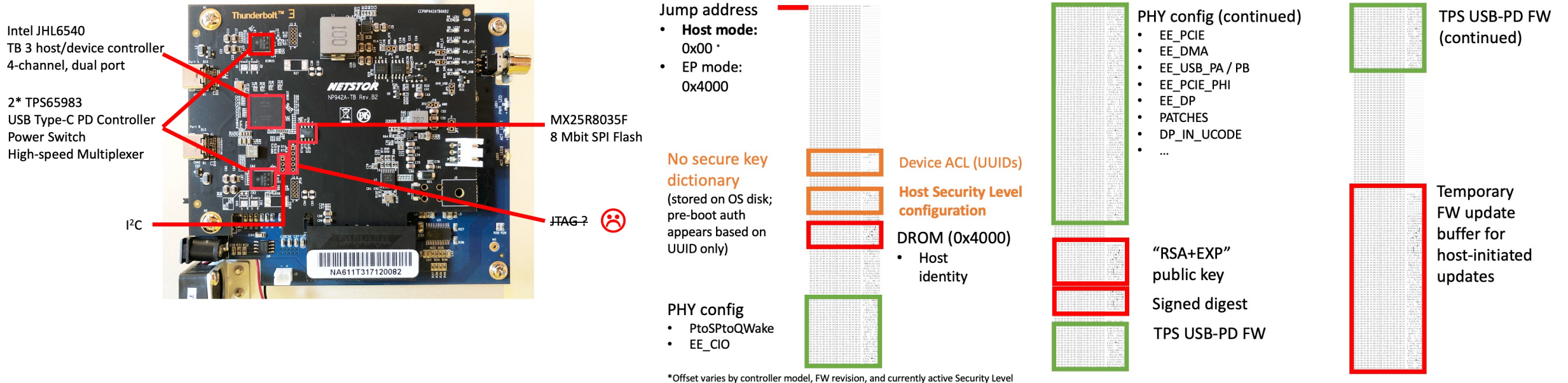
Our analysis of Thunderbolt hardware architecture



# Reverse Engineering Thunderbolt

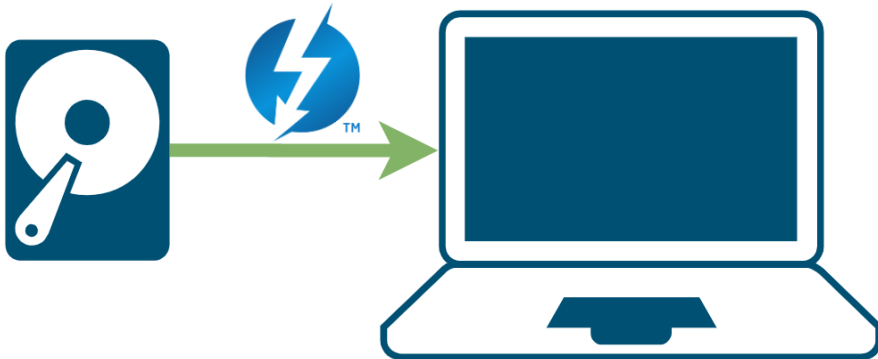
## Dissecting Thunderbolt-equipped systems and devices

- Reversed Thunderbolt host and device controller firmware
- 5 vendors, 24 systems across 8 generations of systems: Intel, Apple, Lenovo, HP, Dell, Gigabyte
- 5 generations of Thunderbolt controllers: Falcon Ridge (TB2), Alpine Ridge-2015, Alpine Ridge-2016, Titan Ridge, Ice Lake (TB3)



