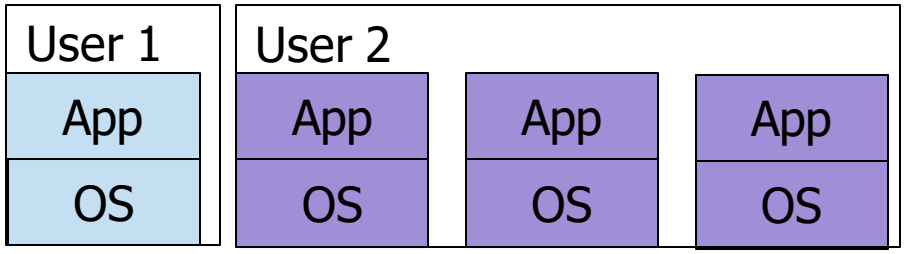
Cyclone: Detecting Contention-Driven Attacks via Cyclic Interference

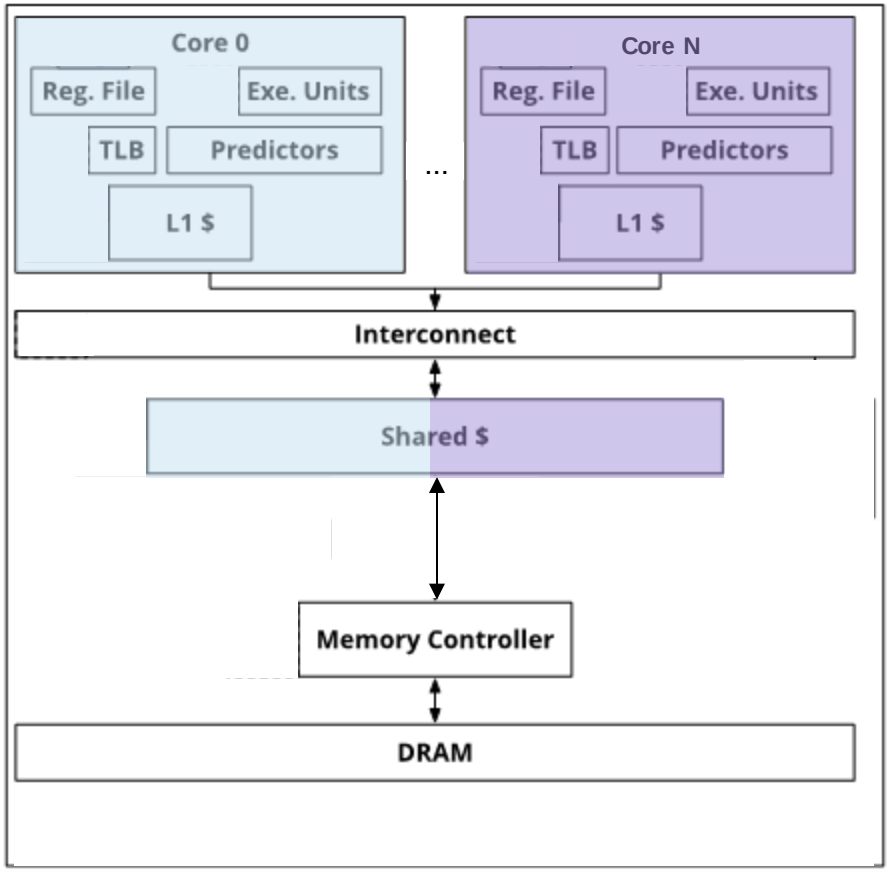
Austin Harris*, Shijia Wei*, Prateek Sahu, Pranav Kumar, Todd Austin[1], Mohit Tiwari
University of Texas at Austin, [1]University of Michigan Ann Arbor

The University of Texas at Austin
Electrical and Computer Engineering
Cockrell School of Engineering

Sharing Resource Across Security Domains

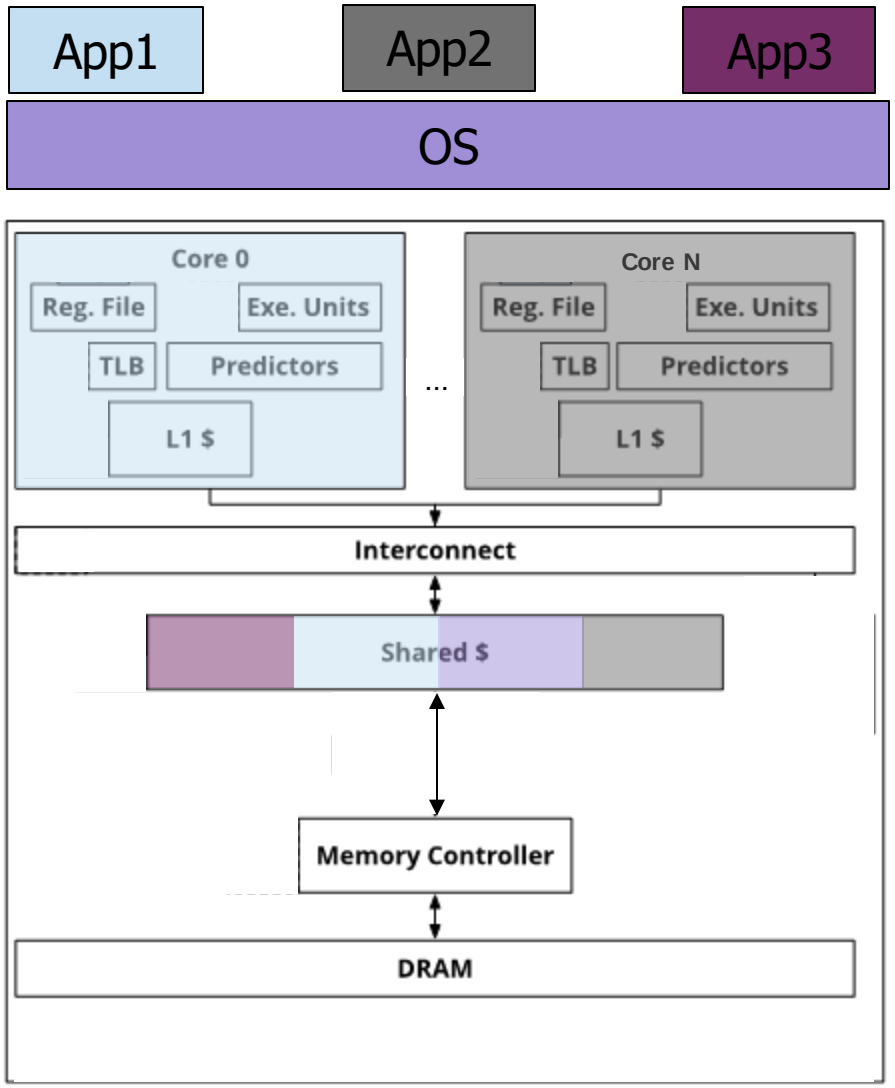
- Security domains
  - Virtual machines on the public cloud





