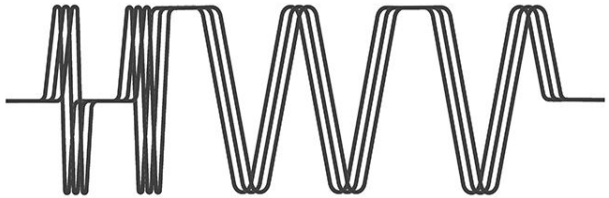


Introduction to PCI Express and DMA attacks

Andrey Konovalov <andreyknvl@gmail.com>

PHDays 2019, Hack Zone
May 22nd 2019

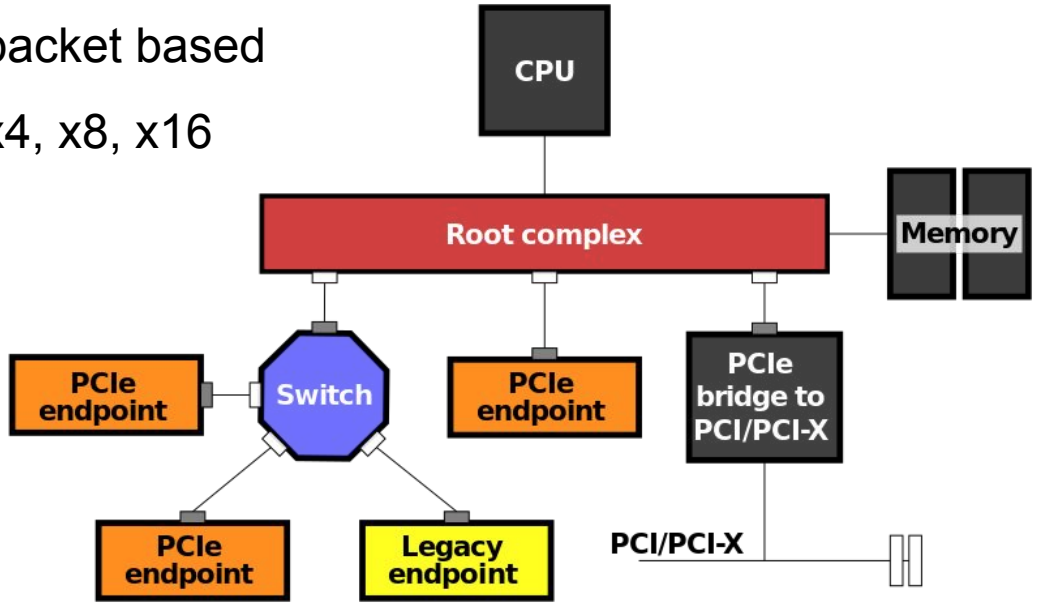
Agenda

- Part 1: PCIe 101
- Part 2: Hardware for DMA Attacks
- Part 3: Attacking Linux
- Part 4: Attacking Windows
- Part 5: Attacking MacOS

