Time Protection: The Missing OS Abstraction

Qian Ge, Yuval Yarom, Tom Chothia, Gernot Heiser

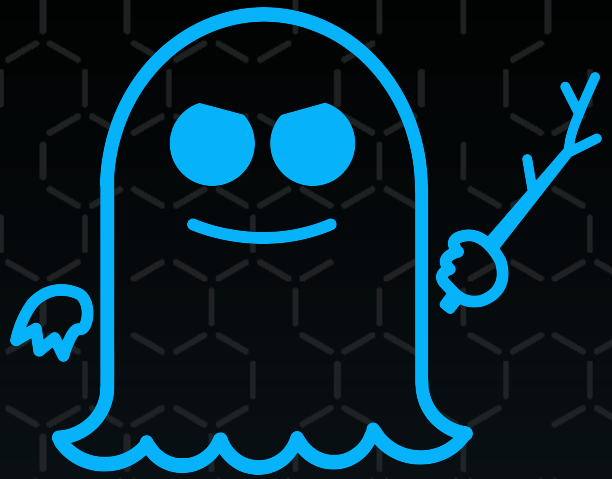
qian.ge@data61.csiro.au

www.data61.csiro.au

UNSW SYDNEY

THE UNIVERSITY of ADELAIDE

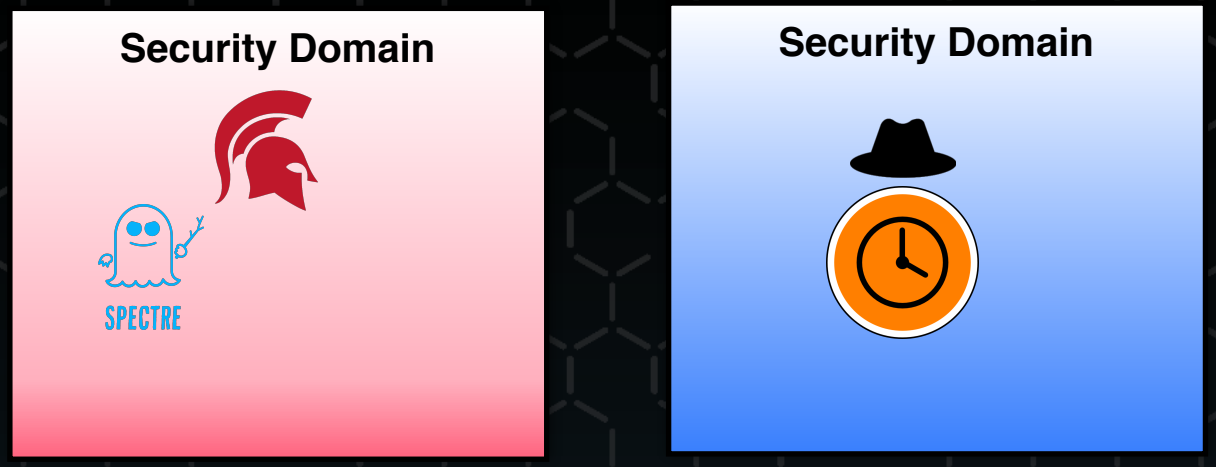
UNIVERSITY OF BIRMINGHAM



SPECTRE

qian.ge@data61.csiro.au

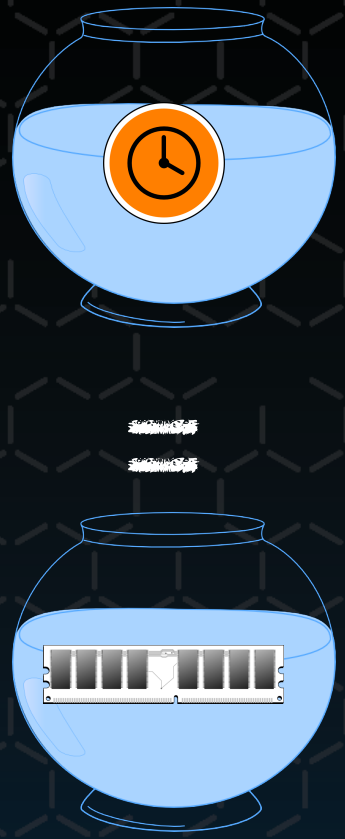
Enforcing time protection at the OS level

