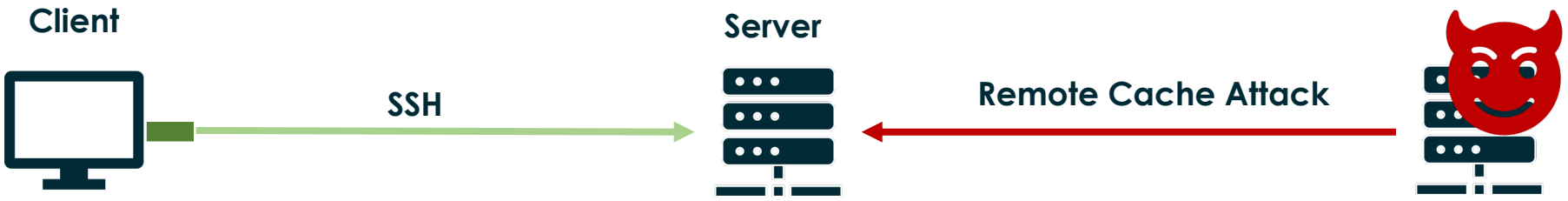
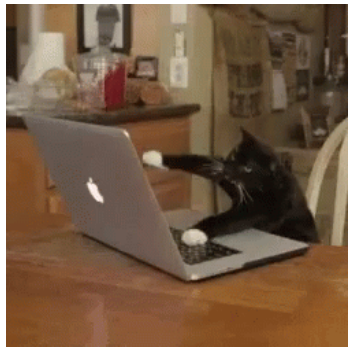
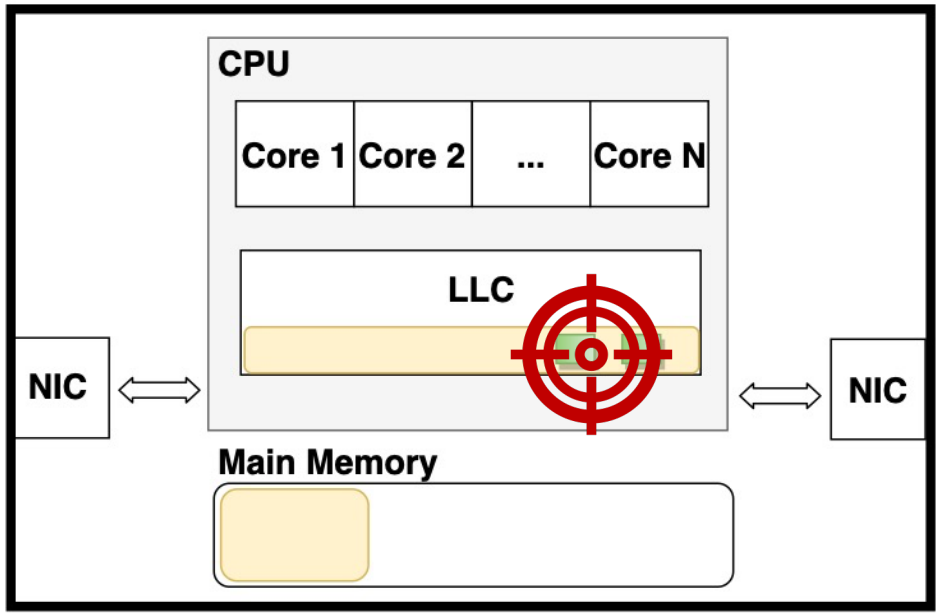
NetCAT: Practical Cache Attacks from the Network

Michael Kurth, Ben Gras, Dennis Andriesse,
Cristiano Giuffrida, Herbert Bos, Kaveh Razavi

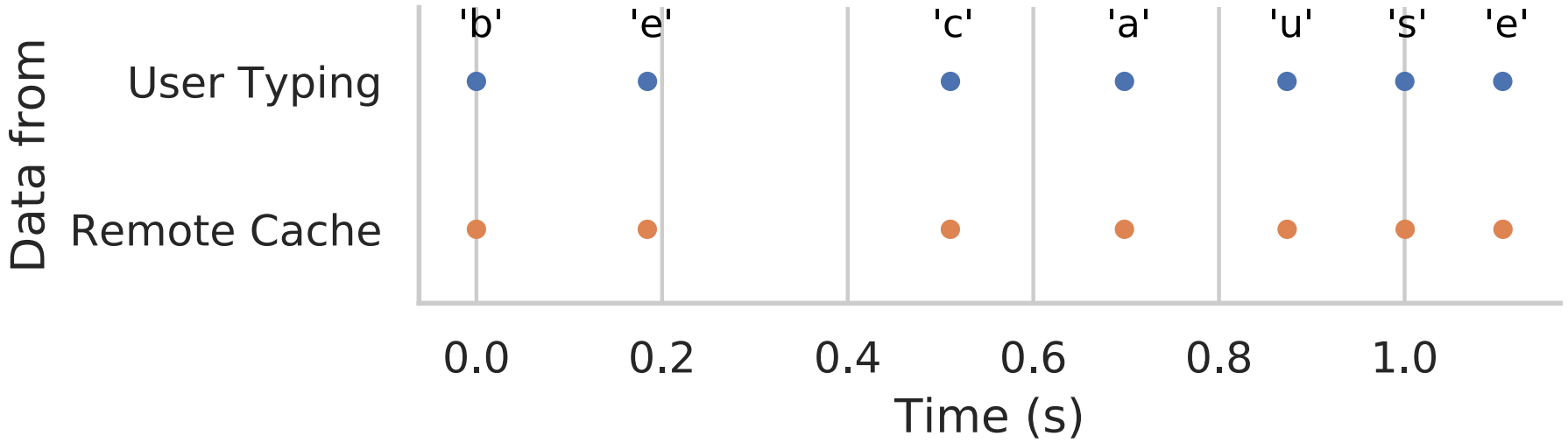
Cache Attack from the Network







Network Cache Attack

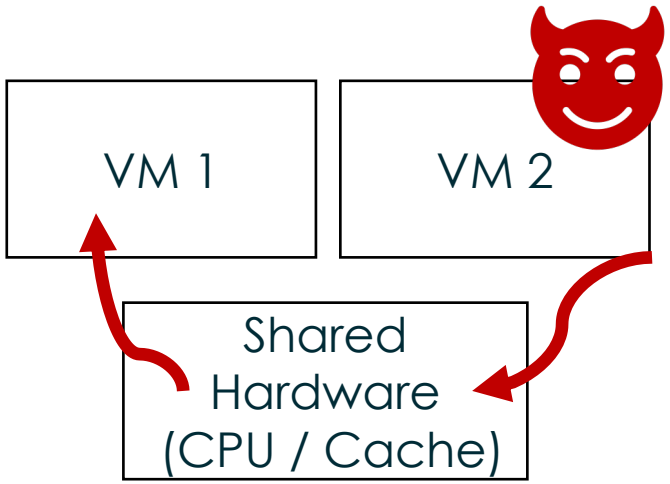


Outline

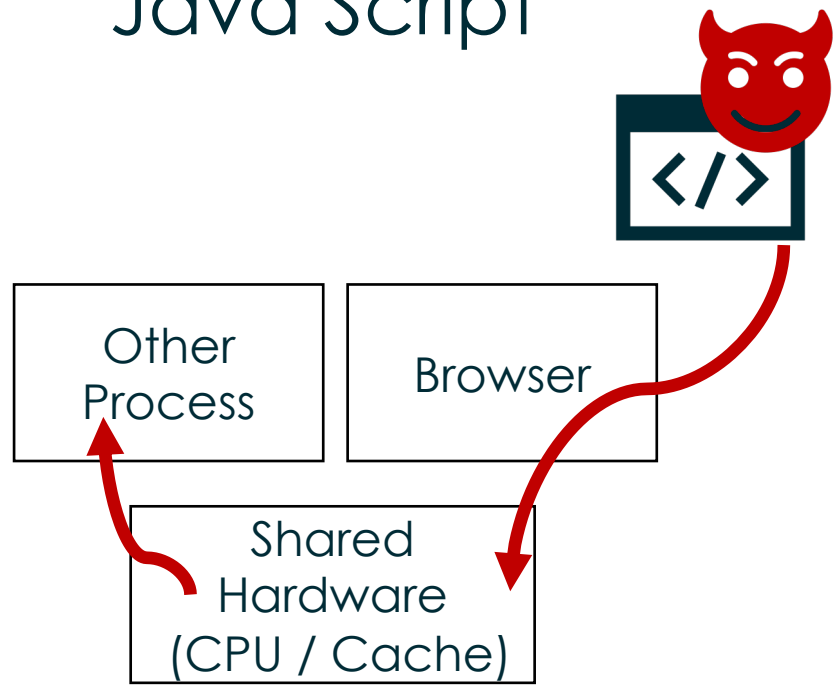
- Background
  - Cache Attacks
  - DDIO
  - RDMA
- NetCAT - CVE-2019-11184
  - Reverse Engineering DDIO
  - End-to-End Attack
  - Demo
- Conclusion

Cache Attacks (prev.)