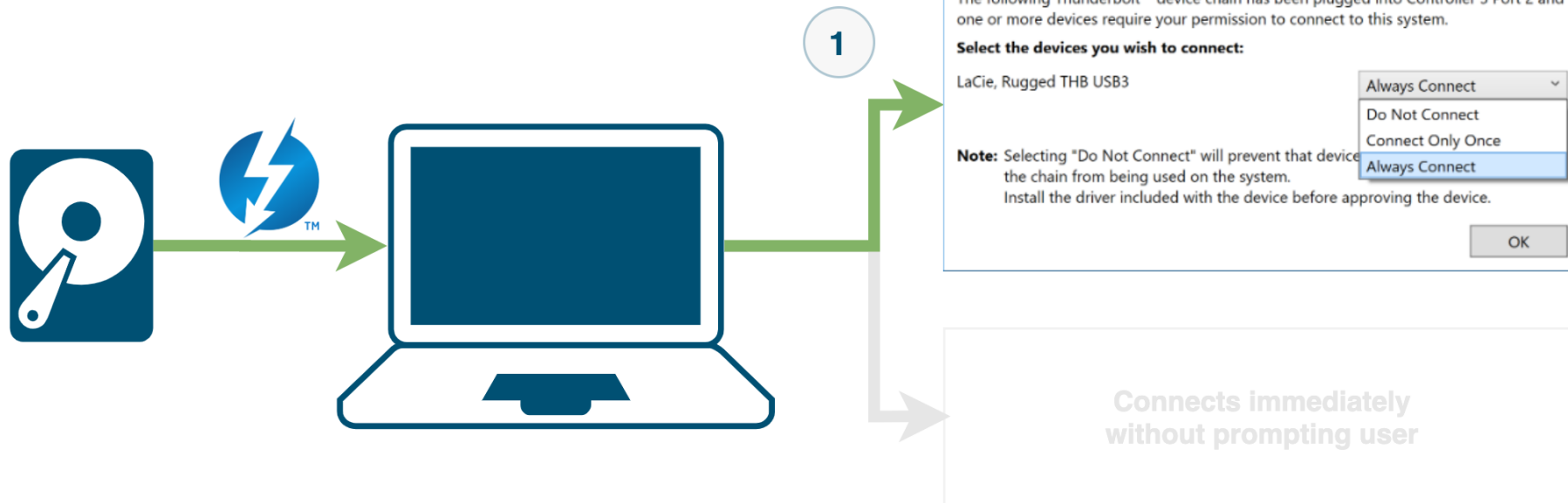
# Thunderbolt Security Architecture

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



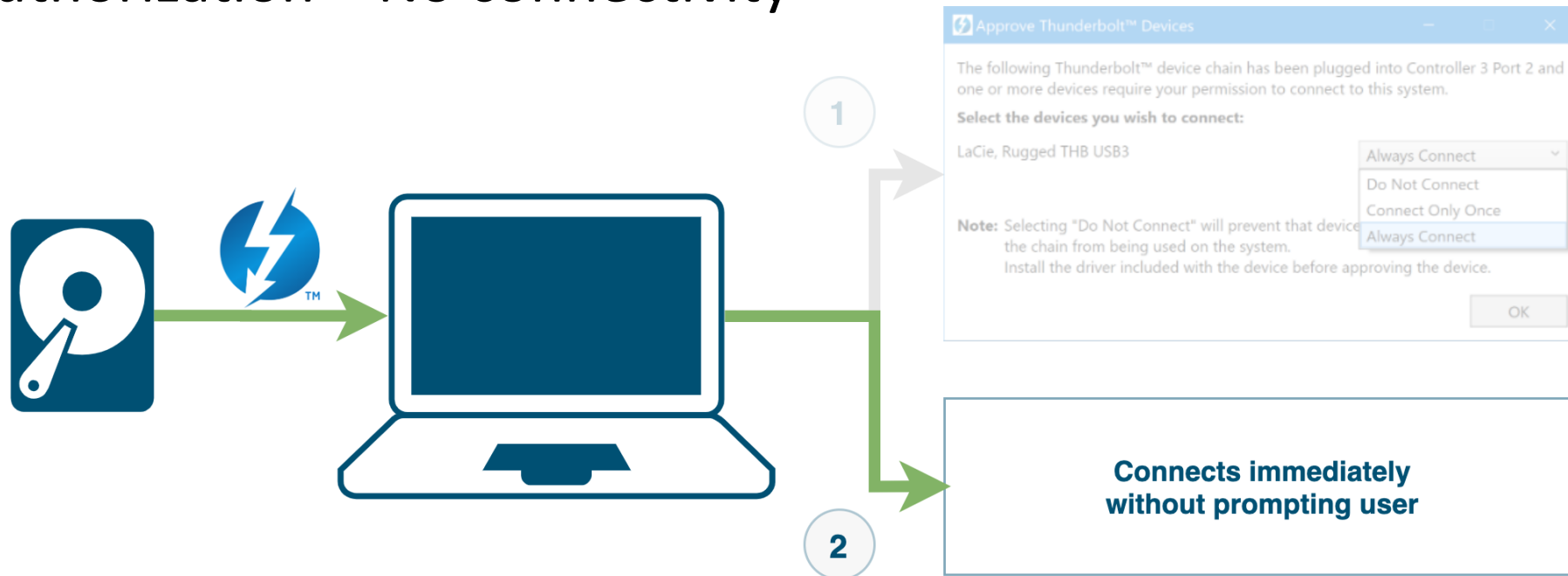
# Thunderbolt Security Architecture

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



# Thunderbolt Security Architecture

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





# When Lightning Strikes Thrice: Breaking Thunderbolt 3 Security



Thunderspy (<https://thunderspy.io>) is a research project focused on reverse engineering the security properties of Thunderbolt.

So far, we have disclosed seven vulnerabilities in public:

1. Inadequate firmware verification schemes
2. Weak device authentication scheme
3. Use of unauthenticated device metadata
4. Downgrade attack using backwards compatibility
5. Use of unauthenticated controller configurations
6. SPI flash interface deficiencies
7. No Thunderbolt security under Boot Camp (Apple)\*

\* Thunderbolt controller on-board signature verification remains intact but is insufficient

