

DIRECT MEMORY ACCESS EVERYWHERE

securelyfitz & baelfire 9 AUG 2025

©2025 SecuringHardware.com

JOE FITZPATRICK

- 10+ years of fun with hardware
  - silicon debug
  - security research
  - pen testing of CPUs
  - security training
- Applied Physical Attacks Training:
  - X86 Systems
  - Embedded Systems
  - Hardware Pentesting
  - Own white shoes full of LEDs



Joe FitzPatrick

@securelyfitz

joefitz@securinghardware.com

©2025 SecuringHardware.com

GRACE PARRISH

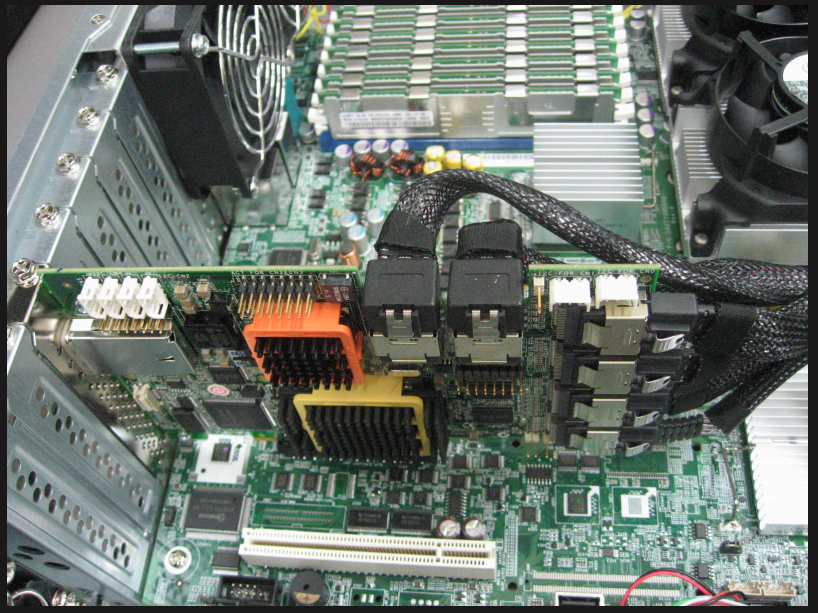
- Studying cybersecurity at OSU
- Working as SOC analyst
- Board level repair technician
- Taught industrial control systems 9 years
    - PLCs
    - HMIs
- Enjoys learning
    - Jack of all trades
- Goal: offensive security career



Grace Parrish

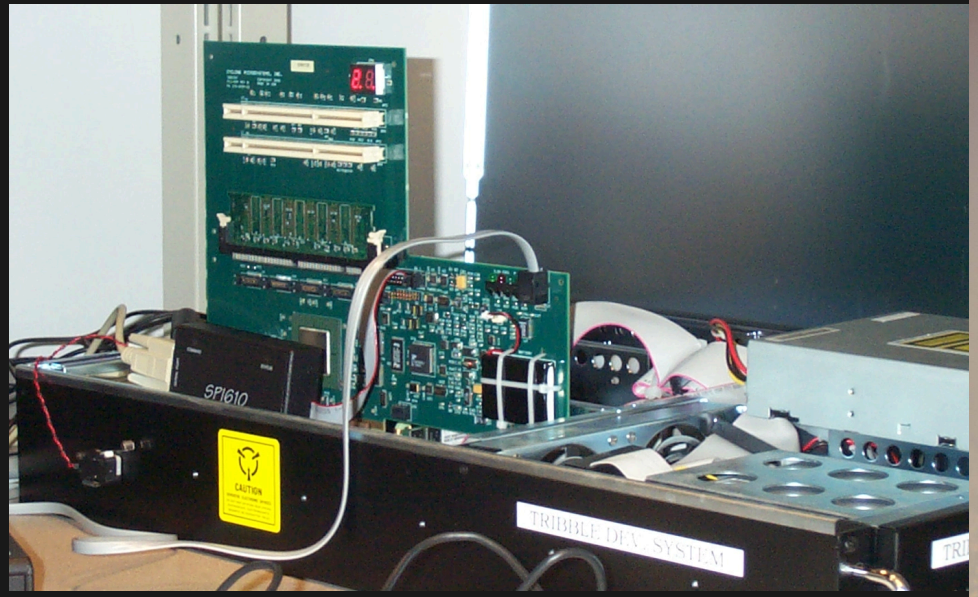
@BaelfireNightshd

©2025 SecuringHardware.com

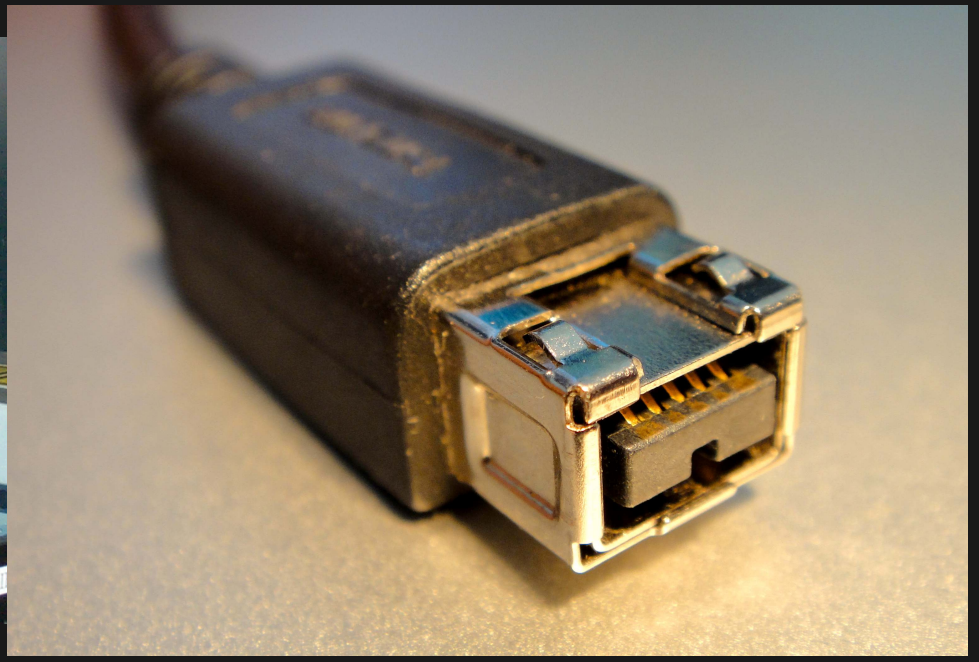


This is PCIe.

©2025 SecuringHardware.com



Tribble, a PCI DMA attack device by Joe Grand

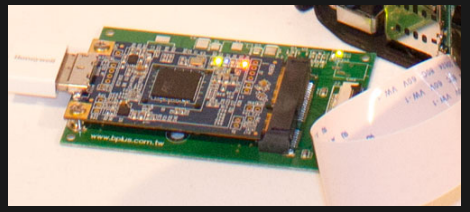


Firewire, external dma spanning 2 millenia

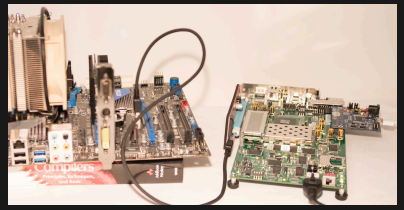
©2025 SecuringHardware.com

A brief tale of epic procrastination:





- 2014: Slotscreamer
- 2016: Pcileech
- 2017: Pcileech FPGA
- 2019: Thunderclap
- 2020: Thunderspy
- more to come...





©2025 SecuringHardware.com

4 QUESTION THREAT MODEL:

1.
2.
3.
4.

©2025 SecuringHardware.com

4 QUESTION THREAT MODEL:

1. **What are we working on?**
2.
3.
4.

©2025 SecuringHardware.com

4 QUESTION THREAT MODEL:

1. **What are we working on?**
2. **What can go wrong?**
3.
4.

©2025 SecuringHardware.com

4 QUESTION THREAT MODEL:

1. **What are we working on?**
2. **What can go wrong?**
3. **What are we going to do about it?**
4.

©2025 SecuringHardware.com

4 QUESTION THREAT MODEL:

1. **What are we working on?**
2. **What can go wrong?**
3. **What are we going to do about it?**
4. **Did we do a good job?**

©2025 SecuringHardware.com

PCIE THREAT MODEL

1. **What are we working on?**

2. **What can go wrong?**

3. **What are we going to do about it?**

4. **Did we do a good job?**

©2025 SecuringHardware.com

PCIE THREAT MODEL

1. **What are we working on?**
   High Speed interconnects
2. **What can go wrong?**

3. **What are we going to do about it?**

4. **Did we do a good job?**

©2025 SecuringHardware.com

PCIE THREAT MODEL

1. **What are we working on?**
   High Speed interconnects
2. **What can go wrong?**
   Malicious Devices
3. **What are we going to do about it?**

4. **Did we do a good job?**

©2025 SecuringHardware.com

PCIE THREAT MODEL

1. **What are we working on?**
   High Speed interconnects
2. **What can go wrong?**
   Malicious Devices
3. **What are we going to do about it?**
   Keep it inside the case
4. **Did we do a good job?**

©2025 SecuringHardware.com

PCIE THREAT MODEL

1. **What are we working on?**
   High Speed interconnects
2. **What can go wrong?**
   Malicious Devices
3. **What are we going to do about it?**
   Keep it inside the case
4. **Did we do a good job?**
   Mostly?