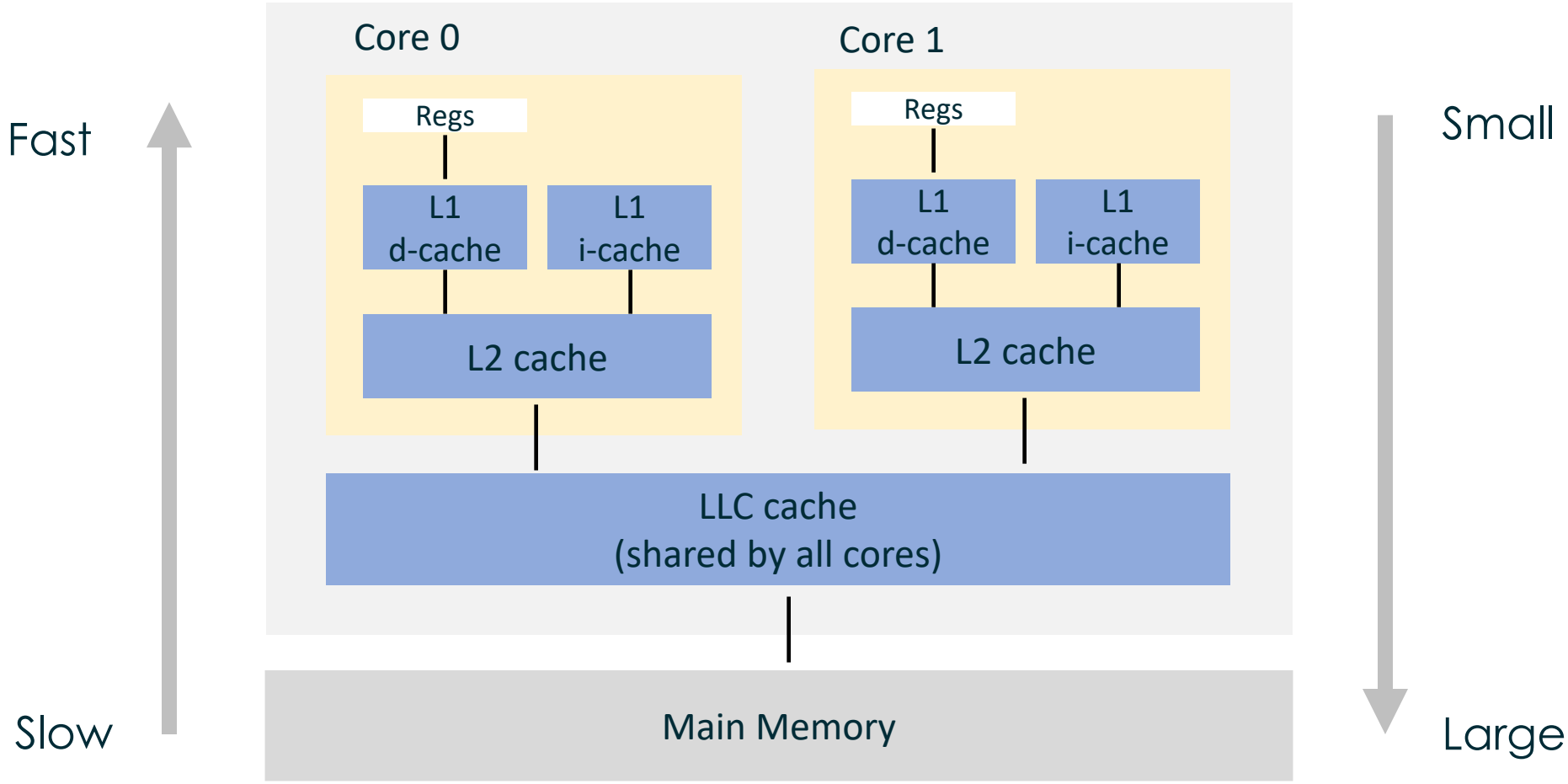
Cloud



Java Script

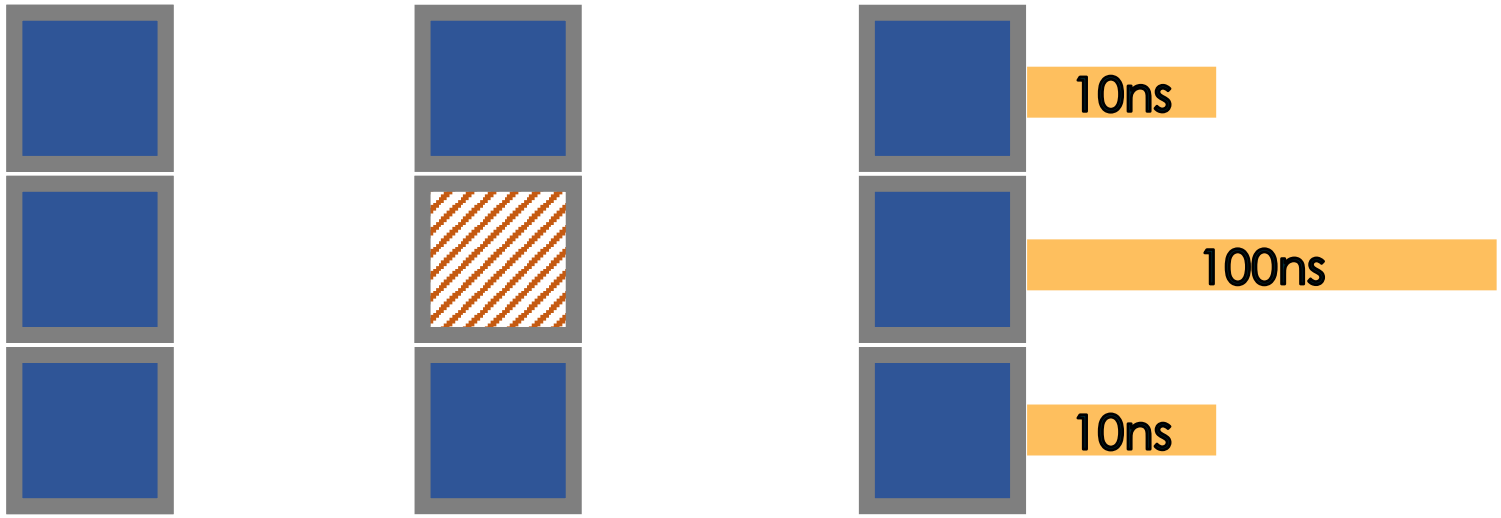


The Memory Wall - Caches



PRIME+PROBE

Cache Lines

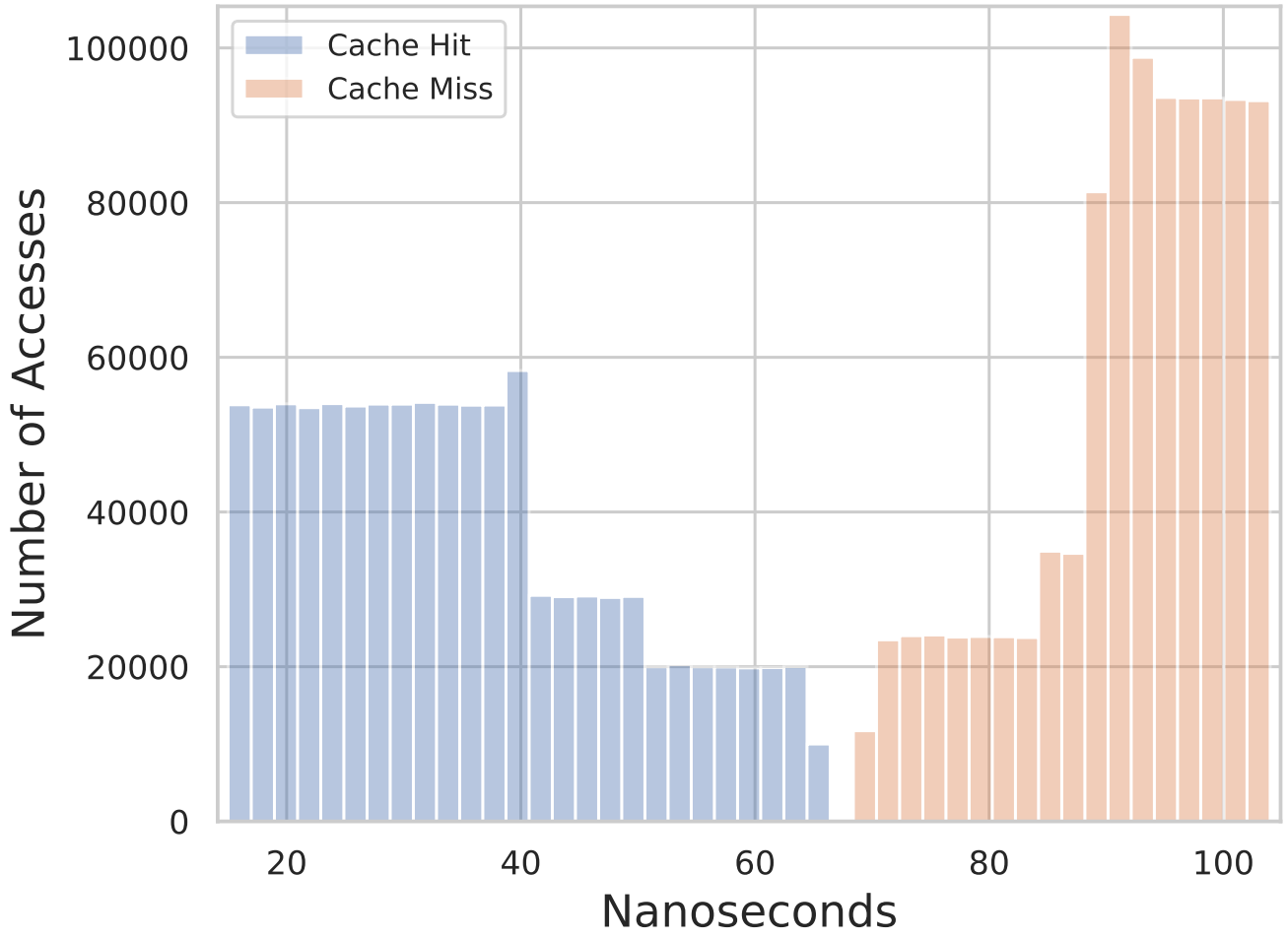


Prime

Victim Access

Probe

Cache Hits & Misses



Cache Attacks

With Cache Hits & Misses we can