Part 1: PCIe 101

PCI Express

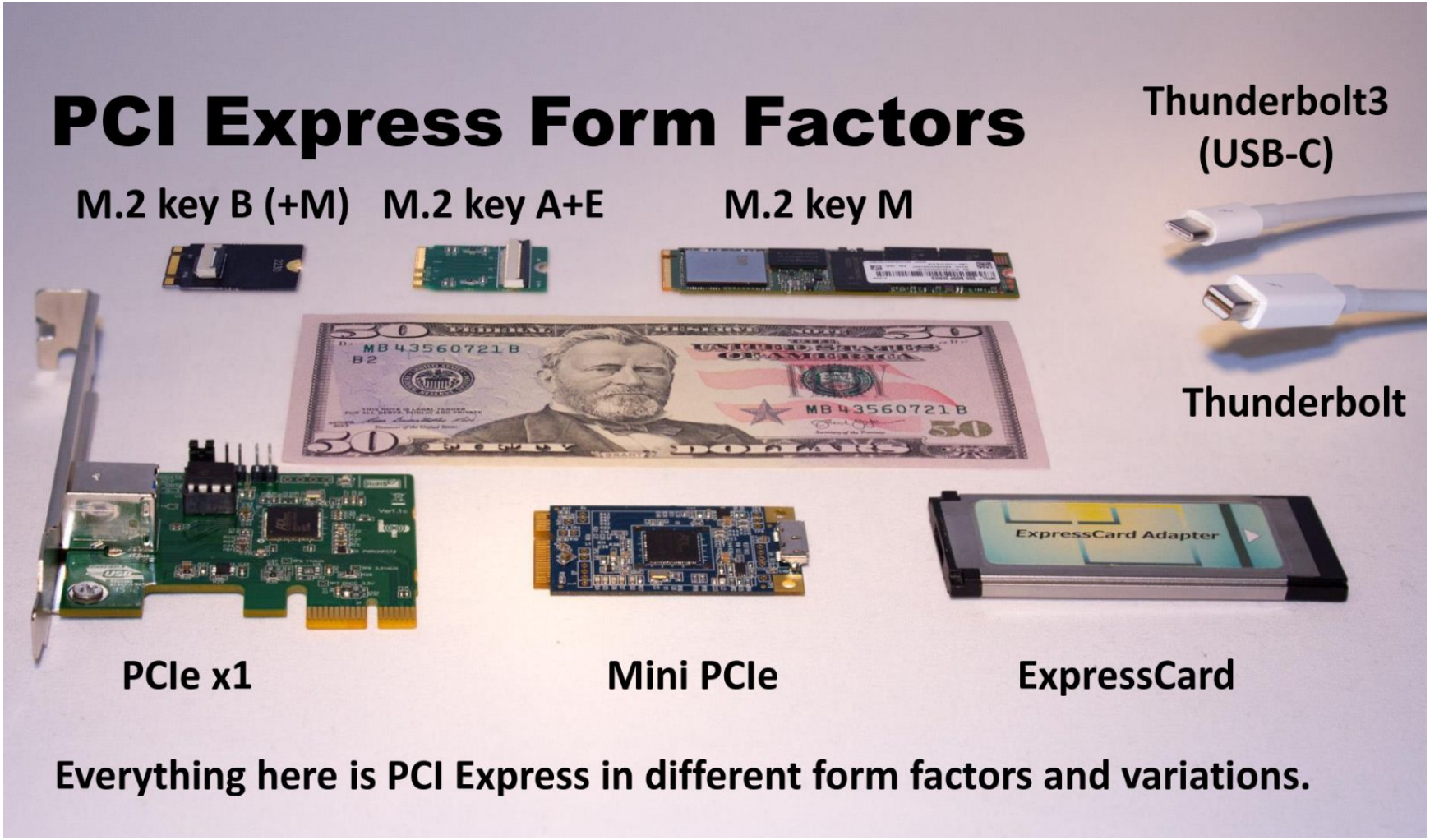
- PCIe is a high-speed serial expansion bus
- Point-to-point communication, packet based
- From 1 to 16 serial lanes - x1, x4, x8, x16
- Hot pluggable (sometimes)
- DMA capable



https://en.wikipedia.org/wiki/PCI_Express

https://github.com/ufrisk/presentations/blob/master/SEC-T-0x0Anniversary-Ulf-Frisk-Evil-Devices-and-Direct-Memory-Attacks.pdf