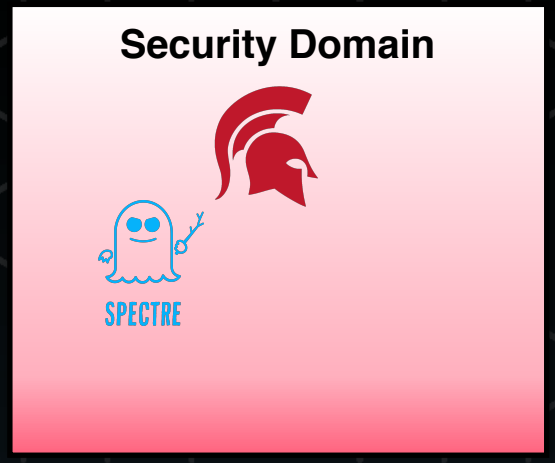


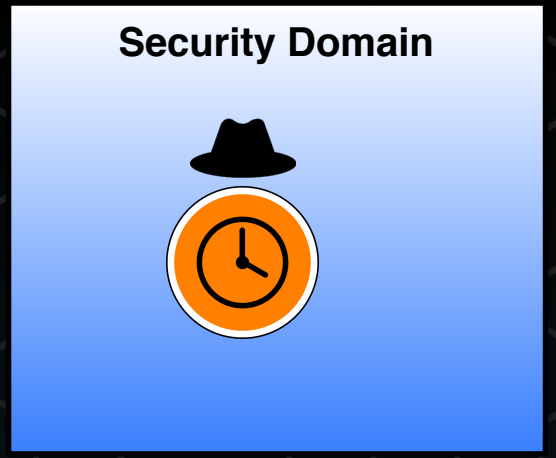
Sending information through timing

qian.ge@data61.csiro.au

Enforcing time protection at the OS level



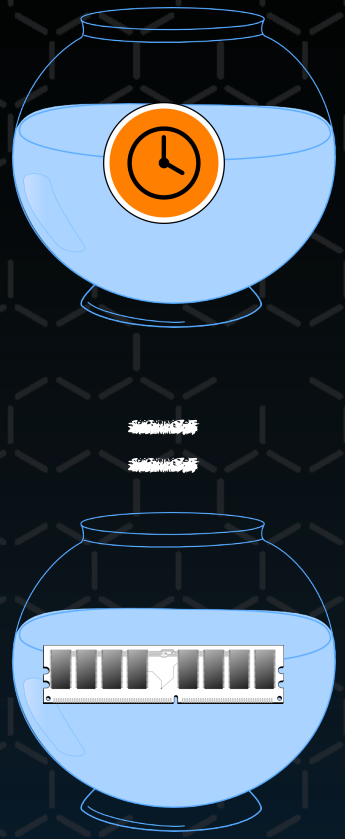


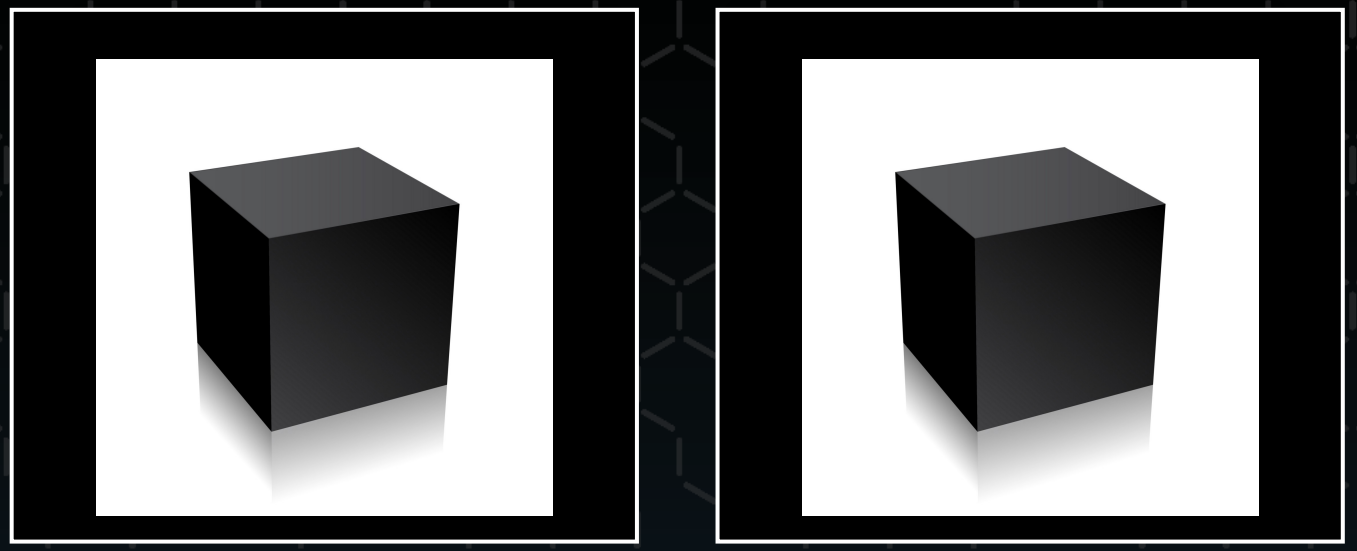


Sending information through timing

qian.ge@data61.csiro.au

Enforcing time protection at the OS level

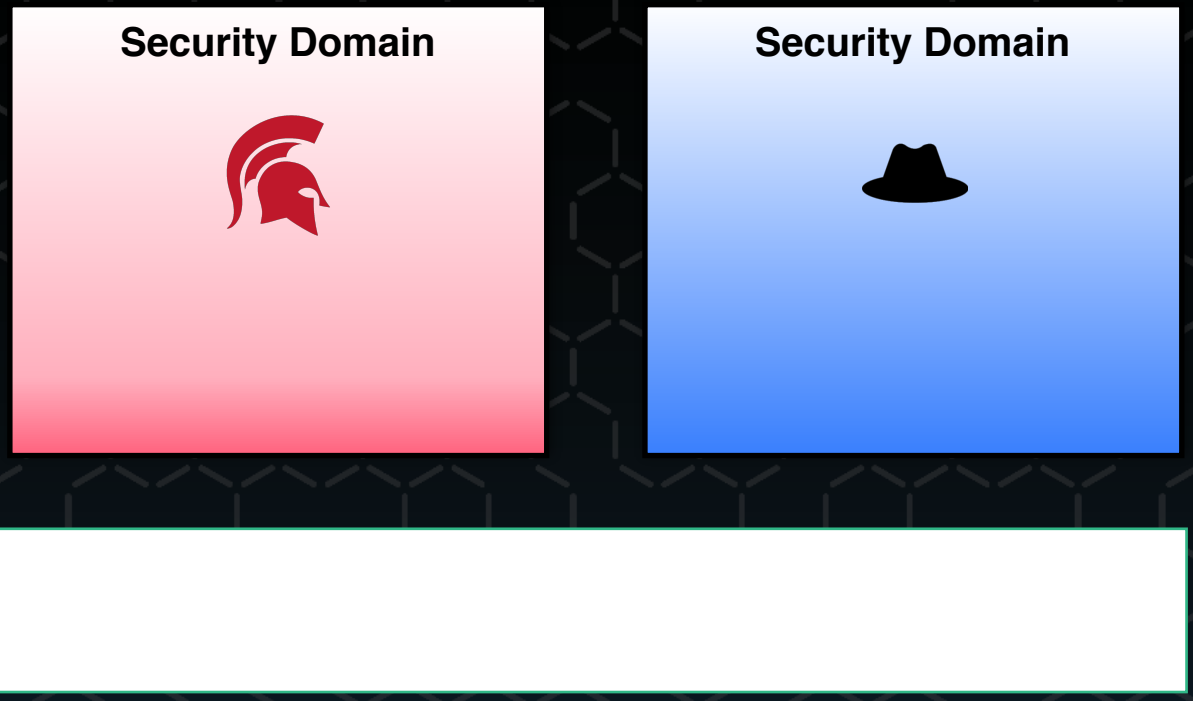




Sending information through timing

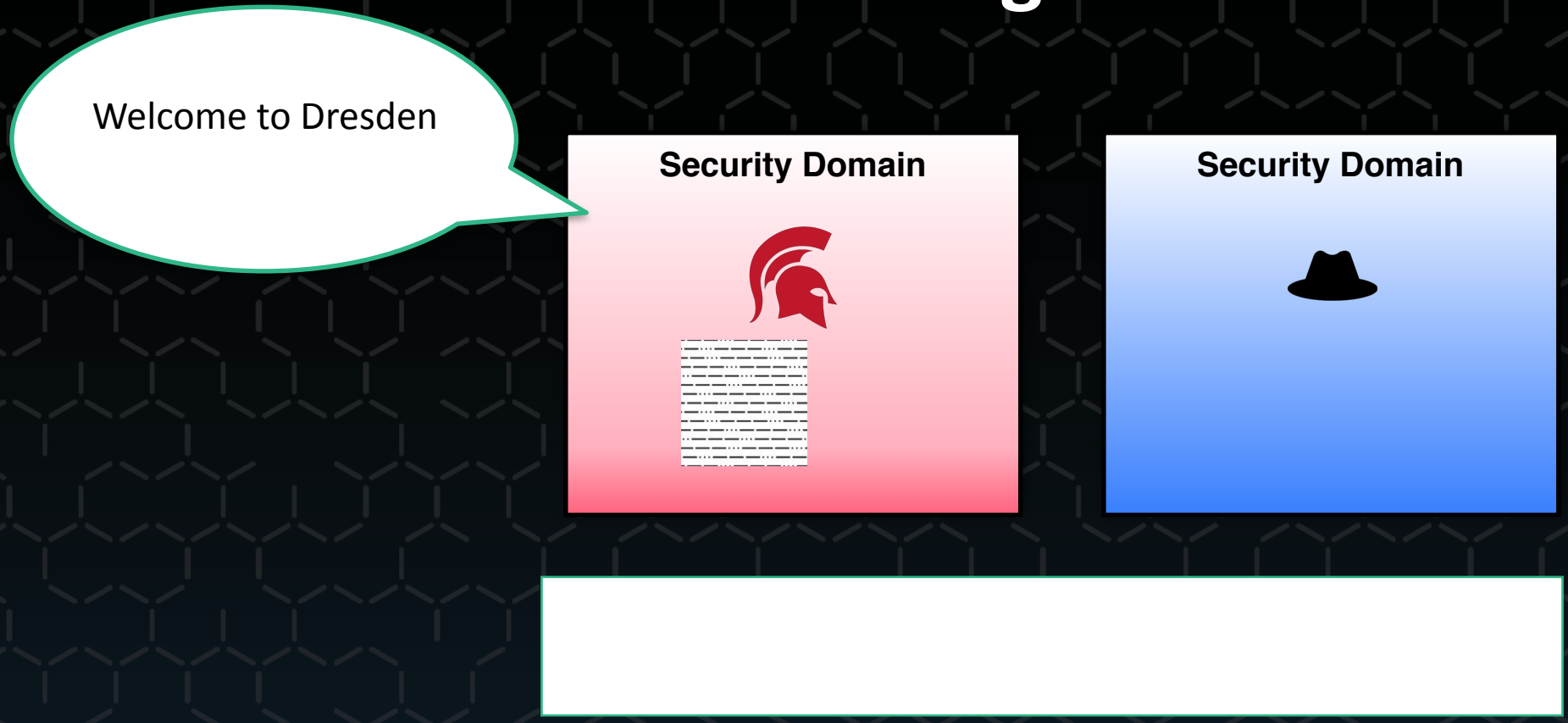
qian.ge@data61.csiro.au

Microarchitectural Timing Channels

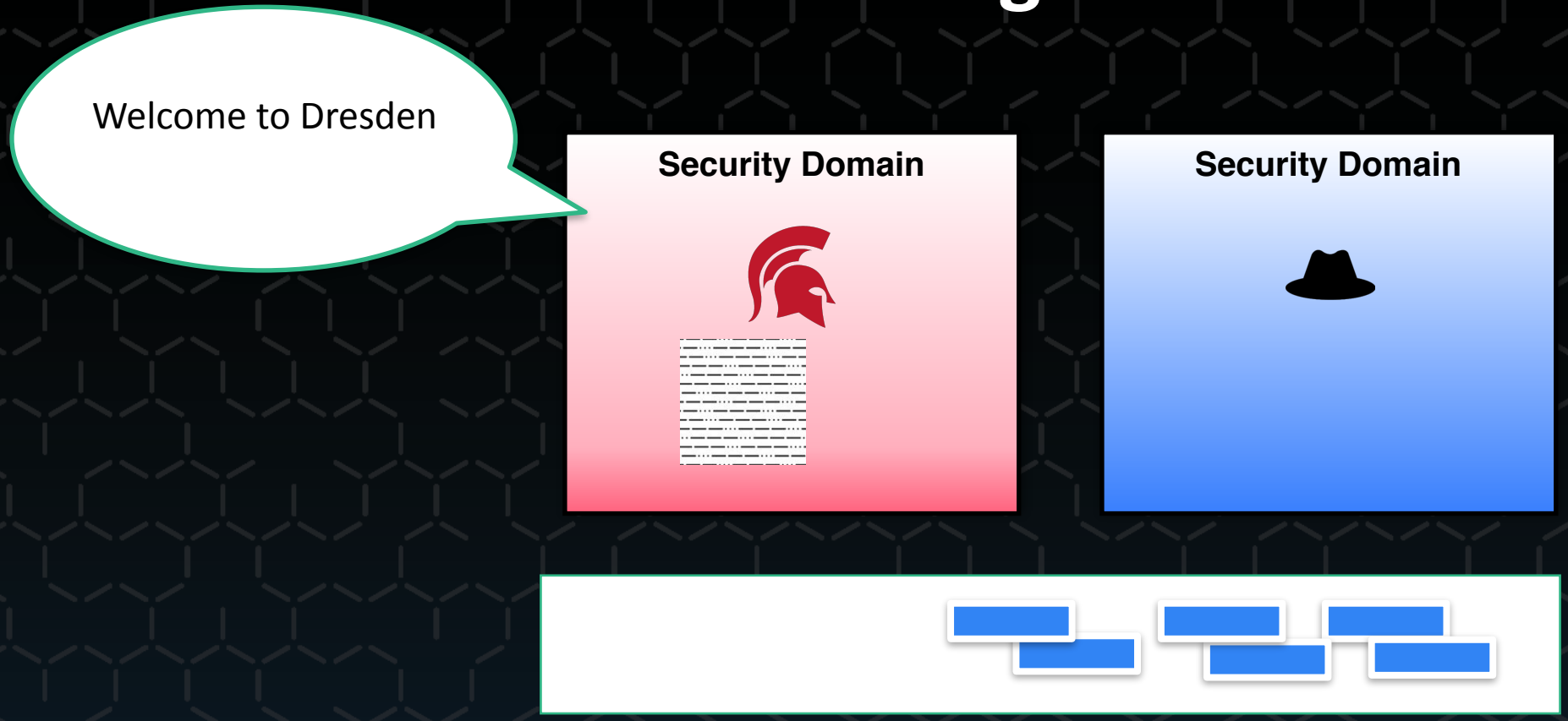


qian.ge@data61.csiro.au

Microarchitectural Timing Channels



Microarchitectural Timing Channels

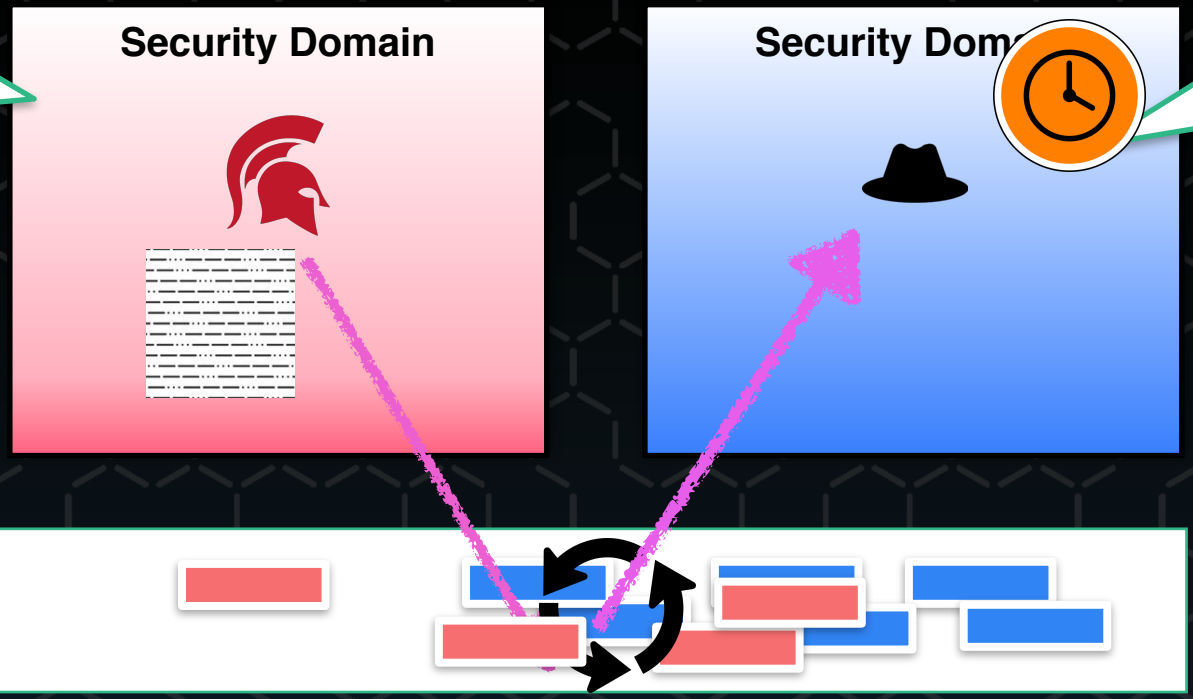


Microarchitectural Timing Channels

qian.ge@data61.csiro.au

Microarchitectural Timing Channels

Welcome to Dresden



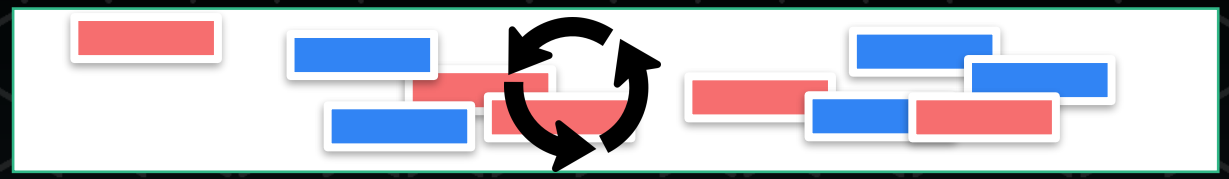
Fast Fast Slow Fast Fast
….. S F S FFF SSSS F