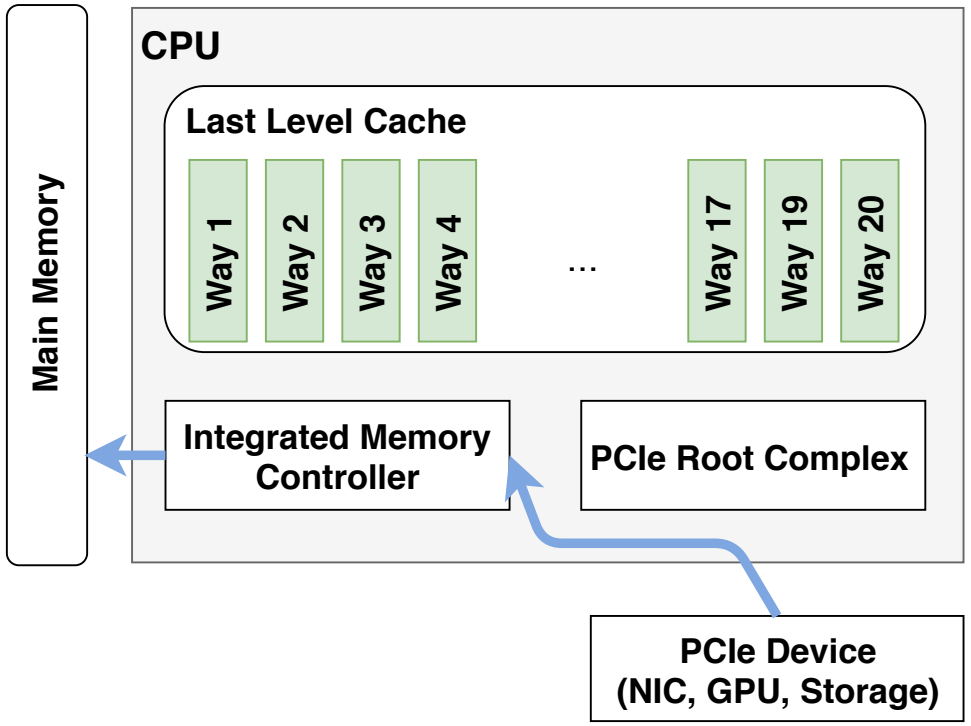
- Leak Crypto Keys (e.g. AES)
- Guess visited Websites
- Leak Memory Contents

DDIO

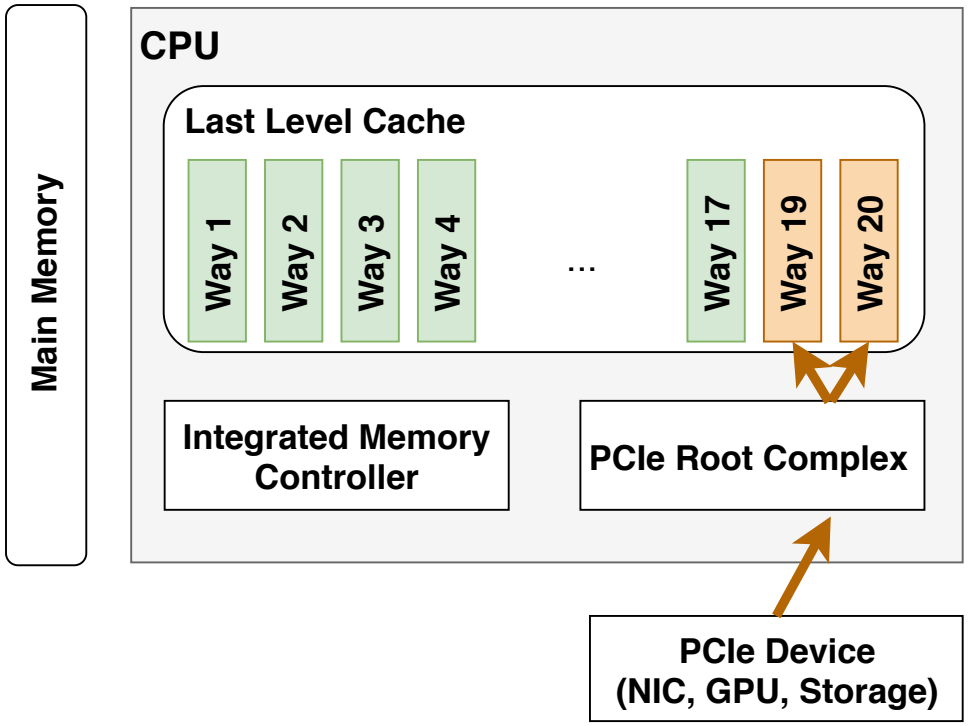
- Data Direct I/O Technology
- Enabled on all Intel server-grade processors since 2012
- Transparent for drivers and OS

