Packet Chasing:

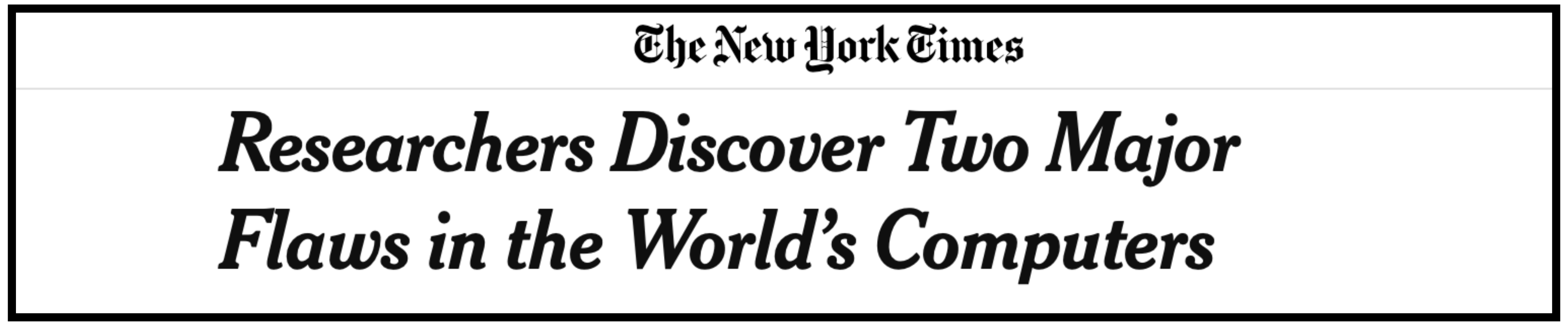
Spying on Network Packets over a Cache Side-Channel

Mohammadkazem (Kazem) Taram, Ashish Venkat, Dean Tullsen

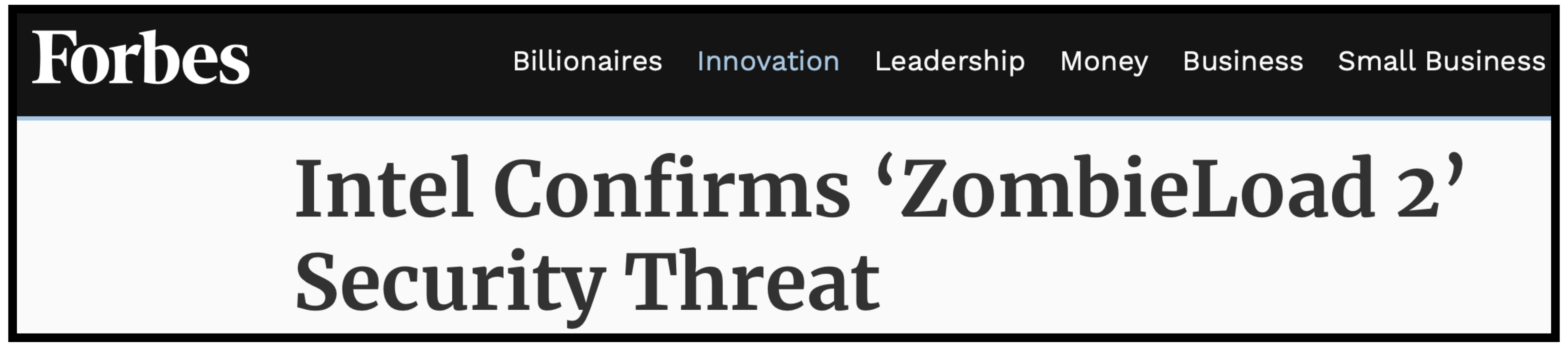
University of California San Diego, University of Virginia

ISCA20

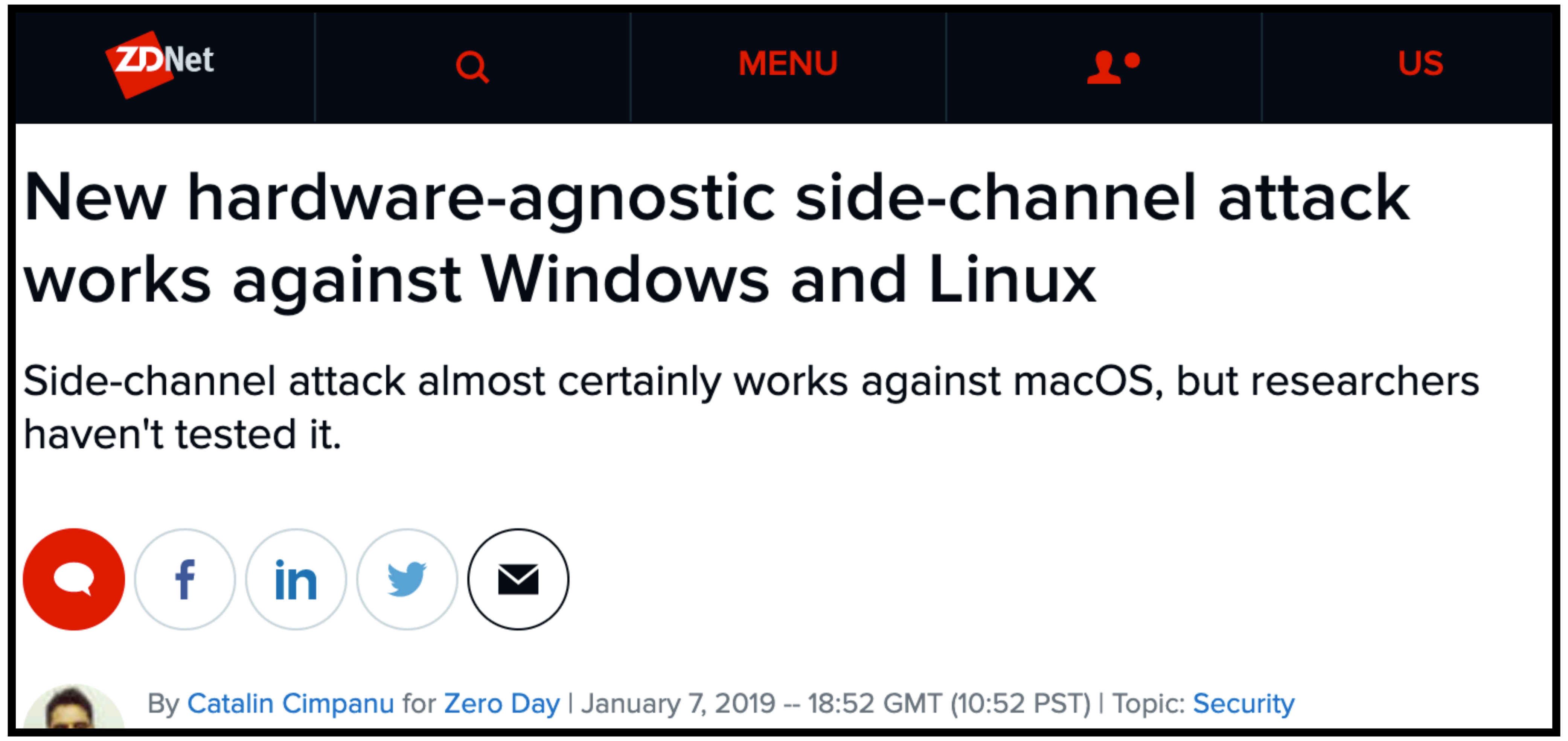
Performance Optimizations, Potential Security Threats



Researchers Discover Two Major Flaws in the World's Computers



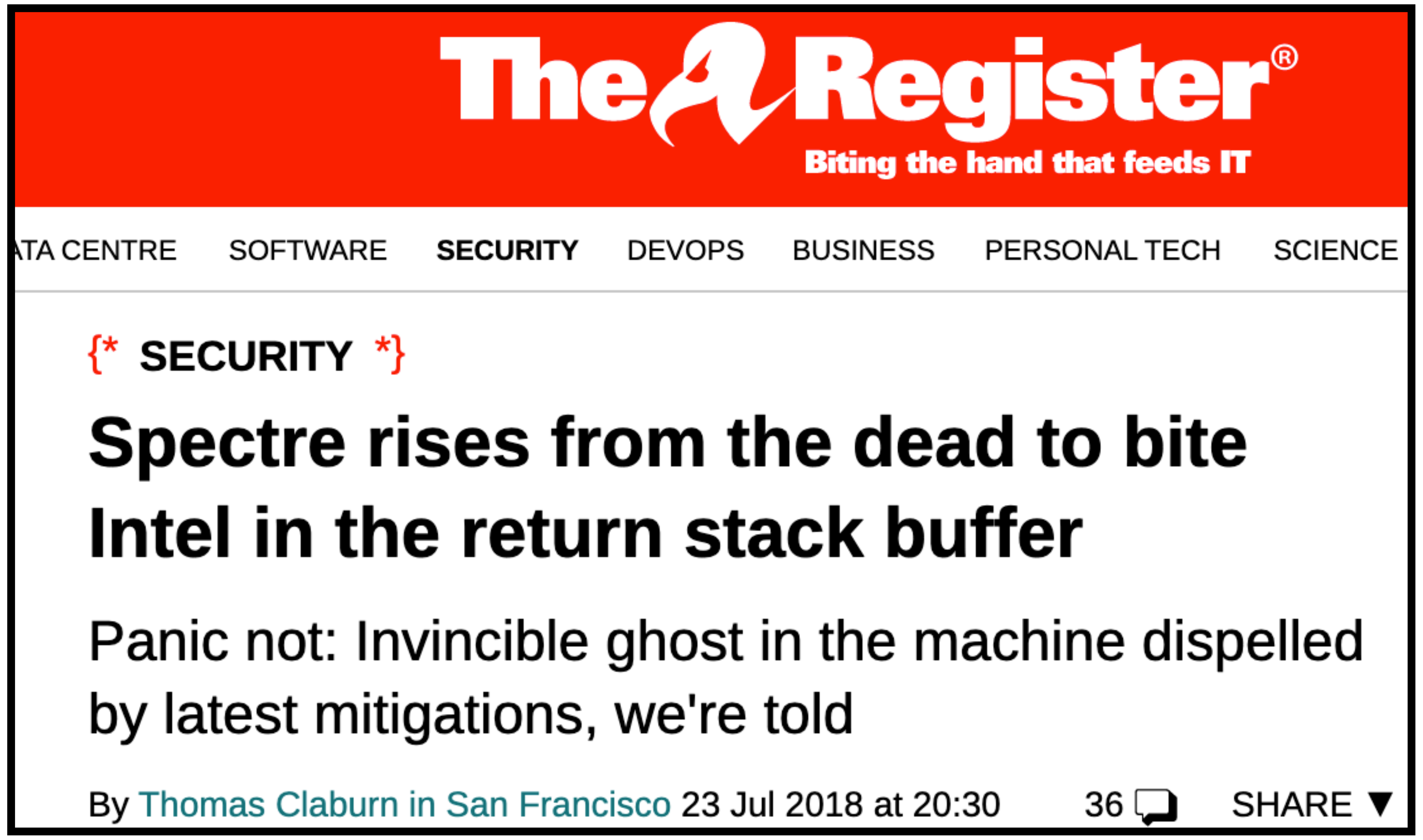
Intel Confirms 'ZombieLoad 2' Security Threat



New hardware-agnostic side-channel attack works against Windows and Linux

Side-channel attack almost certainly works against macOS, but researchers haven't tested it.

By Catalin Cimpanu for Zero Day | January 7, 2019 -- 18:52 GMT (10:52 PST) | Topic: Security



{* SECURITY *}

Spectre rises from the dead to bite Intel in the return stack buffer

Panic not: Invincible ghost in the machine dispelled by latest mitigations, we're told

By Thomas Claburn in San Francisco 23 Jul 2018 at 20:30 36 SHARE ▼

High-Speed Networks

OS-Level Optimizations

Interrupt Coalescing + Polling
Core Sequestering
Asynchronous I/O
Multikernel OS
Message Passing-Optimization

NIC-Level Optimizations

Receive-Side Scaling (RSS)
Protocol Offloading
TCP Segmentation Offload (TSO)
Interrupt Coalescing
Large Receive Offload (LRO)
Header Checksumming

Session-Level Optimizations

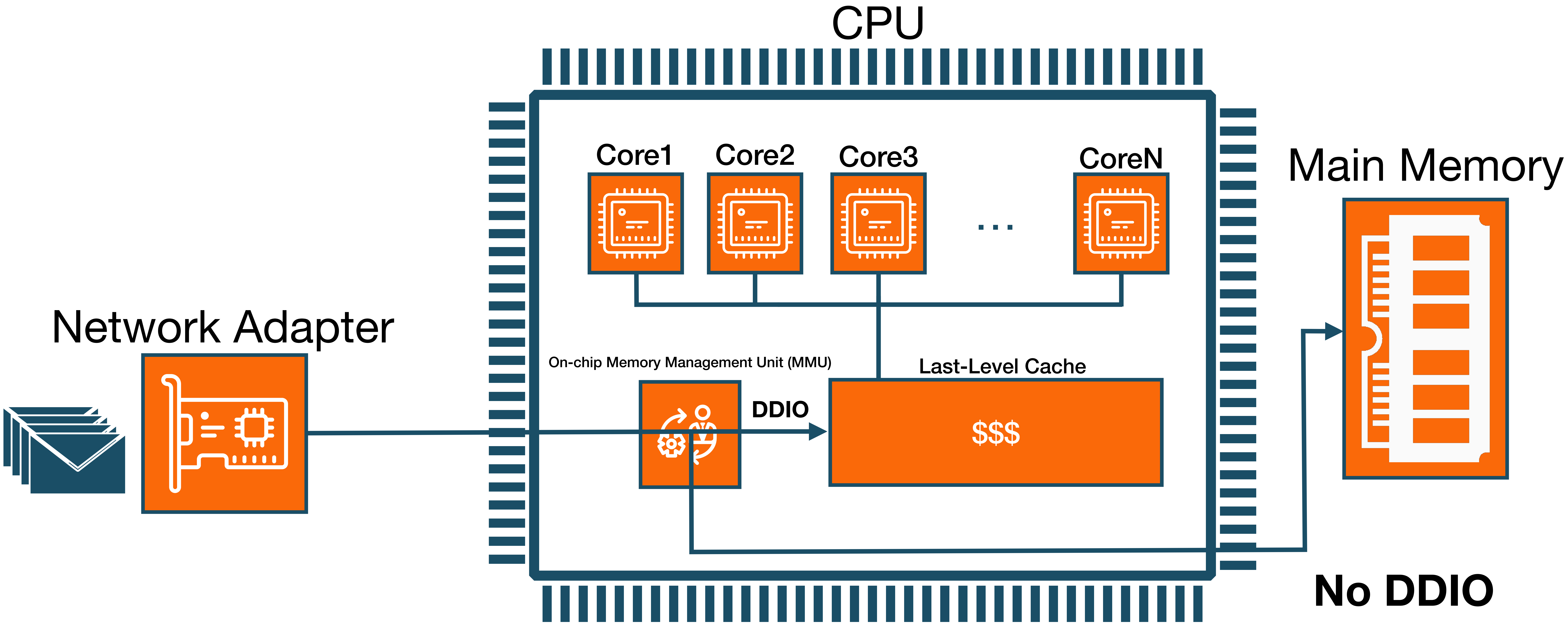
Receiver Zero Copy
OS Bypass Protocols, e.g, DPDK
Application Bypass

Processor-Level Optimizations

(MSI-X) for PCI
Integrated DMA
Cache-Aware Affinitization
Direct Cache Access
Data Directed I/O