Not English, but our protocol…

Shared hardware caches

qian.ge@data61.csiro.au

Contention, Contention, Contention…

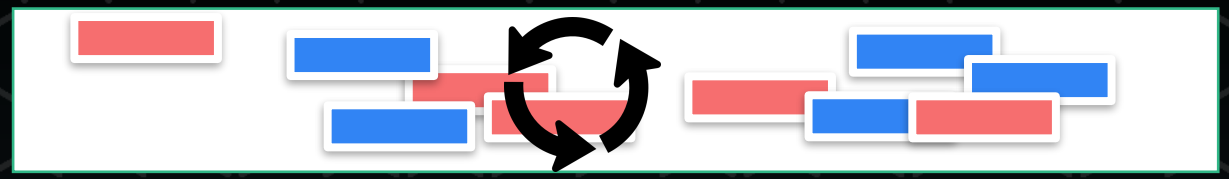


Shared hardware caches

- Contention leaks information via timing
- Caches:
  - capacity-limited
  - stateful
- Resulting on temporal interference during:
  - time-shared access
  - concurrent access

qian.ge@data61.csiro.au

Contention, Contention, Contention…



Shared hardware caches

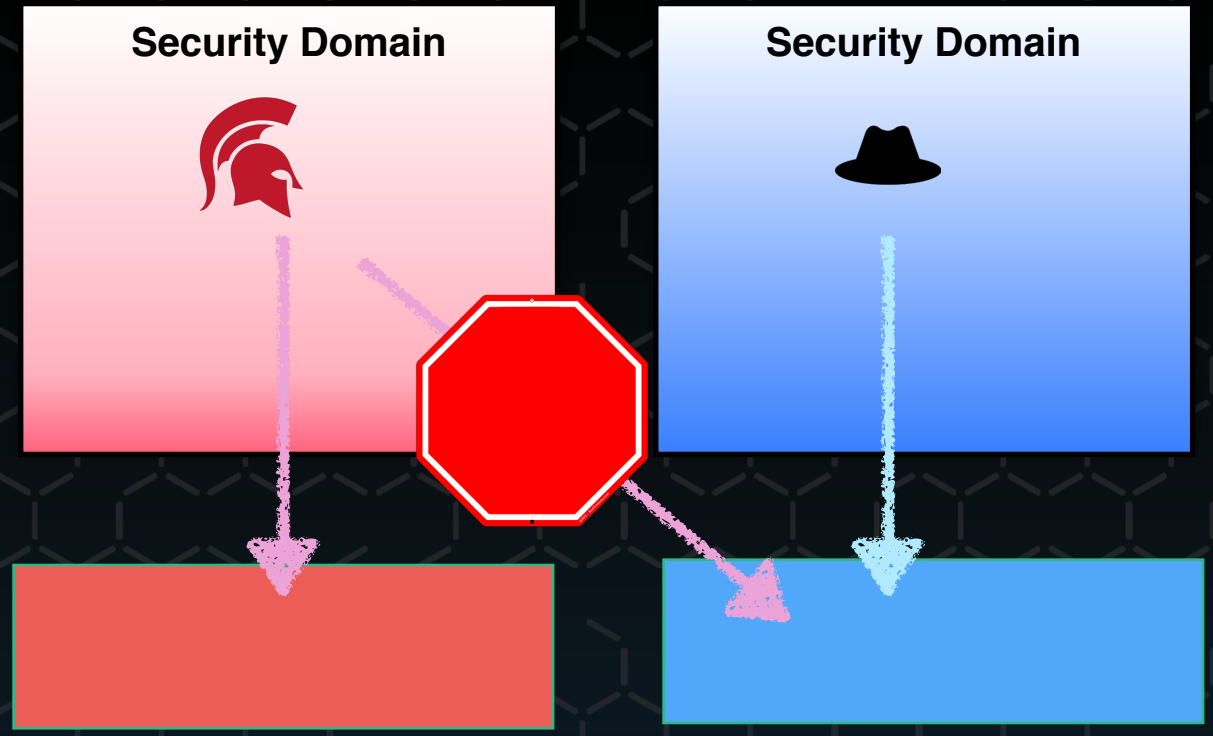
Any state-holding microarchitectural feature:

- Caches, branch predictor, TLB

- Contention leaks information via timing
- Caches:
  - capacity-limited
  - stateful
- Resulting on temporal interference during:
  - time-shared access
  - concurrent access

qian.ge@data61.csiro.au

Preventing Contention by Partitioning



Partitioned caches

qian.ge@data61.csiro.au

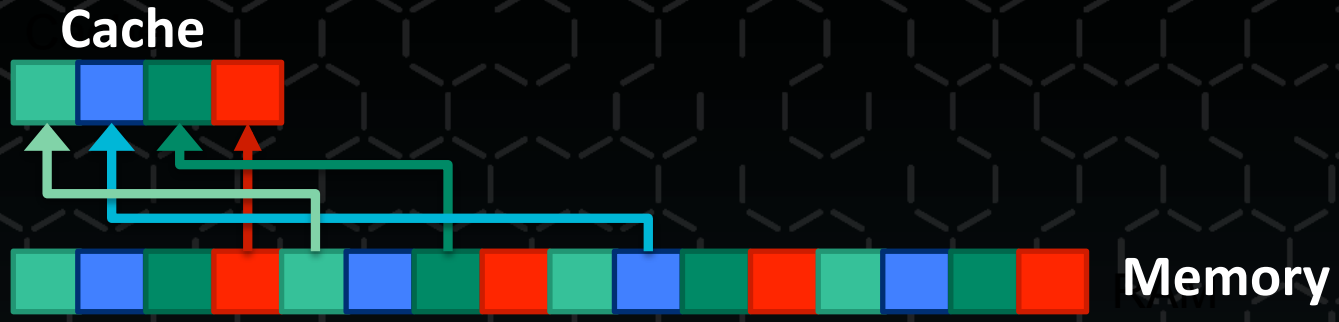
Spatial Partitioning

Cache colouring:

- Distributing coloured cache sets to coloured memory frames
- Memory management policy

qian.ge@data61.csiro.au

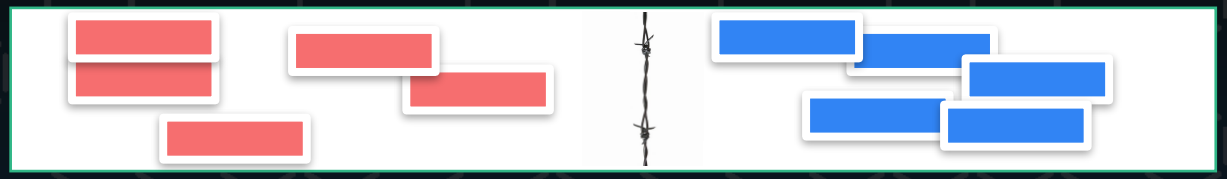
Spatial Partitioning



Cache colouring:

- Distributing coloured cache sets to coloured memory frames
- Memory management policy

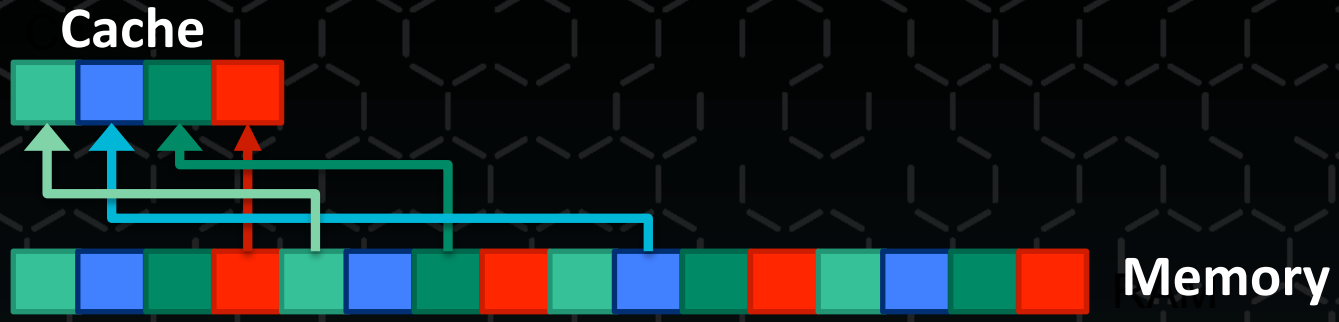
Partition security domains on disjoint cache sets



Shared hardware caches

qian.ge@data61.csiro.au

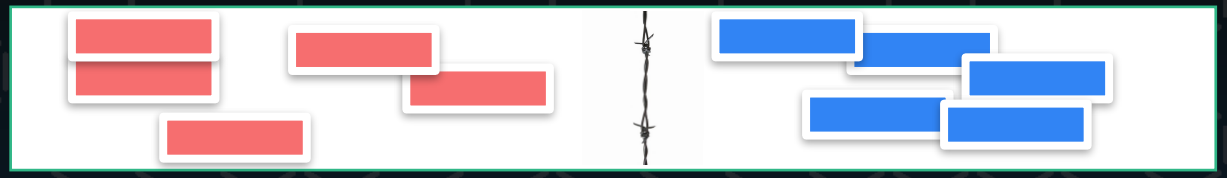
Spatial Partitioning



Cache colouring:

- Distributing coloured cache sets to coloured memory frames
- Memory management policy

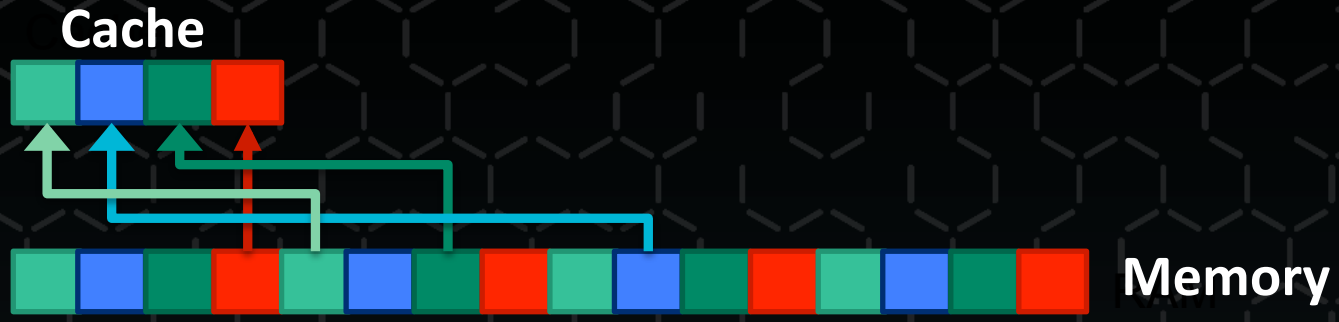
Partition security domains on disjoint cache sets



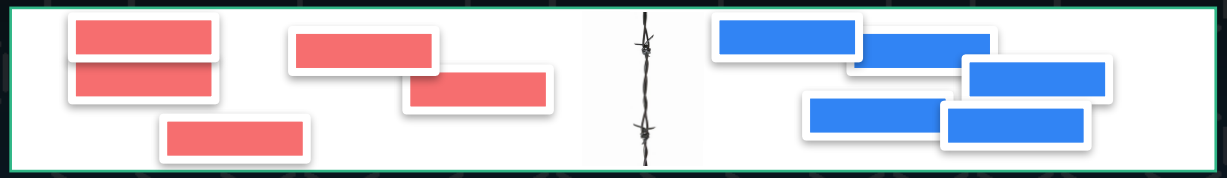
Shared hardware caches

- Resulting on temporal interference during:
  - time-shared access
  - concurrent access

Spatial Partitioning



Partition security domains on disjoint cache sets



Shared hardware caches

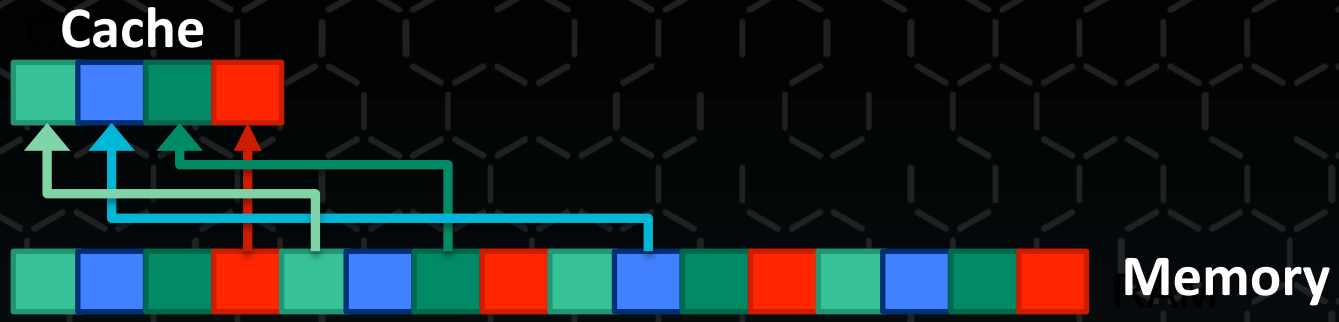
Cache colouring:

- Distributing coloured cache sets to coloured memory frames
- Memory management policy

- Resulting on temporal interference during:
  - time-shared access
  - concurrent access

qian.ge@data61.csiro.au

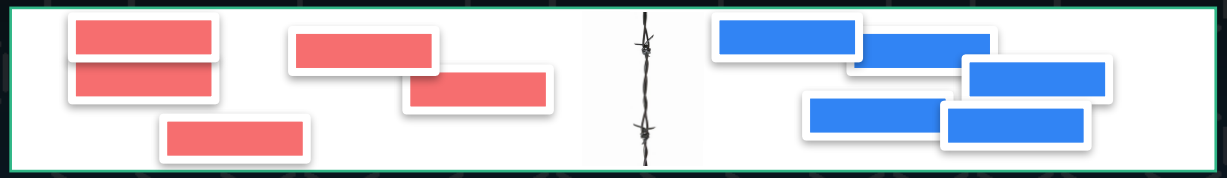
Spatial Partitioning



Cache colouring:

- Distributing coloured cache sets to coloured memory frames
- Memory management policy

Partition security domains on disjoint cache sets



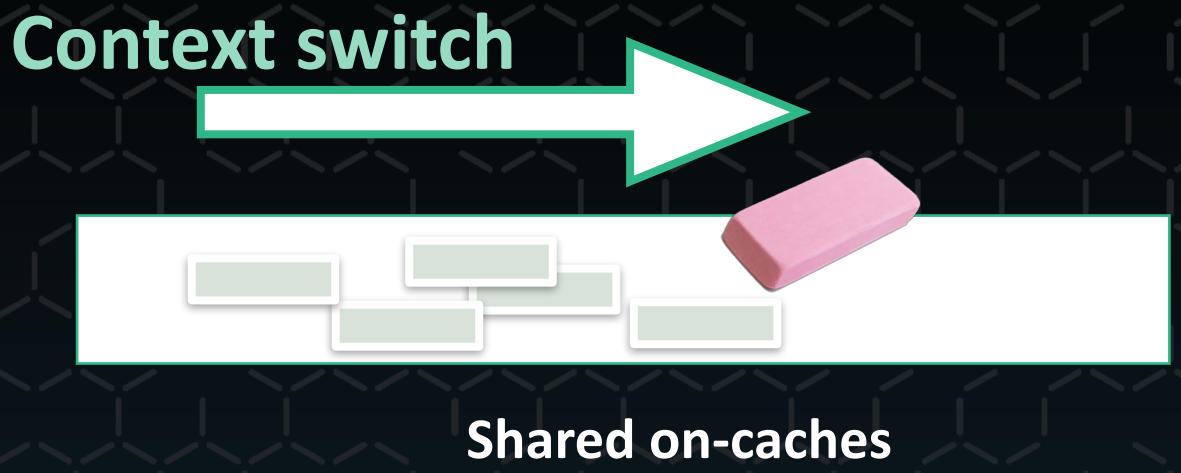
Shared hardware caches

- Resulting on temporal interference during:
  - time-shared access
  - concurrent access