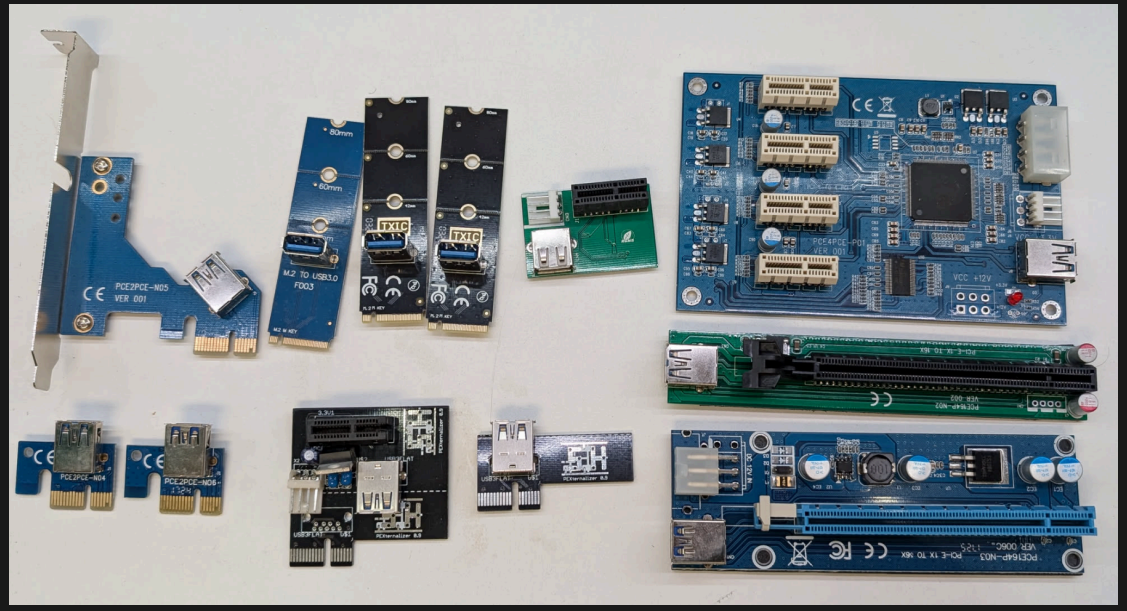
©2025 SecuringHardware.com

ATTACKING PCIE

1. Connect your hardware
2. Enumerate
3. Enable Bus Master
4. Read or Write memory
5. Present at DEF CON

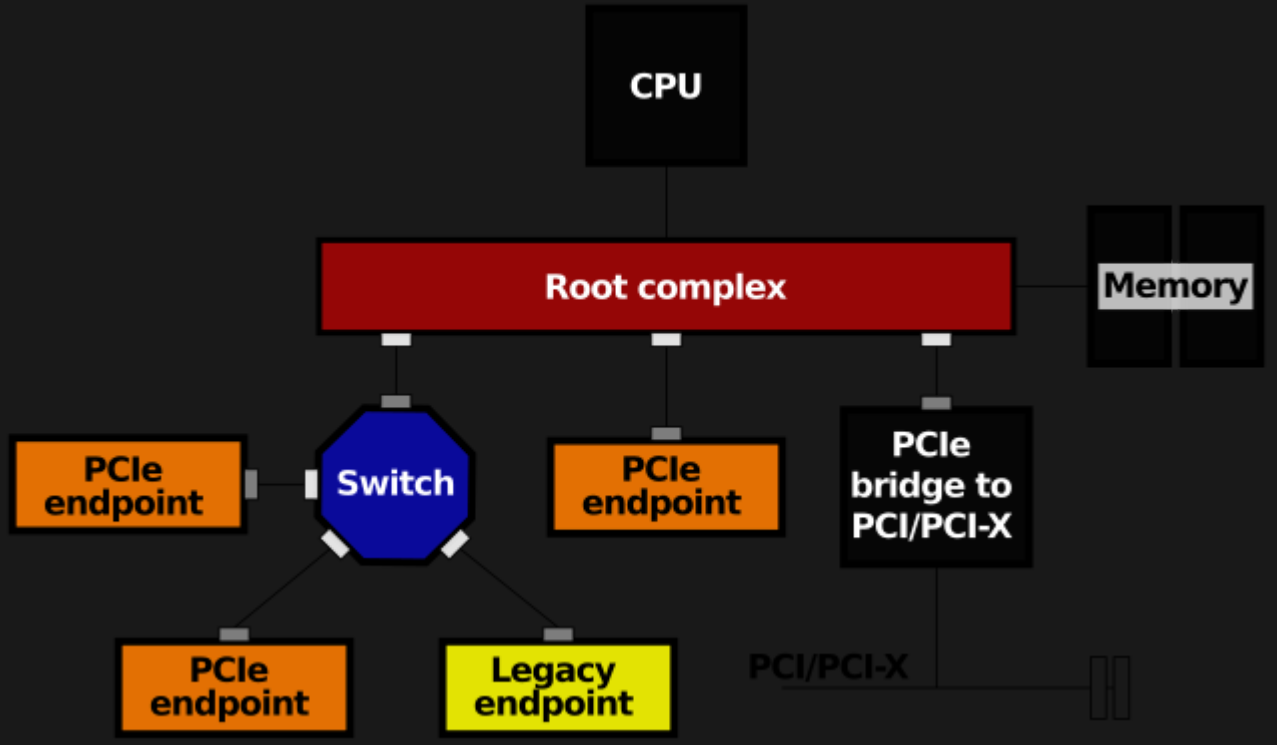
©2025 SecuringHardware.com

CONNECTING HARDWARE



©2025 SecuringHardware.com

ENUMERATING



©2025 SecuringHardware.com

ENUMERATING

```
joefitz@linmax2:~$ lspci -tv
-[0000:00]-+-00.0  Advanced Micro Devices, Inc. [AMD] Strix/Strix Halo Root Complex
           +-00.2  Advanced Micro Devices, Inc. [AMD] Strix/Strix Halo IOMMU
           +-01.0  Advanced Micro Devices, Inc. [AMD] Strix/Strix Halo Dummy Host Bridge
           +-01.1-[01-60]--
           +-01.2-[61-c0]--
           +-02.0  Advanced Micro Devices, Inc. [AMD] Strix/Strix Halo Dummy Host Bridge
           +-02.1-[c1]----00.0  Shenzhen Longsys Electronics Co., Ltd. Lexar NM790 NVME SSD (DRAM-less)
           +-02.2-[c2]----00.0  Genesys Logic, Inc GL9755 SD Host Controller
           +-02.3-[c3]----00.0  Intel Corporation Wi-Fi 6E(802.11ax) AX210/AX1675* 2x2 [Typhoon Peak]
           +-03.0  Advanced Micro Devices, Inc. [AMD] Strix/Strix Halo Dummy Host Bridge
           +-08.0  Advanced Micro Devices, Inc. [AMD] Strix/Strix Halo Dummy Host Bridge
```

©2025 SecuringHardware.com

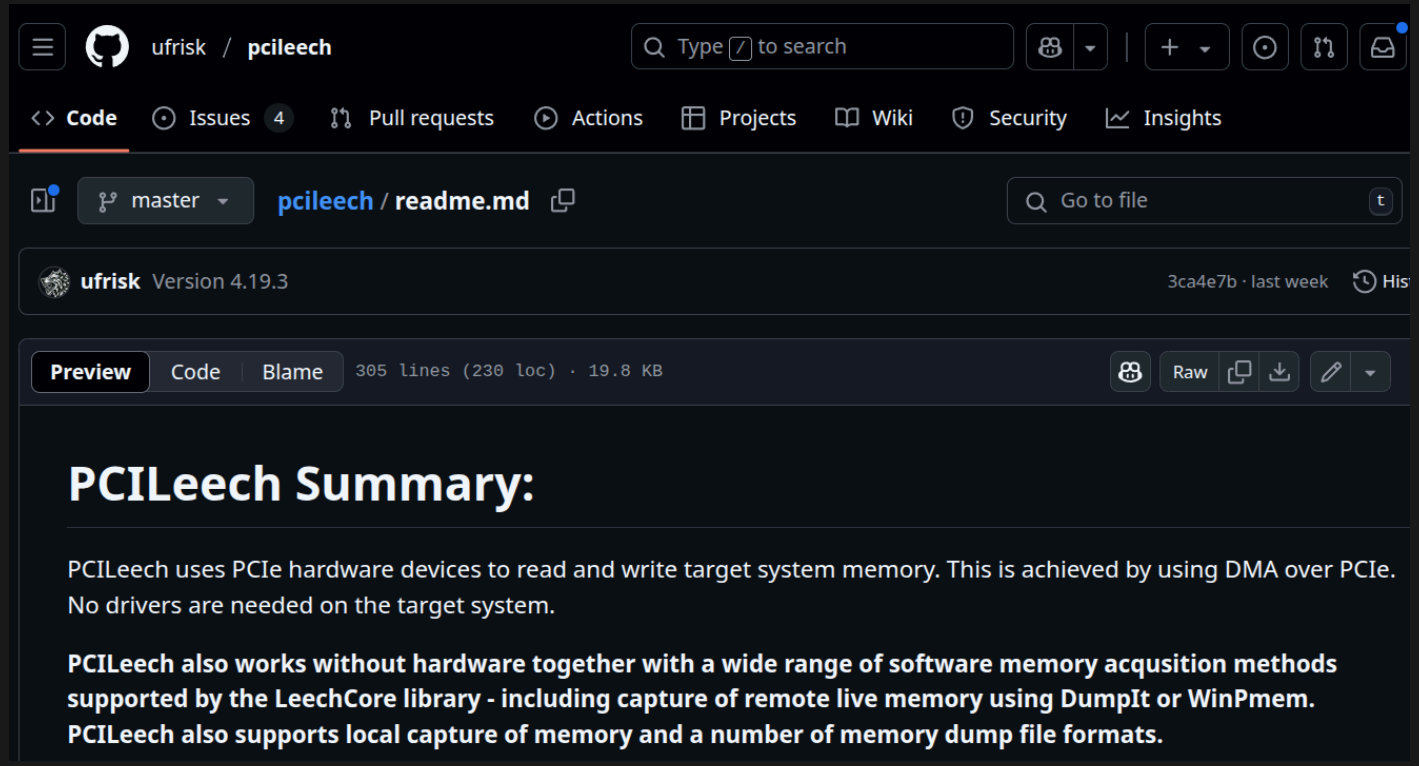
READ/WRITE MEMORY

Table 2-2: PCI Express TLP Packet Types

TLP Packet Types	Abbreviated Name
Memory Read Request	MRd
Memory Read Request - Locked access	MRdLk
Memory Write Request	MWr
IO Read	IORd
IO Write	IOWr
Configuration Read (Type 0 and Type 1)	CfgRd0, CfgRd1
Configuration Write (Type 0 and Type 1)	CfgWr0, CfgWr1
Message Request without Data	Msg
Message Request with Data	MsgD
Completion without Data	Cpl
Completion with Data	CplD
Completion without Data - associated with Locked Memory Read Requests	CplLk
Completion with Data - associated with Locked Memory Read Requests	CplDLk