Sharing Resource Across Security Domains

- Security domains
  - Virtual machines on the public cloud
  - Processes in a shared machine

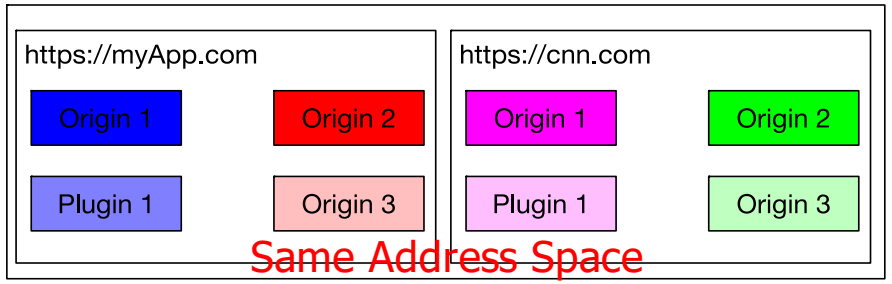


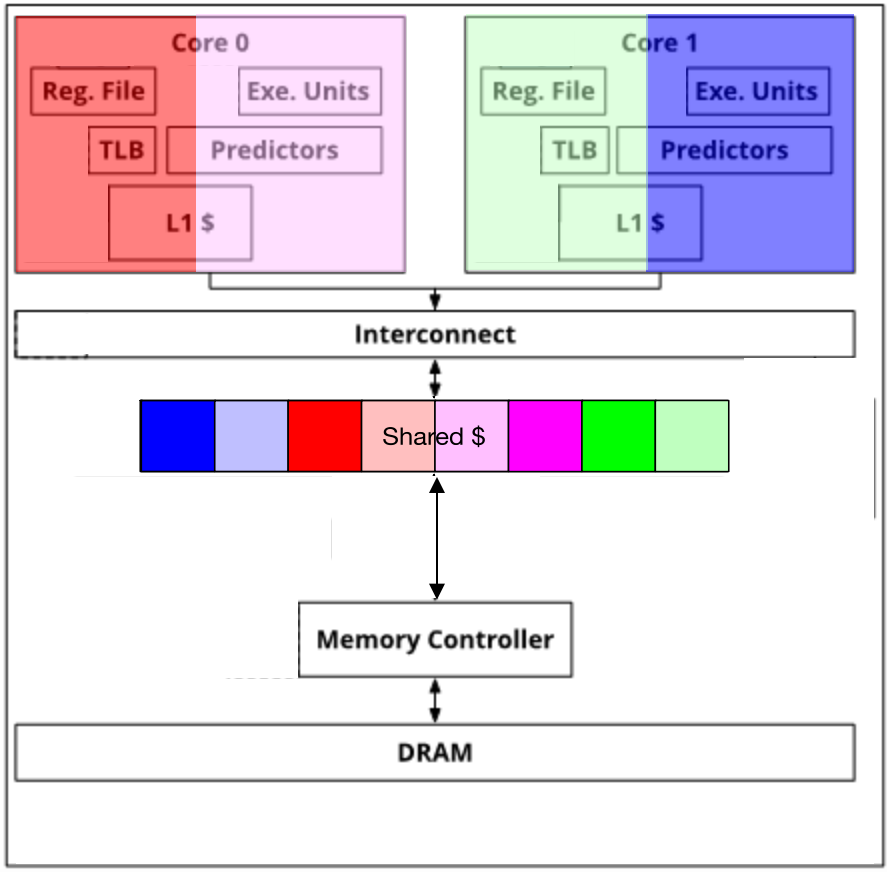
Sharing Resource Across Security Domains

The University of Texas at Austin
Electrical and Computer Engineering
Cockrell School of Engineering

- Security domains
  - Virtual machines on the public cloud
  - Processes in a shared machine
  - Sandboxes in a browser

- Partitioning/flushing can be expensive





Interference

- Interference is root of many micro-arch attacks [Hunger *et al.* HPCA'15, Wang *et al.* ISCA'17, …]