DDIO

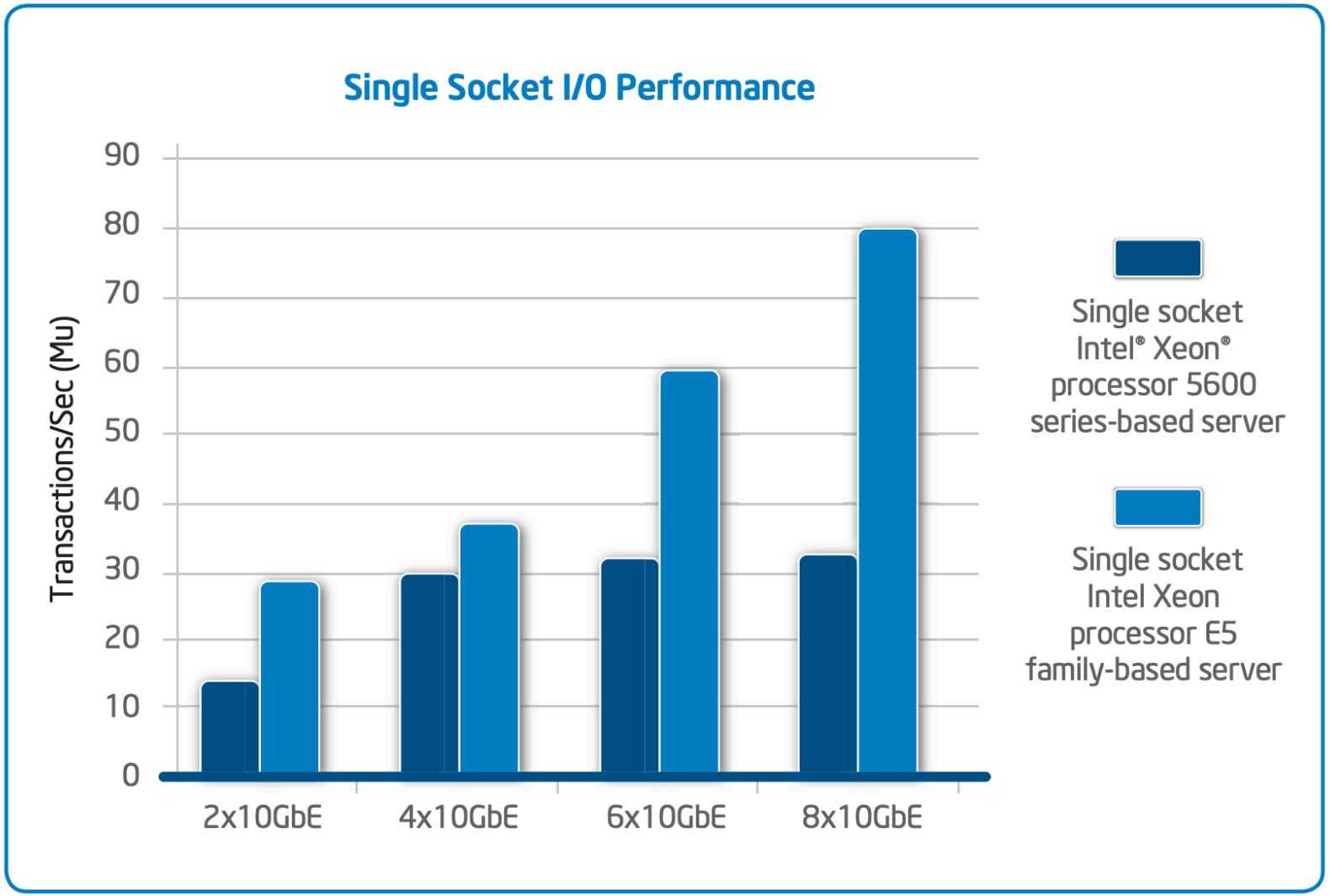
DMA



DDIO



Why is DDIO important?



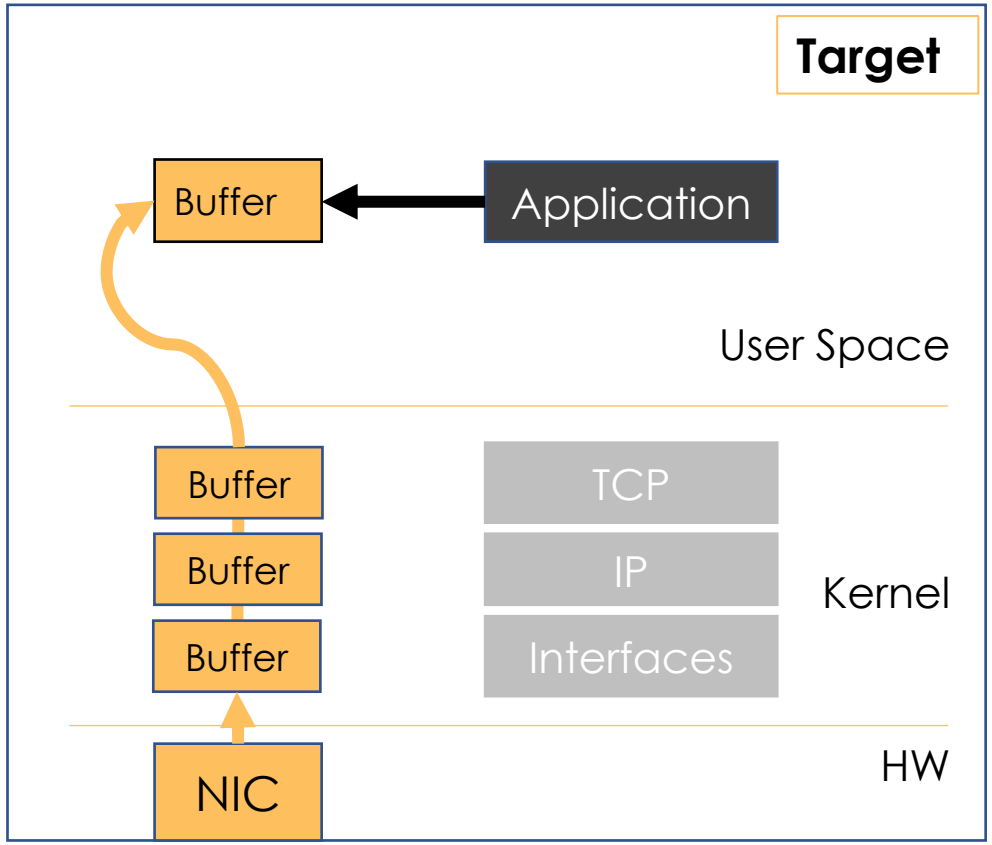
From: Intel Data Direct I/O Technology Overview

Network Cache Attack – Main Challenges

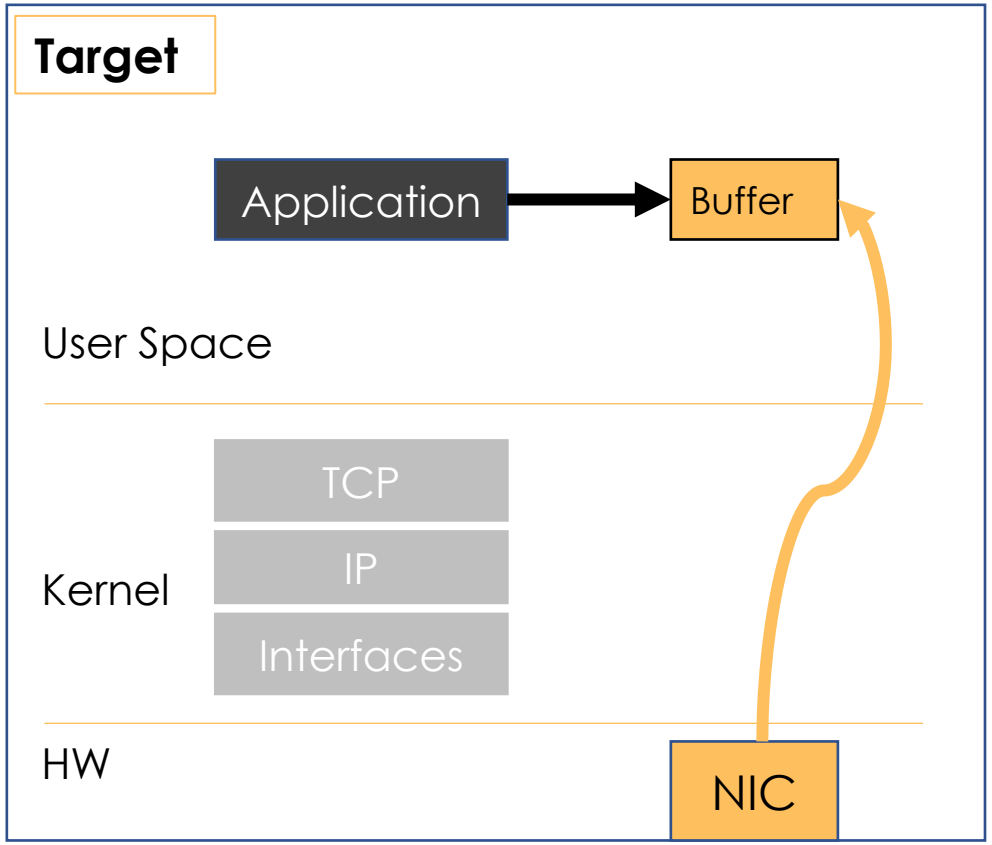
- Inner workings of DDIO
- Remote PRIME+PROBE
- End-to-end attack