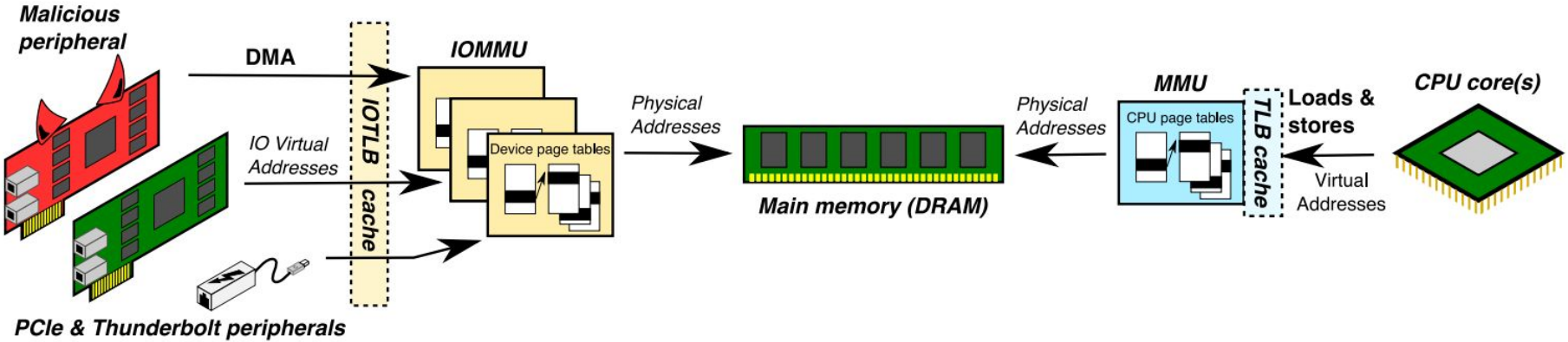
PCI Express Form Factors



Everything here is PCI Express in different form factors and variations.

Input-Output Memory Management Unit

- IOMMU limits access by DMA-enabled peripherals to system memory
- Physical address space is virtualized to produce a number of I/O virtual address (IOVA) spaces (per device or per group of devices)

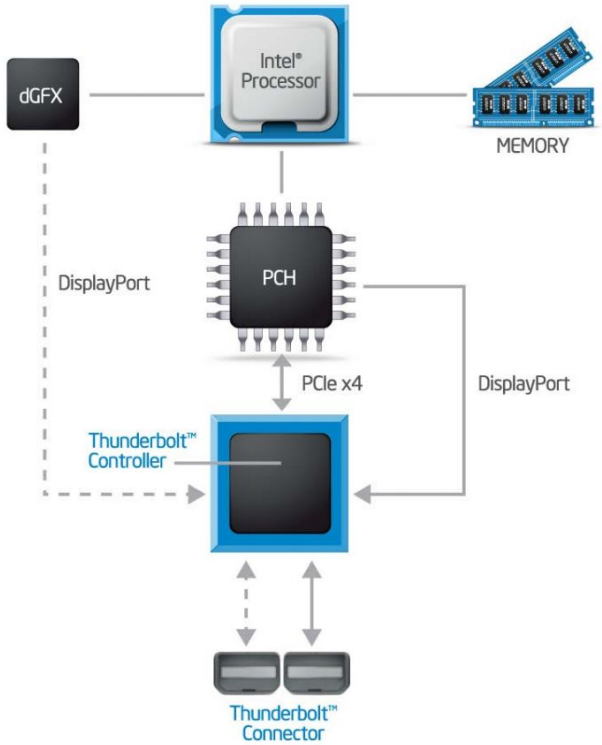


http://thunderclap.io/thunderclap-paper-ndss2019.pdf

Thunderbolt

- Tunnels PCIe and DisplayPort over USB Type-C or mini DisplayPort connectors
- Hot pluggable
- Security policies (selected via a BIOS option)

- SL 0: No limitations (2011+)
- SL 1: Ask for permission to connect device (2013+)
- SL 2: HW cryptographic authentication (2014+)
- SL 3: DisplayPort only (2013+)



DMA Attacks Applications

- Evil maid (physical access to locked laptop/desktop/server machines)
- Research (reverse engineering of proprietary hardware with secure boot)
  - iPhone NVMe NAND reverse engineering by Oleg Kupreev and Vladimir Putin [1], [2]
  - Breaking UEFI security with software DMA attacks by Dmytro Oleksiuk aka Cr4sh
- Attacking hosts via compromised PCIe devices
  - Over The Air: Exploiting Broadcom's Wi-Fi Stack Gal Beniamini

Part 2: Hardware for DMA Attacks

History of DMA Attacks

- 2011: Attack over FireWire with Inception
- 2015: Attack over PCIe with SLOTSCREAMER on USB3380 by Joe FitzPatrick and Miles Crabil
- 2016: Attack over PCIe with pcileech on USB3380 by Ulf Frisk
- 2017: Attack over PCIe with a custom toolkit for Xilinx SP605 FPGA board by Dmytro Oleksiuk aka Cr4sh (now supported by pcileech as well)
- 2019: Attack targeting kernel drivers over PCIe with Intel Arria 10 SoC board aka Thunderclap