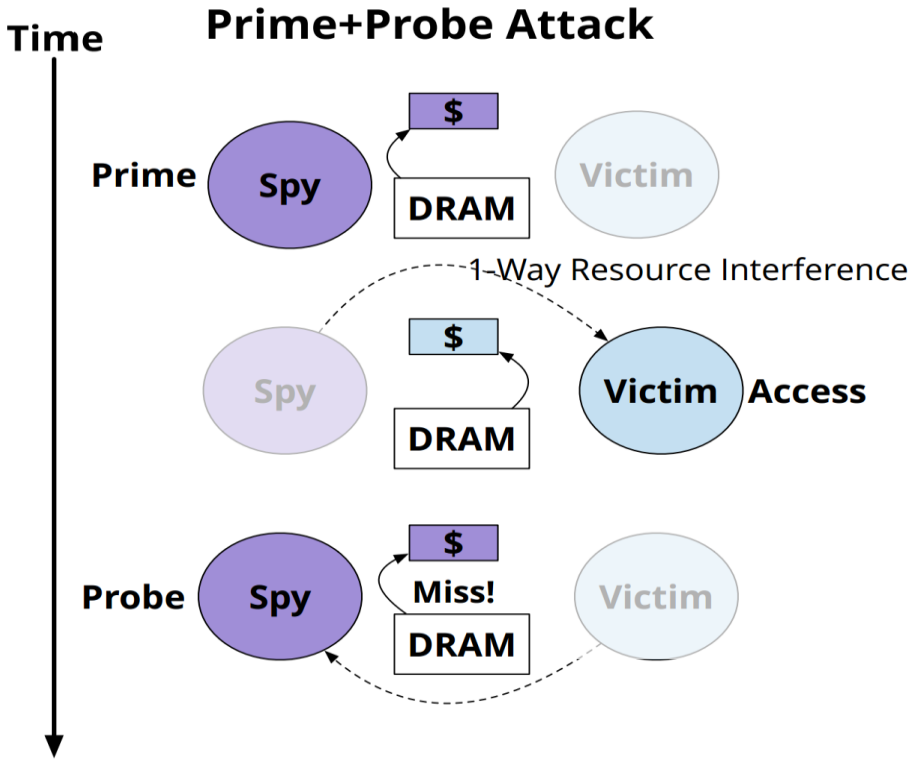
Attack Types

- Prime+Probe
- Flush+Reload
- Evict+Reload

X

Resources

- Caches
- TLBs
- Predictors
- Queues
- Memory



Interference

- Interference is root of many micro-arch attacks [Hunger *et al.* HPCA'15, Wang *et al.* ISCA'17, …]

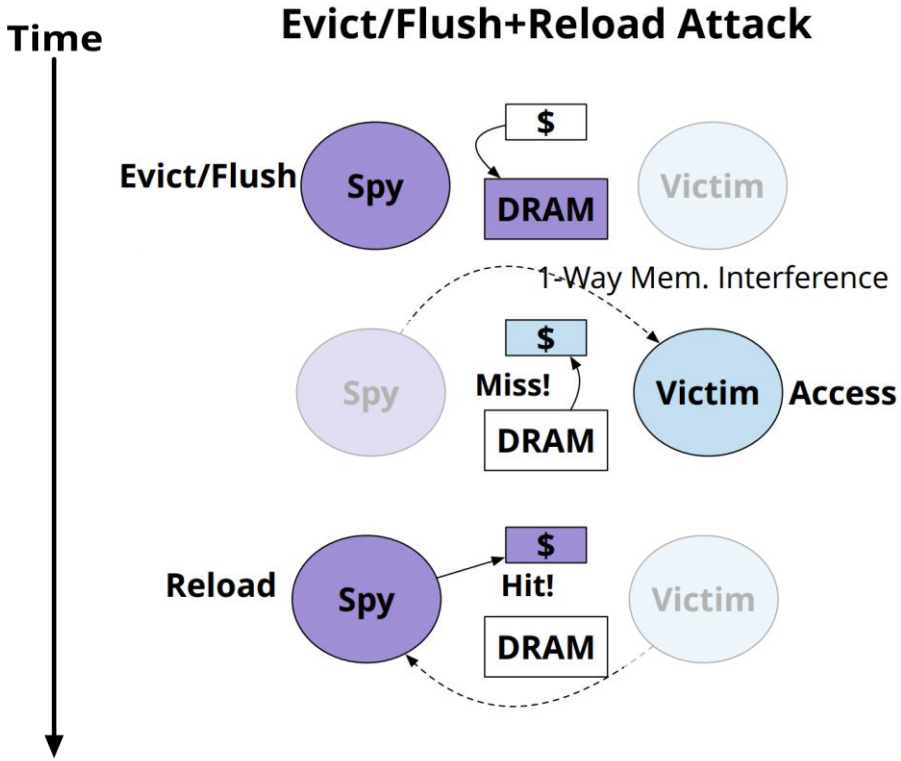
Attack Types

- Prime+Probe
- Flush+Reload
- Evict+Reload

X

Resources

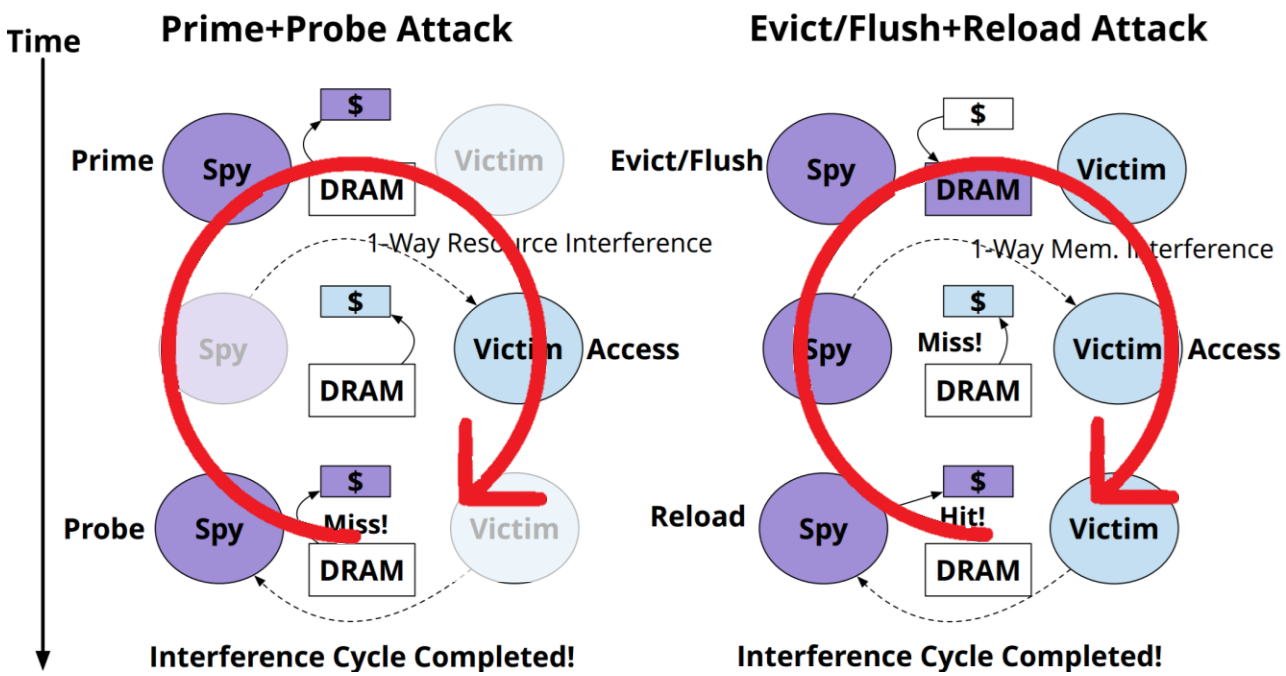
- Caches
- TLBs
- Predictors
- Queues
- Memory