RDMA

TCP



RDMA



RDMA

- Available on Public Clouds
- SMBDirect / NFS over RDMA
- Applications:
  - High Performance Computing (HPC)
  - Data Centers / Cloud
  - Storage

Network Cache Attack

- DDIO + RDMA
  - RDMA operations have accesses not only to the pinned memory region but also to parts of the LLC.
  - Foundation for our attack

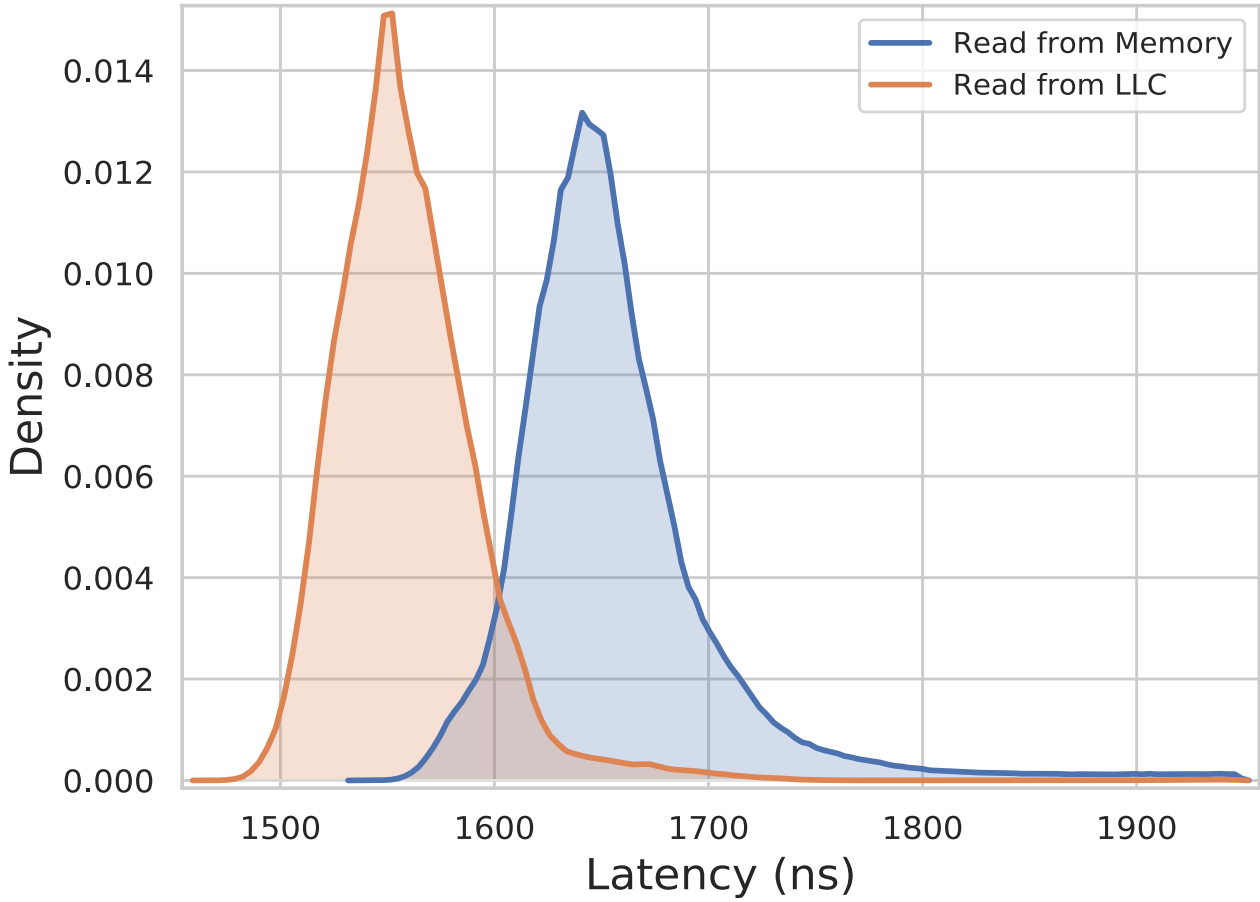
Reverse Engineering DDIO

- How does DDIO interact with the LLC?

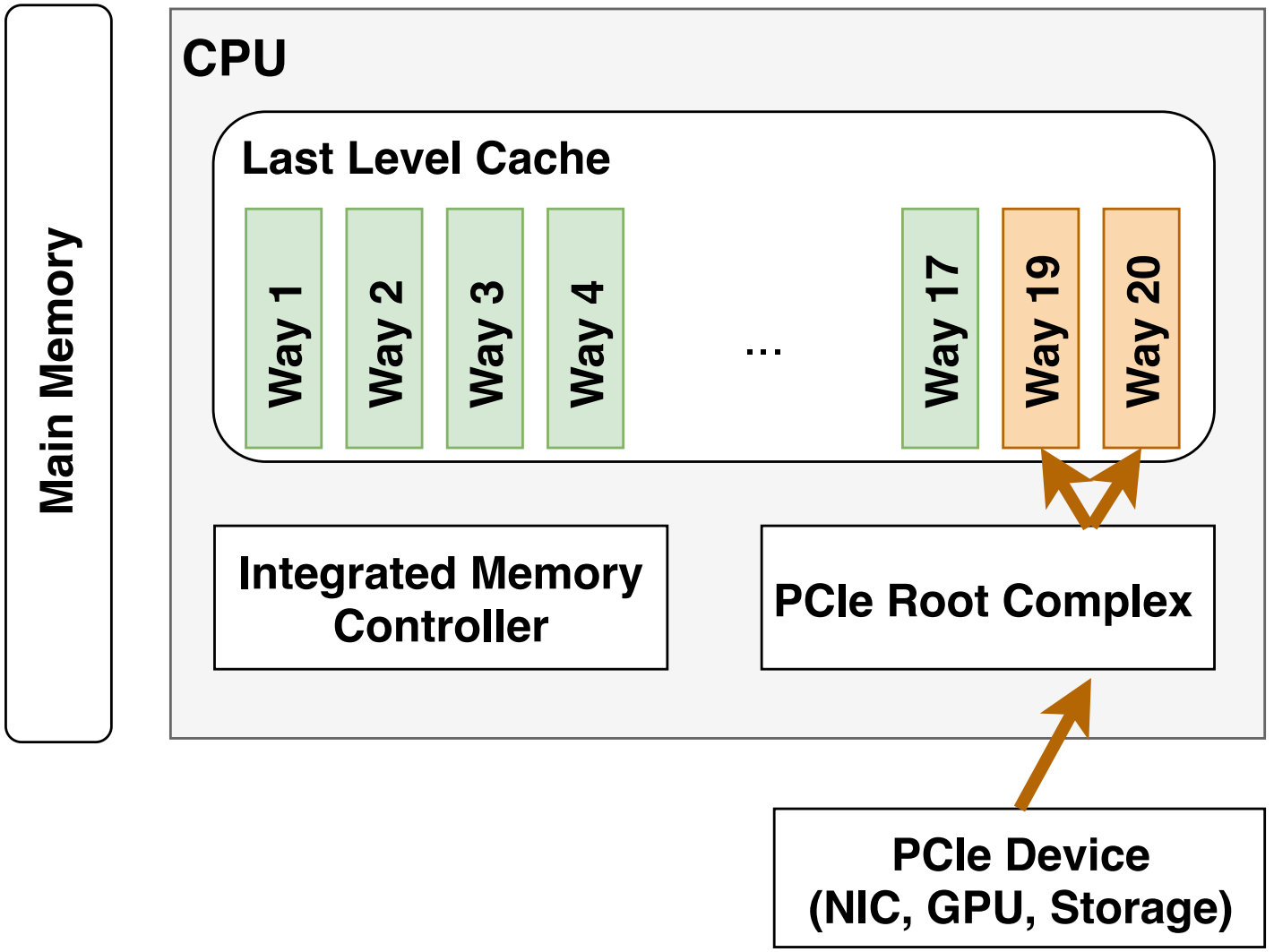
- Which portion of the cache can we access?