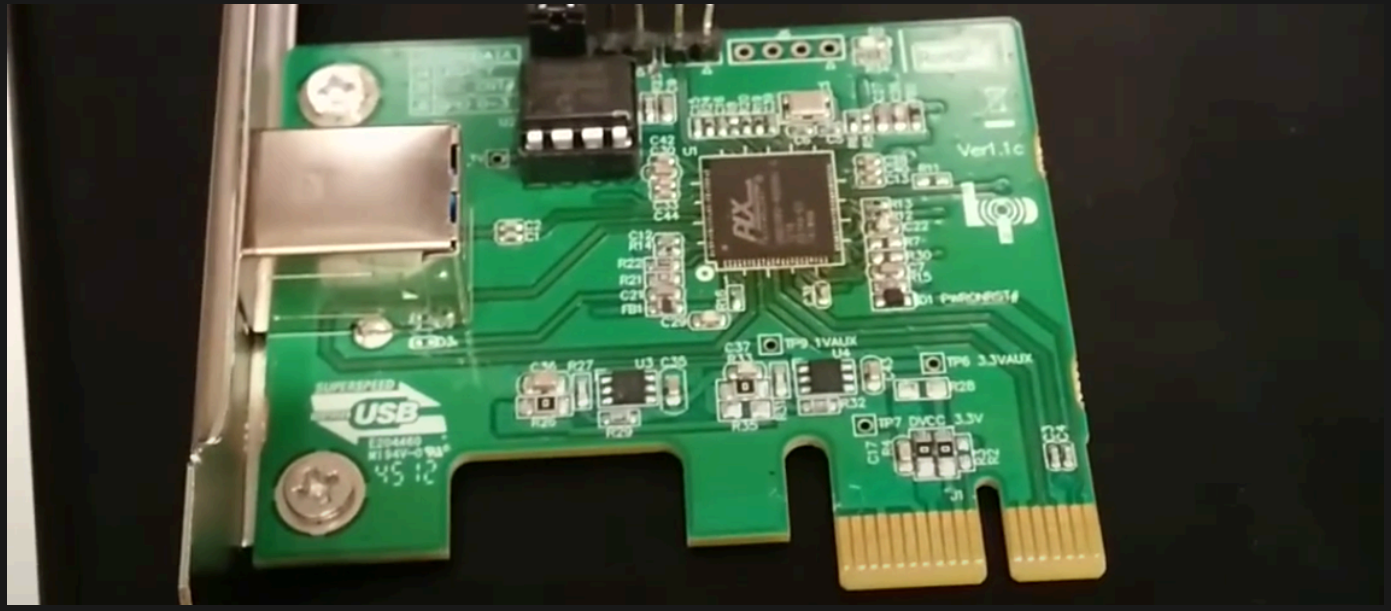
©2025 SecuringHardware.com

PCILEECH



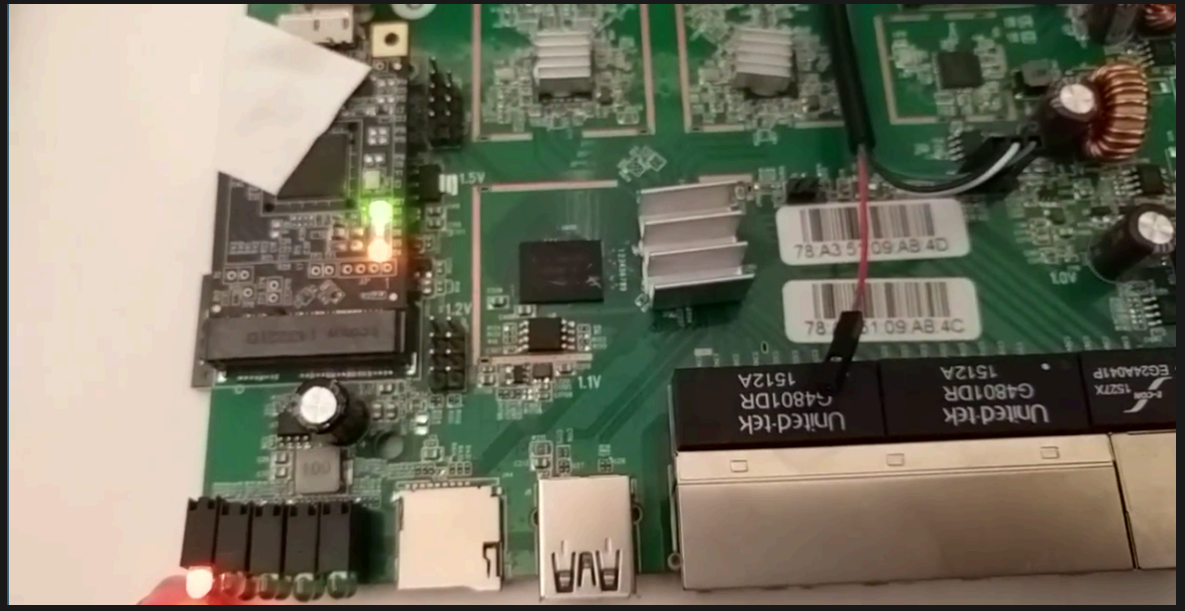
©2025 SecuringHardware.com

EXAMPLE: DUMPING MEMORY

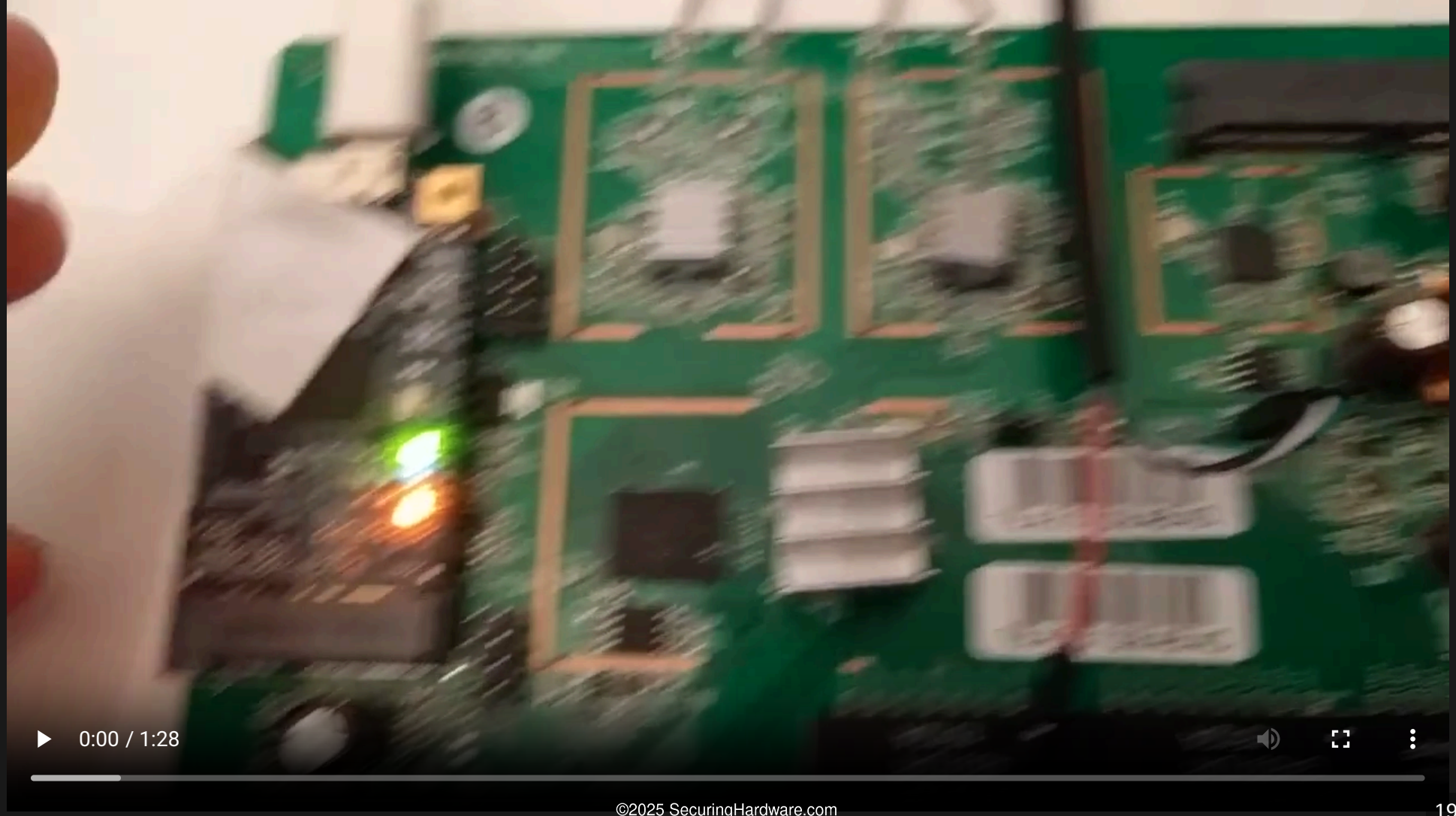


©2025 SecuringHardware.com

EXAMPLE: LOCKSCREEN BYPASS



©2025 SecuringHardware.com



©2025 SecuringHardware.com

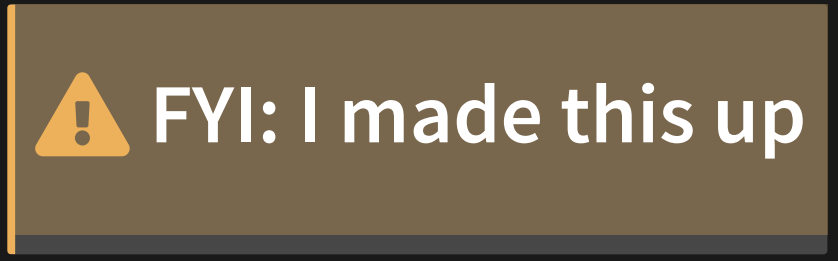
KEY TAKEAWAY:

PCIE IS PERMISSIVE BY DESIGN

©2025 SecuringHardware.com

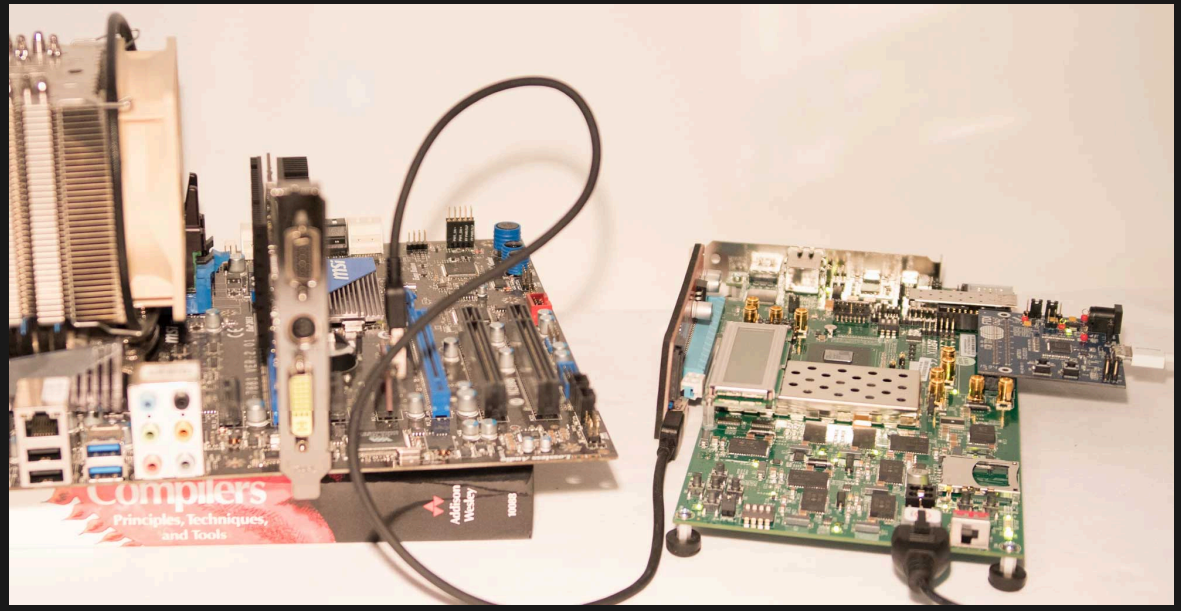
Joe's DMA Attack Taxonomy:

- Tethered
- Drive-By
- Embedded



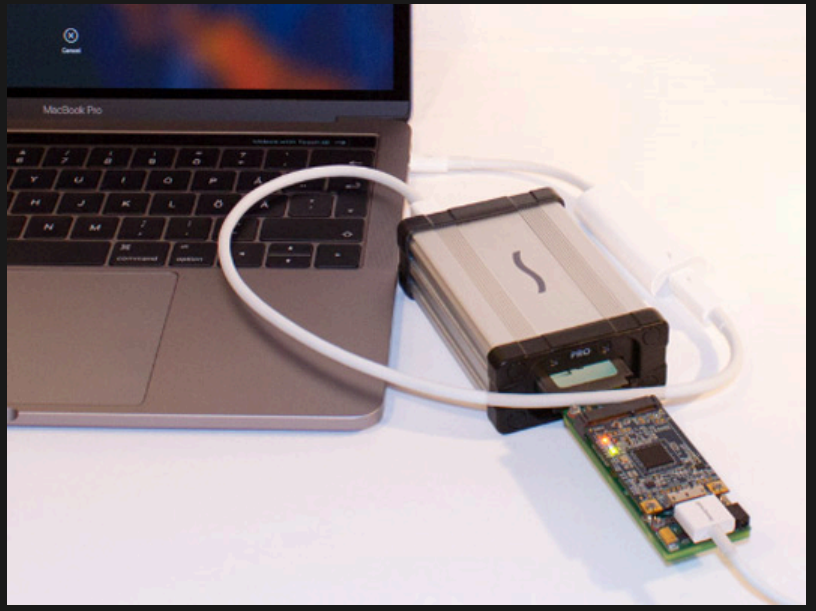
©2025 SecuringHardware.com

TETHERED



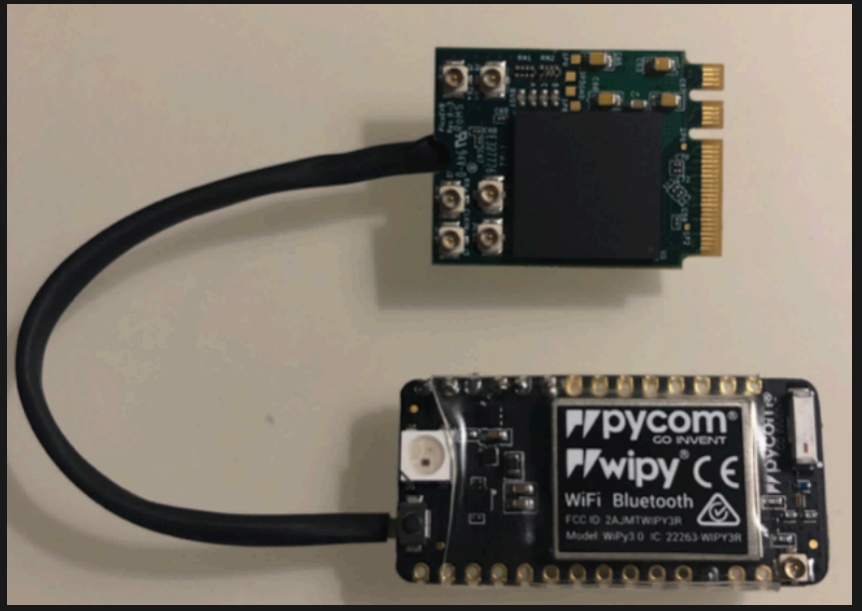
©2025 SecuringHardware.com

DRIVE-BY



©2025 SecuringHardware.com

EMBEDDED



©2025 SecuringHardware.com

Types of DMA Attacks

	Short Term	**Long Term**
Quick access/ hot plug	Drive By	Tethered
Internal access/ reboot	Tethered	Embedded

©2025 SecuringHardware.com

MULTITENANT THREAT MODEL

1. **What are we working on?**

2. **What can go wrong?**

3. **What are we going to do about it?**

4. **Did we do a good job?**

©2025 SecuringHardware.com

MULTITENANT THREAT MODEL

1. **What are we working on?**
   Make $ by sharing hardware
2. **What can go wrong?**

3. **What are we going to do about it?**

4. **Did we do a good job?**

©2025 SecuringHardware.com

MULTITENANT THREAT MODEL

1. **What are we working on?**
   Make $ by sharing hardware
2. **What can go wrong?**
   Hardware assisted tenant hopping
3. **What are we going to do about it?**

4. **Did we do a good job?**

©2025 SecuringHardware.com

MULTITENANT THREAT MODEL

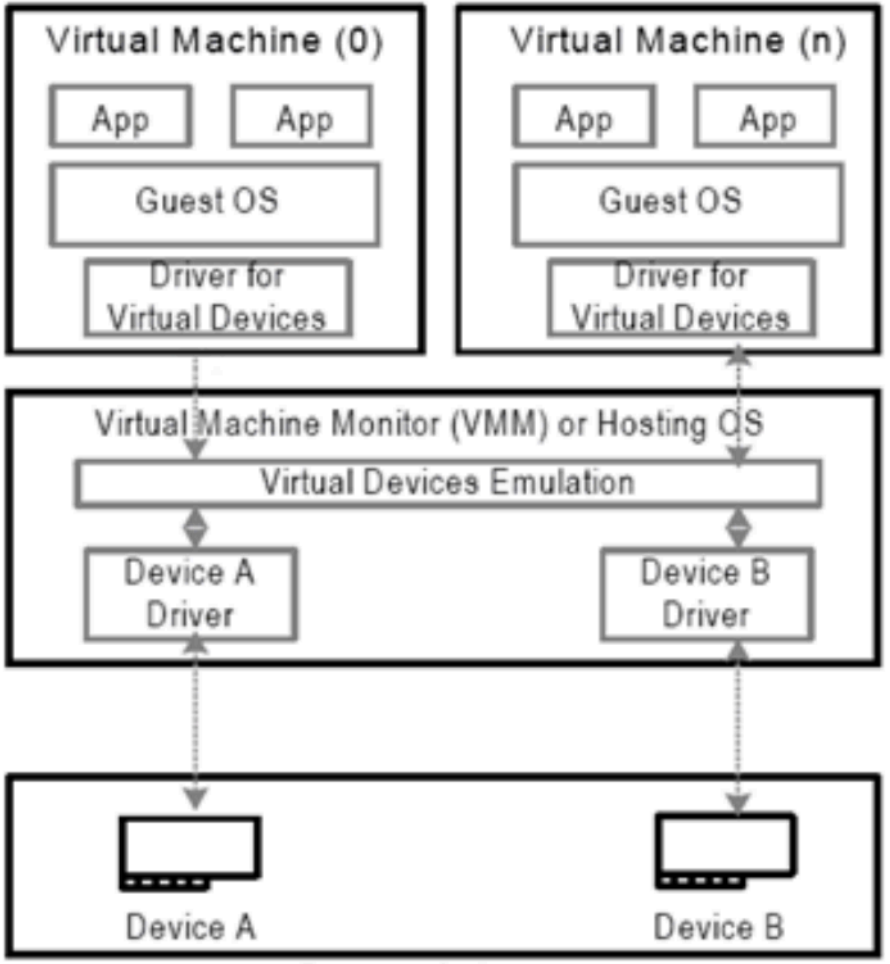
1. **What are we working on?**
   Make $ by sharing hardware
2. **What can go wrong?**
   Hardware assisted tenant hopping
3. **What are we going to do about it?**
   IOMMU!
4. **Did we do a good job?**

©2025 SecuringHardware.com

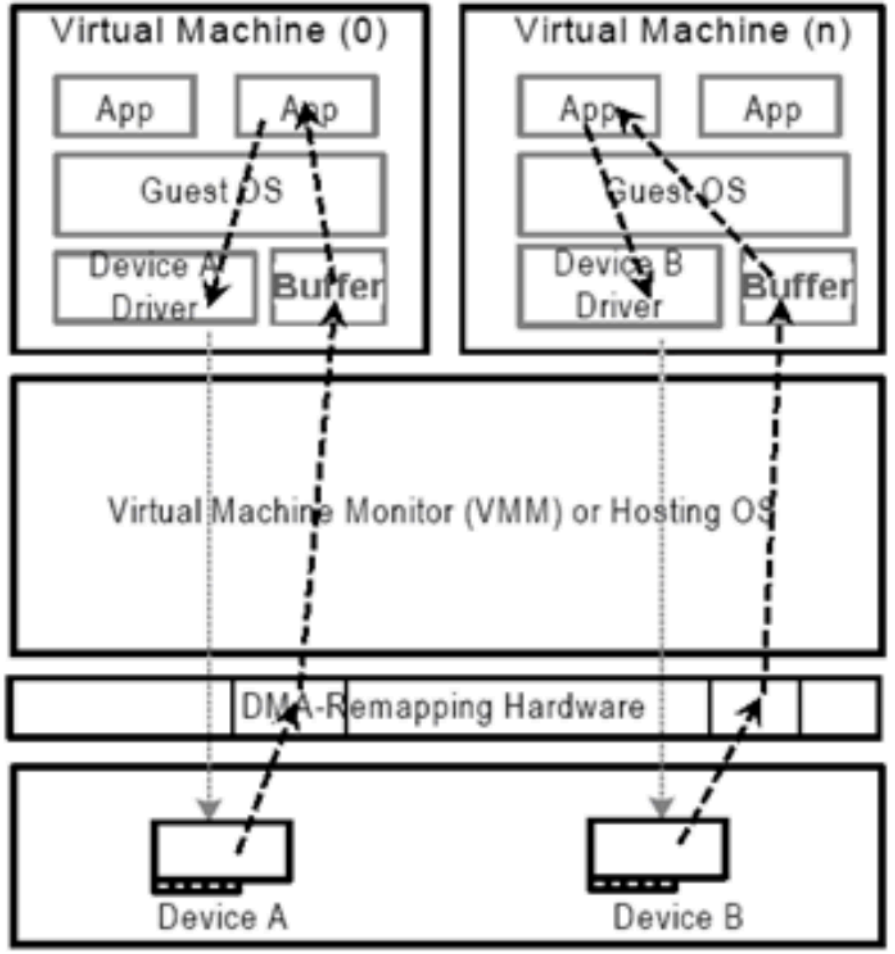
MULTITENANT THREAT MODEL

1. **What are we working on?**
   Make $ by sharing hardware
2. **What can go wrong?**
   Hardware assisted tenant hopping
3. **What are we going to do about it?**
   IOMMU!
4. **Did we do a good job?**
   Mostly?