Cyclic Interference

The University of Texas at Austin
Electrical and Computer Engineering
Cockrell School of Engineering

- Interference is root of many micro-arch attacks [Hunger *et al.* HPCA'15, Wang *et al.* ISCA'17, …]

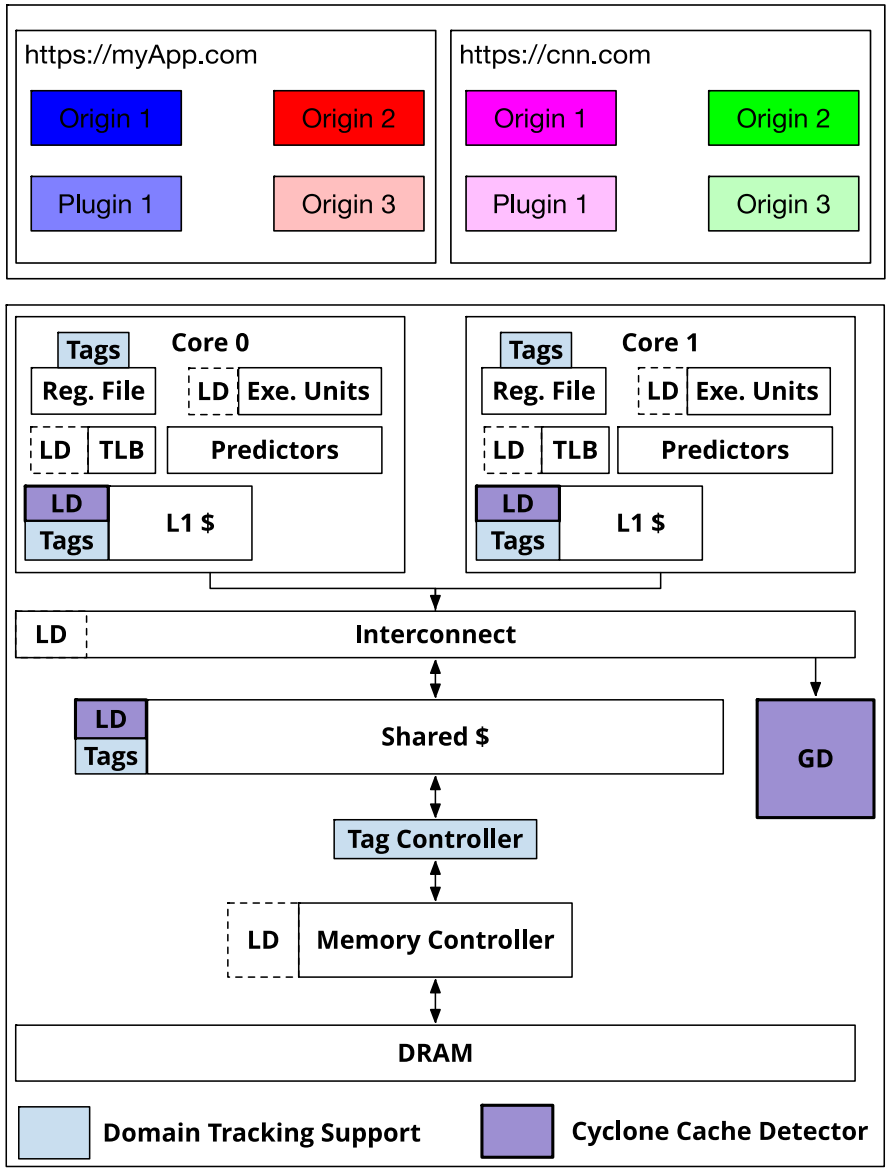


- Cyclic Interference is a robust feature
  - Opportunity: detect attacks as anomalous cyclic interference

Cyclone Architecture

The University of Texas at Austin
Electrical and Computer Engineering
Cockrell School of Engineering