Base Hardware

USB3380 Boards

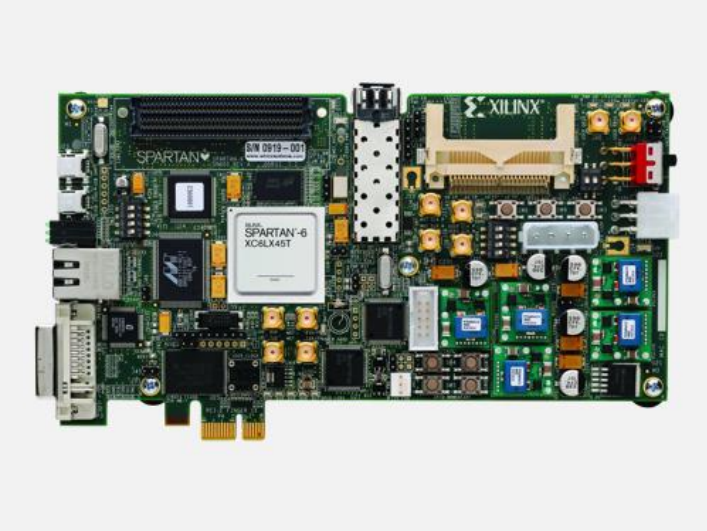
- USB3380EVB (156$) and PP3380-AB (208$), but End-Of-Life
- 150 MB/s, 32-bit access only (64-bit with code injection), no TLP access

http://www.bplus.com.tw/Adapter/USB3380EVB.html

http://www.bplus.com.tw/Adapter/PP3380-AB.html

Xilinx FPGA Boards

- Xilinx SP605 ($650) and Xilinx AC701 ($1295)
- 75 and 150 MB/s, 64-bit access, TLP access

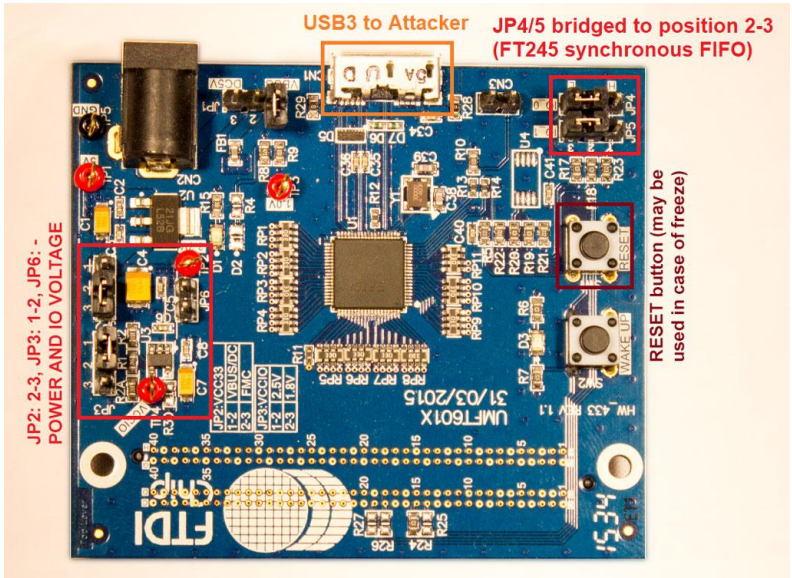


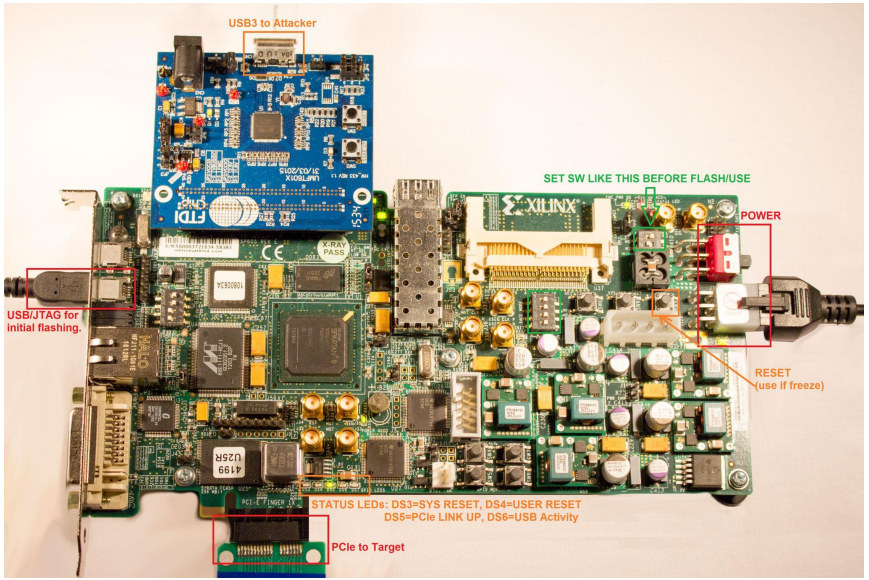
https://www.xilinx.com/products/boards-and-kits/ek-s6-sp605-g.html