©2025 SecuringHardware.com



Example Software-based I/O Virtualization



Direct Assignment of I/O Devices

©2008 Sec...ng Hardware Corp

KEY TAKEAWAY:

DMA MITIGATIONS EXIST

©2025 SecuringHardware.com

THUNDERBOLT THREAT MODEL

1. **What are we working on?**

2. **What can go wrong?**

3. **What are we going to do about it?**

4. **Did we do a good job?**

©2025 SecuringHardware.com

THUNDERBOLT THREAT MODEL

1. **What are we working on?**
   High speed peripherals
2. **What can go wrong?**

3. **What are we going to do about it?**

4. **Did we do a good job?**

©2025 SecuringHardware.com

THUNDERBOLT THREAT MODEL

1. **What are we working on?**
   High speed peripherals
2. **What can go wrong?**
   Malicious devices
3. **What are we going to do about it?**

4. **Did we do a good job?**

©2025 SecuringHardware.com

THUNDERBOLT THREAT MODEL

1. **What are we working on?**
   High speed peripherals
2. **What can go wrong?**
   Malicious devices
3. **What are we going to do about it?**
   Authenticate and Isolate devices
4. **Did we do a good job?**

©2025 SecuringHardware.com

THUNDERBOLT THREAT MODEL

1. **What are we working on?**
   High speed peripherals
2. **What can go wrong?**
   Malicious devices
3. **What are we going to do about it?**
   Authenticate and Isolate devices
4. **Did we do a good job?**
   In time… yes!

©2025 SecuringHardware.com

About those mitigations:

- Thunderbolt released
- OSX 10.8.2
- Windows 10 1802
- Linux 5.0

©2025 SecuringHardware.com

About those mitigations:

- Thunderbolt released *(2011)*
- OSX 10.8.2
- Windows 10 1802
- Linux 5.0

©2025 SecuringHardware.com

About those mitigations:

- Thunderbolt released *(2011)*
- OSX 10.8.2 *(2012, +1 year)*
- Windows 10 1802
- Linux 5.0

©2025 SecuringHardware.com

About those mitigations:

- Thunderbolt released *(2011)*
- OSX 10.8.2 *(2012, +1 year)*
- Windows 10 1802 *(2018, + 7 years)*
- Linux 5.0

©2025 SecuringHardware.com

About those mitigations:

- Thunderbolt released *(2011)*
- OSX 10.8.2 *(2012, +1 year)*
- Windows 10 1802 *(2018, + 7 years)*
- Linux 5.0 *(2019, + 8 years)*

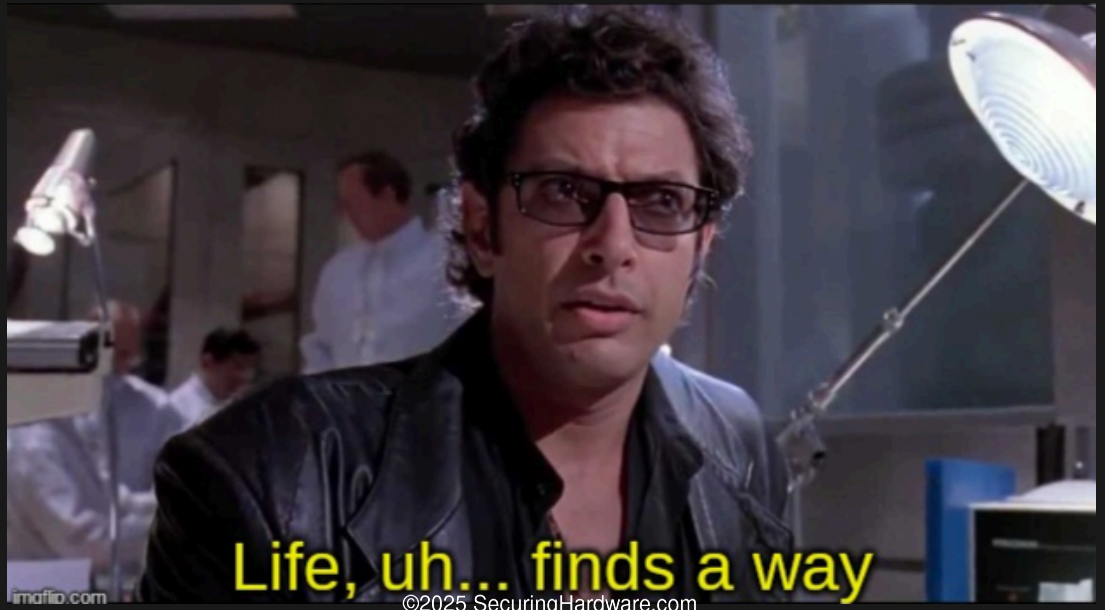
©2025 SecuringHardware.com

KEY TAKEAWAY:

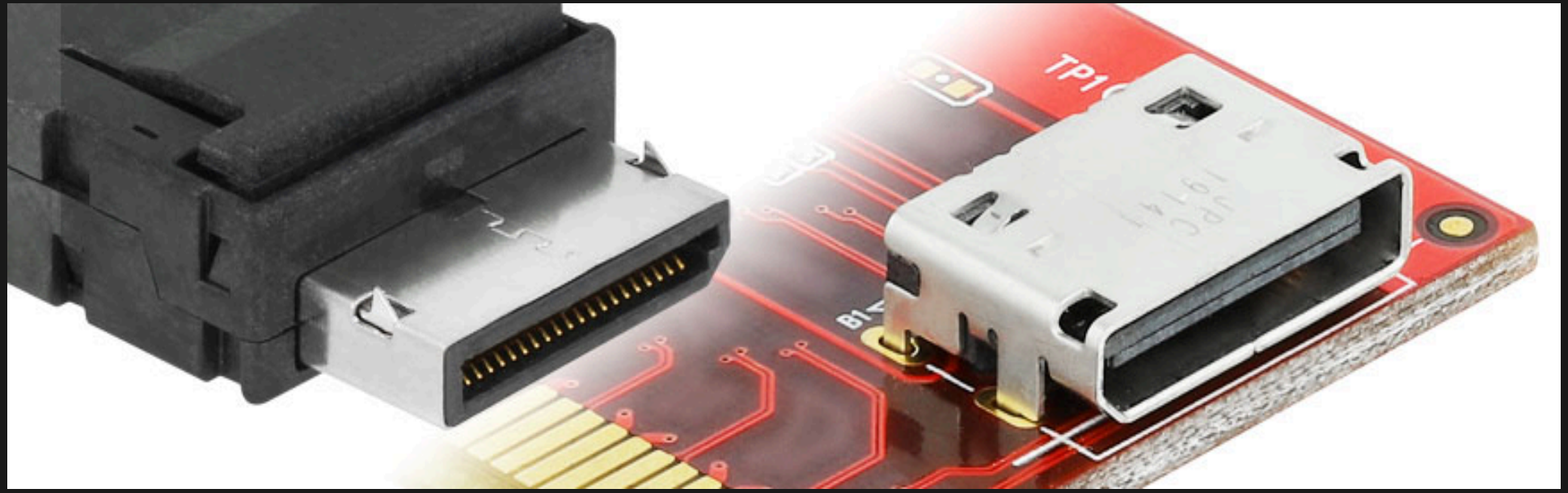
THUNDERBOLT GOT FIXED, EVENTUALLY

©2025 SecuringHardware.com

HOW ARE WE GONNA DO DRIVE-BY DMA ATTACKS WHEN THUNDERBOLT IS AT LEAST SOMEWHAT SECURED?



©2025 SecuringHardware.com



©2025 SecuringHardware.com



©2025 SecuringHardware.com

OCULINK THREAT MODEL

1. What are we working on?

2. What can go wrong?

3. What are we going to do about it?

4. Did we do a good job?

©2025 SecuringHardware.com

OCULINK THREAT MODEL

1. **What are we working on?**
   High speed peripherals
2. **What can go wrong?**

3. **What are we going to do about it?**

4. **Did we do a good job?**

©2025 SecuringHardware.com

OCULINK THREAT MODEL

1. **What are we working on?**
   High speed peripherals
2. **What can go wrong?**
   Malicious devices
3. **What are we going to do about it?**

4. **Did we do a good job?**

©2025 SecuringHardware.com

OCULINK THREAT MODEL

1. **What are we working on?**
   High speed peripherals
2. **What can go wrong?**
   Malicious devices
3. **What are we going to do about it?**
   Only use it in secured locations?
4. **Did we do a good job?**