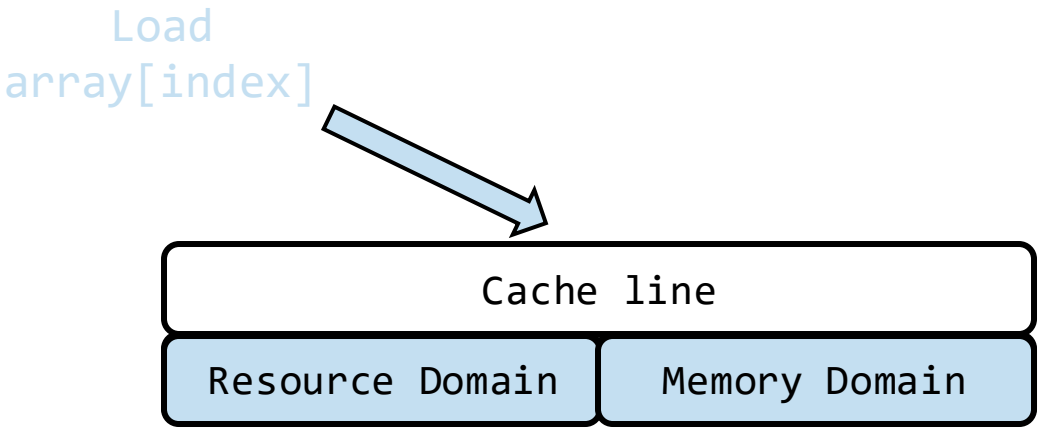
- Software defined security domains
  - OS kernel, Sandbox engine (e.g. browser)
  - Micro-arch Info. Flow Tracking
- Configurable Local Detectors (LDs) for each µarch component
  - Non-Invasive, snooping
  - Track cyclic interference
  - Simple logic (e.g. thresholding)
- Programmable Global Detector (GD)
  - Off the critical path, programmable
  - Correlates across components
- Domain propagation
  - Memory locations, hardware resource
  - Speculative

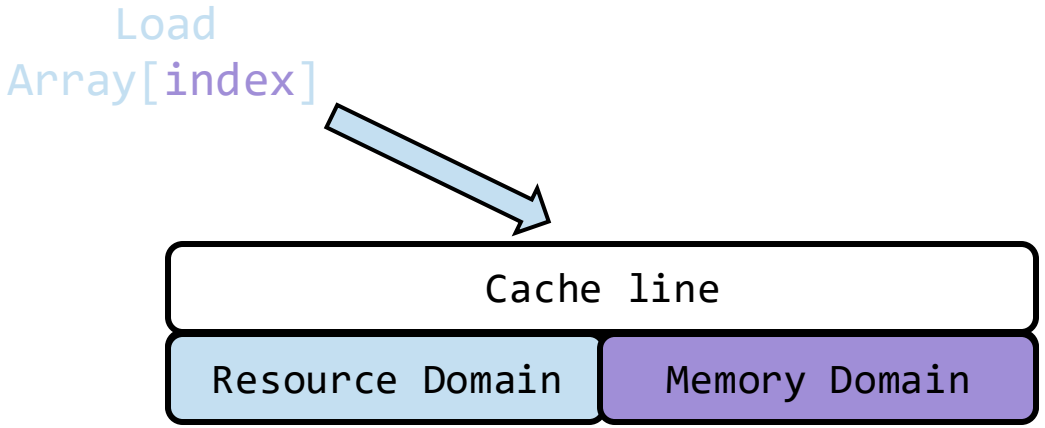


Domain Propagation in the microarchitecture

The University of Texas at Austin
Electrical and Computer Engineering
Cockrell School of Engineering

- Resource Domain and Memory Domain to track two types of interference
  - Cyclic Resource Interference (CRI)
  - Cyclic Memory Interference (CMI)
- Propagate domains in the microarchitecture based on access initiator and addressor
  - accessed by an unclassified domain?
  - accessed by an unclassified domain but indexed with classified inputs?