Cannot be supported by on-core caches

qian.ge@data61.csiro.au

Temporal Partitioning

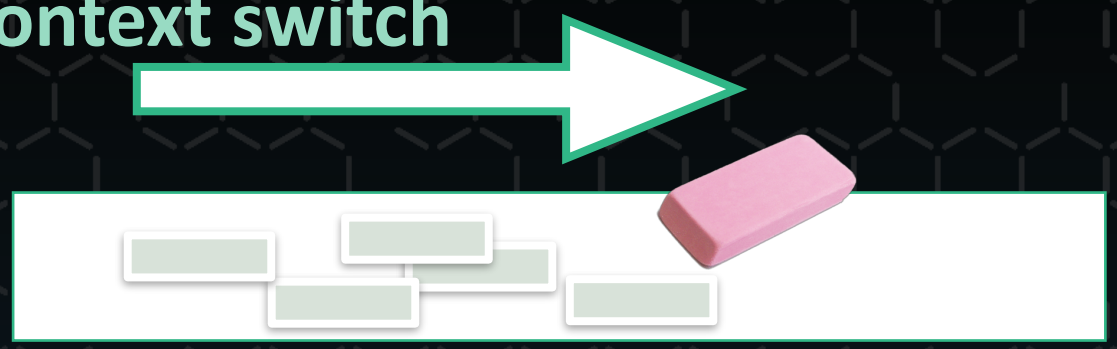


Flushing on-core caches:

- Resetting states

qian.ge@data61.csiro.au

Temporal Partitioning



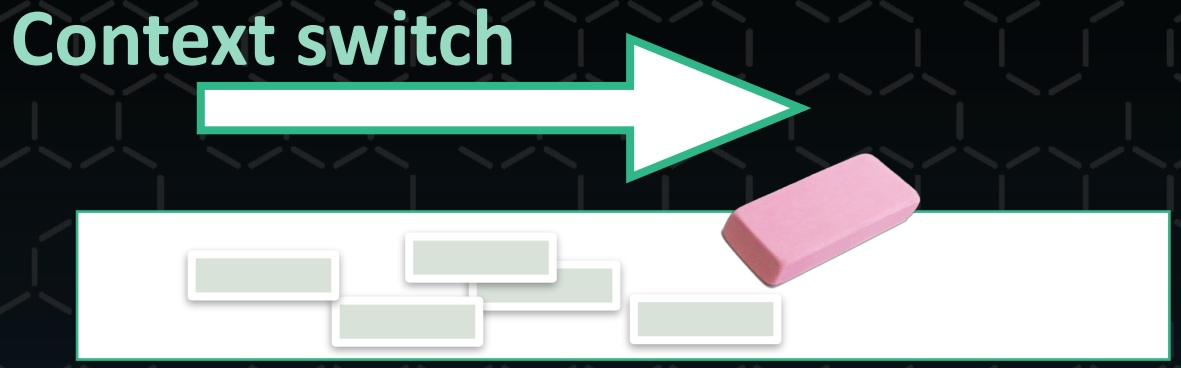
Flushing on-core caches:

- Resetting states

- Resulting on temporal interference during:
  - time-shared access
  - concurrent access

qian.ge@data61.csiro.au

Temporal Partitioning



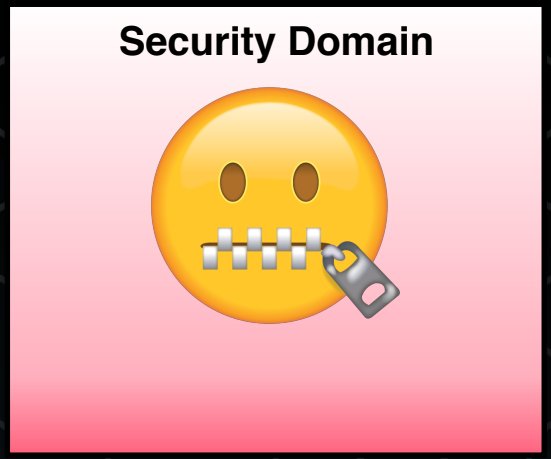
Flushing on-core caches:

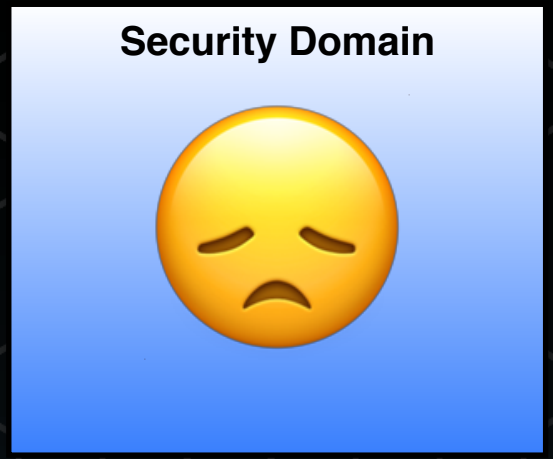
- Resetting states

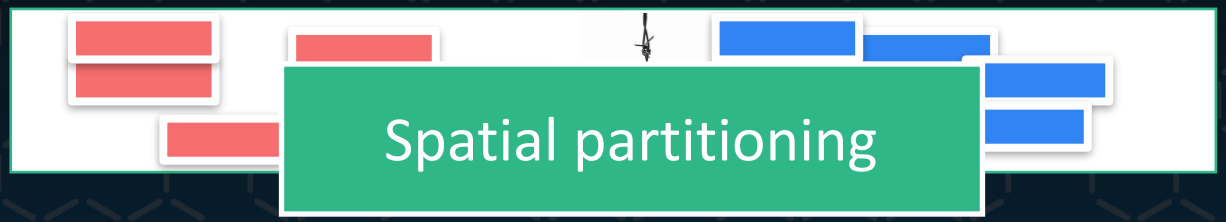
- Resulting on temporal interference during:
  - time-shared access
  - concurrent access