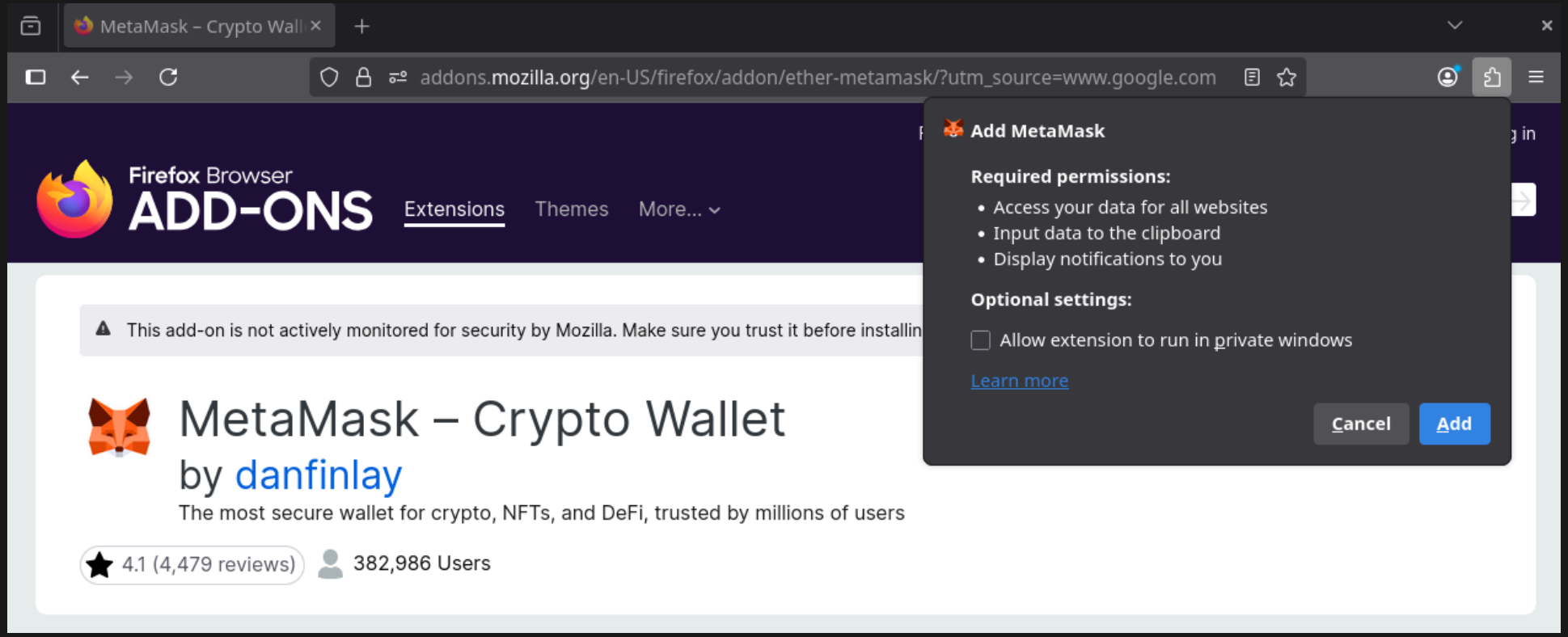
©2025 SecuringHardware.com

OCULINK THREAT MODEL

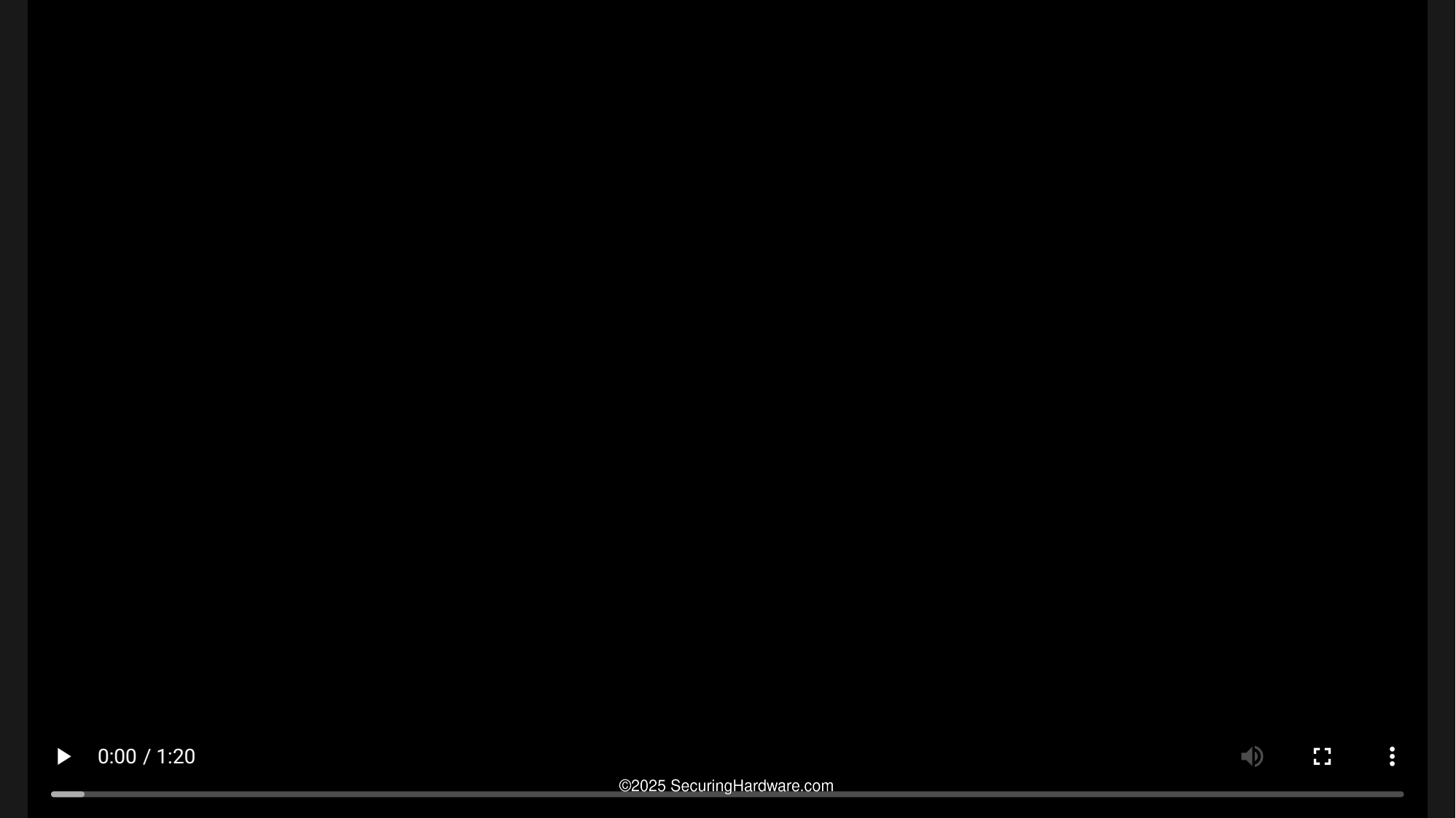
1. **What are we working on?**
   High speed peripherals
2. **What can go wrong?**
   Malicious devices
3. **What are we going to do about it?**
   Only use it in secured locations?
4. **Did we do a good job?**
   Not really.

©2025 SecuringHardware.com

Example: Metamask



©2025 SecuringHardware.com


0:00 / 1:20
©2025 SecuringHardware.com

©2025 SecuringHardware.com

https://github.com/pierce403/PASIV

Preview | Code | Blame | 102 lines (74 loc) · 4.87 KB | Raw

PASIV: Peripheral Attack Simulation and Introspection Vehicle

PASIV is a comprehensive test harness for emulating, executing, and analyzing Direct Memory Access (DMA) attacks within a controlled QEMU/KVM environment. This framework aims to provide researchers and security professionals with a powerful, scriptable, and repeatable platform for studying DMA vulnerabilities and defenses.



Project Goals

- Automate the setup of vulnerable and hardened virtual machine targets.
- Integrate with leading memory forensics tools like PCILeech, memflow, and MemProcFS.
- Provide a modular framework for developing and executing custom DMA attack payloads.
- Enable the study and verification of IOMMU-based defenses.
- Serve as a research platform for advanced DMA attack and defense techniques.

©2025 SecuringHardware.com

DMA GAMING CHEATS

Now, the attacker is the owner.

This changes the threat model!

This is currently an arms race!

©2025 SecuringHardware.com

DMA cheat for Faceit CS2

Only cheat



$30

- ✔ CS2 cheat for 1 month ⓘ

* you should have DMA Card with Firmware to use this cheat

Buy now

Basic package



$720

- ✔ CS2 cheat for 1 month ⓘ
- ✔ DMA PCIe Card 75T ⓘ
- ✔ Firmware for Faceit

* with this package you will be able to use only radar hack on second PC

Out of stock

Full package



$930

- ✔ CS2 cheat for 1 month ⓘ
- ✔ DMA PCIe Card 75T ⓘ
- ✔ Firmware for Faceit
- ✔ Makcu for Aimbot ⓘ
- ✔ DP Fuser for ESP on monitor ⓘ

Out of stock

©2025 SecuringHardware.com

Pcileech-DMA-NVMe-VMD / README.md

Ptolemaios9 Update README.md 97e9651 · 5 days ago History

Preview Code Blame 21 lines (15 loc) · 1.57 KB Raw

Pcileech-DMA-NVMe-VMD

🤬**Many firmware scammers sell Beaters free and open source VMD firmware at high prices.**

How to get help

discord：https://discord.gg/beater

🔥Beaters DC channel offers free firmware (Many scammers firmware distributors are angry because Beater has made VMD firmware available for free，Try to discredit Beater by claiming that the free firmware is unsafe so that users can buy their paid Poor quality firmware.),BeaterFreeVMD play the games you want to play!VGK has implemented VMD detection not long ago, and EAC BE still runs well. Beater Never tried to sell VMD firmware solutions for profit.

Requirements↓

- Intel CPU (11th Generation or newer) in the main PC where the DMA card is installed.
- Intel VMD (Virtual RAID on CPU) must be enabled in BIOS.
- Specific Intel drivers must be installed on Windows.
- A Windows reinstall may be required for proper driver initialization and device recognition.

⚠VMD firmware solution has been discovered by game developers, but it is still safe， It has been free and open source from the beginning.

©2025 SecuringHardware.com

Hardware based memory aqusition methods:

Please find a summary of the supported hardware based memory acquisition methods listed below. All hardware based memory acquisition methods are supported on both Windows and Linux. The FPGA based methods however sports a slight performance penalty on Linux and will max out at approx: 90MB/s compared to 150MB/s on Windows.

Device	Type	Interface	Speed	64-bit memory access	PCIe TLP access	Project Sponsor
Screamer PCIe Squirrel	FPGA	USB-C	190MB/s	Yes	Yes	💖
ZDMA	FPGA	Thunderbolt3	1000MB/s	Yes	Yes	💖
LeetDMA	FPGA	USB-C	190MB/s	Yes	Yes	💖
AC701/FT601	FPGA	USB3	190MB/s	Yes	Yes	
USB3380-EVB	USB3380	USB3	150MB/s	No	No	
DMA patched HP iLO	BMC	TCP	1MB/s	Yes	No	

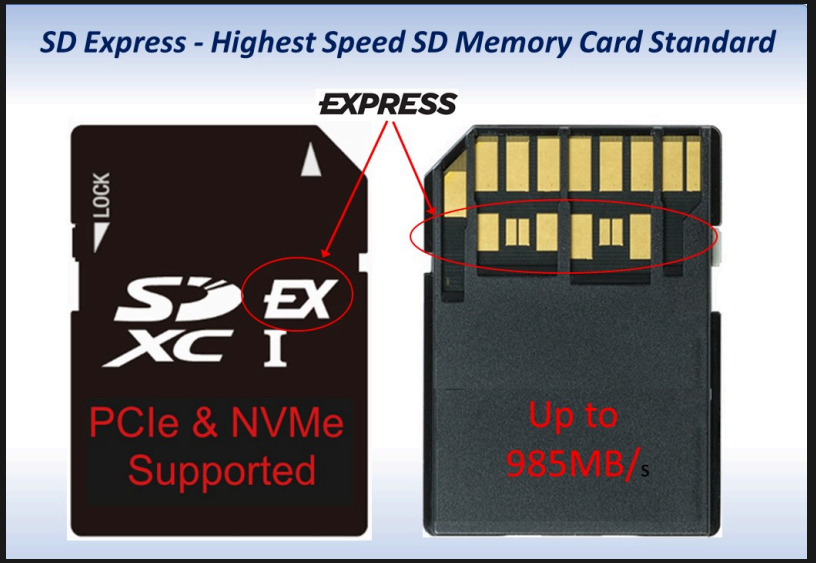
©2025 SecuringHardware.com

KEY TAKEAWAY:
CHANGING FORM FACTOR
=
CHANGING THREAT MODEL

©2025 SecuringHardware.com



CF Express



SD Express

©2025 SecuringHardware.com

CFE/SDE THREAT MODEL

1. **What are we working on?**

2. **What can go wrong?**

3. **What are we going to do about it?**

4. **Did we do a good job?**

©2025 SecuringHardware.com

CFE/SDE THREAT MODEL

1. **What are we working on?**
   High speed small storage
2. **What can go wrong?**

3. **What are we going to do about it?**

4. **Did we do a good job?**

©2025 SecuringHardware.com

CFE/SDE THREAT MODEL

1. **What are we working on?**
   High speed small storage
2. **What can go wrong?**
   Malicious devices? Counterfeit devices?
3. **What are we going to do about it?**

4. **Did we do a good job?**

©2025 SecuringHardware.com

CFE/SDE THREAT MODEL

1. **What are we working on?**
   High speed small storage
2. **What can go wrong?**
   Malicious devices? Counterfeit devices?
3. **What are we going to do about it?**
   ???
4. **Did we do a good job?**

©2025 SecuringHardware.com

CFE/SDE THREAT MODEL

1. **What are we working on?**
   High speed small storage
2. **What can go wrong?**
   Malicious devices? Counterfeit devices?
3. **What are we going to do about it?**
   ???
4. **Did we do a good job?**
   ???