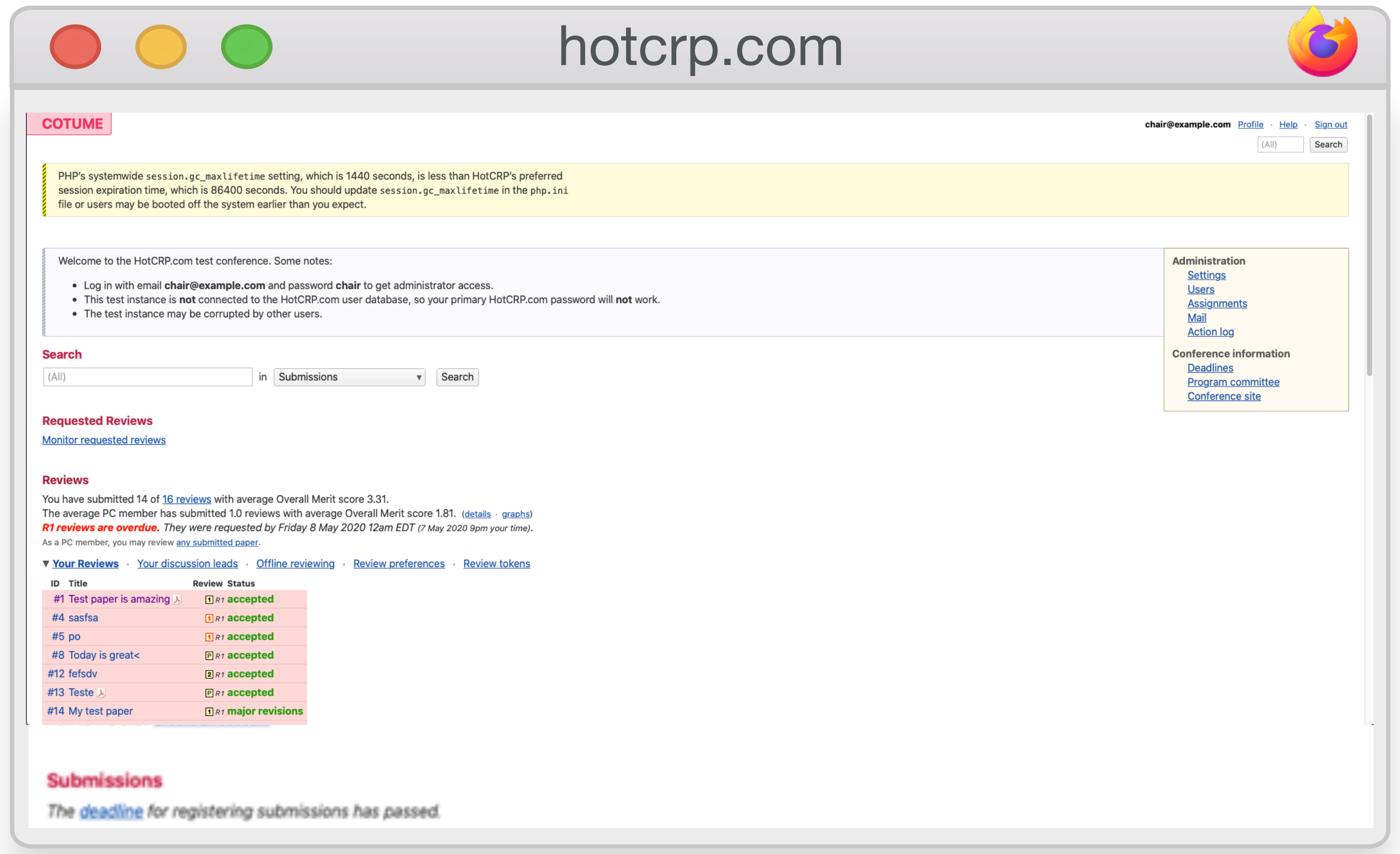
Categories: A Survey of End-System Optimizations for High-Speed Networks, Hanford et al., ACM Comput. Surv., 2018, icons: https://icons8.com

Intel Data Directed I/O (DDIO)



Packet Chasing: Attack Overview

hotcrp.com



PHP's systemwide `session.gc_maxlifetime` setting, which is 1440 seconds, is less than HotCRP's preferred session expiration time, which is 86400 seconds. You should update `session.gc_maxlifetime` in the `php.ini` file or users may be booted off the system earlier than you expect.

Welcome to the HotCRP.com test conference. Some notes:

- Log in with email **chair@example.com** and password **chair** to get administrator access.
- This test instance is **not** connected to the HotCRP.com user database, so your primary HotCRP.com password will **not** work.
- The test instance may be corrupted by other users.

Administration
Settings
Users
Assignments
Mail
Action log

Conference information
Deadlines
Program committee
Conference site

Search

(All) in Submissions ▾ Search

Requested Reviews

Monitor requested reviews

Reviews

You have submitted 14 of 16 reviews with average Overall Merit score 3.31.
The average PC member has submitted 1.0 reviews with average Overall Merit score 1.81. (details · graphs)
R1 reviews are overdue. *They were requested by Friday 8 May 2020 12am EDT (7 May 2020 9pm your time).*
As a PC member, you may review any submitted paper.

▼ Your Reviews · Your discussion leads · Offline reviewing · Review preferences · Review tokens

ID	Title	Review	Status
#1	Test paper is amazing	1 R1	accepted
#4	sasfsa	1 R1	accepted
#5	po	1 R1	accepted
#8	Today is great<	P R1	accepted
#12	fefsdv	2 R1	accepted
#13	Teste	P R1	accepted
#14	My test paper	1 R1	major revisions

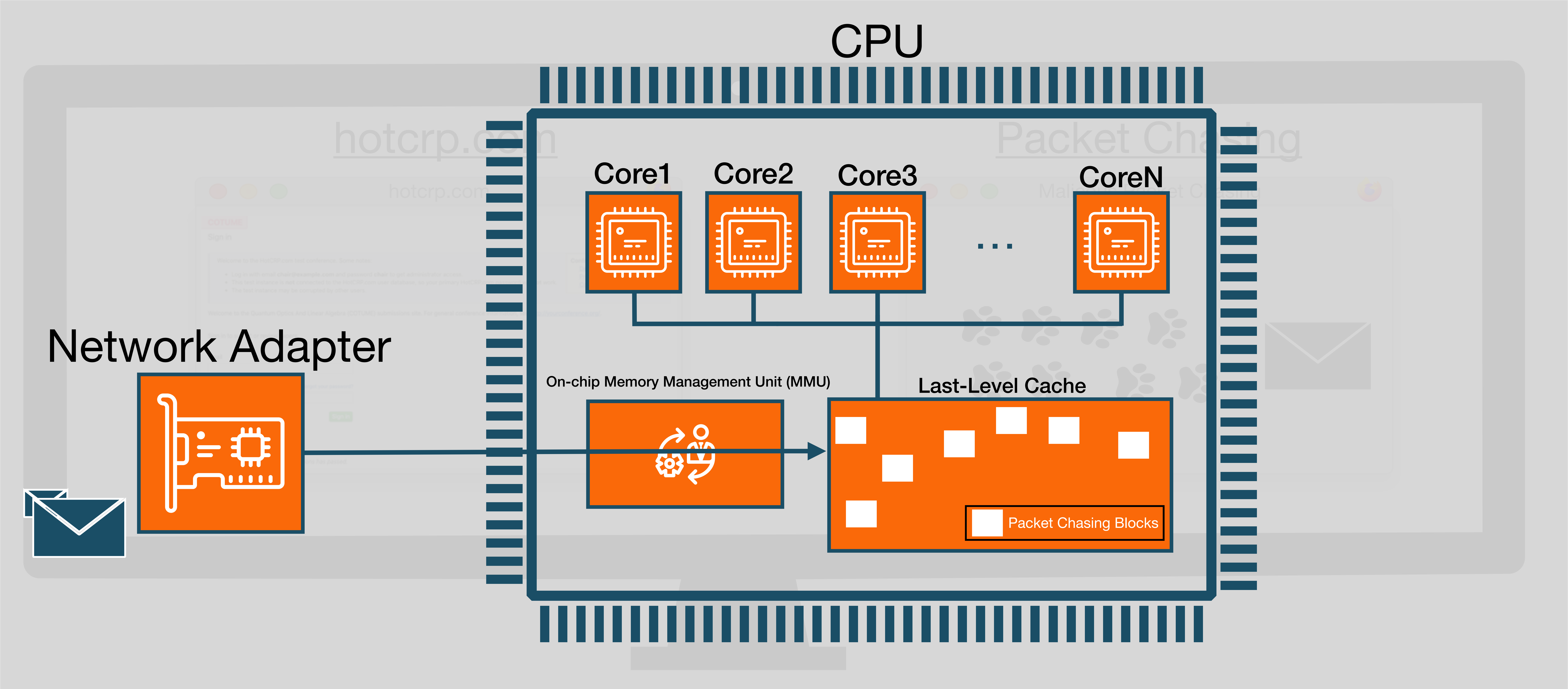
Submissions

The deadline for registering submissions has passed.

Packet Chasing

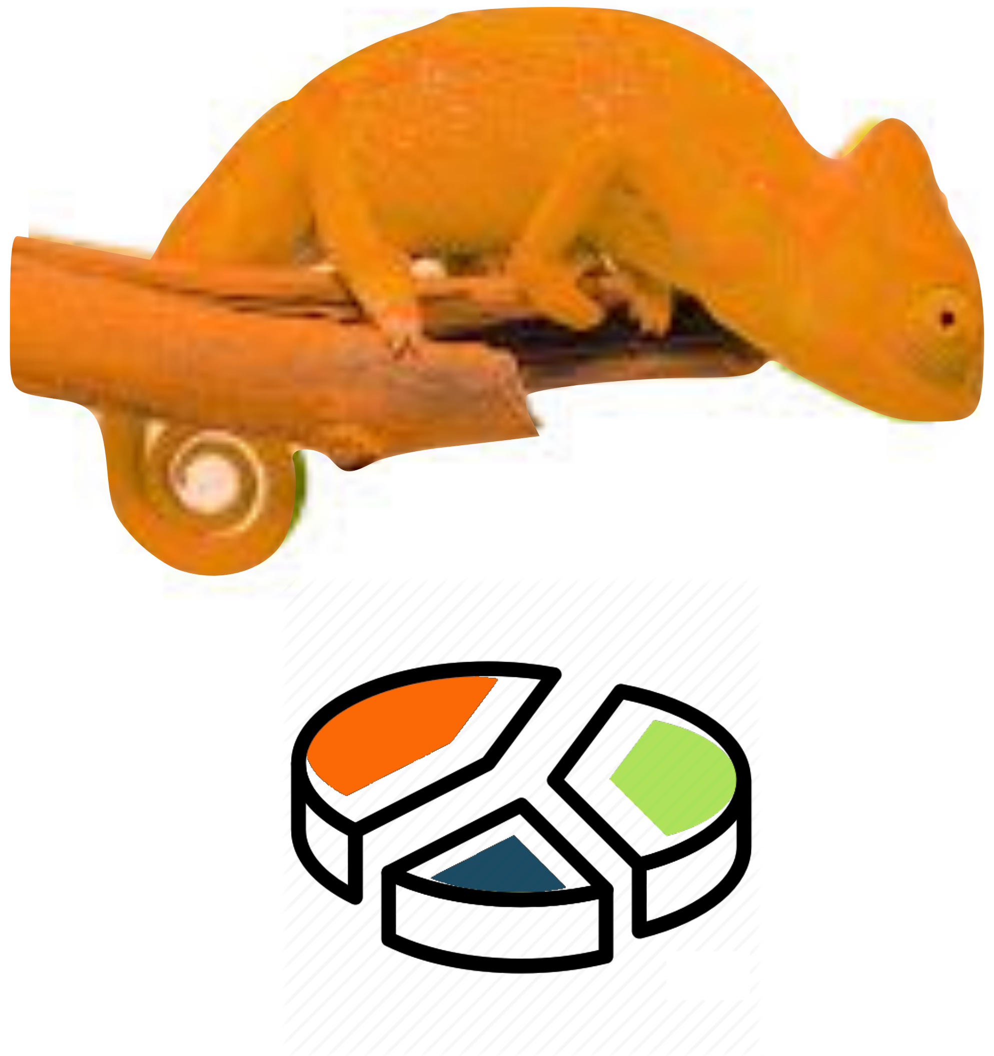
Successful Login Detected

Packet Chasing: Attack Overview

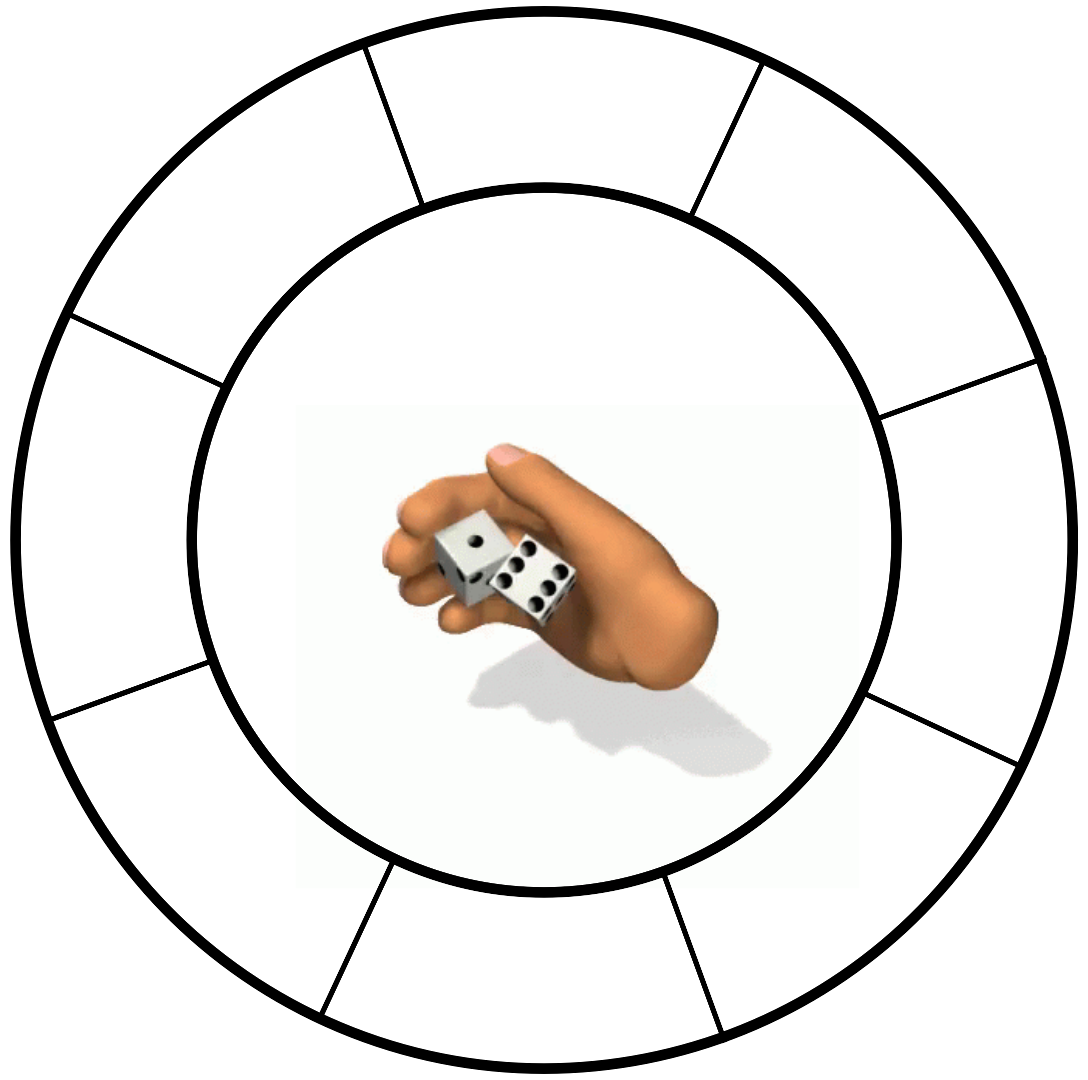


CVE-2019-11184 was assigned to track this issue.
Similar vulnerability is also discovered by NetCat, a concurrent work, that exploits DDIO to reveal keystroke