qian.ge@data61.csiro.au

Preventing Temporal Interference through Partitioning

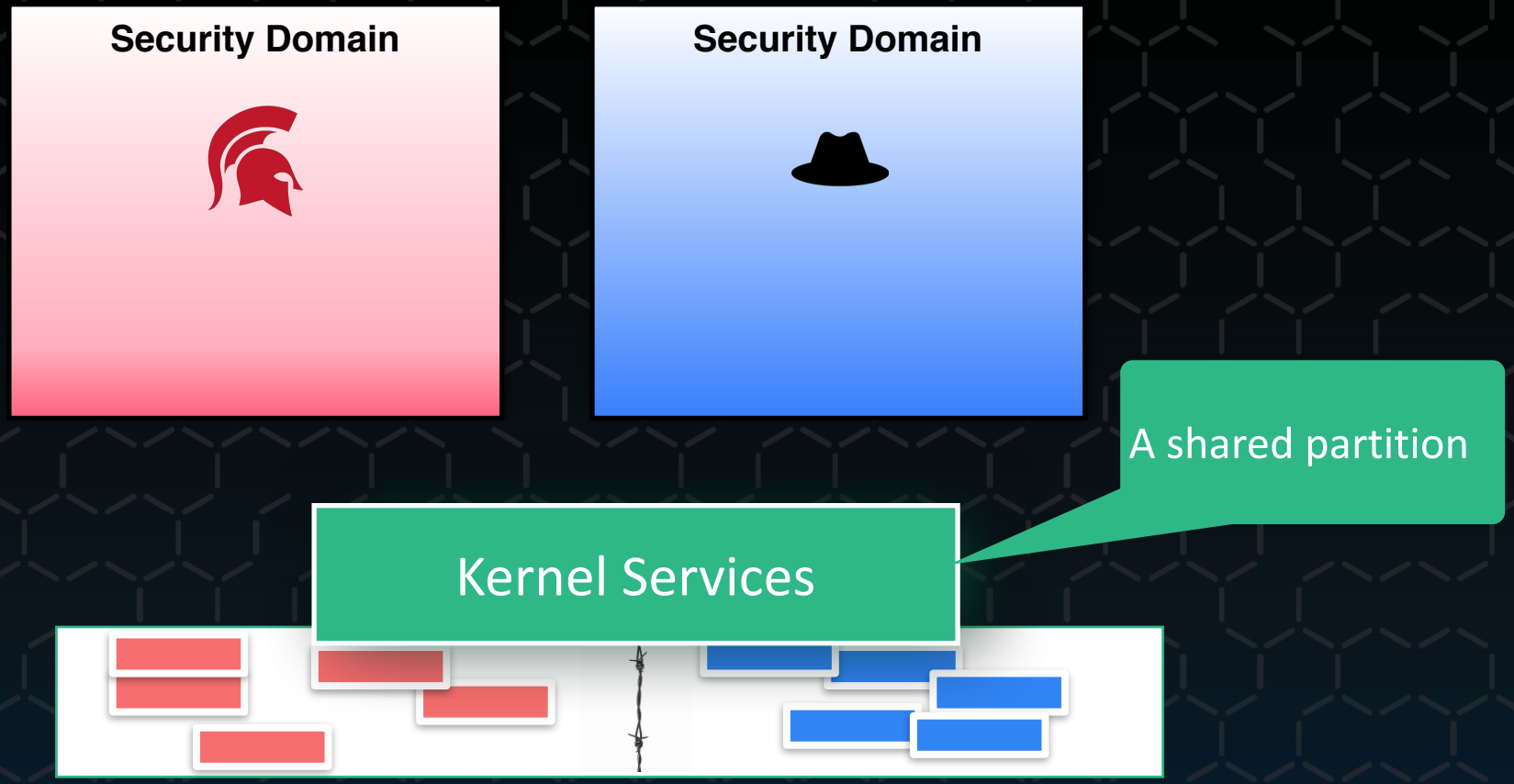






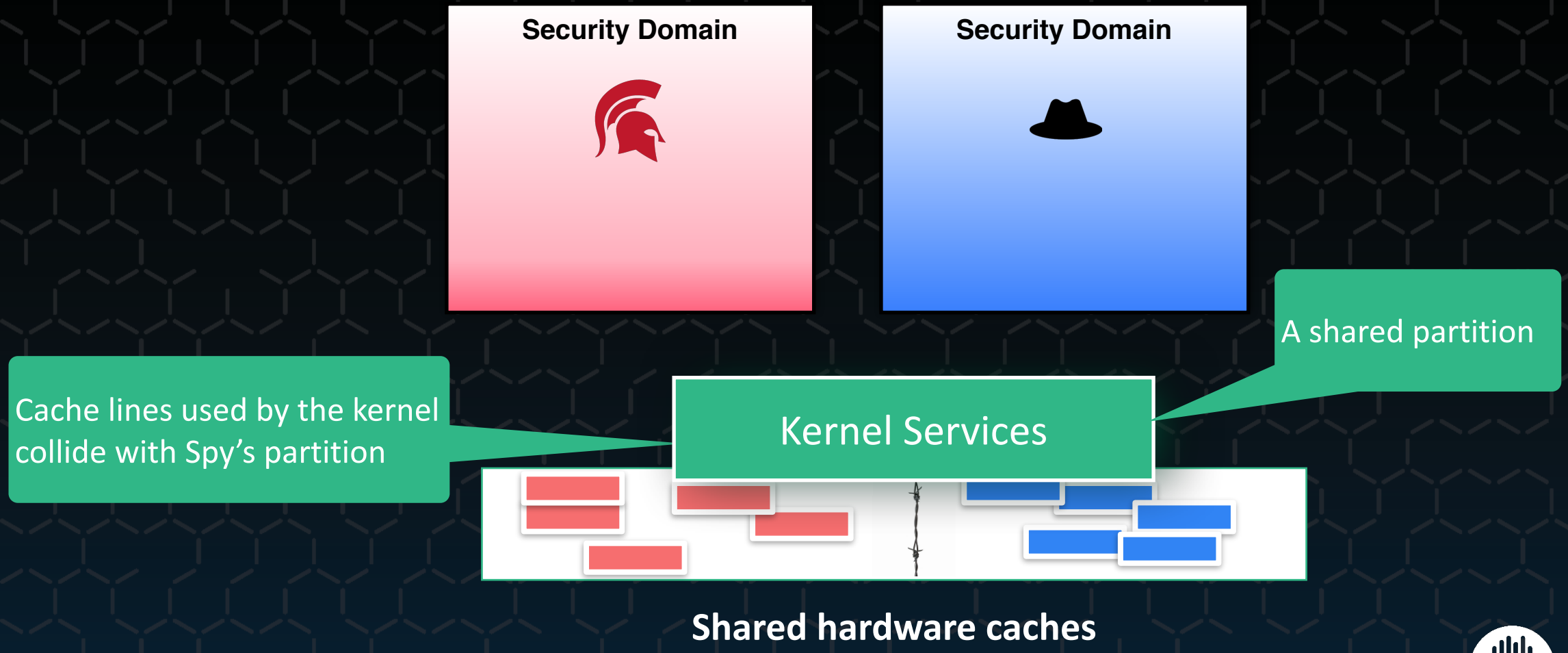
qian.ge@data61.csiro.au

Wait, Everyone Shares the Kernel….



qian.ge@data61.csiro.au

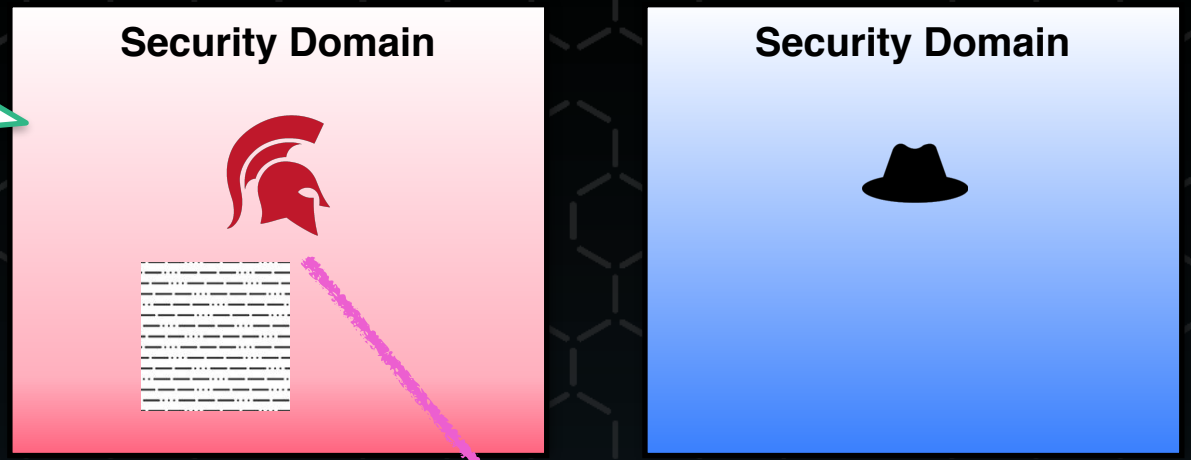
Wait, Everyone Shares the Kernel….



qian.ge@data61.csiro.au

Wait, Everyone Shares the Kernel….

Poster Session
@ 17:15



Cache lines used by the kernel collide with Spy's partition

A shared partition

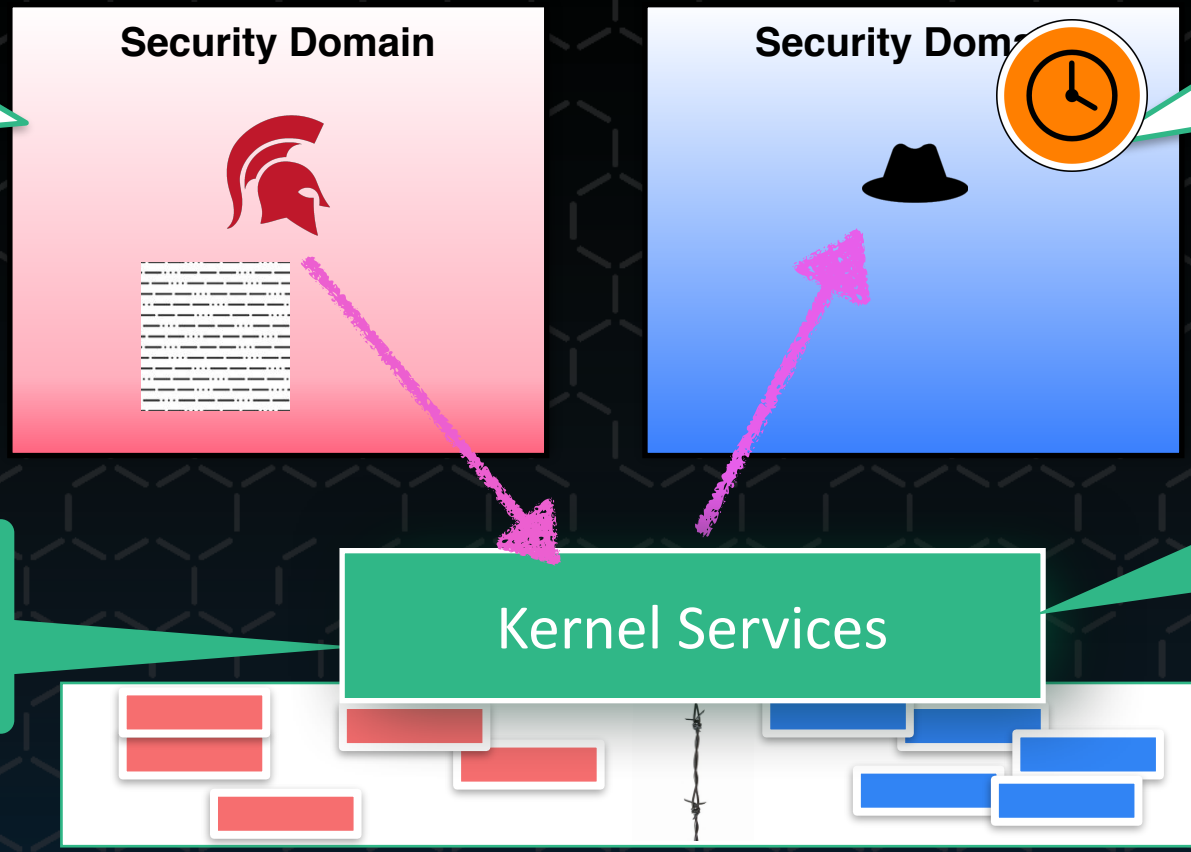
Kernel Services

Shared hardware caches

qian.ge@data61.csiro.au

Wait, Everyone Shares the Kernel….