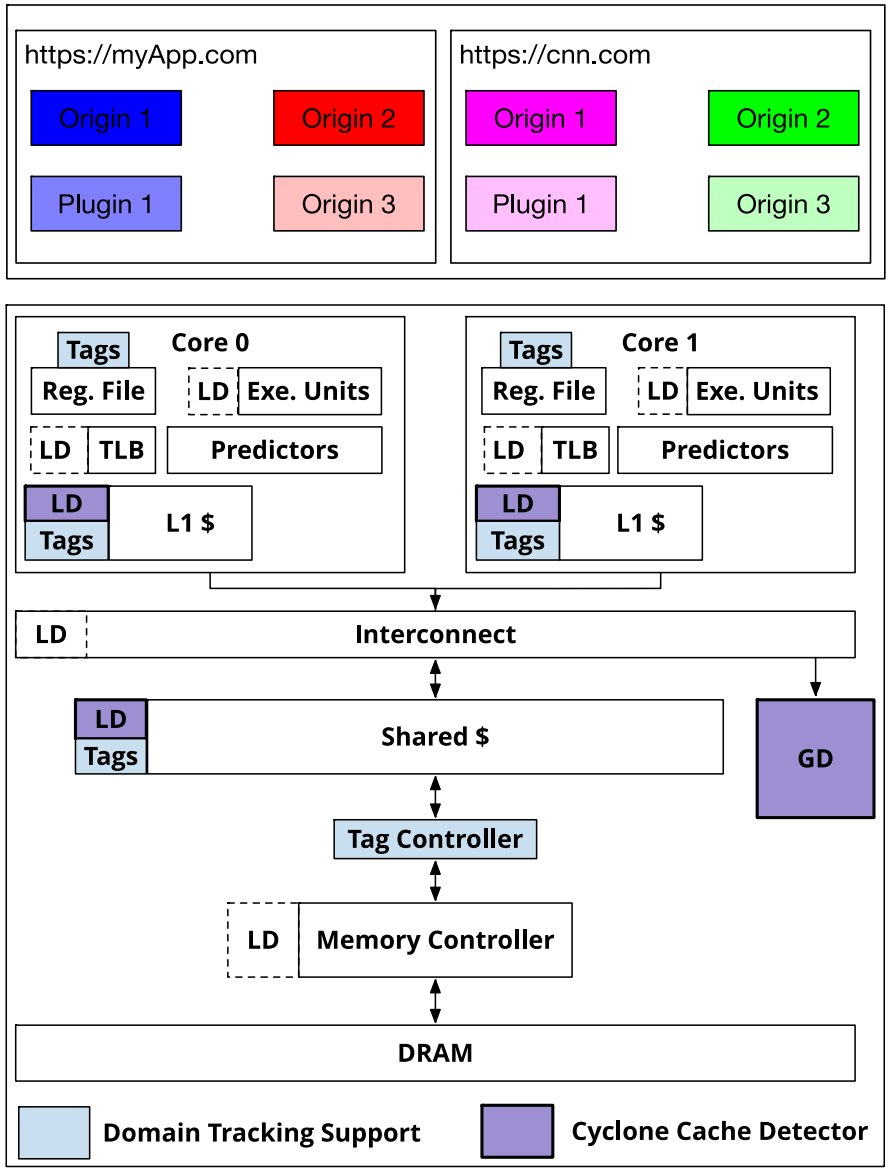


- Downgrade register domains on committed store operations

Cyclone Architecture

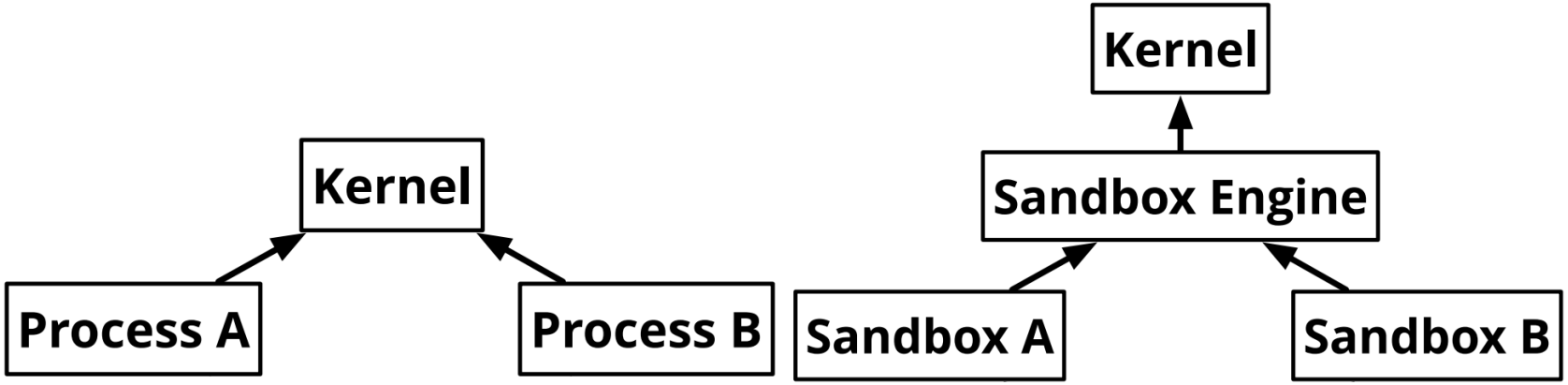
The University of Texas at Austin
Electrical and Computer Engineering
Cockrell School of Engineering

- Software defined security domains
  - OS kernel, Sandbox engine (e.g. browser)
  - Micro-arch Info. Flow Tracking
- Configurable Local Detectors (LDs) for each µarch component
  - Non-Invasive, snooping
  - Track cyclic interference
  - Simple logic (e.g. thresholding)
- Programmable Global Detector (GD)
  - Off the critical path, programmable
  - Correlates across components
- Domain propagation
  - Memory locations, hardware resource
  - Speculative
- Declassification
  - OS
  - Sandbox engine



Declassification

- Lattice defines the "secrets"
- But higher privileged software operates on lower domains' memory
  - Process creation (fork)
  - Memory management (Copy-On-Write, zero-init)
- Proper declassification is needed



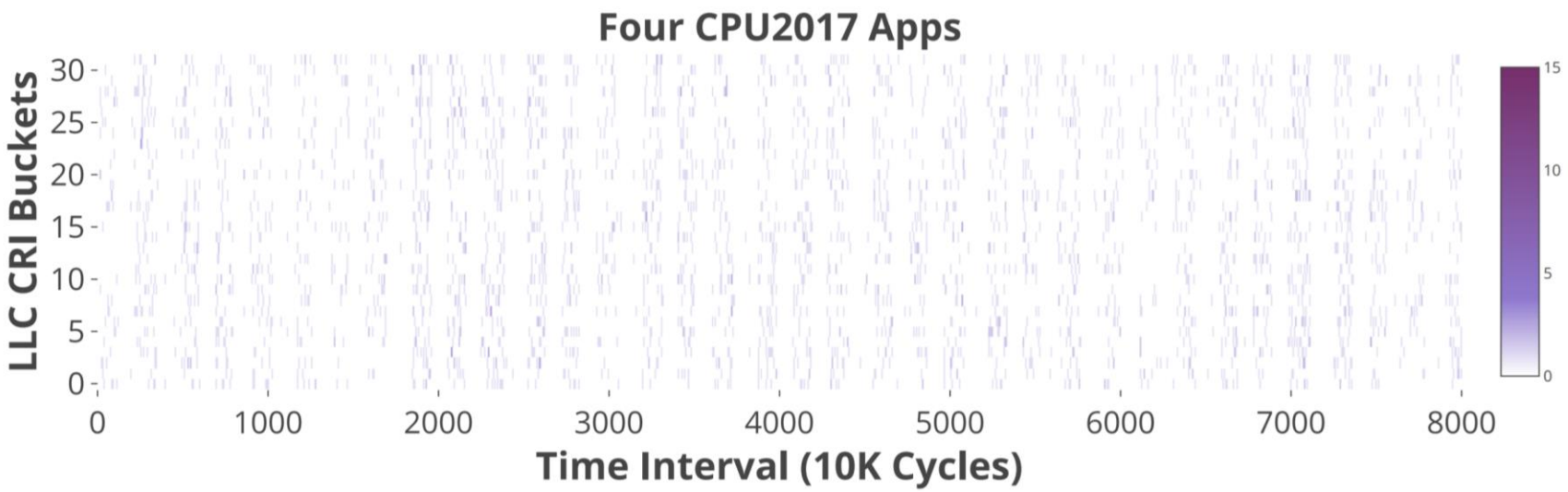
(a) Coarse-Grained isolation *(b) Fine-Grained isolation*