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

Partially sped up to fit CSNG session. Please refer to our [YouTube recording](#) for the complete real-time footage.



# Institutional impact

## Corporate first contact

Thunderspy was reported for coordinated disclosure to key strategic vendors and institutions, including:

- ▶ Apple
- ▶ Intel (who informed Dell, HP, and Lenovo)
- ▶ Microsoft
- ▶ Linux kernel security team
- ▶ Major Linux distro vendors, including Red Hat, Debian, Canonical
- ▶ MITRE Corporation
- ▶ NCSC-NL
- ▶ TWCERT-CC
- ▶ Major ODMs, including Clevo, Compal, Quanta (next slide)

# Institutional impact

## Corporate first contact

We worked with major ODMs to contact all affected vendors, including:

- ▶ Razer
- ▶ Asus
- ▶ Huawei
- ▶ Gigabyte
- ▶ Medion
- ▶ Acer
- ▶ MSI
- ▶ Dynabook (formerly Toshiba)
- ▶ BTO
- ▶ SKIKK
- ▶ PNY
- ▶ System76

# Industry response (selected)

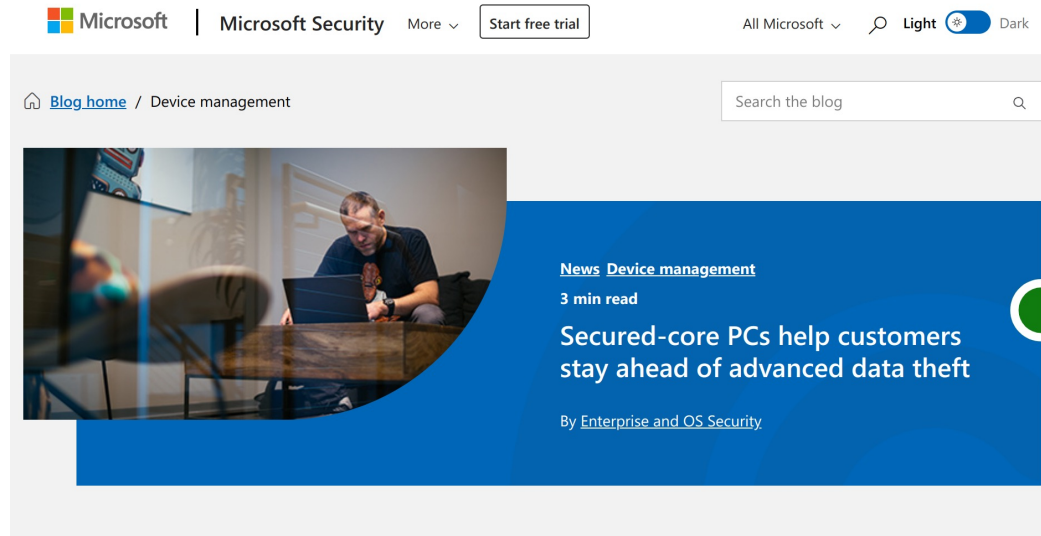
## Intel

In our vulnerability disclosure procedure so far, Intel has stated the following:

- All vulnerabilities confirmed for Thunderbolt 1, 2, and 3
- Thunderbolt 3
  - No fix for in-market systems – all Thunderbolt-equipped systems released 2011-2018, and several  $\geq$  2019, remain unpatched against Thunderspy
  - Intel-suggested mitigation: Kernel DMA Protection
    - Only available on some (not all) Thunderbolt 3 systems released 2019 – 2021
    - Narrow mitigation scope: mitigates arbitrary DMA, does not address TS vulnerabilities 1-3 and other PCIe-inherent attack vectors
- USB4
  - No spec-mandated mitigations to Thunderspy
- Thunderbolt 4
  - Mitigates Thunderspy by incorporating additional hardware protections, and
  - Thunderbolt 4 requires Kernel DMA Protection as part of vendor product certification

# Industry response (selected)

## Microsoft



The screenshot shows the Microsoft Security blog interface. At the top, there's a navigation bar with the Microsoft logo, 'Microsoft Security', a 'Start free trial' button, and a search bar. Below the navigation, the breadcrumb 'Blog home / Device management' is visible. The main content area features a large blue banner with a photo of a person working on a laptop. The article title is 'Secured-core PCs help customers stay ahead of advanced data theft', with a sub-headline 'News Device management' and a '3 min read' indicator. The author is listed as 'By Enterprise and OS Security'.

May 13, 2020



Threat trends

Microsoft Security Insights

Windows

Researchers at the Eindhoven University of Technology recently revealed information around "[Thunderspy](#)," an attack that relies on leveraging direct memory access (DMA) functionality to compromise devices. An attacker with physical access to a system can use Thunderspy to read and copy data even from systems that have encryption with password protection enabled.

[Secured-core PCs](#) provide customers with Windows 10 systems that come configured from OEMs with a set of hardware, firmware, and OS features enabled by default, mitigating Thunderspy and any similar attacks that rely on malicious DMA.

### How Thunderspy works

Like any other modern attack, Thunderspy relies on not one but multiple building blocks being chained together. Below is a summary of how Thunderspy can be

## Defense against hardware and firmware exploits

### *Leveraging hardware for security*

At the heart of the Surface Laptop 4, the device leverages the Trusted Platform Module 2.0 (TPM) and the AMD Ryzen™ Mobile Processors with System Guard to boot securely and minimize the impact of firmware vulnerabilities by sandboxing firmware to protect critical subsystems and sensitive data. Kernel Direct Memory Access Protection is pre-enabled on these devices, helping to ensure that the system is protected against malicious and unintended Direct Memory Access (DMA) attacks for all DMA-capable devices, such as PCI devices, thwarting the entire class of drive-by DMA attacks like [Thunderspy](#).

### [Surface expands its Secured-core Portfolio with new Surface Laptop 4]

### Thunderspy DMA Peripheral Attack

Researchers at the Eindhoven University of Technology recently revealed information around "[Thunderspy](#)," an attack that relies on leveraging direct memory access (DMA) functionality to compromise devices. An attacker with physical access to a system can use Thunderspy to read and copy data even from systems that have encryption with password protection enabled.

[Secured-core PCs](#) provide customers with Windows 11 systems that come configured from OEMs with a set of hardware, firmware, and OS features enabled by default, mitigating Thunderspy and any similar attacks that rely on malicious DMA.