©2025 SecuringHardware.com







©2025 SecuringHardware.com

EXAMPLE: CFEXPRESS ATTACK



©2025 SecuringHardware.com

EXAMPLE: CFEXPRESS ATTACK



©2025 SecuringHardware.com

EXAMPLE: CFEXPRESS ATTACK



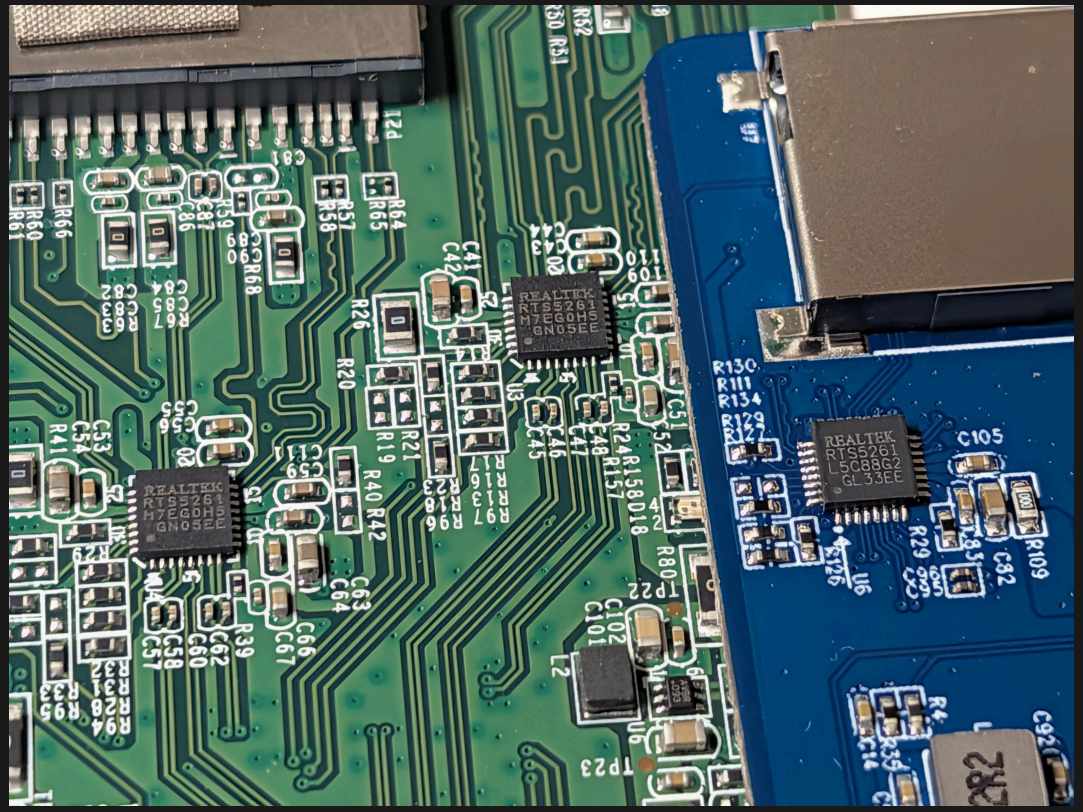
©2025 SecuringHardware.com

SWITCH 2 SDEXPRESS PROGRESS



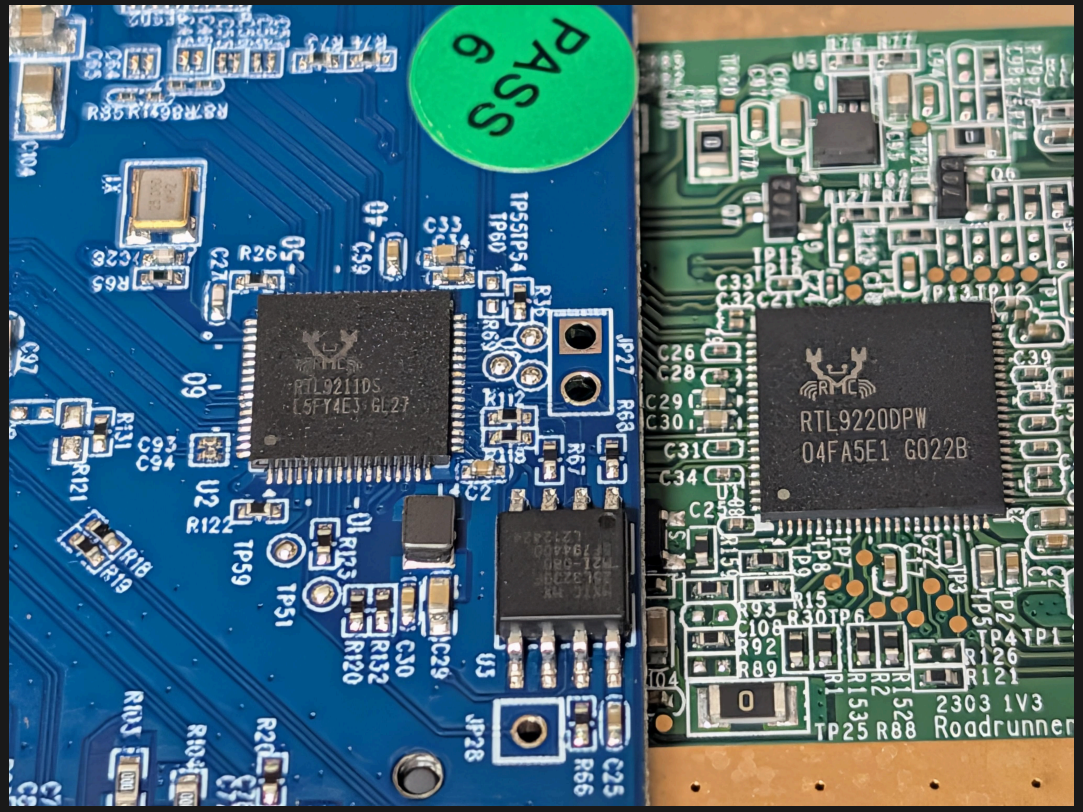
©2025 SecuringHardware.com

SDExpress Progress



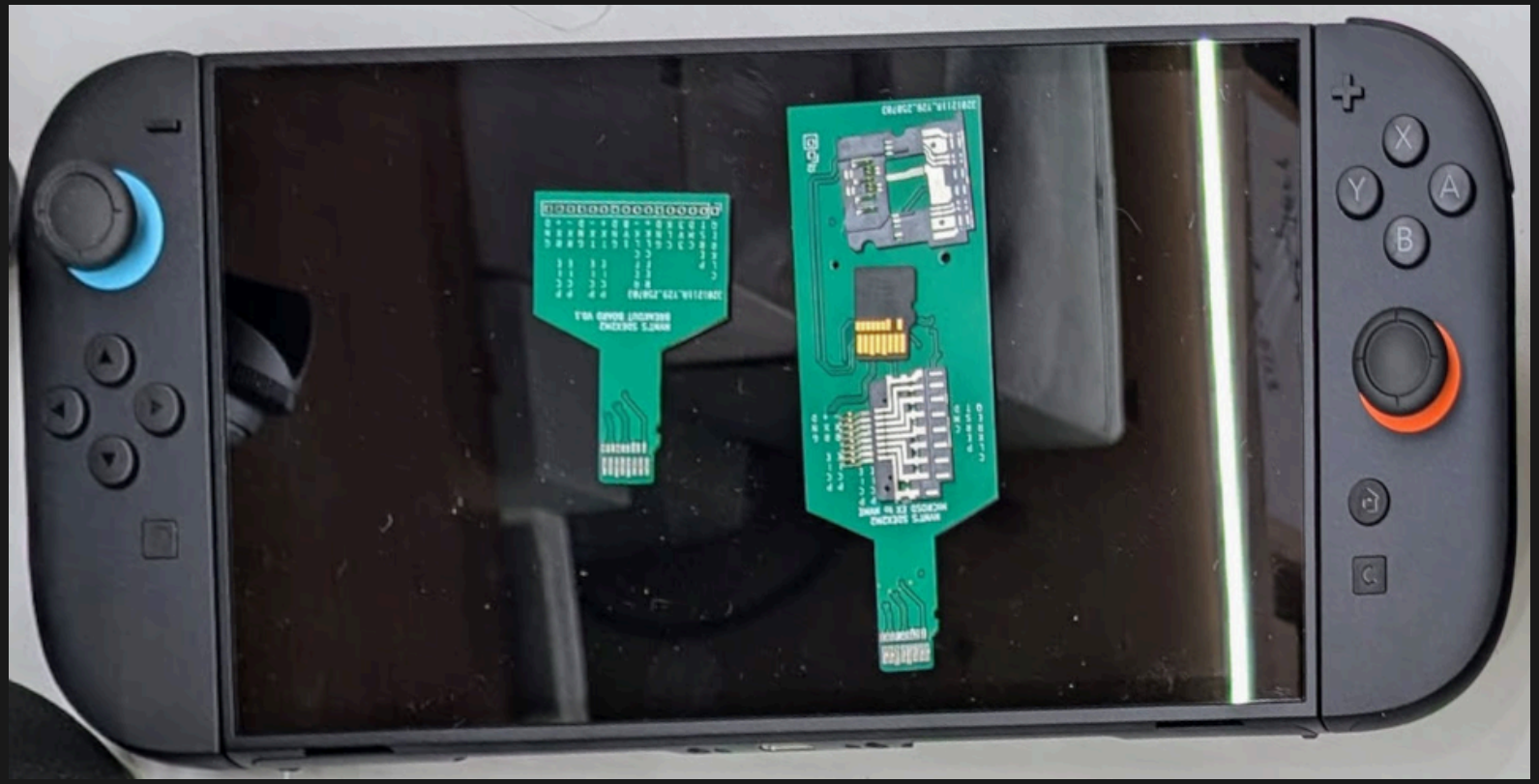
©2025 SecuringHardware.com

SDExpress Progress



©2025 SecuringHardware.com

Who wants to see a switch 2 jailbreak?



©2025 SecuringHardware.com

KEY TAKEAWAY:

PCIE IS PERVASIVE!