Packet Chasing: Overview of Defenses

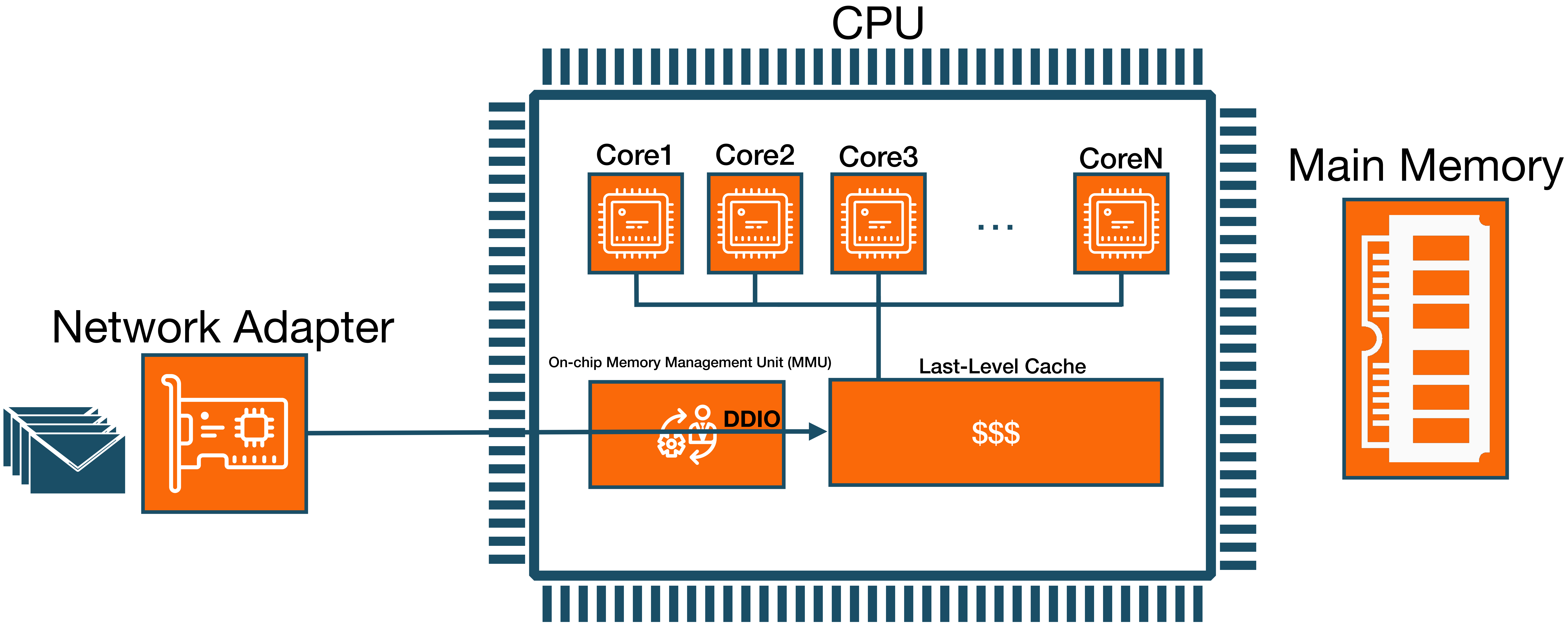


Adaptive Partitioning

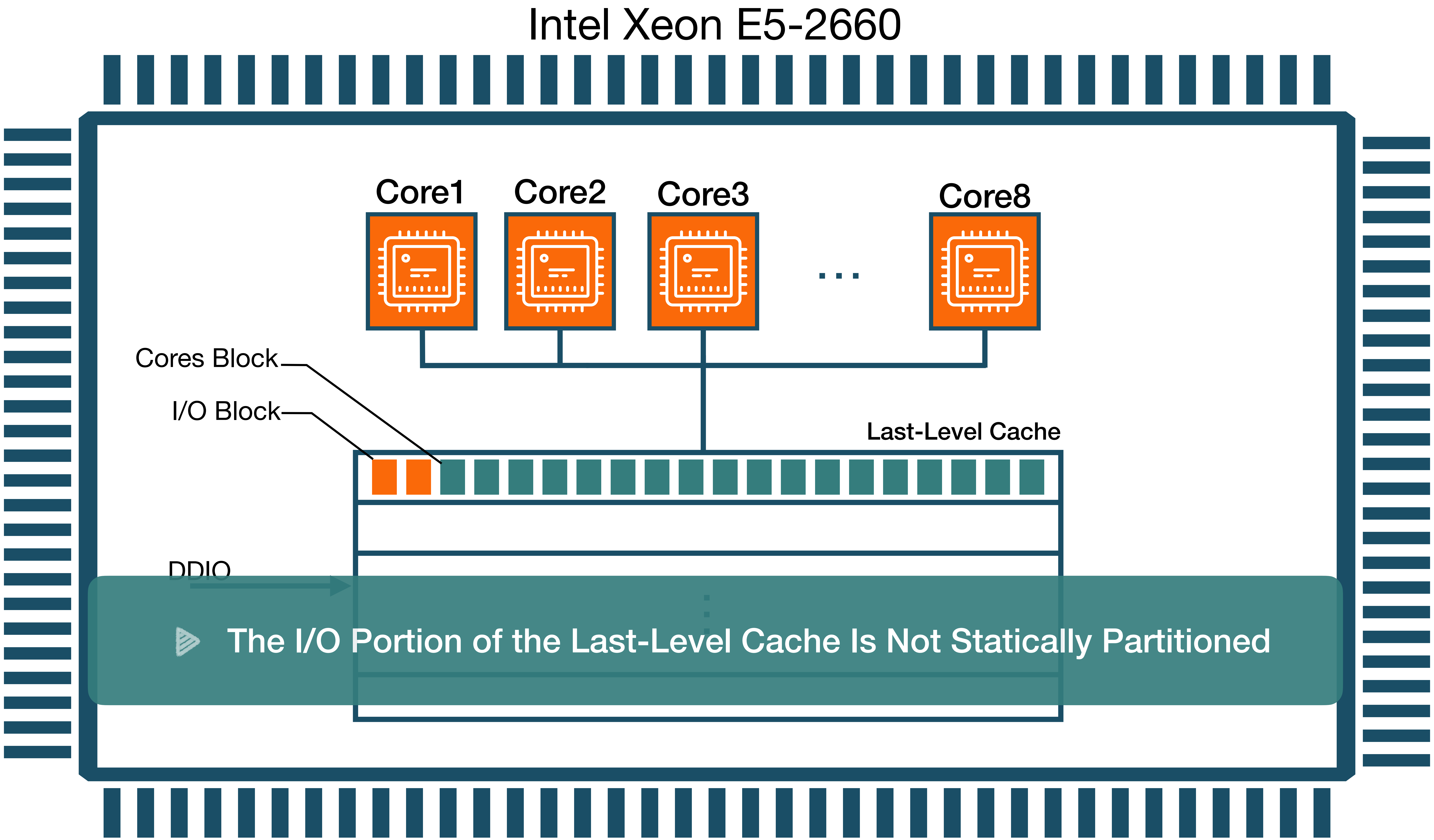


Ring Buffer Randomization

Intel DDIO Details



Intel DDIO Details

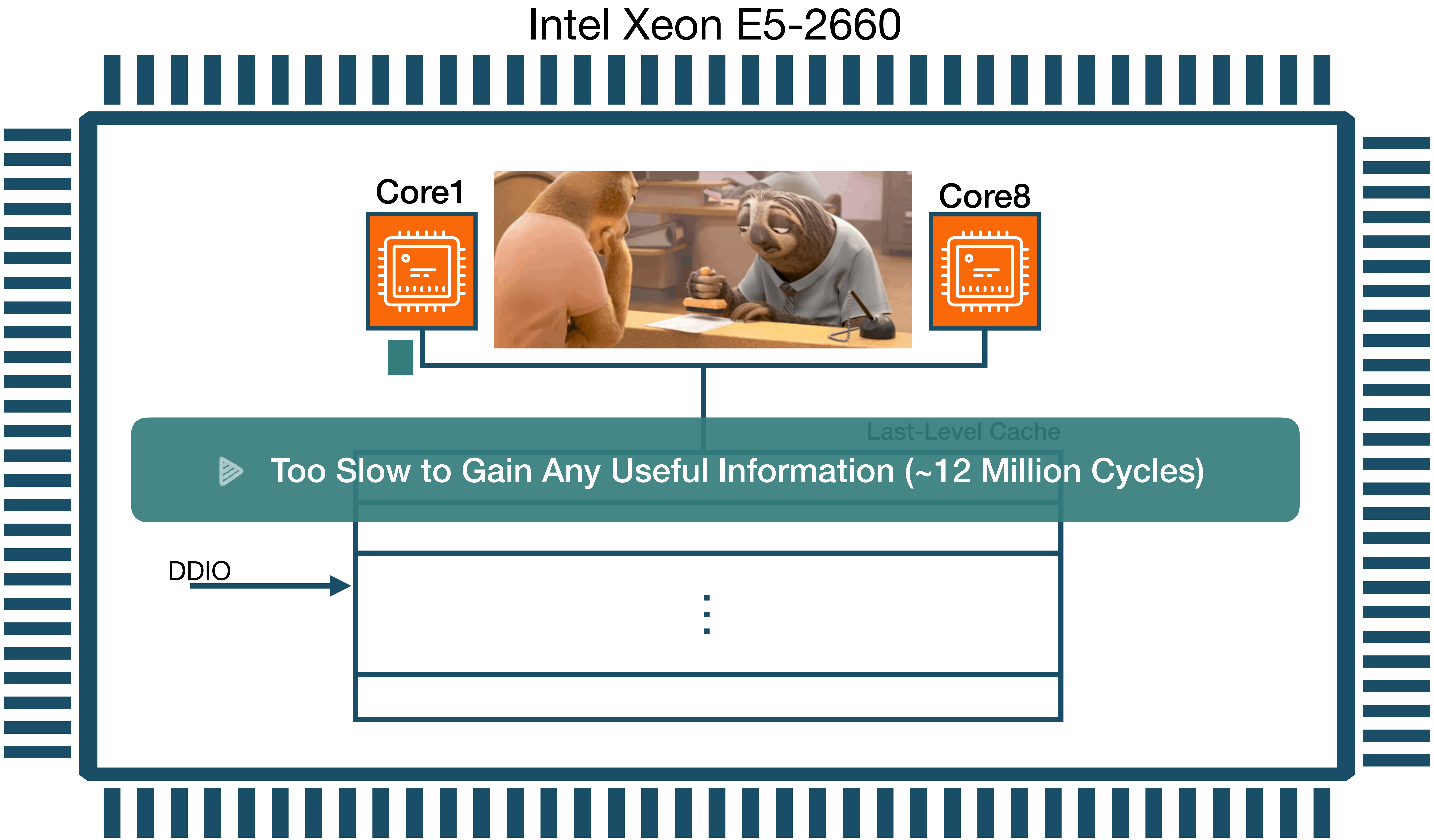


The I/O Portion of the Last-Level Cache Is Not Statically Partitioned

Experimental Setup

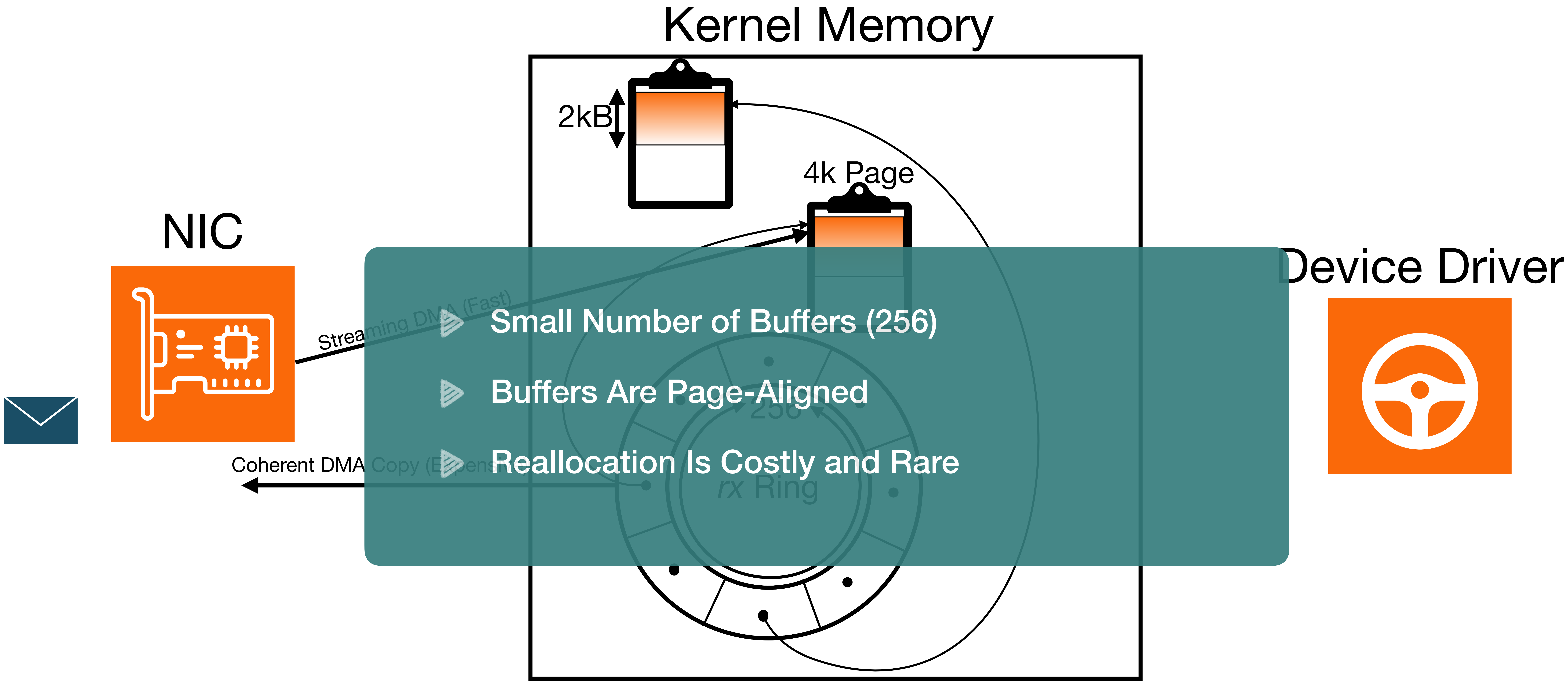
- Intel’s Gigabit Ethernet (IGB) driver version 5.3
- Intel I350 network adapter
- Intel Xeon E5-2660 with 20 MB last level cache with 16k cache sets
- Mastik Micro-Architectural Side-Channel Toolkit