### [Windows 11 Secured-Core PC – Enterprise Evaluation Guide]

### [Secured-core PCs help customers stay ahead of advanced data theft]

# Industry response (selected)

MITRE Corporation

**CAPEC-665: Exploitation of Thunderbolt Protection Flaws**

Attack Pattern ID: 665  
Abstraction: Detailed

View customized information:

**Description**

An adversary leverages a firmware weakness within the Thunderbolt protocol, on a computing device to manipulate Thunderbolt controller firmware in order to exploit vulnerabilities in the implementation of authorization and verification schemes within Thunderbolt protection mechanisms. Upon gaining physical access to a target device, the adversary conducts high-level firmware manipulation of the victim Thunderbolt controller SPI (Serial Peripheral Interface) flash, through the use of a SPI Programming device and an external Thunderbolt device, typically as the target device is booting up. If successful, this allows the adversary to modify memory, subvert authentication mechanisms, spoof identities and content, and extract data and memory from the target device. Currently 7 major vulnerabilities exist within Thunderbolt protocol with 9 attack vectors as noted in the Execution Flow.

**Likelihood Of Attack**  
Low

**Typical Severity**  
Very High

**Relationships**

Nature	Type	ID	Name
ChildOf		276	<a href="#">Inter-component Protocol Manipulation</a>
PeerOf		148	<a href="#">Content Spoofing</a>
PeerOf		151	<a href="#">Identity Spoofing</a>
PeerOf		458	<a href="#">Flash Memory Attacks</a>
CanFollow		390	<a href="#">Bypassing Physical Security</a>

View Name	Top Level Categories
<a href="#">Domains of Attack</a>	<a href="#">Software</a> , <a href="#">Communications</a>
<a href="#">Mechanisms of Attack</a>	<a href="#">Abuse Existing Functionality</a>

[CAPEC-665: Exploitation of Thunderbolt Protection Flaws – CAPEC Version 3.5]

## Addressing Thunderspy, One Weakness at A Time



CWE/CAPEC · Follow

3 min read · Apr 20, 2021



Does your company produce hardware? If you don't take security into account, consumers won't trust your hardware, and they will act accordingly: by buying elsewhere to minimize risk. This is especially true for corporate purchasing where large organizations view security as a critical requirement. Let's take a look at a recent vulnerability and see how a brand's reputation can be protected by mitigating its underlying weaknesses.

Thunderspy is the name for some impressive attacks on Thunderbolt 3 systems, discovered by Bjorn Ruytenberg. Thunderbolt is a proprietary I/O protocol that allows for a two-way high-bandwidth PCIe port for external devices to have Direct Memory Access-enabled I/O. The technology provides

[Addressing Thunderspy, One Weakness at A Time – CWE/CAPEC Blog]