https://www.xilinx.com/products/boards-and-kits/ek-a7-ac701-g.html

Xilinx FPGA Boards

- Both boards also require [FTDI UMFT601X-B](#) (77$)

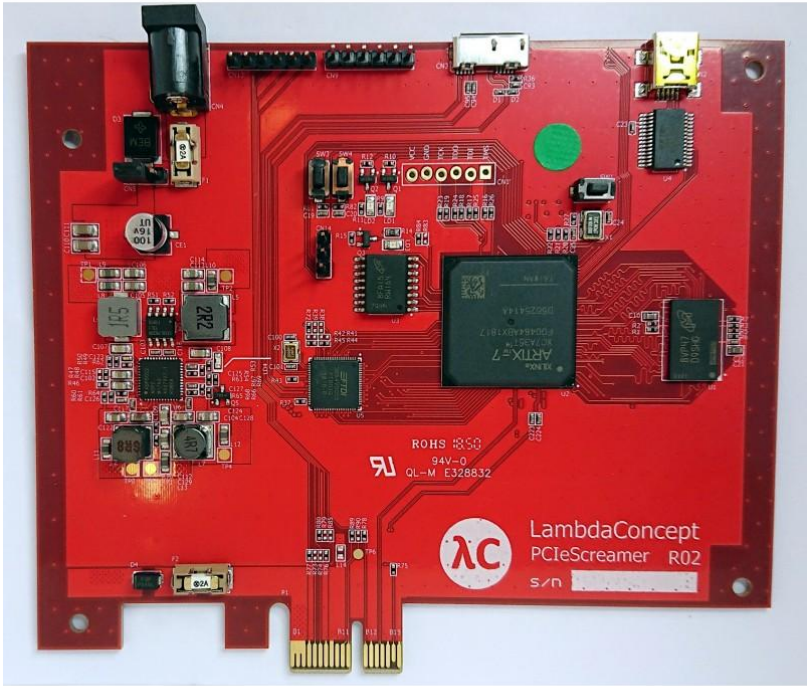




https://github.com/ufrisk/pcileech-fpga/tree/master/sp605_ft601

PCIe Screamer (R02)

- PCIe Screamer (R02) (300$)
- 100 MB/s, 64-bit access, TLP access
- R01 was extremely unstable



http://shop.lambdaconcept.com/home/32-pciescreamerR02.html

Comparison

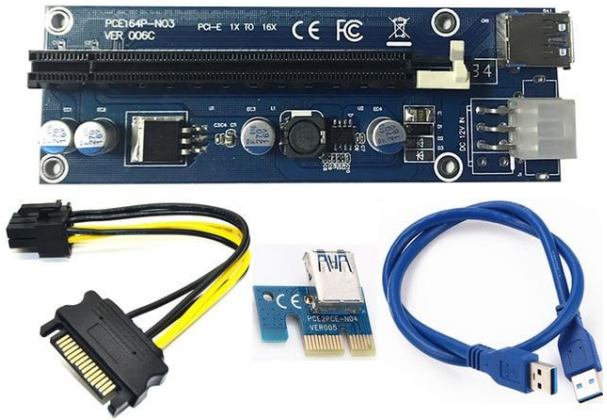
Device	Type	Interface	Speed	64-bit memory access	PCIe TLP access	
AC701/FT601	FPGA	USB3	150MB/s	Yes	Yes	1372 $
PCIeScreamer	FPGA	USB3	100MB/s	Yes	Yes	300 $
SP605/FT601	FPGA	USB3	75MB/s	Yes	Yes	727 $
SP605/TCP	FPGA	TCP/IP	100kB/s	Yes	Yes	
USB3380-EVB	USB3380	USB3	150MB/s	No	No	(156 $)
PP3380	USB3380	USB3	150MB/s	No	No	(208 $)
DMA patched HP iLO	TCP/IP	TCP	1MB/s	Yes	No	

https://github.com/ufrisk/pcileech

Risers and Adapters

Cheap PCIe Risers

- Unnamed PCIe => PCIe (7$)
- Unnamed Mini PCIe => PCIe (7$)



https://www.aliexpress.com/item/PCI-E-PCI-E-Express-1X-to-16X-Riser-Card-USB-3-0-Extender-Cable-SATA/32793338698.html

https://www.aliexpress.com/item/USB-3-0-Mini-PCI-E-to-PCI-E-PCI-Express-1X-to-16X-Extender-Riser/32815761203.html