Poster Session
@ 17:15



Fast Fast Slow Fast Fast
….. S F S FFF SSSS F

Cache lines used by the kernel collide with Spy's partition

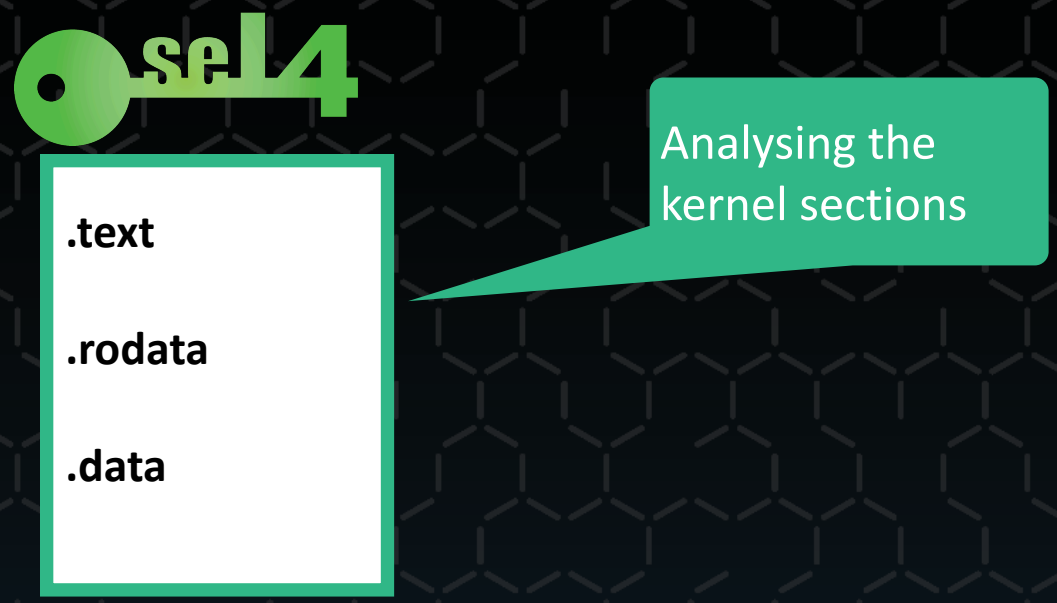
A shared partition

qian.ge@data61.csiro.au

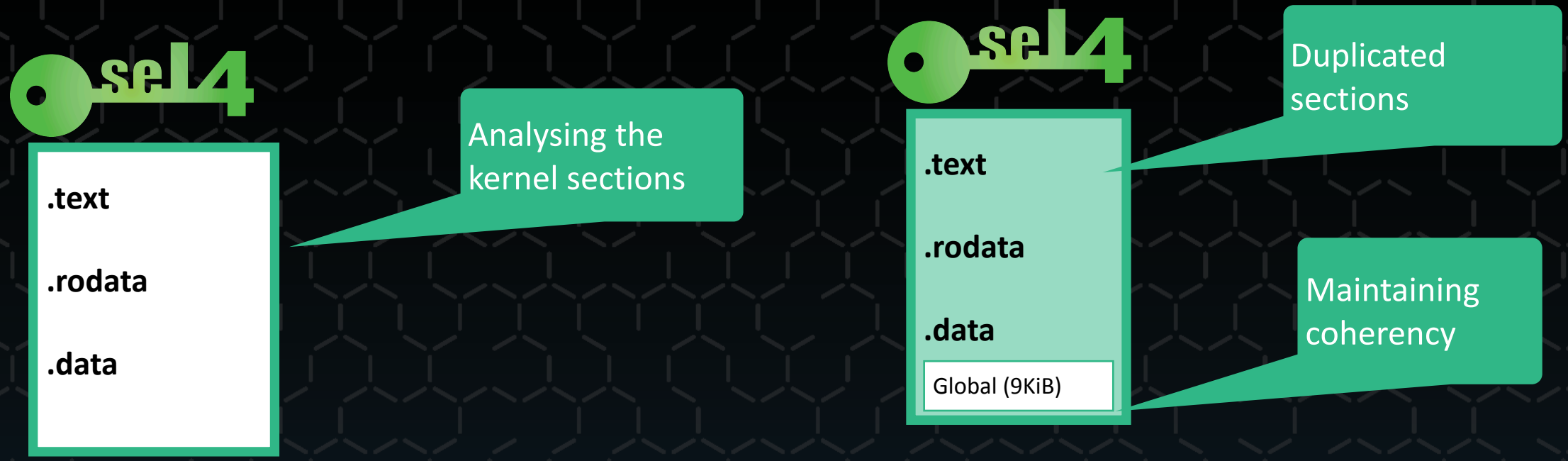
Kernel Services

qian.ge@data61.csiro.au

Cloning the Kernel Image



Cloning the Kernel Image



Cloning the Kernel Image

.text

.rodata

.data

Analysing the kernel sections

.text

.rodata

.data

Global (9KiB)

Duplicated sections

Maintaining coherency

Kernel Clone:
Generating a copy of the kernel image with user-level managed memory

qian.ge@data61.csiro.au

Cloning the Kernel Image

.text

.rodata

.data

Analysing the kernel sections

.text

.rodata

.data

Global (9KiB)

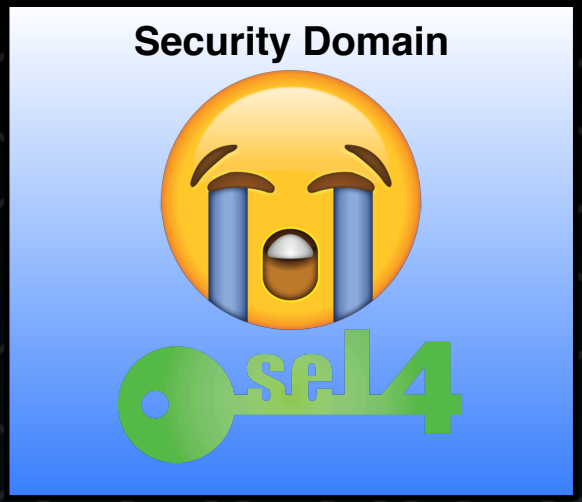
Duplicated sections

Maintaining coherency

Kernel Clone:
Generating a copy of the kernel image with user-level managed memory

qian.ge@data61.csiro.au

Dedicated Kernel Images



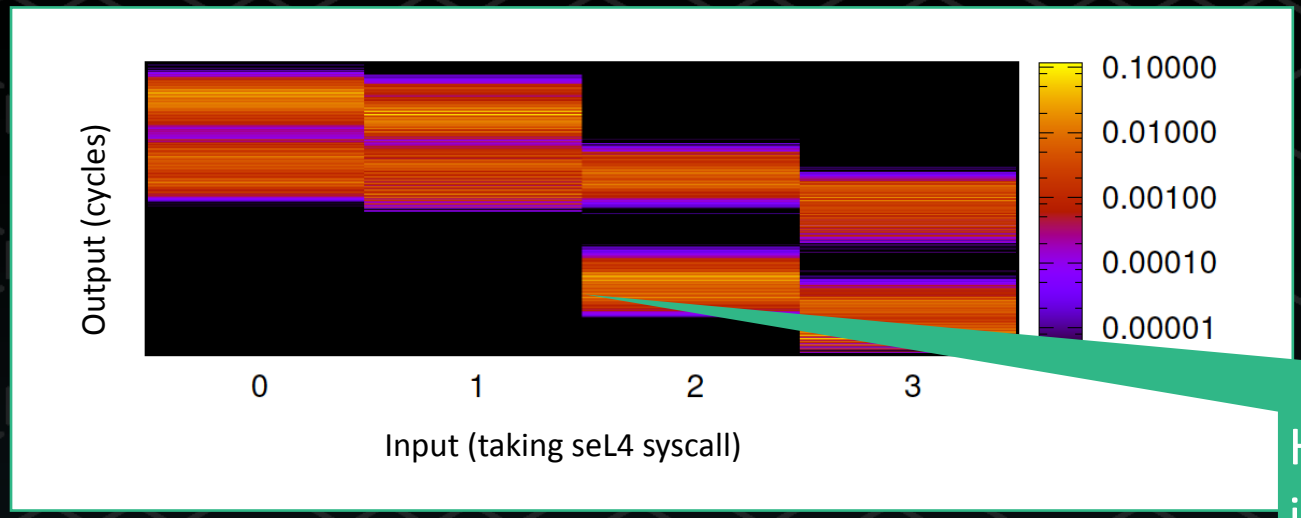
Shared Global Data

Temporal partitioning

Deterministic usage

Spatial partitioning

Timing Channel through the Shared Kernel



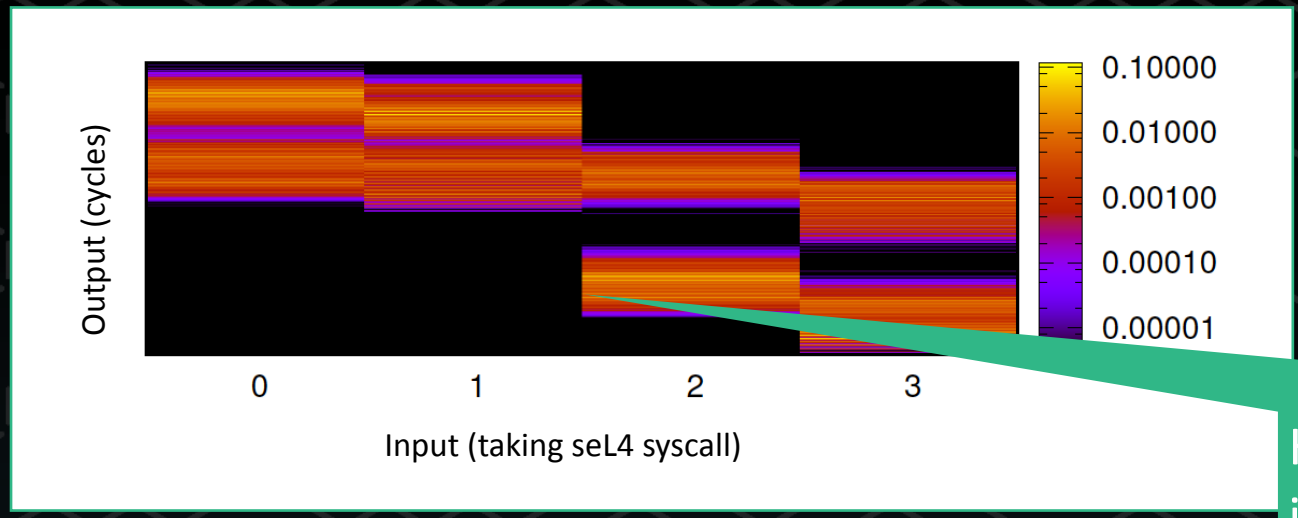
Channel matrix: conditional probability of observing the output signal (time, spy) given the input signal (system-call number, Trojan)