# Public awareness

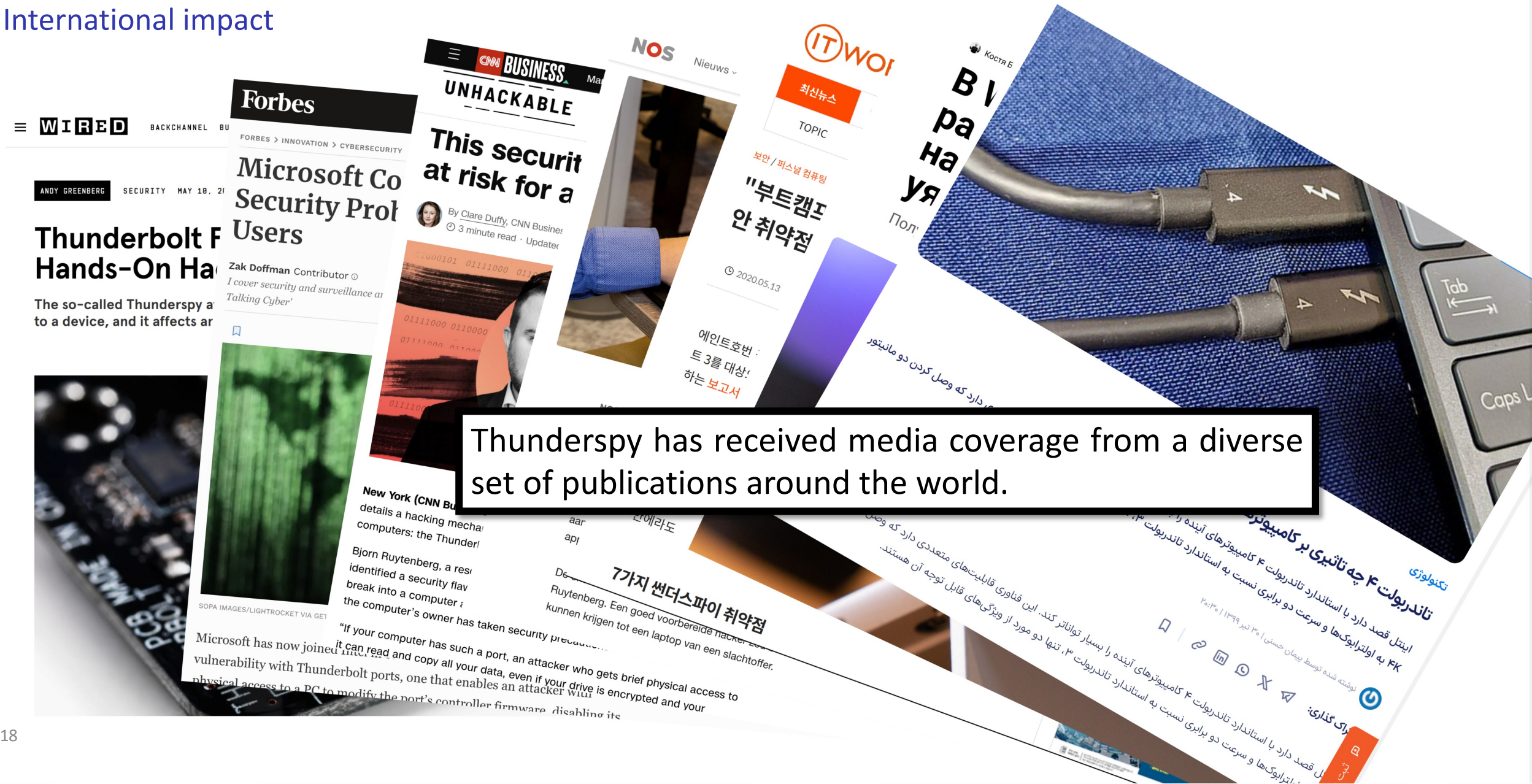
Helping users, developers, and the general public

Presented this research in an academic setting as a Masters project at TU/e and at top-ranking conferences, including:

- ▶ [Black Hat USA](#)
- ▶ [Chaos Communication Congress](#)
- ▶ [Dutch Design Week](#)

# Media coverage

## International impact



Thunderspy has received media coverage from a diverse set of publications around the world.

# Thunderspy – Public Disclosure

Raising awareness and improving user security

Creating freely available tools with source code helps to empower users and is an important part of security research. We have published:

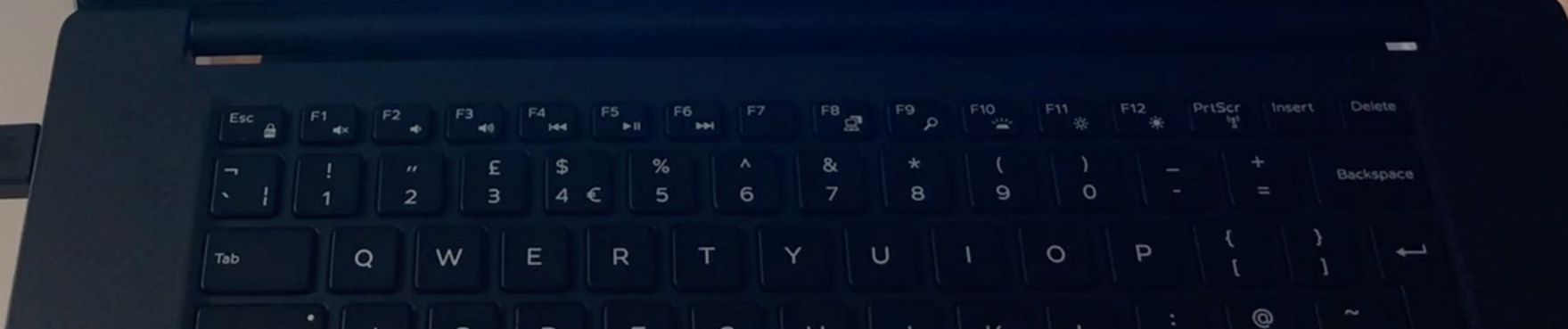
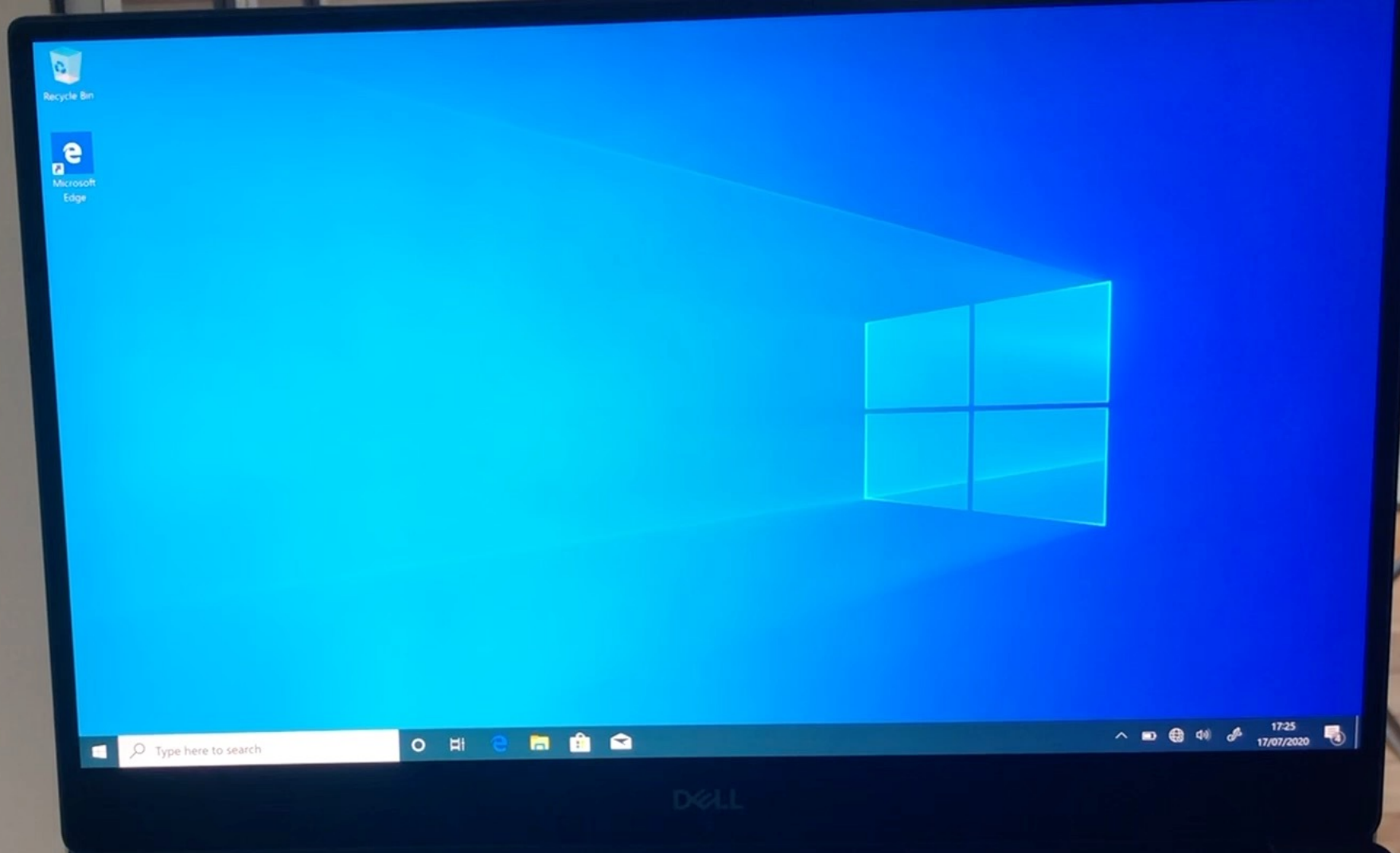
- [Spycheck](#), a free and open-source (GPL) tool for Windows and GNU/Linux to detect if a system is susceptible to Thunderspy
- [tcfp](#), a free and open-source (GPL) tool to patch Thunderbolt controller firmware; PoC demonstrating Thunderspy vulnerabilities
- [SPIblock](#), a free and open-source (GPL) tool to reconfigure Thunderbolt flash memory security settings; PoC demonstrating Thunderspy vulnerabilities