Reads served from memory vs LLC

```
t1 = timed_rdma_read(offsetX);
rdma_write (offsetX);
t2 = timed_rdma_read(offsetX);
```

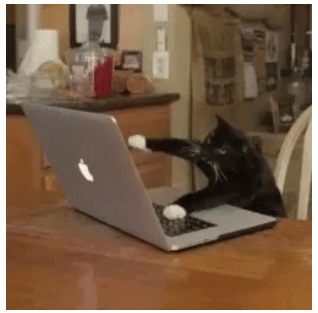


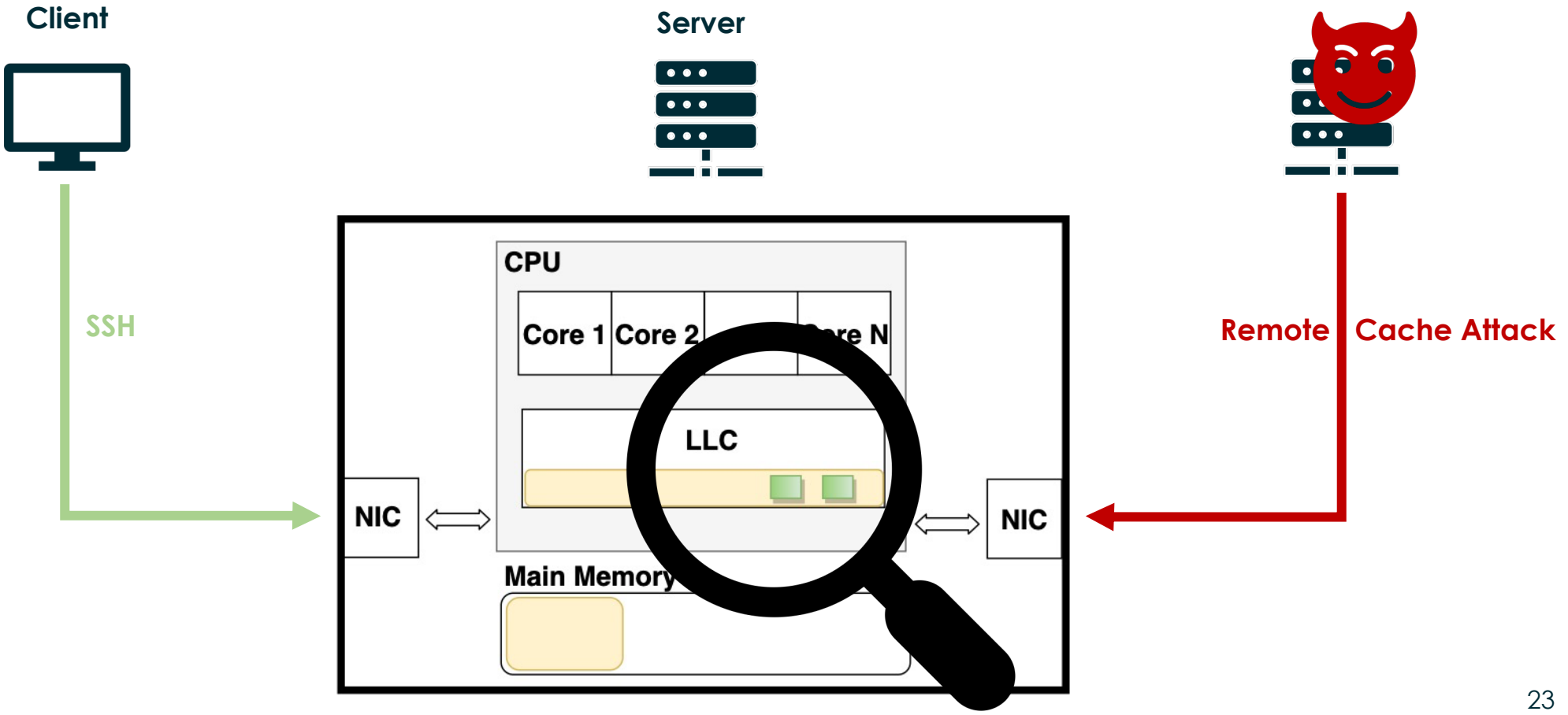
DDIO Allocation Limitation



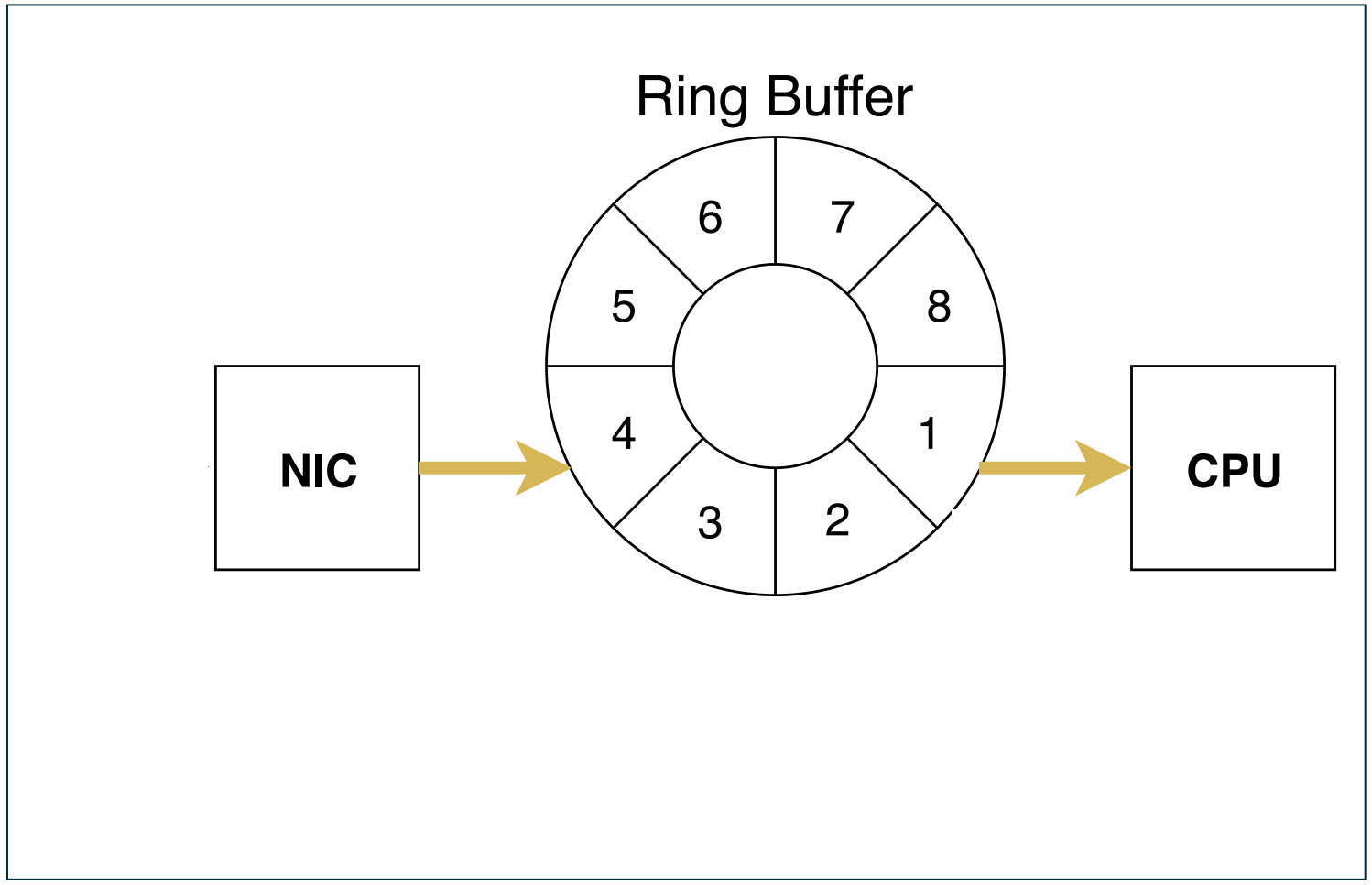
End-to-End Attack

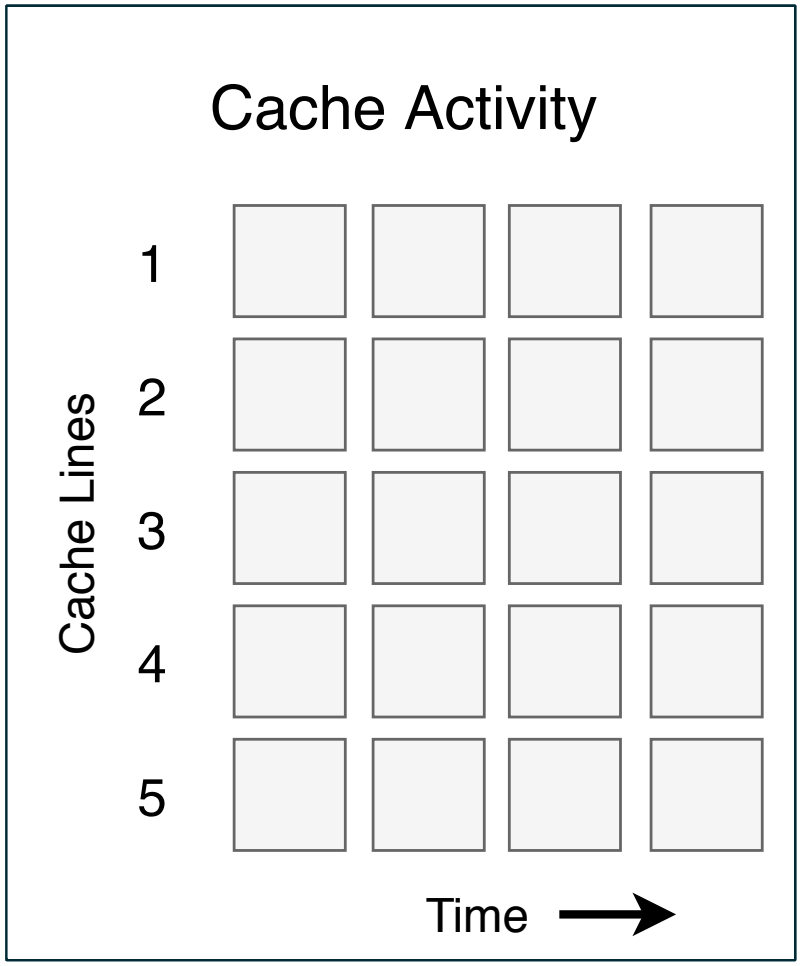
Cache Attack from the Network



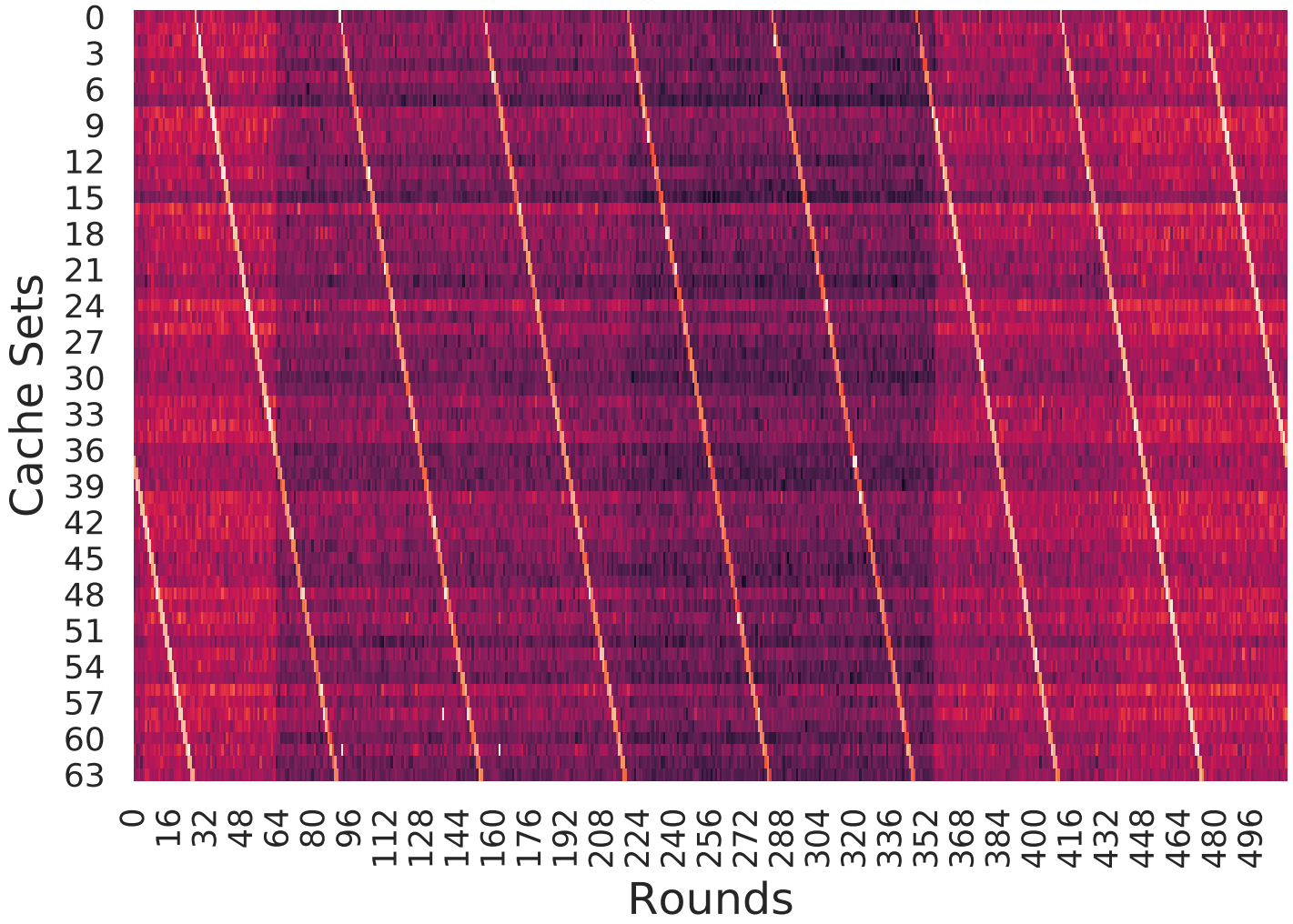


NIC's ring buffer



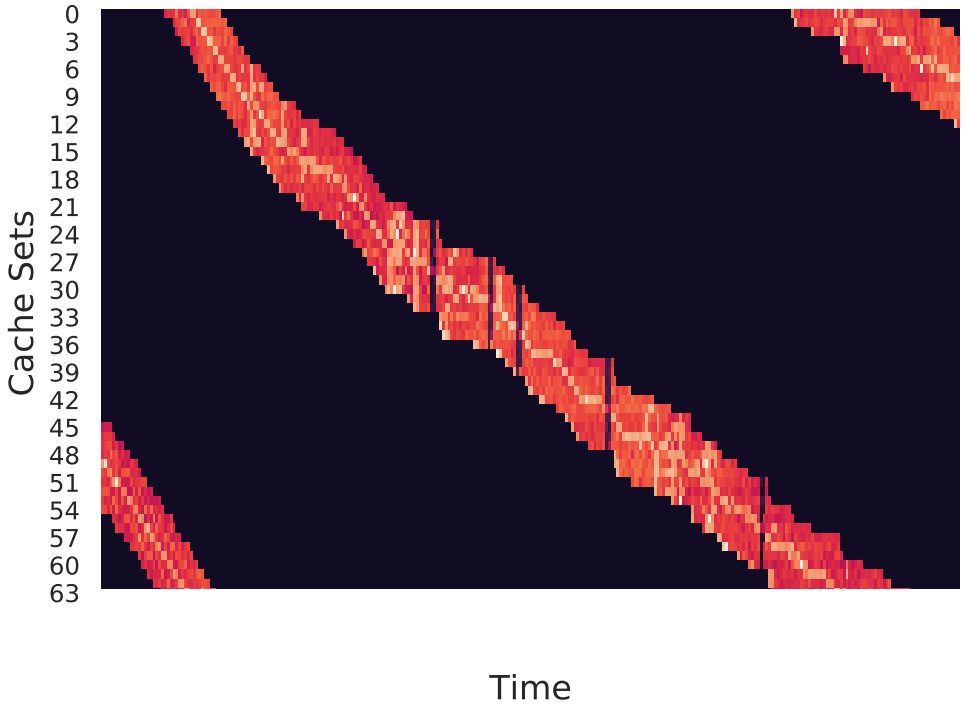


Detecting the NIC's ring buffer in LLC

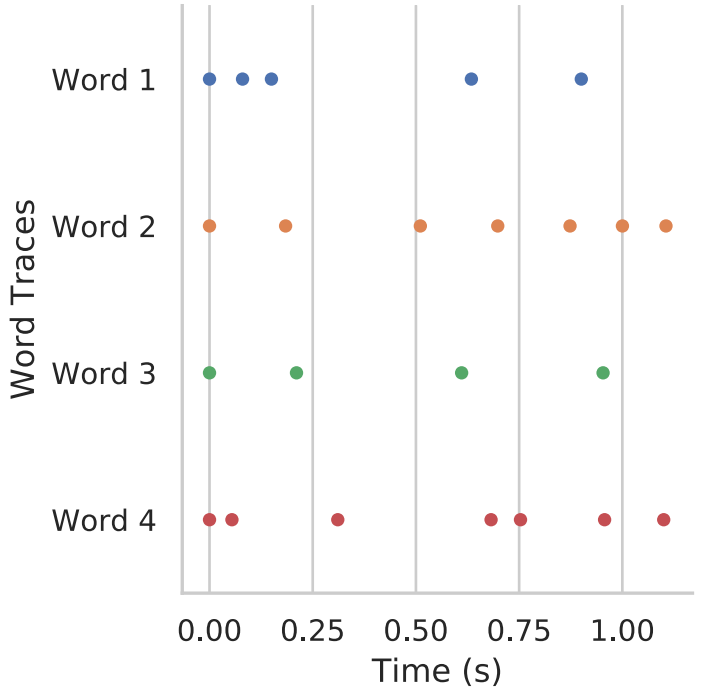


Tracking the Ring Buffer

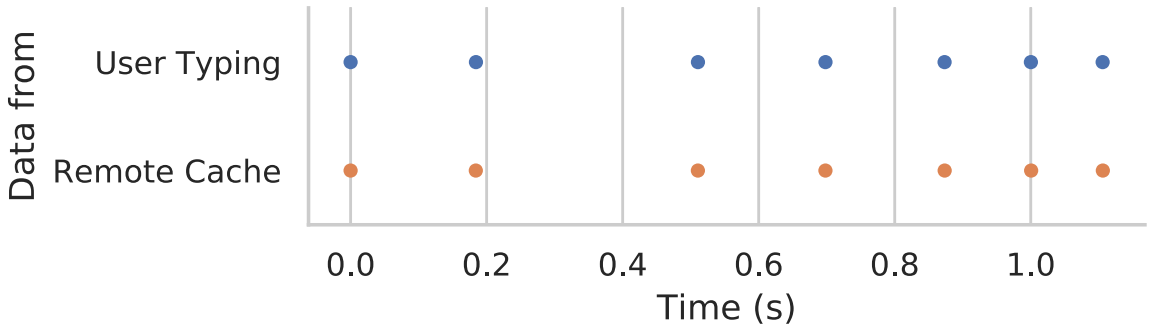
Online Tracker



Offline Extractor



Map inter-packet arrival times to Words

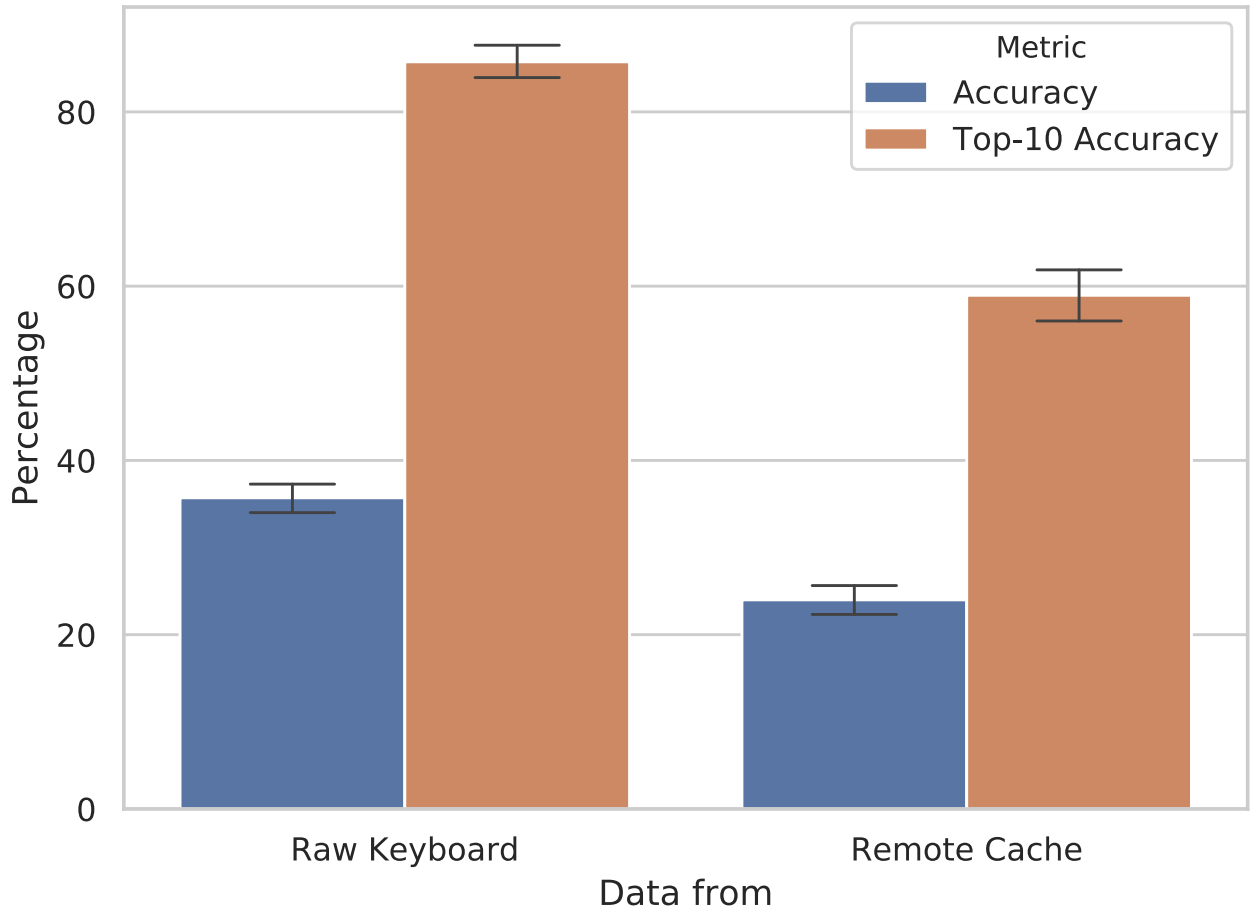


“because”

Map inter-packet arrival times to Words