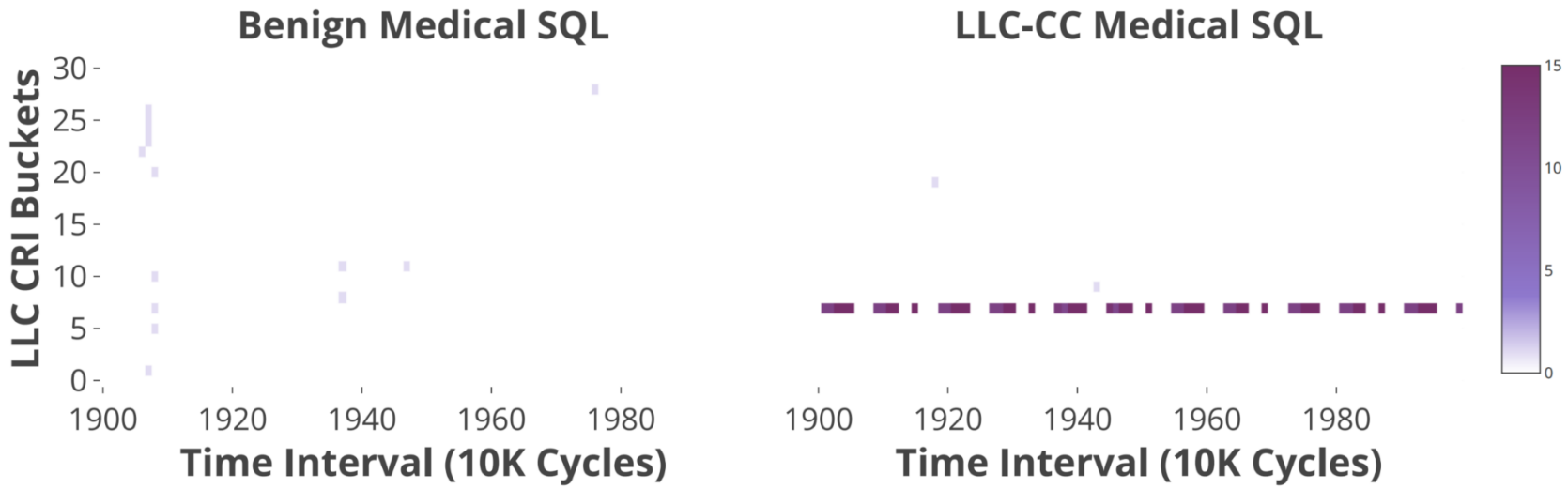
Evaluation Challenges

- Detection false positives
  - Stress test with concurrent SPEC2017
- Attacks on privacy-sensitive applications
  - Medical database, face recognition, ECG classification
    - Cross-process cache covert-channels
  - Web browser
    - Spectre-V1 password-stealing attack in JavaScript
- OS/JavaScript Engine required to demonstrate attacks
  - Gem5 ARMv8 OoO running Ubuntu
  - PhantomJS (WebKit)
- Baseline
  - State-of-the-Art Contention Tracking
  - (Improved) Bucketed Contention Tracking