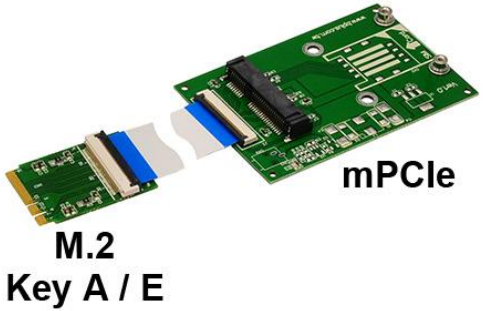
EXP GDC Beast Video Card Dock

- EXP GDC Beast Video Card Dock (36$): ExpressCard/34 => PCIe
  - + Mini PCIe Cable for EXP GDC Beast (17$): Mini PCIe => PCIe
  - + M.2 A Key Cable for EXP GDC Beast (29$): M.2 Key A+E => PCIe

https://www.aliexpress.com/item/Express-Card-Mini-PCI-E-Version-Expresscard-V8-0-EXP-GDC-Beast-PCIe-PCI-E-PCI/32845629718.html

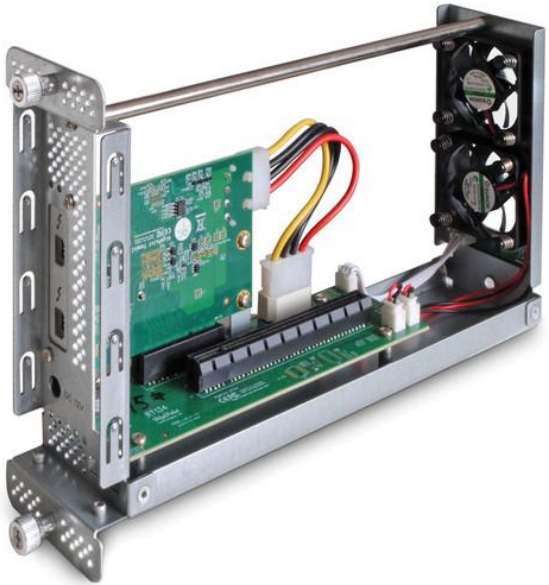
Bplus PCIe Risers

- PE3B (130$): ExpressCard => mini-PCIe
- PE3A (100$): ExpressCard => PCIe
- ADP (50$): PCIe => mini-PCIe
- P15S-P15F (60$): M.2 Key A+E => mini-PCIe



Thunderbolt 2/3 Graphics Card Docks

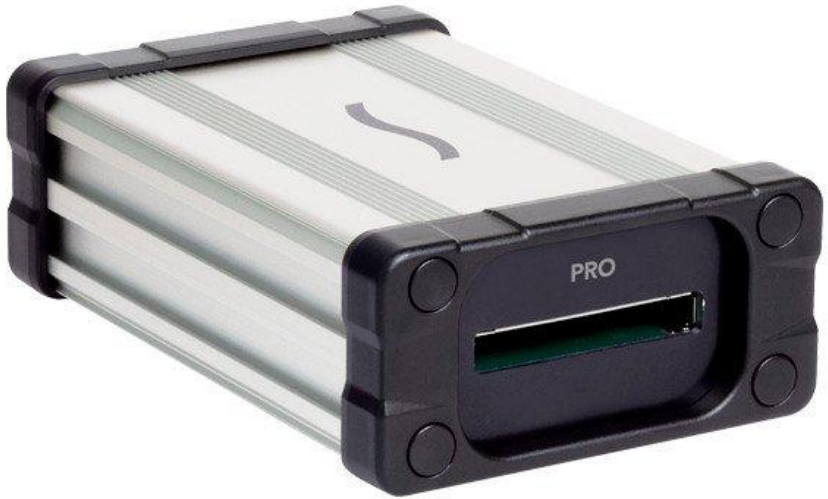
- HighPoint RocketStor 6361A ($340): Thunderbolt 2 => PCIe
- And many others



https://www.techinferno.com/index.php?/forums/topic/7527-us233-highpoint-rocketstor-6361a-pcie-chassis-16gbps-tb2/