Probing All the Cache



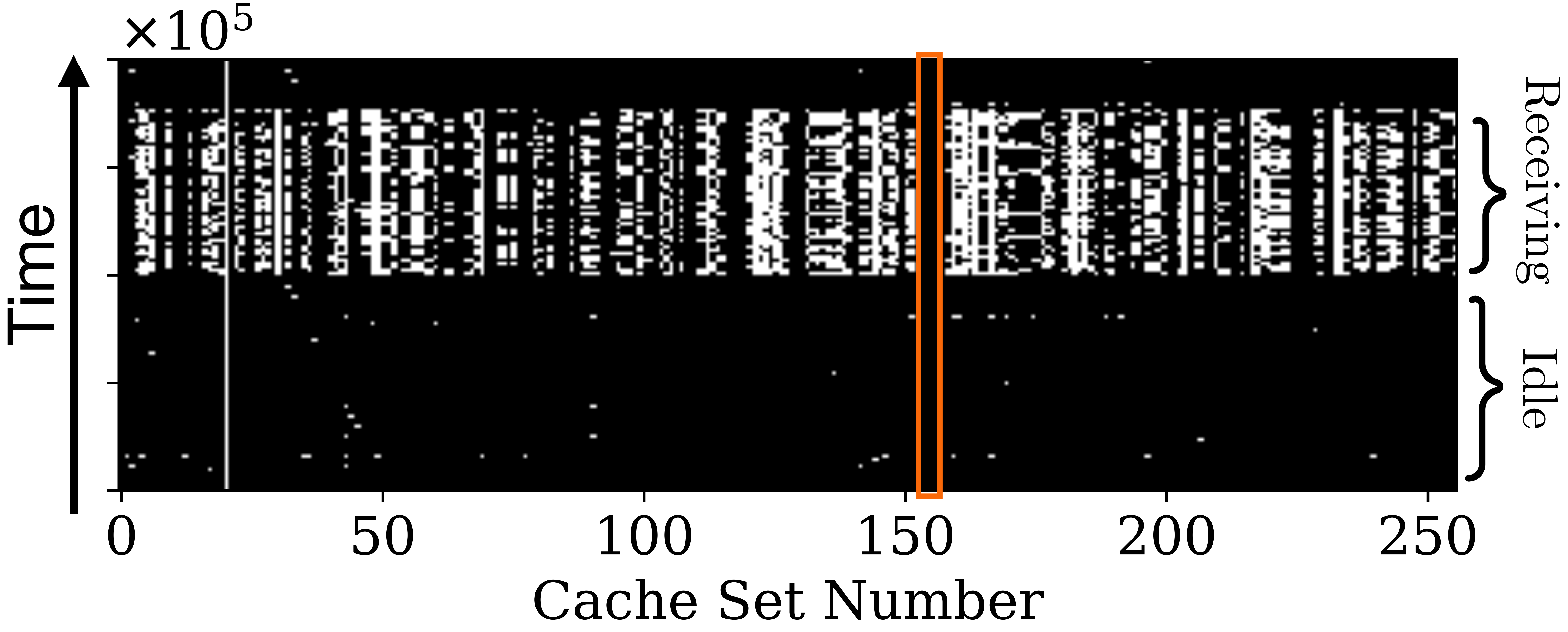
Too Slow to Gain Any Useful Information (~12 Million Cycles)

Ring Buffer Allocation



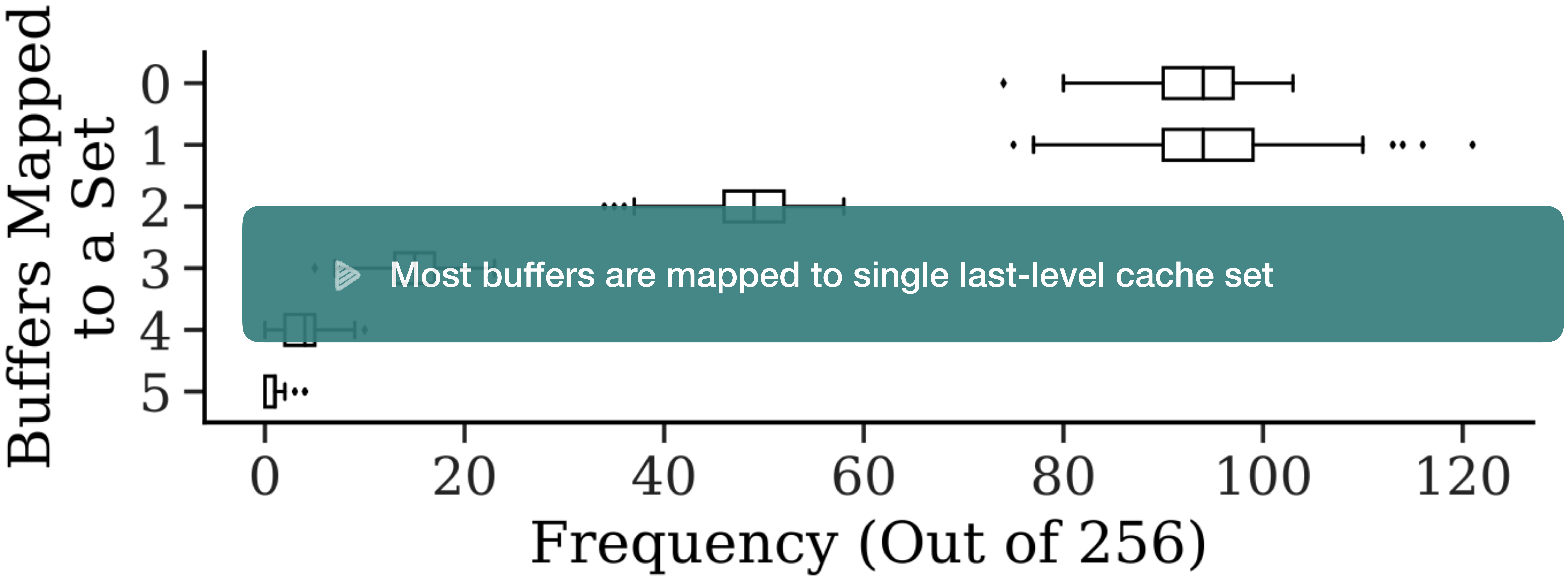
- Small Number of Buffers (256)
- Buffers Are Page-Aligned
- Reallocation Is Costly and Rare