Raw channel

Horizontal variation indicates a channel

qian.ge@data61.csiro.au

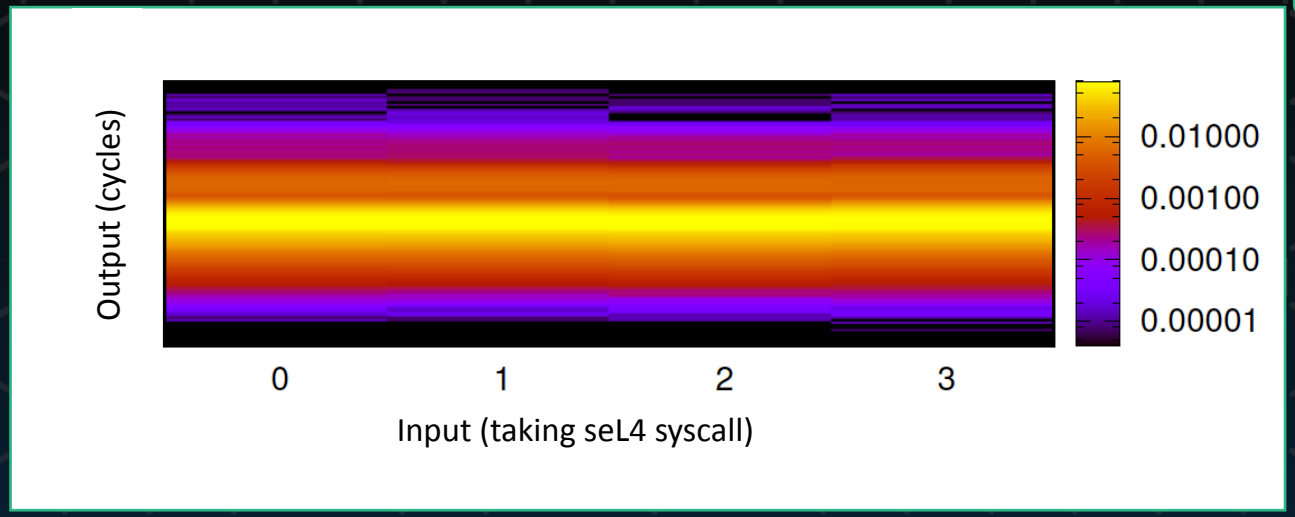
Timing Channel through the Shared Kernel



Channel matrix: conditional probability of observing the output signal (time, spy) given the input signal (system-call number, Trojan)

Raw channel

Horizontal variation indicates a channel



Prevented by cloned kernel

qian.ge@data61.csiro.au

How realistic is cloning?

.text

.rodata

.data

Global (9KiB)

x86	Arm
224 KiB	120 KiB

Memory consumption

Arch	seL4 Clone	Linux fork + exec
x86	79 µs	257 µs
Arm	608 µs	4,300 µs

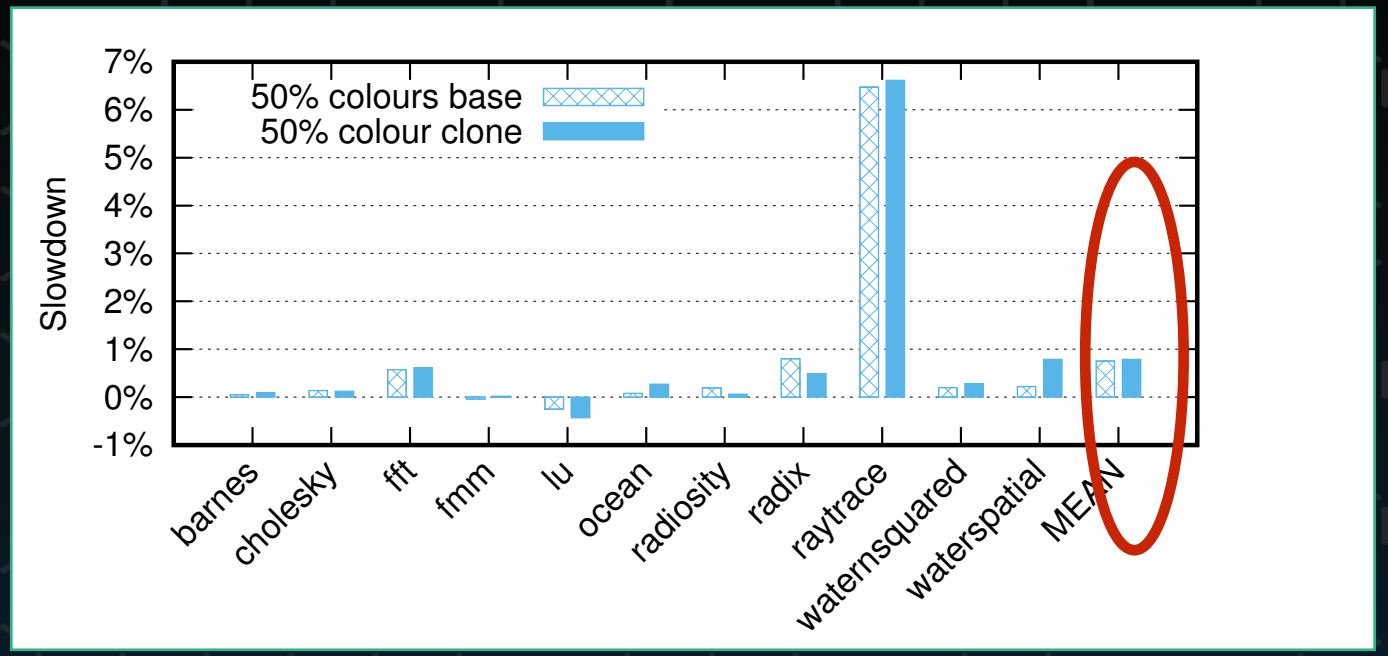
Efficiency

qian.ge@data61.csiro.au

Performance Impact

The cost of colouring a domain:

- 50% of the cache colour
- 50% of the cache colour + a coloured kernel

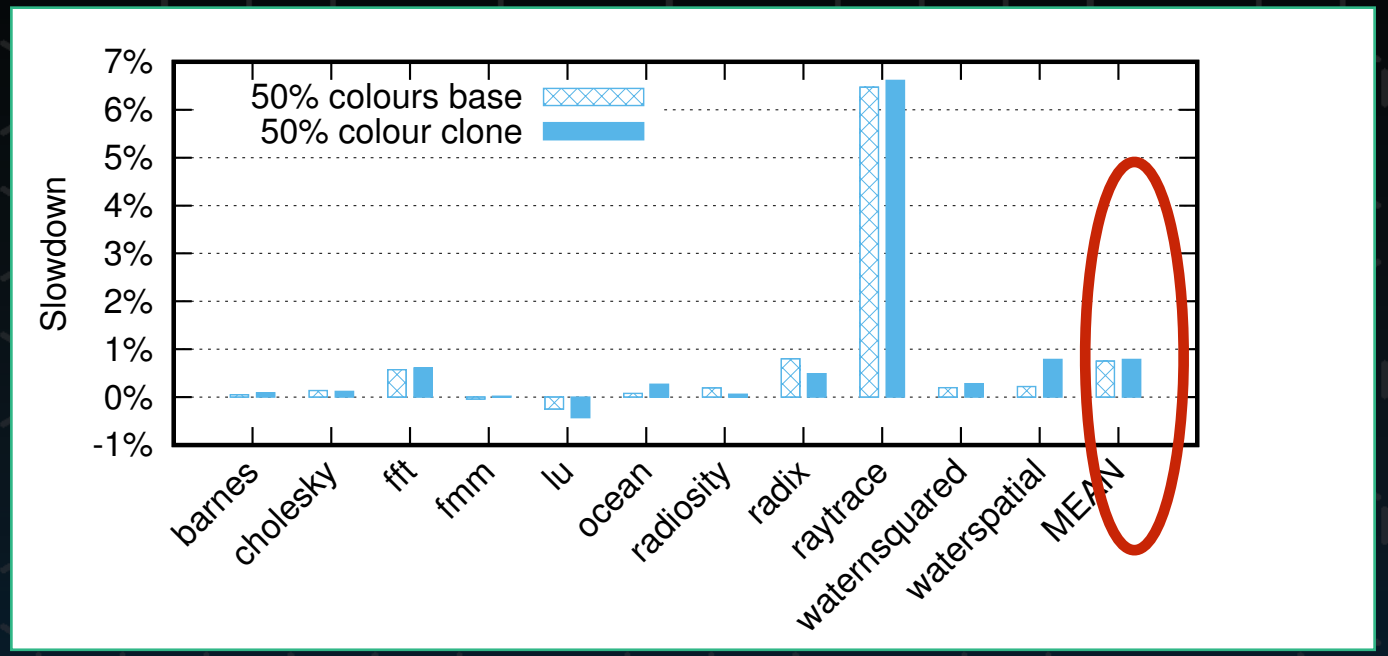


The slowdown of splash-2 against base line kernel

Performance Impact

The cost of colouring a domain:

- 50% of the cache colour
- 50% of the cache colour + a coloured kernel



The slowdown of splash-2 against base line kernel

The cost of time protection:

- spatial partition + temporal partition

x86	Arm
3.38%	1.09%

The geometric mean

qian.ge@data61.csiro.au

We have also done:

- Partition IRQs
- Domain-switch actions
- A deterministic domain switching latency
- Preventing timing channels:
  - Shared kernel, Intra-core, cross-core, domain-switch latency, timer
- Performance evaluation:
  - IPC, domain switching latency, kernel cloning, cache colouring, time protection

qian.ge@data61.csiro.au

Summary

- Define temporal isolation as a mandatory (black-box mechanisms) enforcement provided by the OS.
- Time protection for preventing microarchitectural timing channels
- Effective on closing studied timing channels
- Low overhead

THANK YOU

Trustworthy Systems
Qian Ge
PhD candidate

e qian.ge@data61.csiro.au
w https://ts.data61.csiro.au/projects/TS/timingchannels/

www.data61.csiro.au