Evaluation Challenges

- Detection false positives
  - Stress test with concurrent SPEC2017

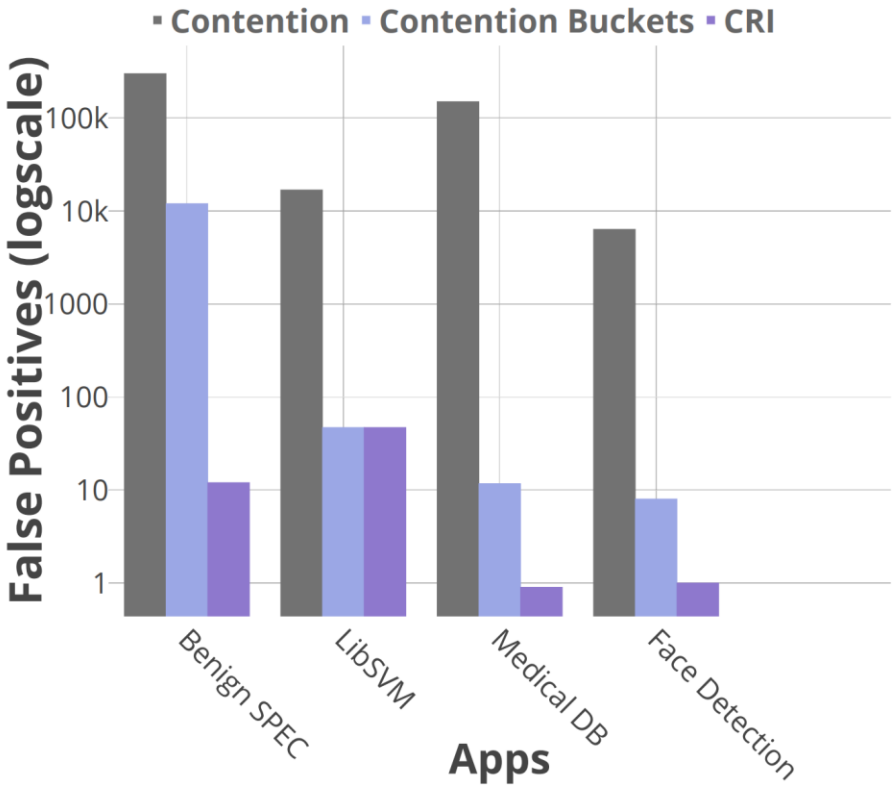


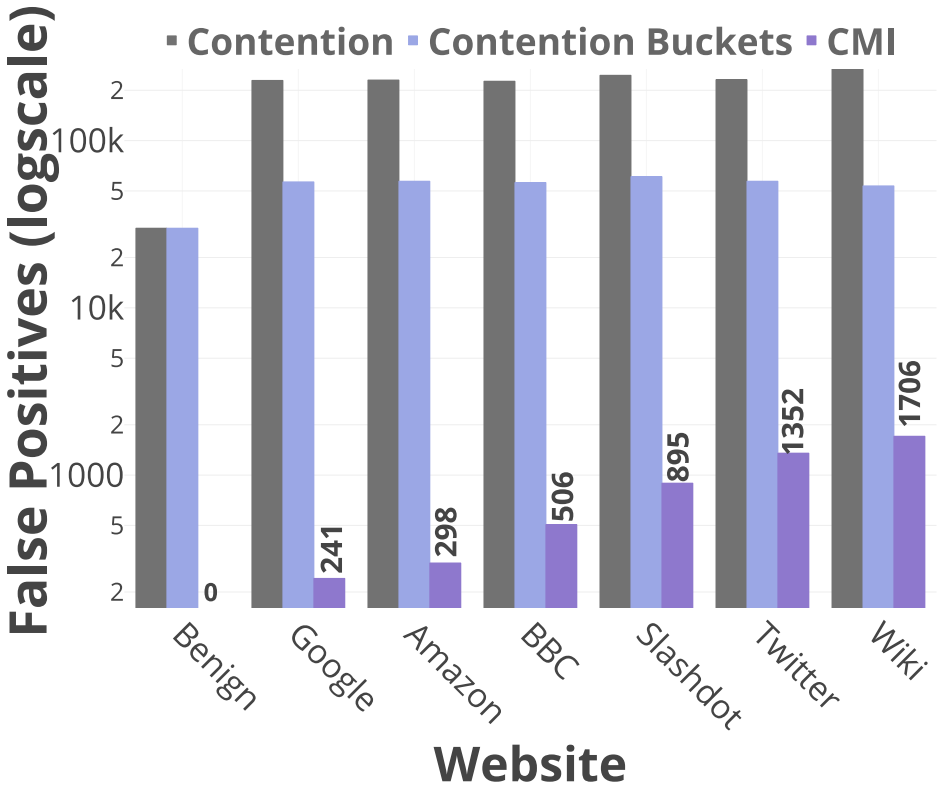


Results: low false positives with *close to 100% detection rates*

The University of Texas at Austin
Electrical and Computer Engineering
Cockrell School of Engineering

- Detecting resource-based covert channel
  - Attack using set-targeted LLC Prime+Probe
  - Cyclone detects attacks through Cyclic Resource Interference (CRI)
- Detecting memory-based leak (Spectre V1)
  - Spectre.js in PhantomJS using Evict+Reload
  - Cyclone detects attacks through Cyclic Memory Interference (CMI)

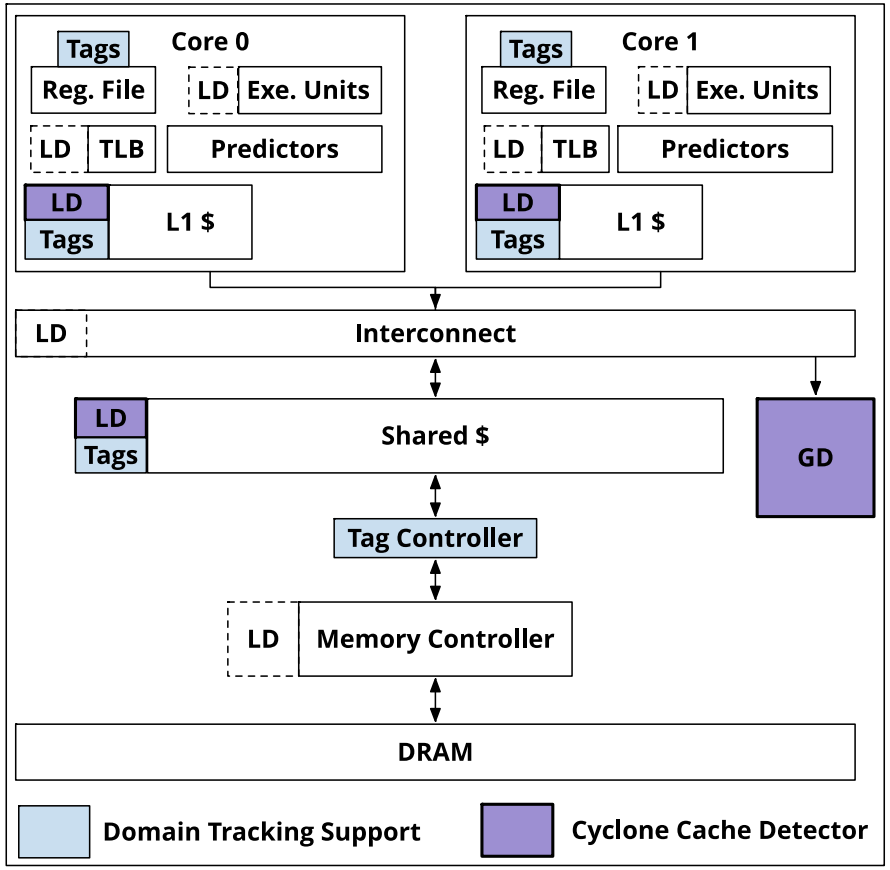




Q&A

The University of Texas at Austin
Electrical and Computer Engineering
Cockrell School of Engineering

- Ongoing work
  - RISC-V Prototype (BOOM)
  - Integration with software-level detection (e.g., OSQuery)



Thank You!

http://spark.ece.utexas.edu/
Austin Harris (austinharris@utexas.edu)
Shijia Wei (shijiawei@utexas.edu)