Cache Footprint of Ring Buffer



White dot = detected activity on a set

Sets to Monitor



Most buffers are mapped to single last-level cache set

Detecting Packet Size

Probing First Block of Page-Aligned Buffers

🟧🟦🟦🟦

Probing Second Block of Page-Aligned Buffers

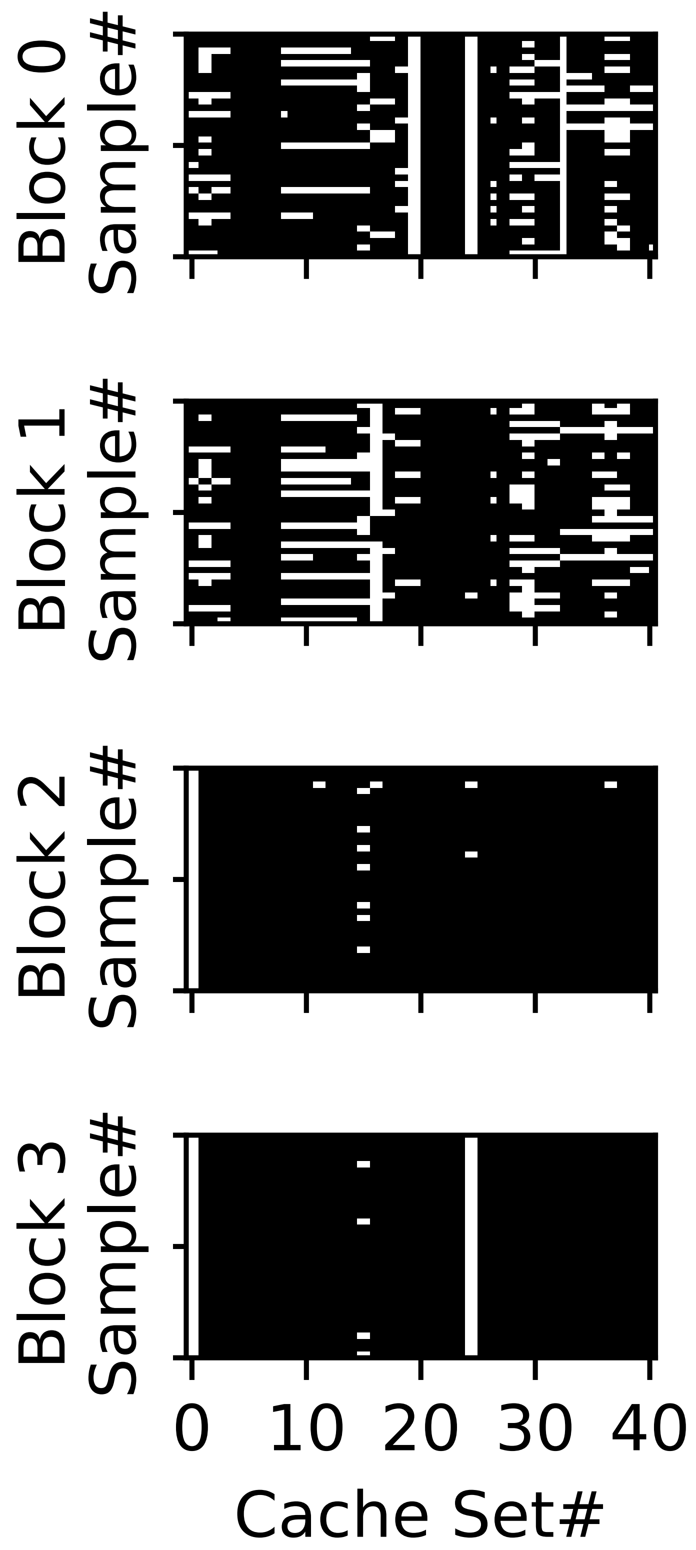
🟦🟧🟦🟦

Probing Third Block of Page-Aligned Buffers

🟦🟦🟧🟦

Probing Fourth Block of Page-Aligned Buffers

🟦🟦🟦🟧



2-Block Packets

Detected Activity on Block 0 and 1

No Activity on Block 2 and 3

} 2 Cache Blocks

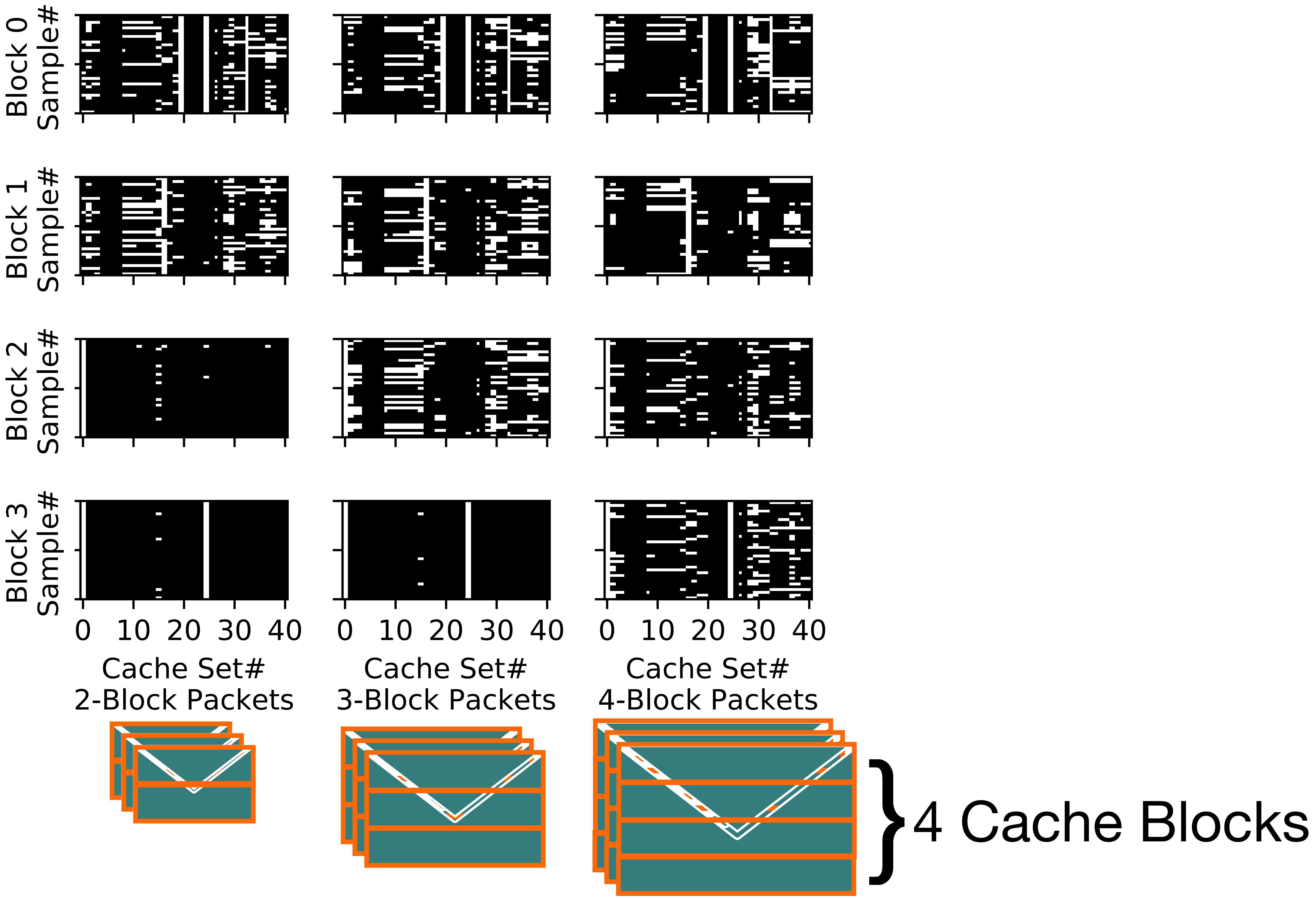
Detecting Packet Size

Probing First Block of Page-Aligned Buffers 🟧🟩🟩🟩

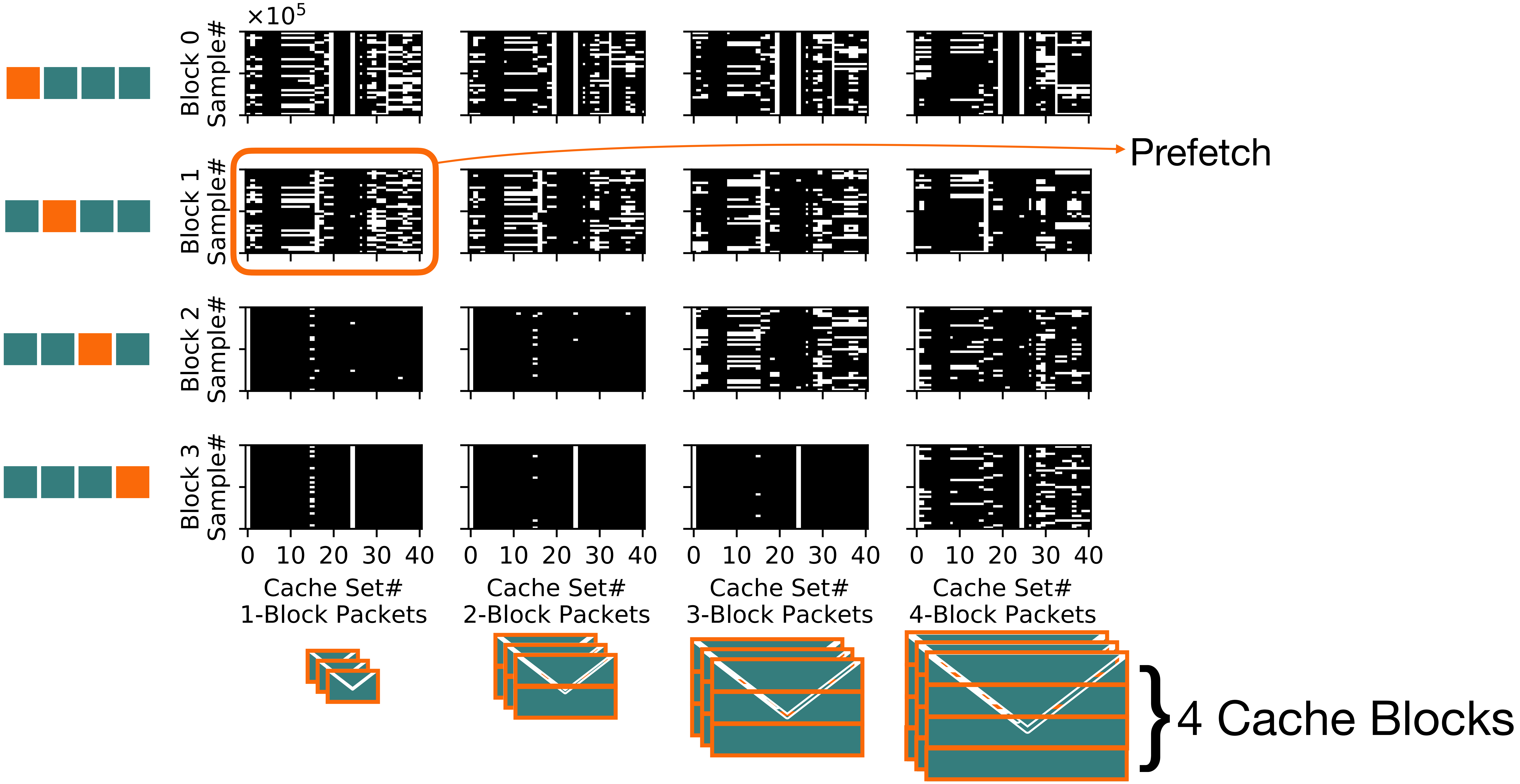
Probing Second Block of Page-Aligned Buffers 🟩🟧🟩🟩

Probing Third Block of Page-Aligned Buffers 🟩🟩🟧🟩

Probing Fourth Block of Page-Aligned Buffers 🟩🟩🟩🟧



Detecting Packet Size



Prefetch

4 Cache Blocks

How many sets do we need to probe?

No knowledge about packet buffer locations

Need to probe 16,384 sets

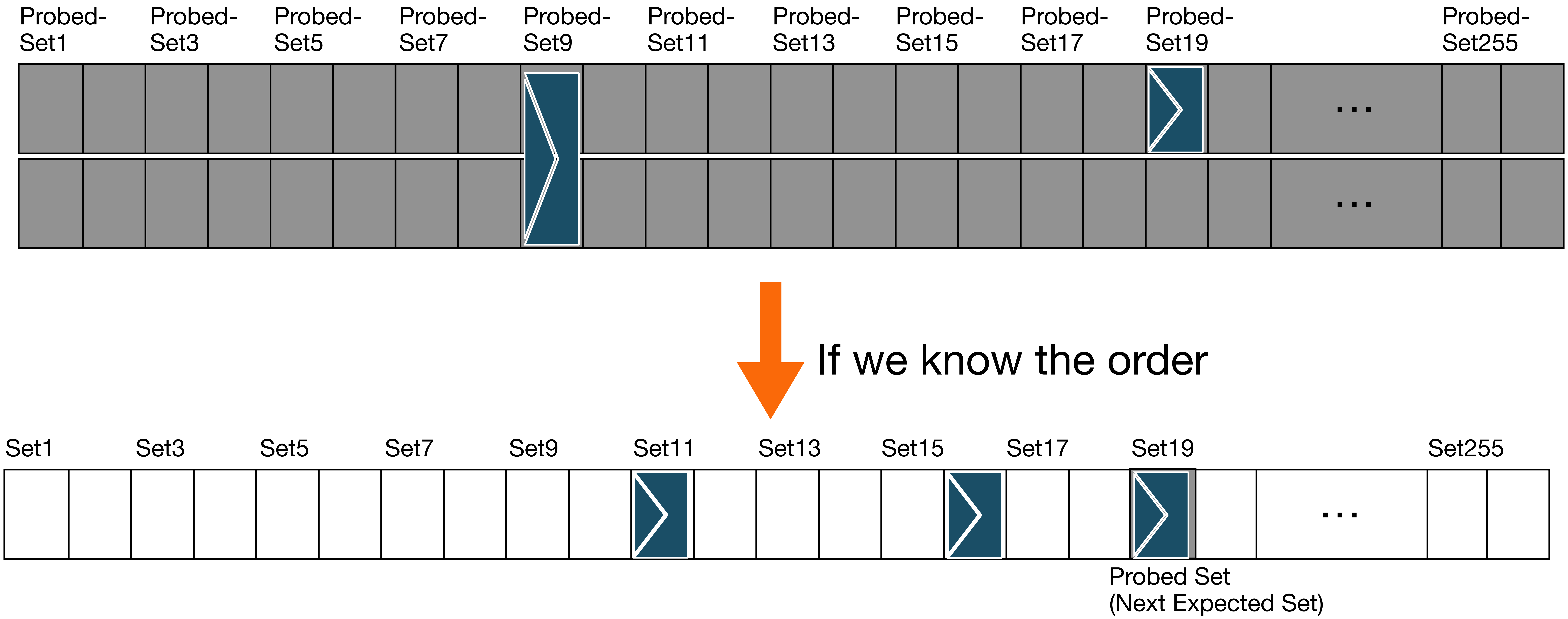
Know all packet buffers are page aligned

Need to probe 256 sets

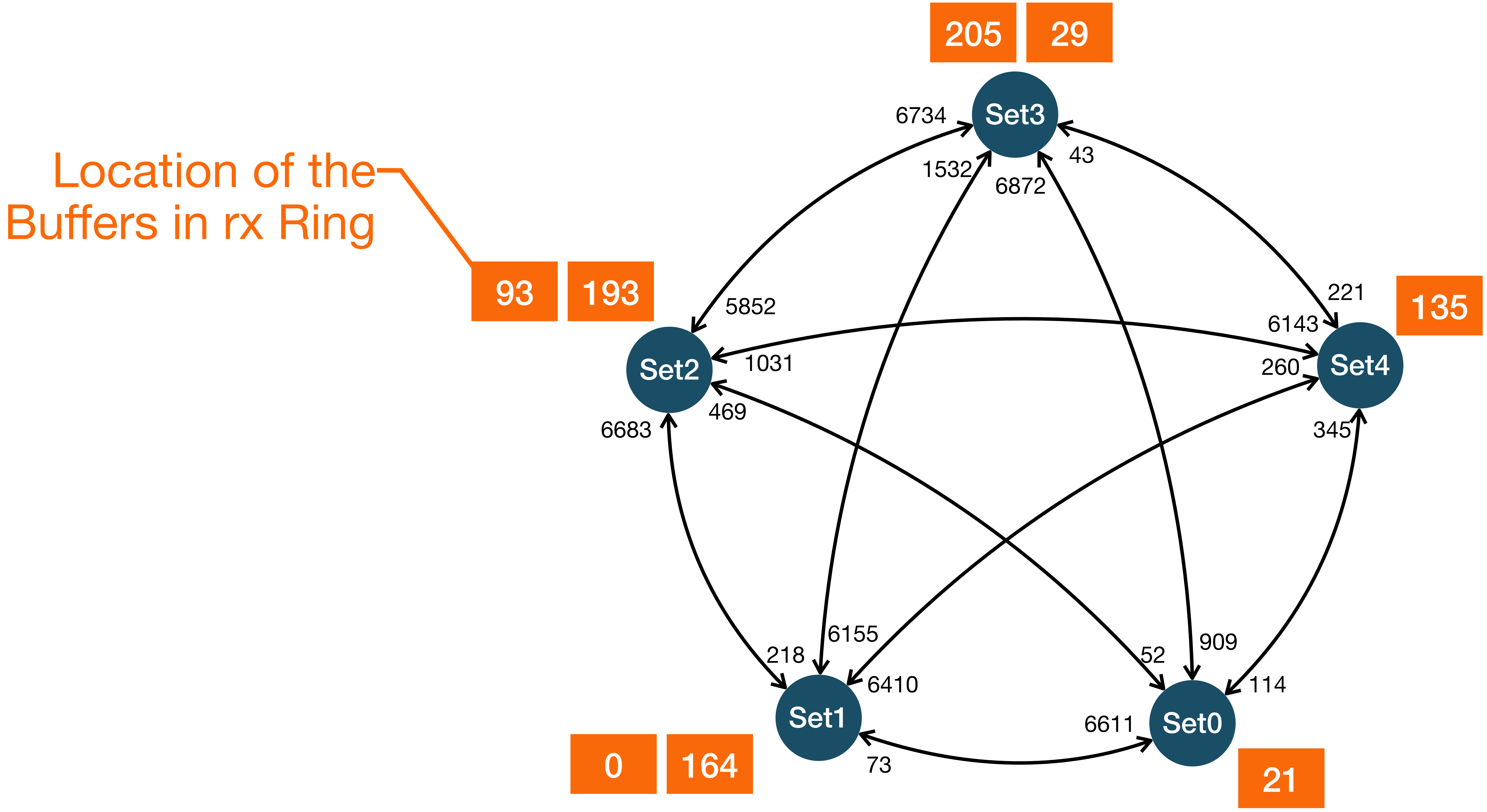
Know addresses and sequence order of all buffers