Millions of systems released 2011-2018, and several  $\geq$  2019, remain unpatched against Thunderspy. To help protect users, we have additionally published:

- [kDMAp-patcher](#), an experimental OS-agnostic BIOS extension to enable Kernel DMA Protection on systems where vendors have otherwise left users entirely vulnerable

# Demo 2 – Kernel DMA Protection Patcher

## Patching kDMAp onto unsupported machines



# Industry response to kdmmap-patcher (selected)

Lenovo



## Intel Thunderbolt Vulnerabilities

**Lenovo Security Advisory:** LEN-31390

**Potential Impact:** Information disclosure, privilege escalation

**Severity:** High

**Scope of Impact:** Industry-wide

**CVE Identifier:** CVE-2019-14630

### Summary Description:

Intel reported potential security vulnerabilities, requiring physical access and dedicated equipment, in Intel Thunderbolt that could allow a malicious peripheral device to access secret data and change system behavior on systems with Thunderbolt interfaces.

### Mitigation Strategy for Customers (what you should do to protect yourself):

Intel recommends the following guidelines for a robust DMA protection solution:

**Lenovo issues BIOS updates to retroactively patch Kernel DMA Protection onto in-market ThinkPad systems**

later) for systems with newer Intel processors (2019 or later).

### Product Impact:

#### Kernel DMA Protections Supported

- ThinkPad P1 Gen. 1 (BIOS version [N2EUJ26W](#) or later)
- X1 Extreme Gen. 1 (BIOS version [N2EUJ26W](#) or later)
- P52 (BIOS version [N2CUJ28W](#) or later)
- P72 (BIOS version [N2CUJ28W](#) or later)
- ThinkPad P1 Gen. 2
- X1 Extreme Gen. 2, X1 Carbon Gen7/ 8, X1 Yoga 4th Gen, X390, X390 Yoga
- ThinkPad P43s, P53, P53s, P73
- ThinkPad T490/T490s, T590
- Lenovo S940-14IWL, Yoga S940-14IWL
- ThinkPad L13 1st Gen\_Intel\_CML,
- ThinkPad E490s /ThinkPad S3/ ThinkPad E490/E590/R490/R590
- ThinkPad L390 Yoga
- ThinkPad S2 Yoga 4th Gen
- ThinkPad L490/L590
- AIO A940

# Current and future work

**CAPEC-665: Exploitation of Thunderbolt**  
 Attack Pattern ID: 665  
 Abstraction: Detailed

**Description**  
 An adversary leverages a firmware weakness in order to exploit vulnerabilities in the firmware in order to gain physical access to a target device (Peripheral Interface) flash, through the USB-C port. If successful, this allows the adversary to gain access to the device's memory and memory from the target device. Current Execution Flow.

**Likelihood Of Attack**  
 Low

**Typical Severity**  
 Very High

**Relationships**

Nature	Type	ID	Name
ChildOf	S	276	Intel
PeerOf	M	148	Common
PeerOf	M	151	Intel
PeerOf	D	458	Intel

**Thunderbolt 界面遭發現多個資安發動攻擊**  
 發布日期：2020-09-23  
 發布單位:TWCERT/CC  
 點閱次數:3343

**Thunderspy kwetsbaarheden in Thunderbolt**  
 Nieuwsbericht | 11-05-2020 | 16:51


Een onderzoeker van de TU Eindhoven heeft zeven kwetsbaarheden, genaamd [Thunderspy](#), ontdekt in Thunderbolt van Intel. Thunderbolt is een computerpoort, te herkennen aan de bliksemschicht, voor snelle gegevensoverdracht tussen een PC of laptop en andere apparaten en is sinds 2011 in veel laptops en PC's te vinden.


The disclosure and coordination process working with vendors on as of yet undisclosed issues is ongoing.

# Thank You

Feel free to contact me or ask a question today.

 @0Xiphorus

 @0Xiphorus@infosec.exchange

 <https://bjornweb.nl>