©2025 SecuringHardware.com

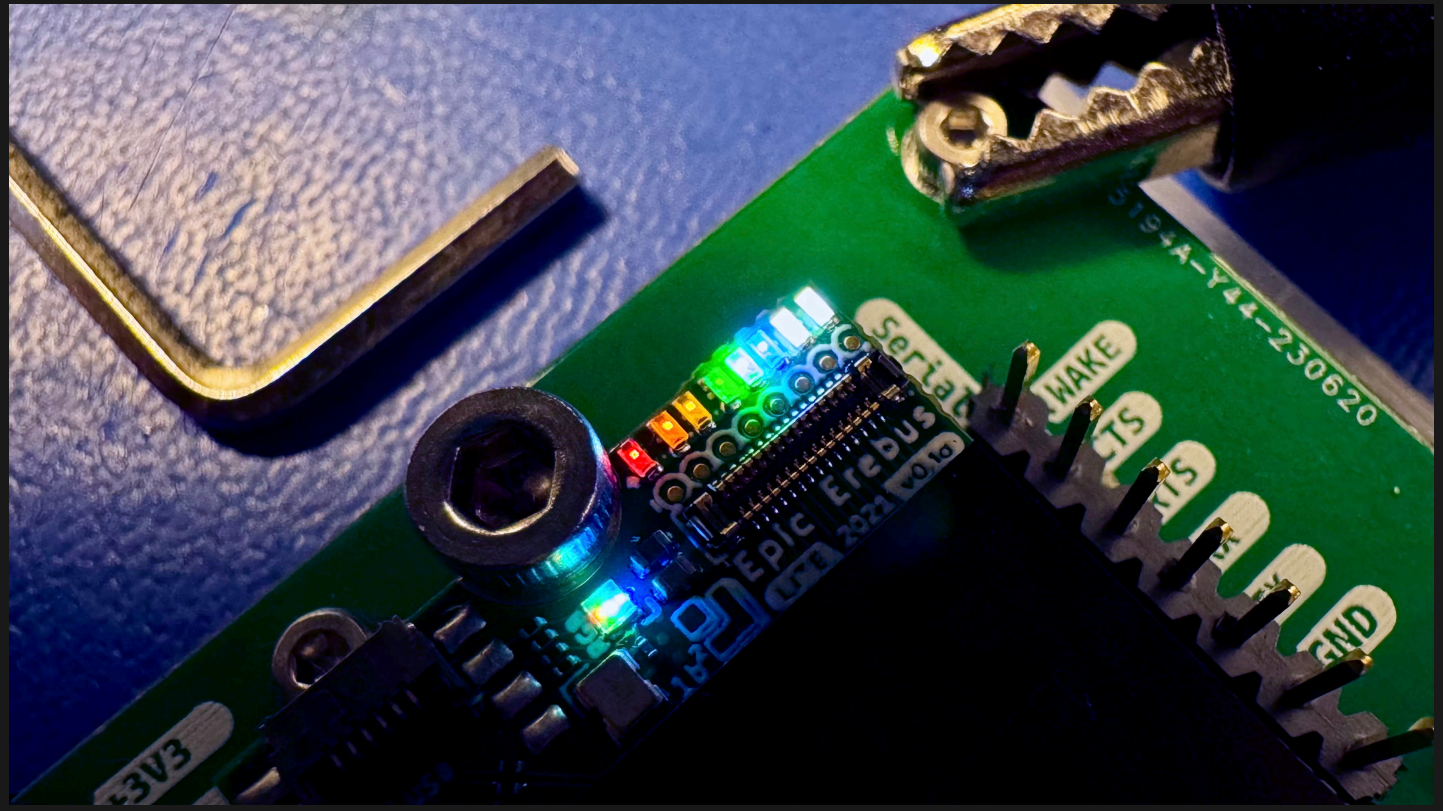
A CONTINUING TALE OF EPIC PROCRASTINATION:

- 2021: Erebus Schematic
- 2022: Erebus PCBs
- 2023: Erebus Test Jig
- 2024: Erebus Assembled
- 2025: Profit?

©2025 SecuringHardware.com



©2025 SecuringHardware.com



©2025 SecuringHardware.com

Other Notes:

The completed solution contains Xilinx proprietary IP cores licensed under the Xilinx CORE LICENSE AGREEMENT. This project as-is published on Github contains no Xilinx proprietary IP. Published source code are licensed under the MIT License. The end user that have downloaded the no-charge Vivado WebPACK from Xilinx will have the proper licenses and will be able to re-generate Xilinx proprietary IP cores by running the build detailed above.

©2025 SecuringHardware.com

Projects Launched



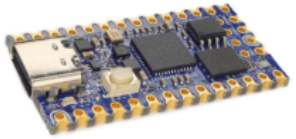
EPIC Erebus

A tiny PCIe DMA tool that's fully customizable with an open toolchain and gateware

Coming Soon

Sign up

Subscribe for project updates.



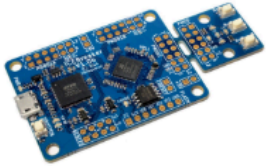
iCEBreaker-bitsy FPGA

An open source iCE40 FPGA dev board in a Teensy form factor

Coming Soon

Sign up

Subscribe for project updates.

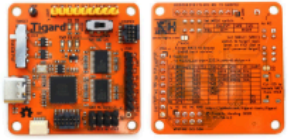


iCEBreaker FPGA

An open source iCE40 FPGA development board designed for teachers and students

992% Funded! **In Stock**

$148,949	14	1,131
raised	updates	backers



Tigard

An open source FT2232H-based, multi-protocol, multi-voltage tool for hardware hacking

Funded! **In Stock**

$145,610	14	1,480
raised	updates	backers



Glasgow Interface Explorer

A highly capable and extremely flexible open source multitool for digital electronics

1,720% Funded! **In Stock**

$430,222	14	2,212
raised	updates	backers

WHY EREBUS?

Platform Security

©2025 SecuringHardware.com



©2025 SecuringHardware.com

KEY TAKEAWAYS:

- PCIe is permissive by design
- DMA Mitigations exist
- Thunderbolt got fixed, eventually
- Form factor changes your threat model
- PCIe is Pervasive!

Progress has been made -

but there's still way more to do!

©2025 SecuringHardware.com

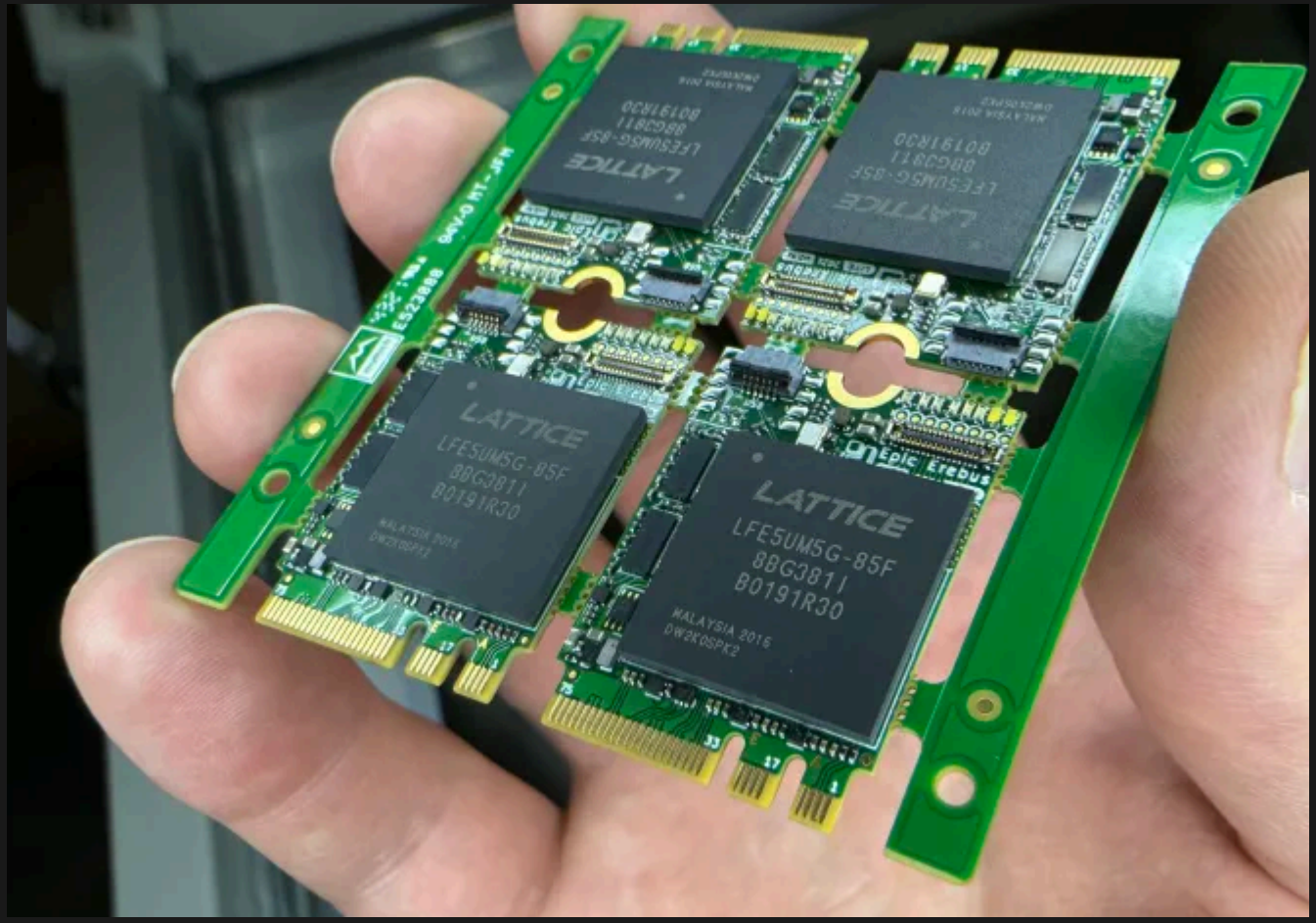
4 QUESTION THREAT MODEL:

1. **What are we working on?**
2. **What can go wrong?**
3. **What are we going to do about it?**
4. **Did we do a good job?**

©2025 SecuringHardware.com



©2025 SecuringHardware.com



©2025 SecuringHardware.com

THANKS

Prior Art/Inspriation:

- Kingpin
- Metlstorm
- Snare
- Carmaa
- Ufrisk
- Mossman

Support/tooling

- Esden
- Aki-Nyan
- Dragonmux
- Whitequark
- Gaya Tech
- Dean Pierce

And many more...

©2025 SecuringHardware.com

DIRECT MEMORY ACCESS EVERYWHERE

Presentation:

github.com/securelyfitz/DirectMemoryAccessEverywhere

Erebus Design:

github.com/epic-erebus

CrowdSupply:

crowdsupply.com/securinghw/erebus

©2025 SecuringHardware.com



DIRECT MEMORY ACCESS EVERYWHERE

securelyfitz & baelfire 9 AUG 2025

©2025 SecuringHardware.com

©2025 Secure Software GmbH