- 20 subjects typing free and transcribed text
- Total of 4’574 unique words, on average 228.7 unique words per subject
- Each word is represented as a point in multidimensional Space
- *k*-nearest neighbors' algorithm (k-NN) to classify measured word

Evaluation


Metric
Accuracy
Top-10 Accuracy
Percentage
0
20
40
60
80
Raw Keyboard
Remote Cache
Data from

CVE-2019-11184 - Demo

michael@son: ~/development/thor 47x14

```
michael@son:~/development/thor$ sh offline_extr
action_and_prediction.sh
```

michael@holyspirit: ~ 46x28

```
michael@holyspirit:~$ ssh -i /home/michael/.ss
h/father_rsa michael@192.168.0.20
```

michael@son: ~/development/thor 47x14

```
Profile ring buffer on page 246
Profile ring buffer on page 247
Profile ring buffer on page 248
Profile ring buffer on page 249
Profile ring buffer on page 250
Profile ring buffer on page 251
Profile ring buffer on page 252
Profile ring buffer on page 253
Profile ring buffer on page 254
Profile ring buffer on page 255
Ring buffer profiling finished!


Enter ring buffer page:
```

Mitigation

- Turn off DDIO or do not use RDMA

- Intel: "*limit direct access from untrusted networks when DDIO & RDMA are enabled*"

The name of our paper

- It was a pun - NetCAT stands for **Net**work **C**ache **AT**tack.

Conclusion

- LLC now directly on the I/O path
- CVE-2019-11184 is the first DDIO side channel vulnerability
- Intel acknowledged findings
  - Public disclosure was on September 10, 2019
  - Bug Bounty payment
- First security analysis on DDIO - future attacks likely

@mik___ @vu5ec