Need to probe 1 set

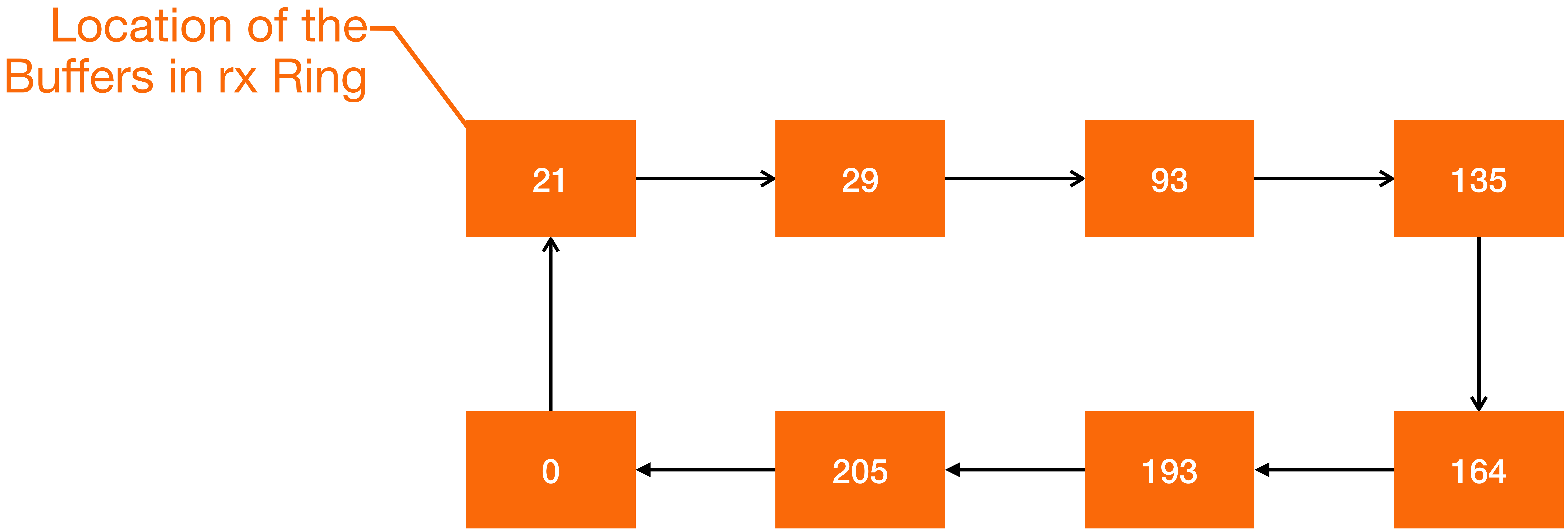
Chasing Packet over Cache



Finding the Order of Buffers

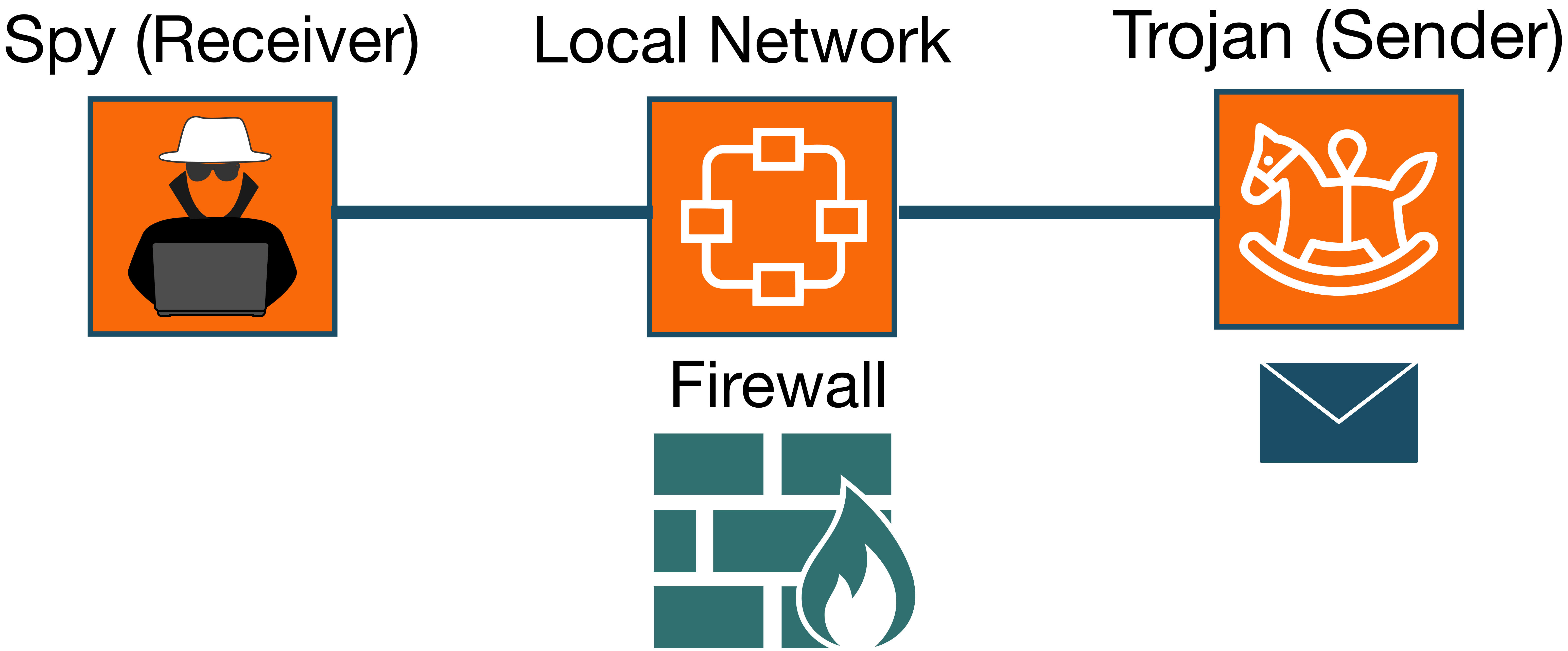


Finding the Order of Buffers

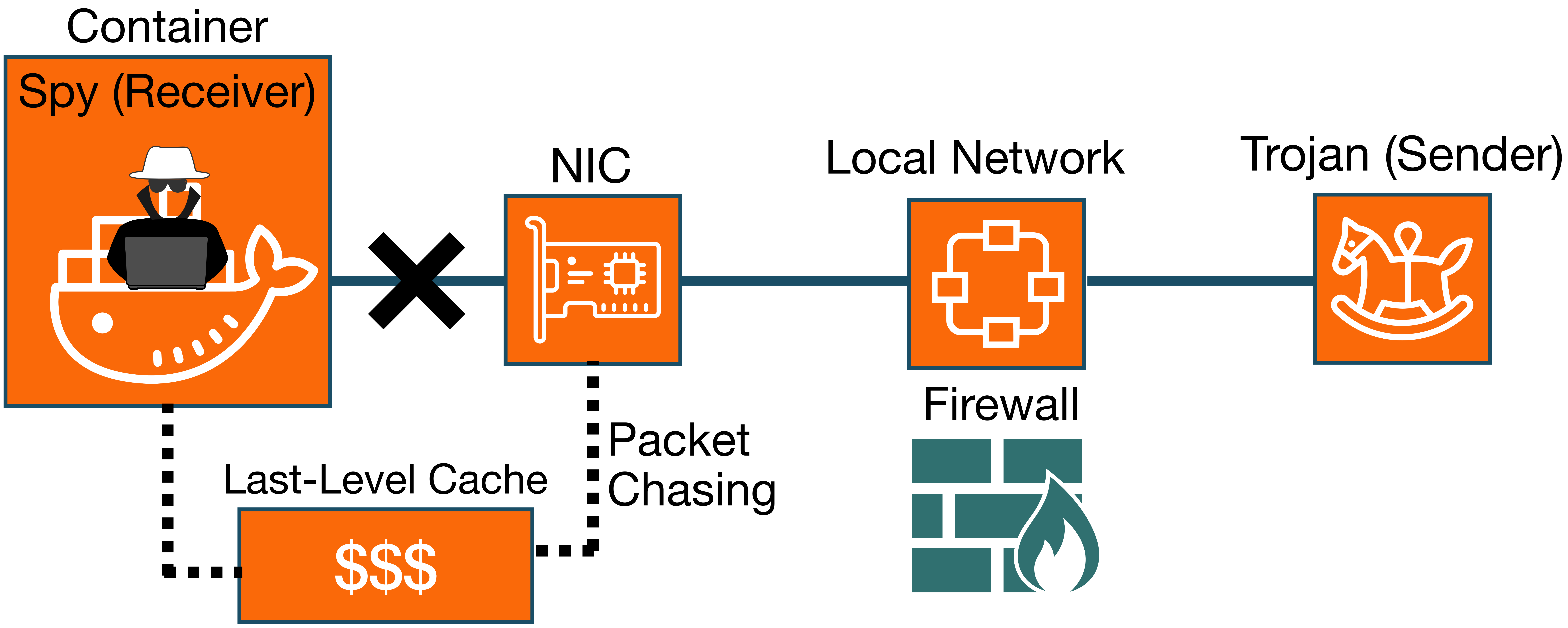


Packet Chasing can Recover the Order of Buffers with ~90% Accuracy

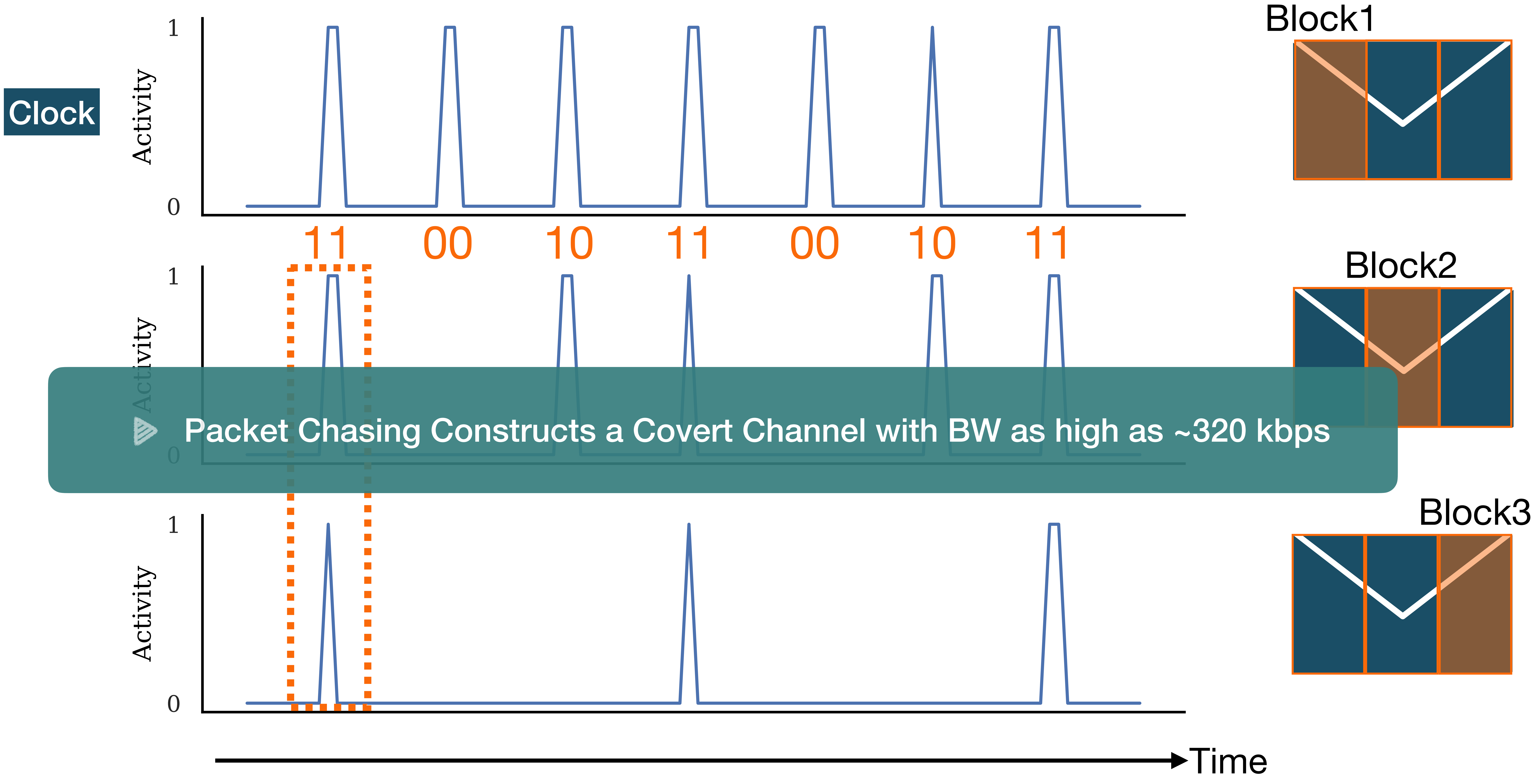
Receiving Packets without Network Access



Receiving Packets without Network Access



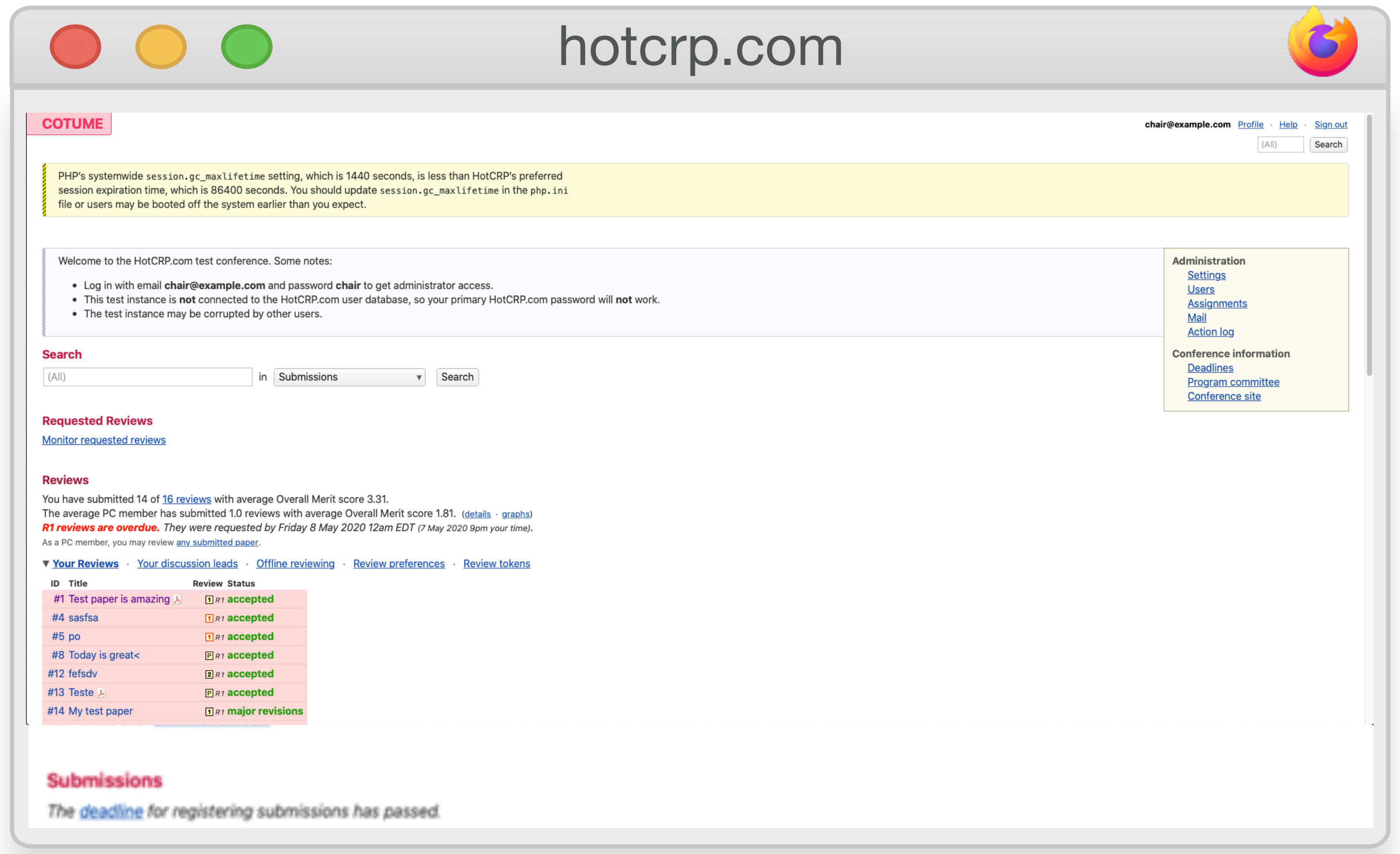
Encoding Covert Messages into Packet Size



Packet Chasing Constructs a Covert Channel with BW as high as ~320 kbps

Exploiting Packet Chasing for Web Fingerprinting

hotcrp.com*



PHP's systemwide `session.gc_maxlifetime` setting, which is 1440 seconds, is less than HotCRP's preferred session expiration time, which is 86400 seconds. You should update `session.gc_maxlifetime` in the `php.ini` file or users may be booted off the system earlier than you expect.

Welcome to the HotCRP.com test conference. Some notes:

- Log in with email **chair@example.com** and password **chair** to get administrator access.
- This test instance is **not** connected to the HotCRP.com user database, so your primary HotCRP.com password will **not** work.
- The test instance may be corrupted by other users.

Search

(All) in Submissions Search

Requested Reviews

Monitor requested reviews

Reviews

You have submitted 14 of 16 reviews with average Overall Merit score 3.31.
The average PC member has submitted 1.0 reviews with average Overall Merit score 1.81. (details · graphs)
R1 reviews are overdue. *They were requested by Friday 8 May 2020 12am EDT (7 May 2020 9pm your time).*
As a PC member, you may review any submitted paper.

▼ Your Reviews · Your discussion leads · Offline reviewing · Review preferences · Review tokens

ID	Title	Review	Status
#1	Test paper is amazing	1 R1	accepted
#4	sasfsa	1 R1	accepted
#5	po	1 R1	accepted
#8	Today is great<	P R1	accepted
#12	fefsdv	2 R1	accepted
#13	Teste	P R1	accepted
#14	My test paper	1 R1	major revisions

Submissions

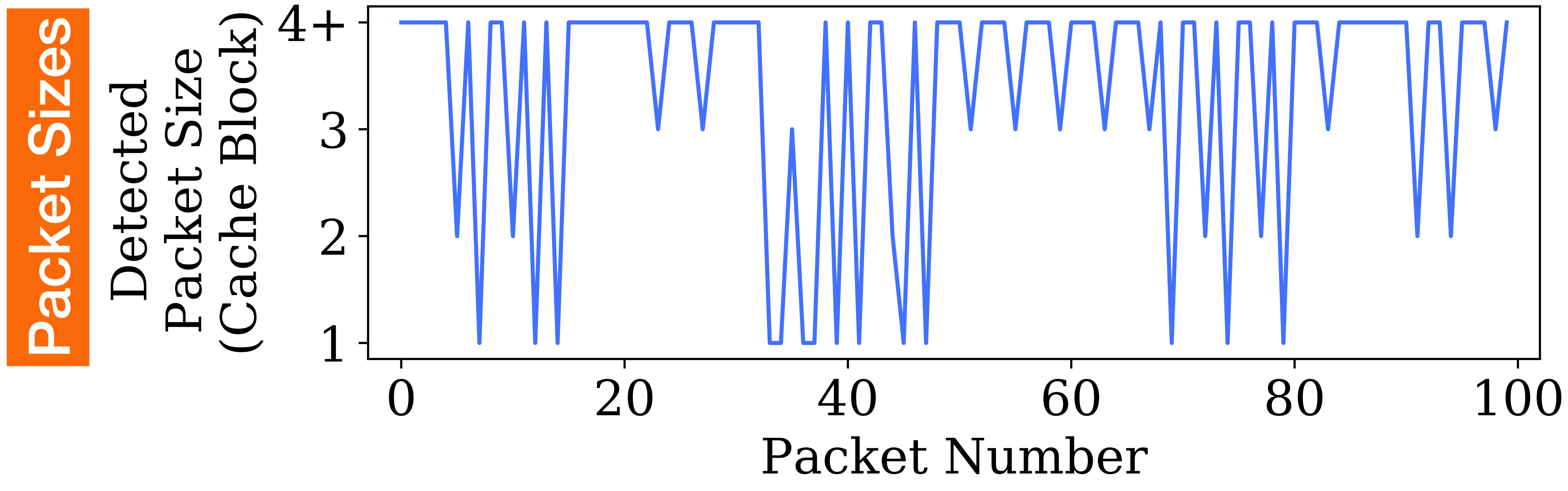
The deadline for registering submissions has passed.

