IOSEC: Protection and Memory Safety for Input/Output Security

A. Theodore Markettos, Robert N. M. Watson, and Simon W. Moore

University of Cambridge

Department of Computer Science and Technology

RISE Annual Conference, London, 14 November 2018

Protection and Memory Safety for Input/Output Security

Thunderbolt 2

Thunderbolt 3 over USB-C

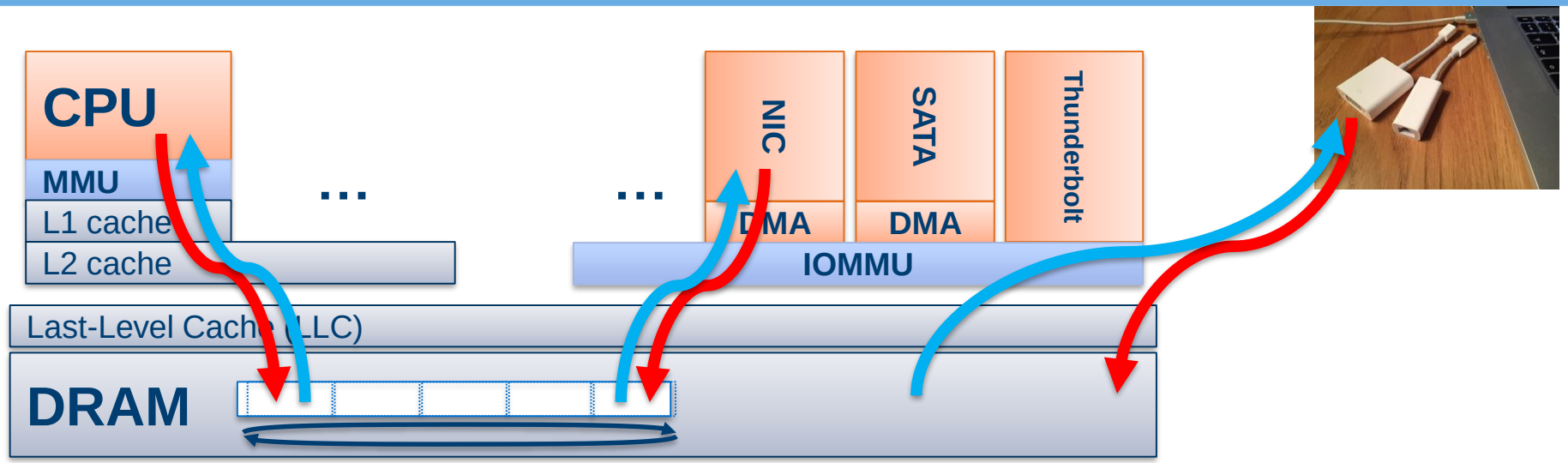
- Modern systems are composed of all kinds of processors; some of them aren't trustworthy
- A notable case is input/output (I/O) – for example USB, smart network cards, GPUs
- Even worse, the rise of pluggable Thunderbolt and USB-C
  - is my charger trustworthy?
- Can we be secure in the face of adversarial devices?

theo.markettos@cl.cam.ac.uk

Current architectures

- Message-passing I/O
  - packet-based interconnect
  - copying of packets to and from memory
  - often packets interpreted by software
  - packetisation can be a bottleneck
  - e.g. USB, SATA, SAS
- Shared-memory I/O
  - I/O devices have rights to read and write system memory (DMA)
  - communicate with CPU by passing pointers to memory blocks
  - more efficient
  - e.g. NVMe, GPUs, PCIe network cards
  - safe?

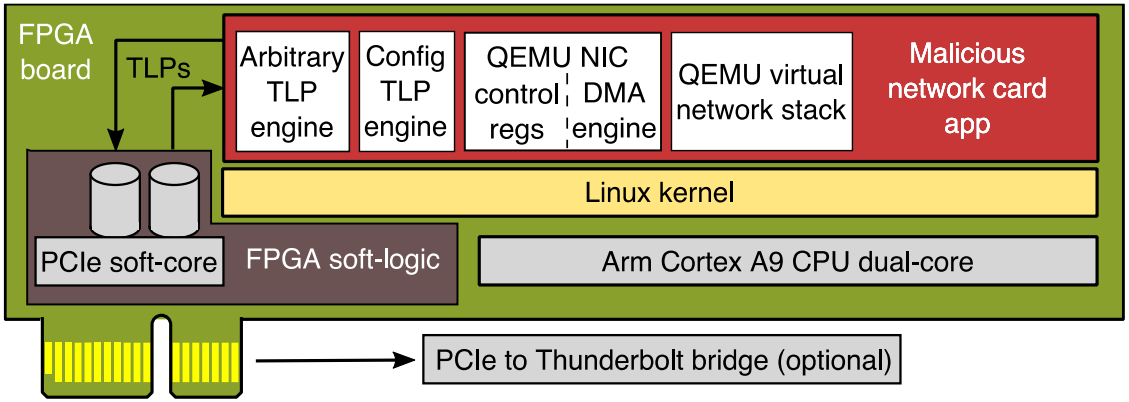
Shared-memory I/O architectures



- Are we doing the right things architecturally?
- State of the art: Input/Output Memory Management Unit (IOMMU)
- How is it used in modern systems?

Thunderclap: an I/O research platform

- Talking to industry, they lament the lack of tools for evaluating I/O protections - so we built some
- Thunderclap - FPGA-based research platform
  - able to run a complex software model of a PCIe network card, interact with the OS and driver stack
  - see what data is exposed to a malicious device
  - explore vulnerability space



theo.markettos@cl.cam.ac.uk

IOMMU use and misuse

- The IOMMU is supposed to defend against malicious DMA from peripherals – but does it?
- The IOMMU has fundamental limitations, and many operating systems only use it to a limited extent
- The IOMMU interface has a lot of similarities with the kernel system-call interface in operating systems, but had little attention
- We discovered multiple new vulnerabilities in Windows, MacOS, FreeBSD and Linux
- Substantial work with vendors regarding mitigations
- Patches now shipped, including major changes in Windows 10 release 1803

Coming soon...

- *“Thunderclap: Exploring Vulnerabilities in Operating-System IOMMU Protection with DMA from Untrustworthy Peripherals”*
  Markettos, Moore, Watson, et. al

  to appear in
  Network and Distributed Systems Security Symposium, February 2019

The future

- Things were bad, how can we make them better?
- Is there a better way to implement an IOMMU to avoid such vulnerabilities?
- Or is there another way to structure I/O?
  - more message-passing I/O?
  - how to share compute safely?
- Can we achieve security *and* performance?
- Lots of hard questions...