Sonnet Echo ExpressCard Pro

- Sonnet Echo ExpressCard Pro (170$): Thunderbolt 2 => ExpressCard/34



https://www.bpm-media.de/produkte/post-it/zubehoer/adapter/sonnet-echo-expresscard/34-thunderbolt-adapter/

Apple T3 to T2 Adapter

- Apple T3 to T2 Adapter (61$): Thunderbolt 3 => Thunderbolt 2

https://www.apple.com/de/shop/product/MMEL2ZM/A/thunderbolt-3-usb%E2%80%91c-auf-thunderbolt-2-adapter

Part 3: Attacking Linux

DMA on Linux

- IOMMU supported, but not enabled by default in Ubuntu/Fedora/RHEL
- Thunderbolt access control supported in UEFI firmware, but not in the kernel
- Usual default mode is SL 1 (ask for permission), but no user prompt
- More details in the Thunderclap paper

Demo: Leaking User Password from gnome-keyring-daemon on Linux via ExpressCard

Part 4: Attacking Windows

DMA on Windows

- Windows 7, 8.1 and 10 Home/Pro (on older hardware) don't use IOMMU
- Windows 10 (on hardware shipped with version 1803+) enables IOMMU for Thunderbolt devices only
- Windows 10 Enterprise uses IOMMU for the optional "Virtualization-Based Security" (VBS) feature to protect the hypervisor and containers only
- Thunderbolt access control supported in UEFI firmware and in the kernel
- Usual default mode is SL 1 (ask for permission to connect device)
- More details in the Thunderclap paper

Demo: Unlocking Windows via ExpressCard

Part 5: Attacking MacOS

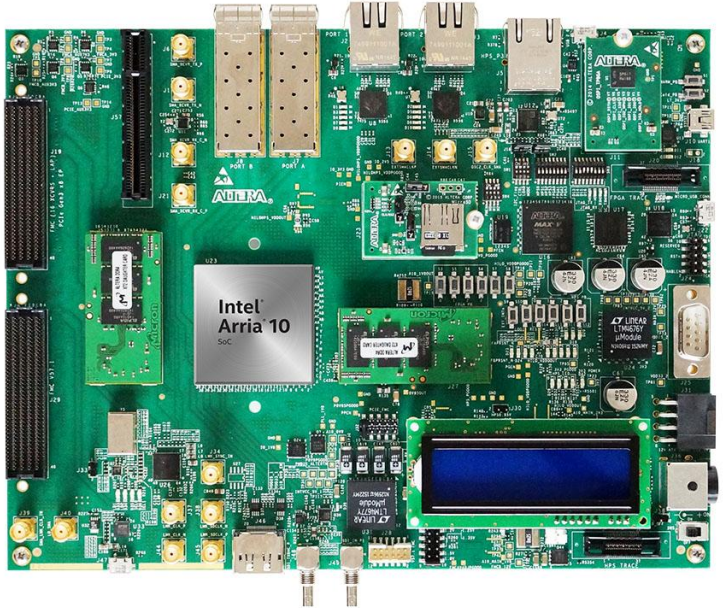
DMA on MacOS

- Supports IOMMU, but uses shared mappings (a single IOMMU page map that is shared among all devices)
- Memory that is exposed to one device is exposed to all
- Every device has full visibility of network traffic continuously
- Whitelisting for Thunderbolt, many Thunderbolt to PCIe bridges are whitelisted
- More details in the Thunderclap paper

Demo: Leaking Cookies from MacBook Pro 2015 via Thunderbolt

Thunderclap

- Reproduced and documented most of the already known results
- Something new: attacking the kernel over PCIe with IOMMU enabled
- Intel Arria 10 SoC Development Kit (4495 $)
- More details in the Thunderclap paper
- thunderclap.io



Thanks!
Questions?

https://github.com/xairy/hardware-village/tree/master/dma

Andrey Konovalov <andreyknvl@gmail.com>