Packet Chasing

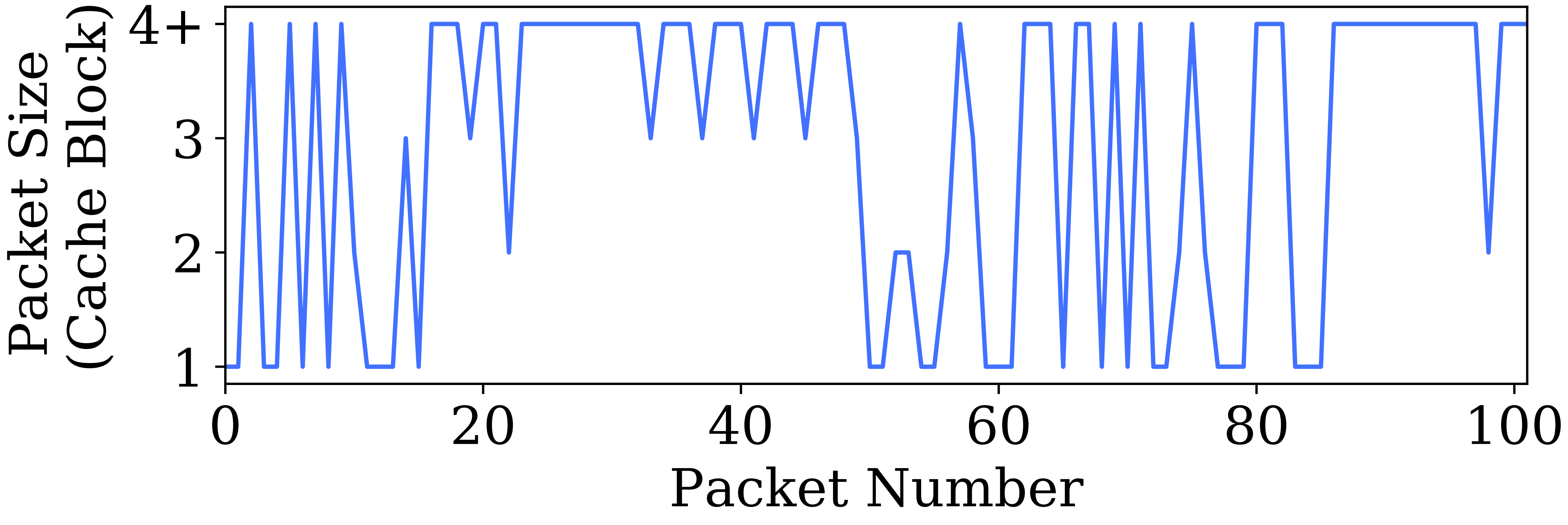
Successful Login Detected

*This is just an example website and the attack is not limited to hotcrp

Website Fingerprinting Attack

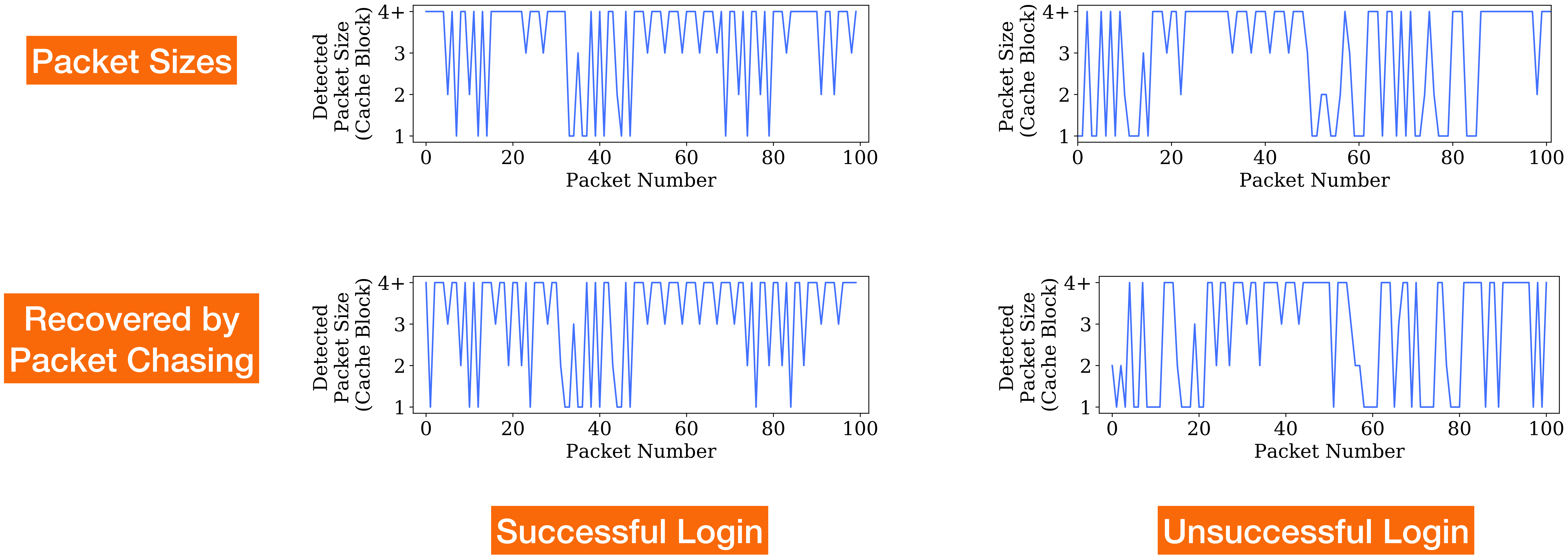


Successful Login



Unsuccessful Login

Website Fingerprinting Attack



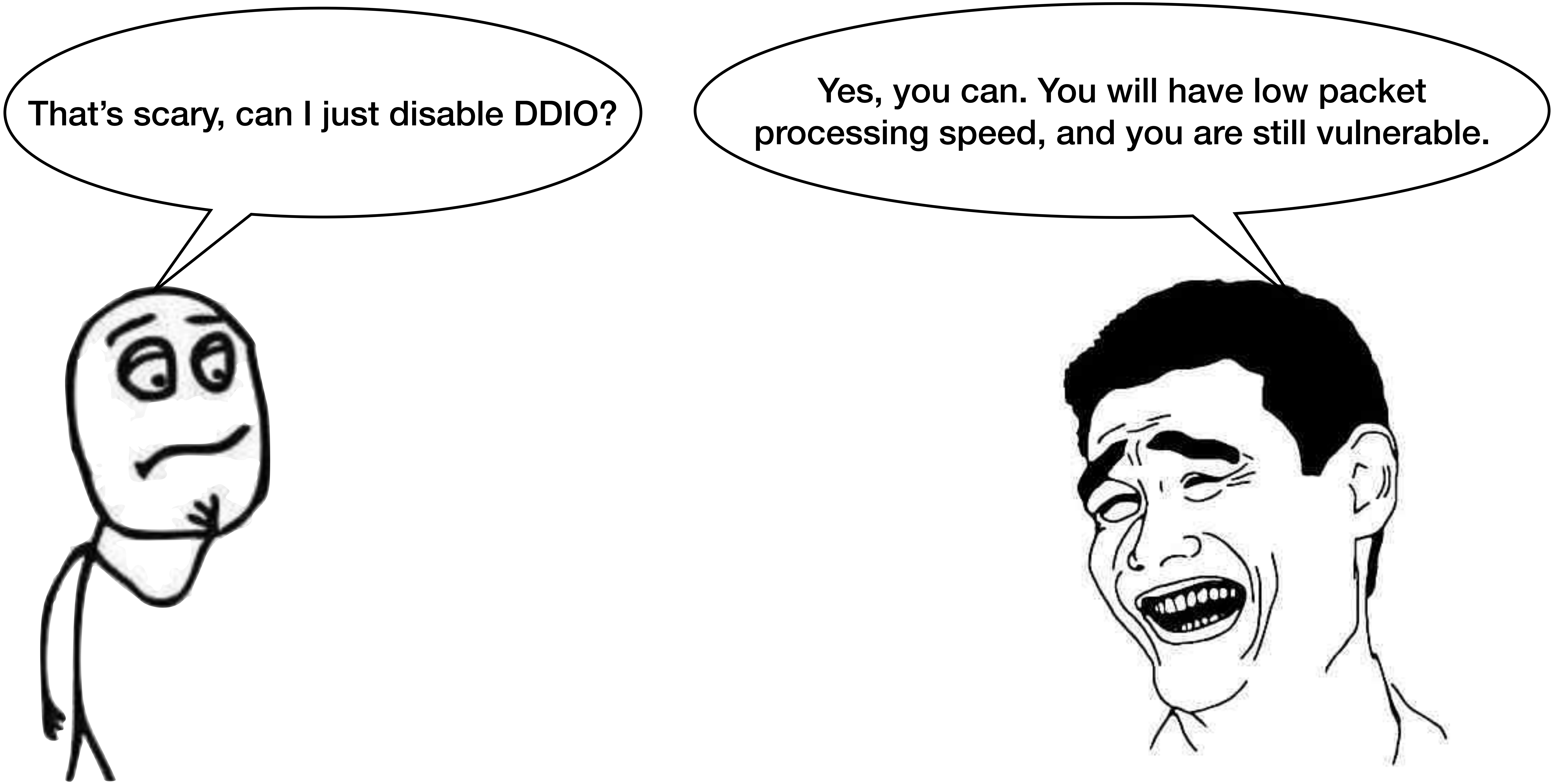
Packet Sizes

Recovered by Packet Chasing

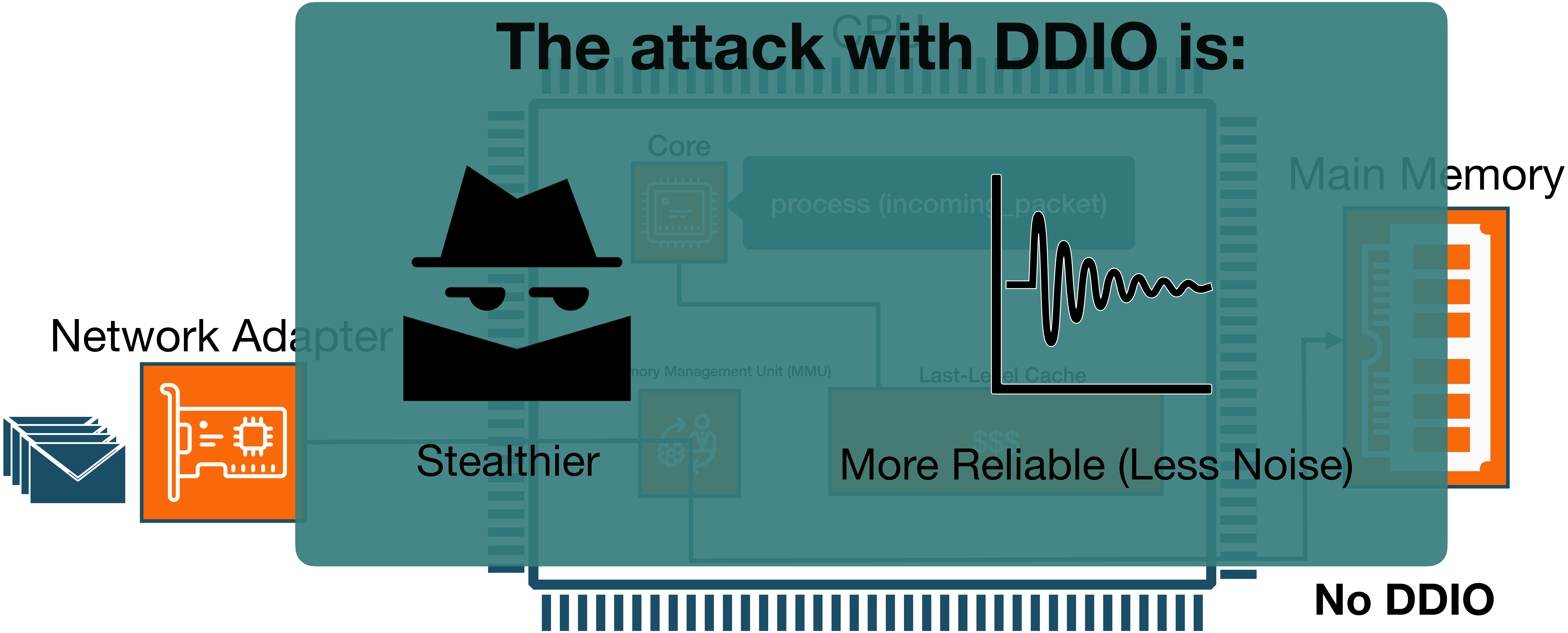
Successful Login

Unsuccessful Login

Disabling DDIO as a Mitigation?


That’s scary, can I just disable DDIO?
Yes, you can. You will have low packet processing speed, and you are still vulnerable.

Disabling DDIO as a Mitigation?



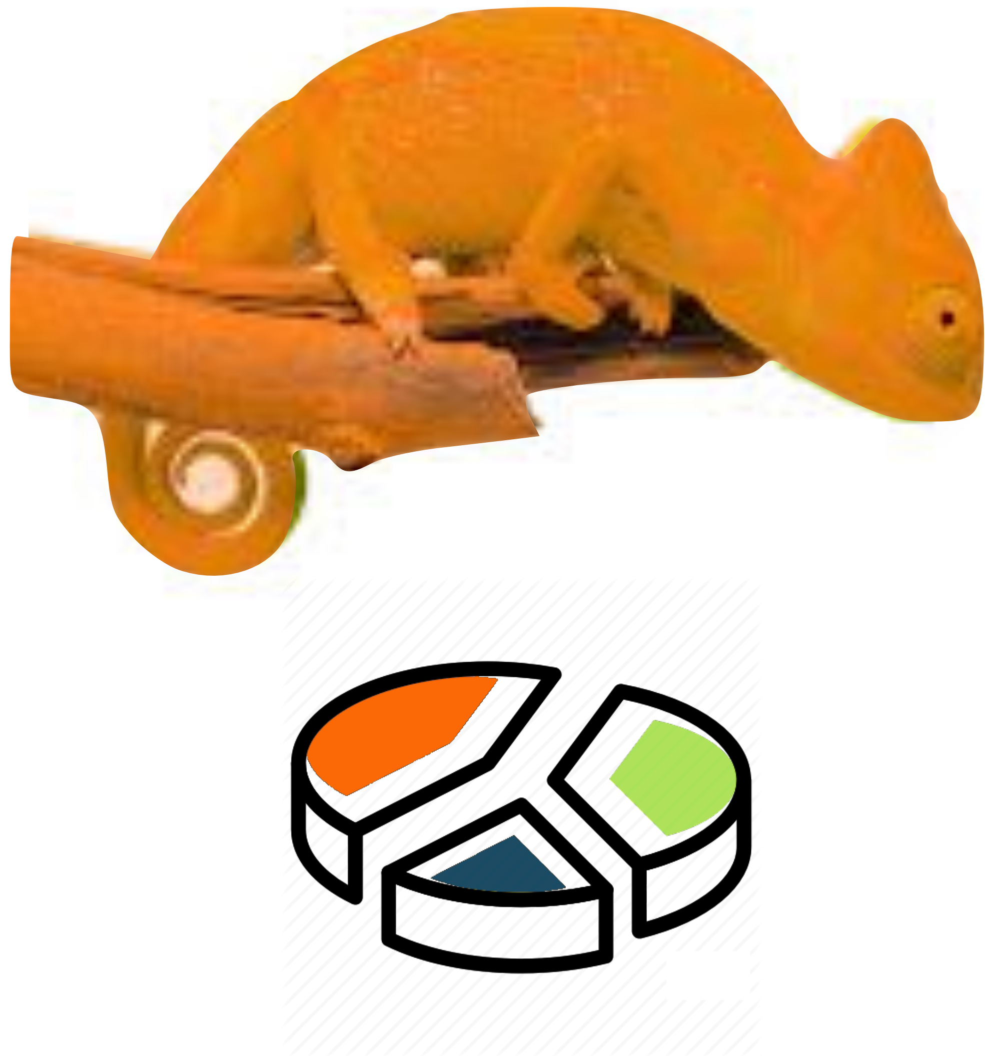
The attack with DDIO is:

Stealthier

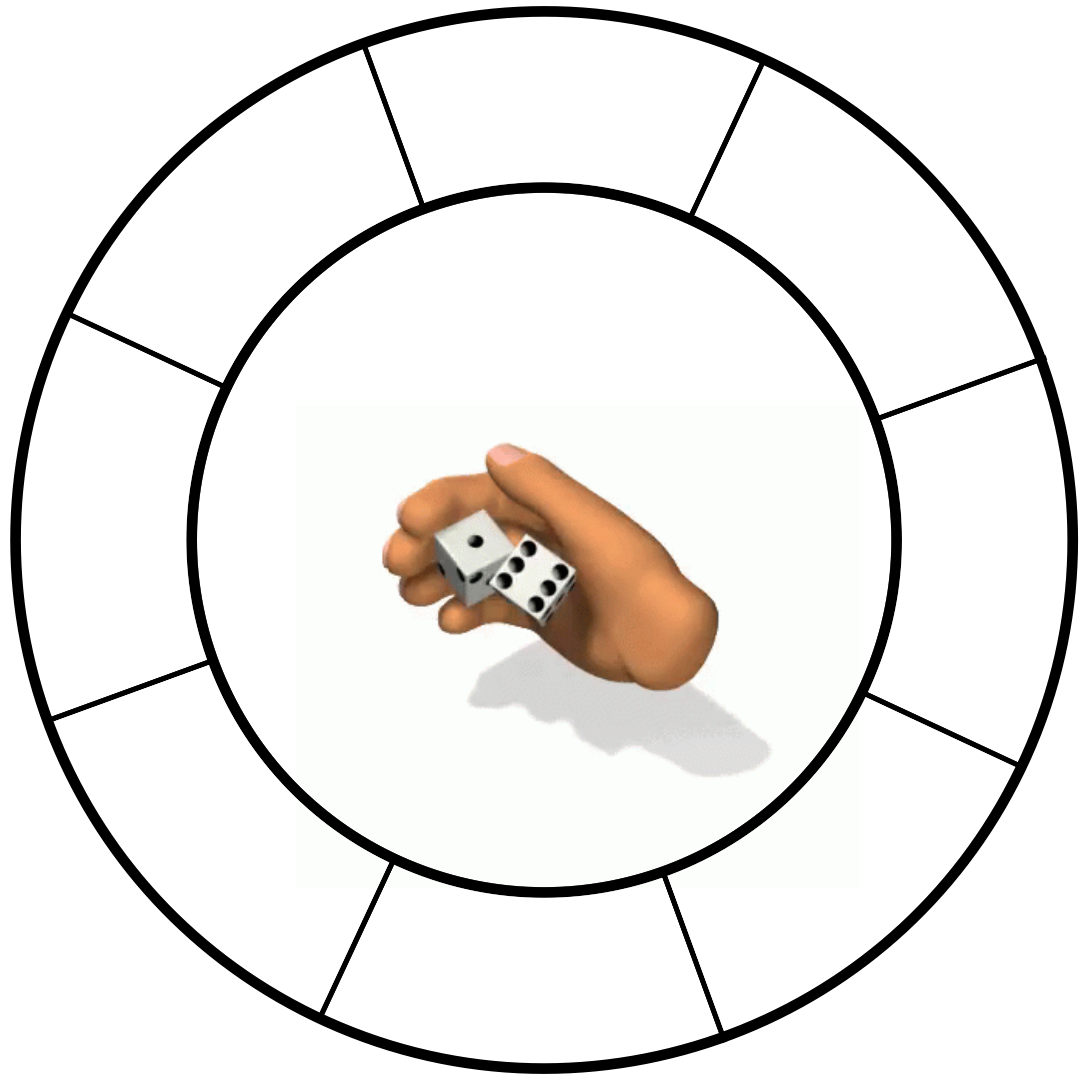
More Reliable (Less Noise)

No DDIO

Packet Chasing: Overview of Defenses

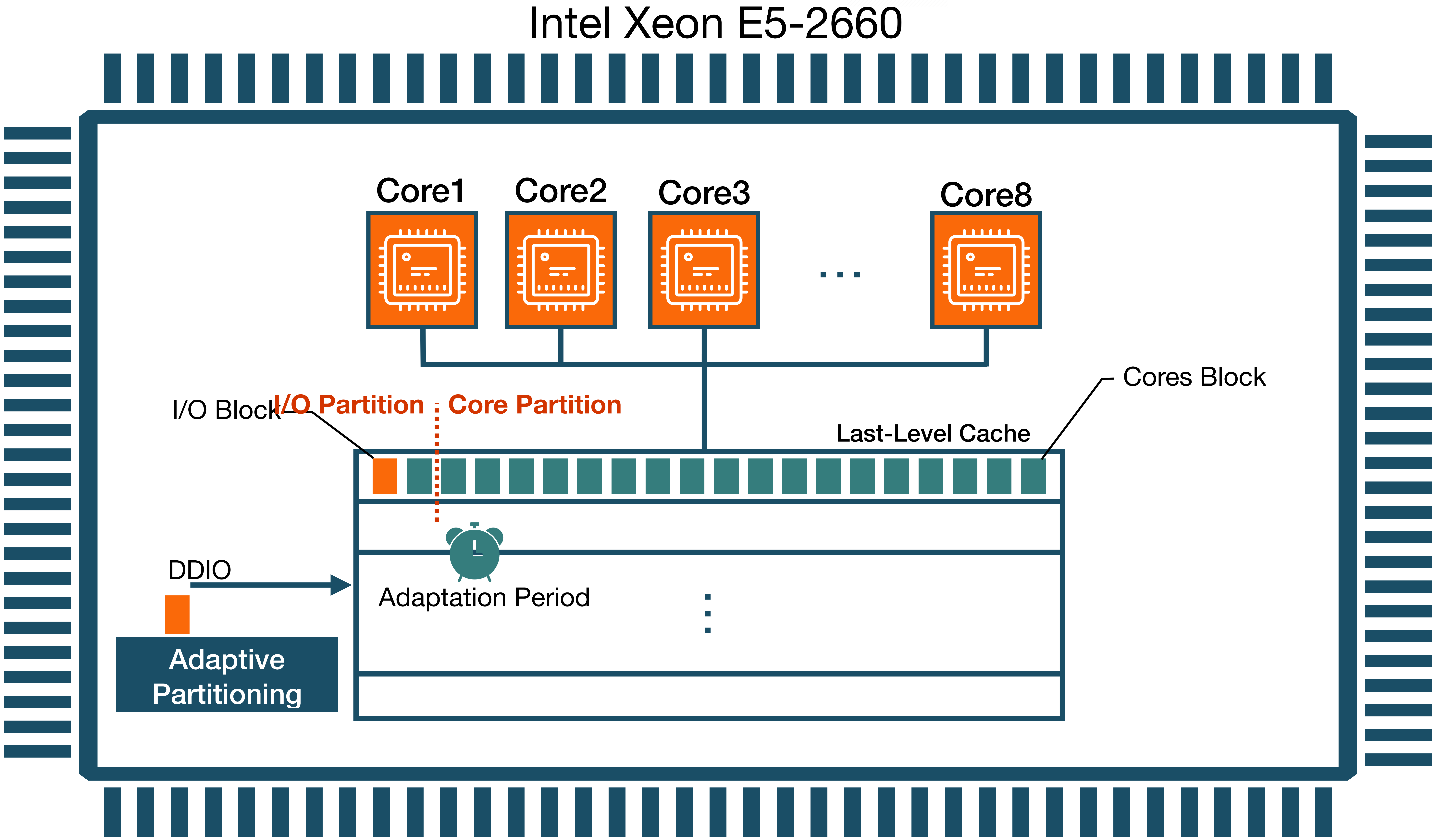


Adaptive Partitioning

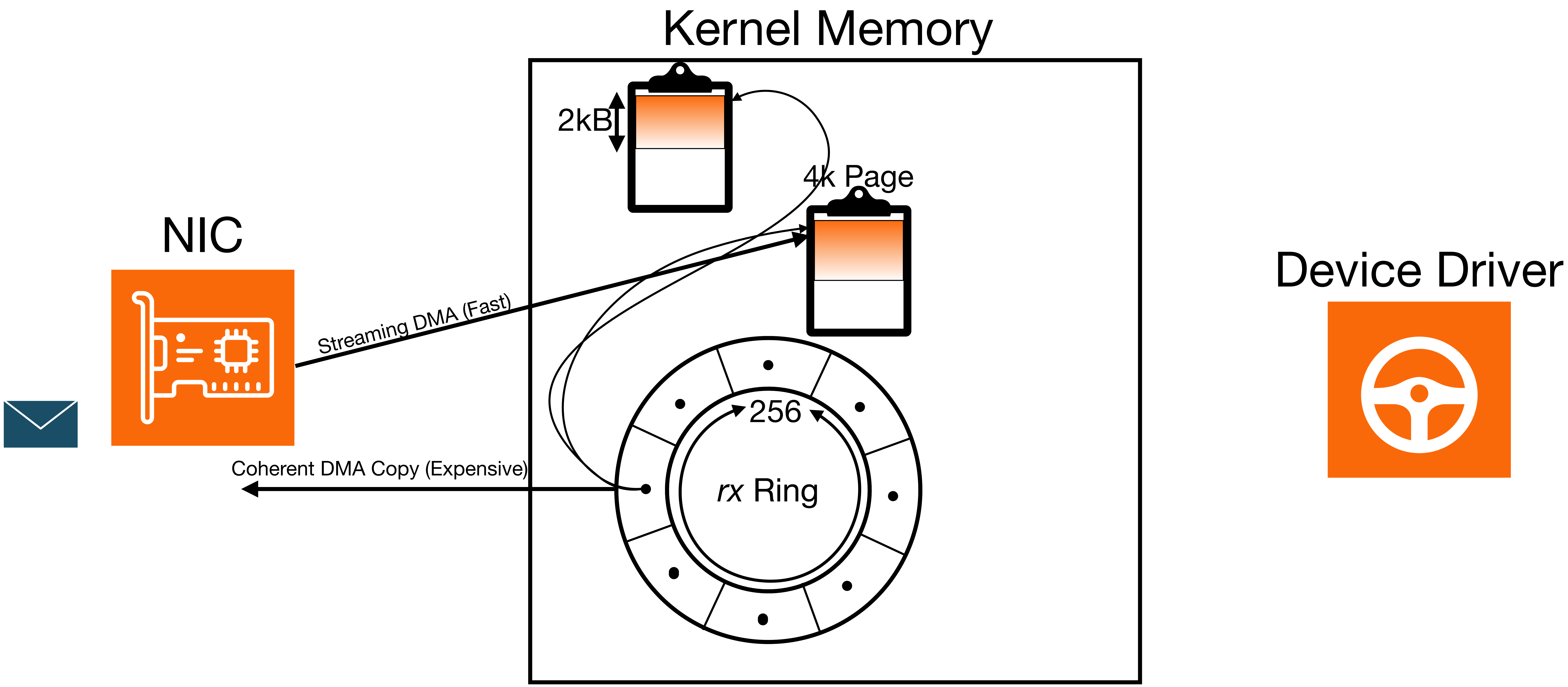


Ring Buffer Randomization

Adaptive Partitioning

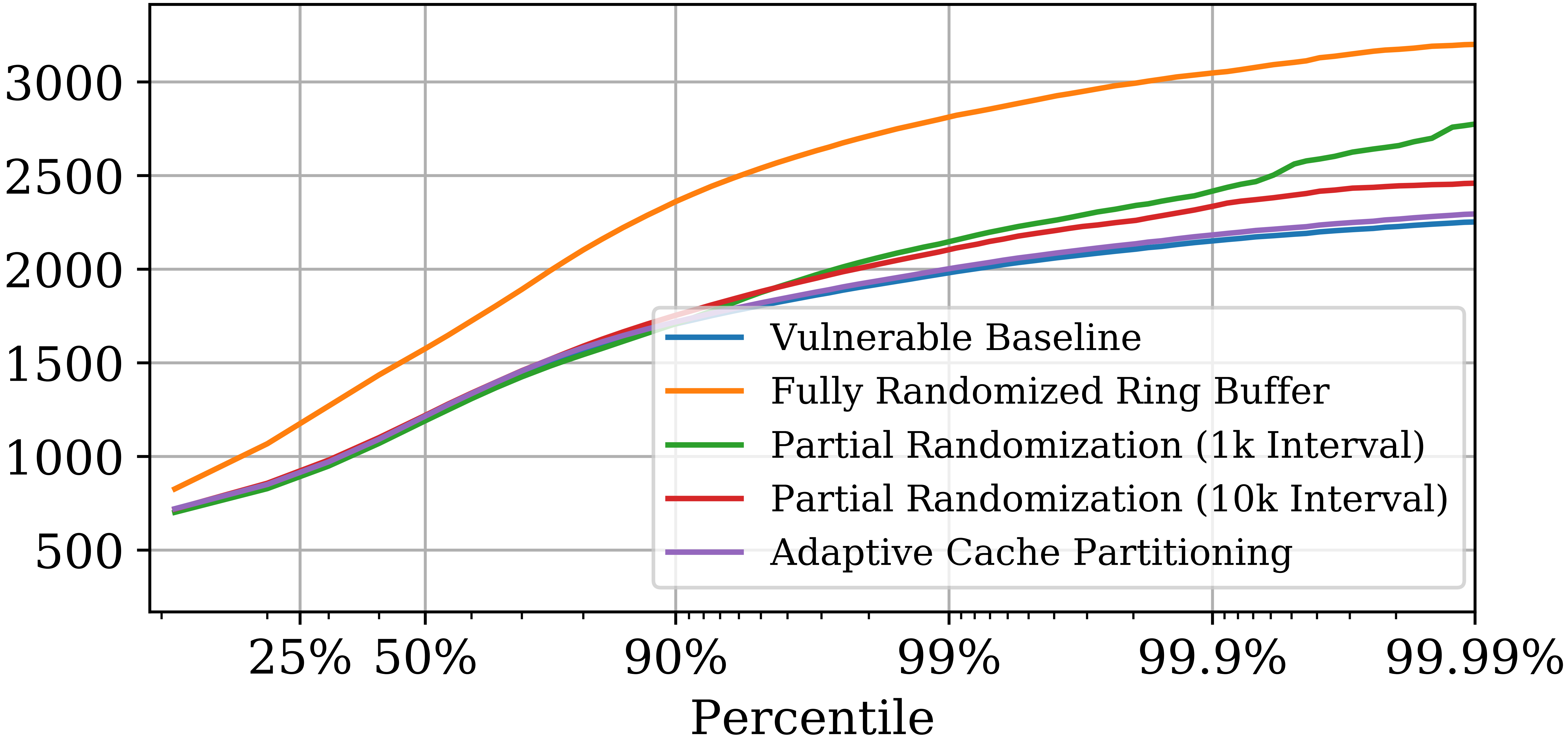


Ring Buffer Randomization



Performance Results

Latency of HTTP
Requests to the Nginx
Web Server (ms)



Conclusion

- Packet Chasing is an attack on the network that doesn’t need access to the network
- High resolution covert and side channel attacks on the network I/O traffic
- While possible without DDIO, attacks are considerably more effective in the presence of DDIO
- Adaptive Partitioning is proposed as a low-overhead hardware mitigation
- Ring Buffer Randomization is proposed as a software-based short-term mitigation