Replicating and Mitigating Spectre Attacks on an Open Source RISC-V Microarchitecture

CARRV 2019 – June 22nd, 2019 - Phoenix, Arizona

Abraham Gonzalez, Ben Korpan, Jerry Zhao, Ed Younis

Krste Asanović

University of California, Berkeley







Outline





- Motivation
- Open-source Approach to Hardware
 - BOOM: Berkeley Out-of-Order Machine
- Replicating Spectre Attacks on BOOM
- Implementing a Speculation Buffer
 - Comparisons
 - Implementation
- Conclusion

Motivation

Exploits Everywhere





Researchers discover seven new Meltdown and Spectre attacks

Experiments showed that processors from AMD, ARM, and Intel are affected.



By Catalin Cimpanu for Zero Day | November 14, 2018 -- 14:44 GMT (06:44 PST) | Topic: Security

SPOOKY ACTION AT A DISTANCE -

New Spectre attack enables secrets to be leaked over a network

It's no longer necessary to run attacker code on the victim system.

PETER BRIGHT - 7/26/2018, 2:40 PM

Intel LazyFP vulnerability: Exploiting lazy FPU state switching

June 6 2018

Beyond Spectre: Foreshadow, a new Intel security problem

Researchers have broken Intel's Software Guard Extensions, System Management Mode, and x86-based virtual

Speculative Store Bypass explained: what it is, how it works

May 21, 2018 Jon Masters, chief ARM architect, Red Hat

Researchers discover SplitSpectre, a new Spectre-like CPU attack

Why are Spectre-style attacks hard?





Attack Scenarios

- User process attacks kernel
- User process attacks user space
- Intra-process sandbox escape
- User process attacks enclaves
- Remote timing attacks

• ...

Covert Channels

- Changes in cache state
- Power consumption
- Resource contention (FPUs, buffers)

• ..

Spectre Variations

Leakage Mechanisms

- Conditional branch
- Indirect jump
- Return instructions
- Speculative store bypass
- Data speculation
- ...

Target CPUs

- ARM
- Intel
- AMD
- RISC-V
- ...

Mitigation Approaches





InvisiSpec/SafeSpec: Blocking unsafe loads from altering the data cache

DAWG: Partition data cache between security domains

StealthMem/CATalyst: Hide visibility of a secure memory region

Context-based fencing: Dynamically stop speculation in secure code

Compiler-inserted fencing: Statically analyze program for Spectre-vulnerable snippets

Lots of interesting approaches, but how to compare them?

Use them together?

M. Yan, et. al. 2018. InvisiSpec: Making Speculative Execution Invisible in the Cache Hierarchy. In MICRO.
K. N. Khasawneh, et. al. 2018. Safespec: Banishing the spectre of a meltdown with leakage-free speculation. Archived.
V. Kiriansky, et. al. 2018. DAWG: A Defense Against Cache Timing Attacks in Speculative Execution Processors. In MICRO.
T. Kim, et. al. 2012. STEALTHMEM: System-Level Protection Against Cache-Based Side Channel Attacks in the Cloud. In USENIX.
F. Liu, et. al. 2016. CATalyst: Defeating last-level cache side channel attacks in cloud computing. In HPCA.
M. Taram, et. Al. 2019. Context-Sensitive Fencing: Securing Speculative Execution via Microsode Customization. In ASPLOS.
Microsoft: 2018. Microsoft's compiler-level Spectre fix shows how hard this problem will be to solve. In Ars Technica.

Open-source Approach to Hardware

Open-source HW + Agile Design Tools + Fast Simulation/Emulation = Security?

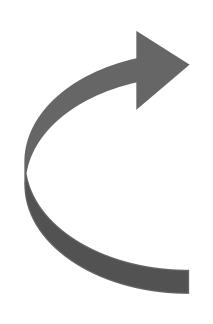
Large proliferation of open-source software stacks, cores, and simulation/design infrastructure

The Open-source RISC-V Approach





Security benefits from open-source work

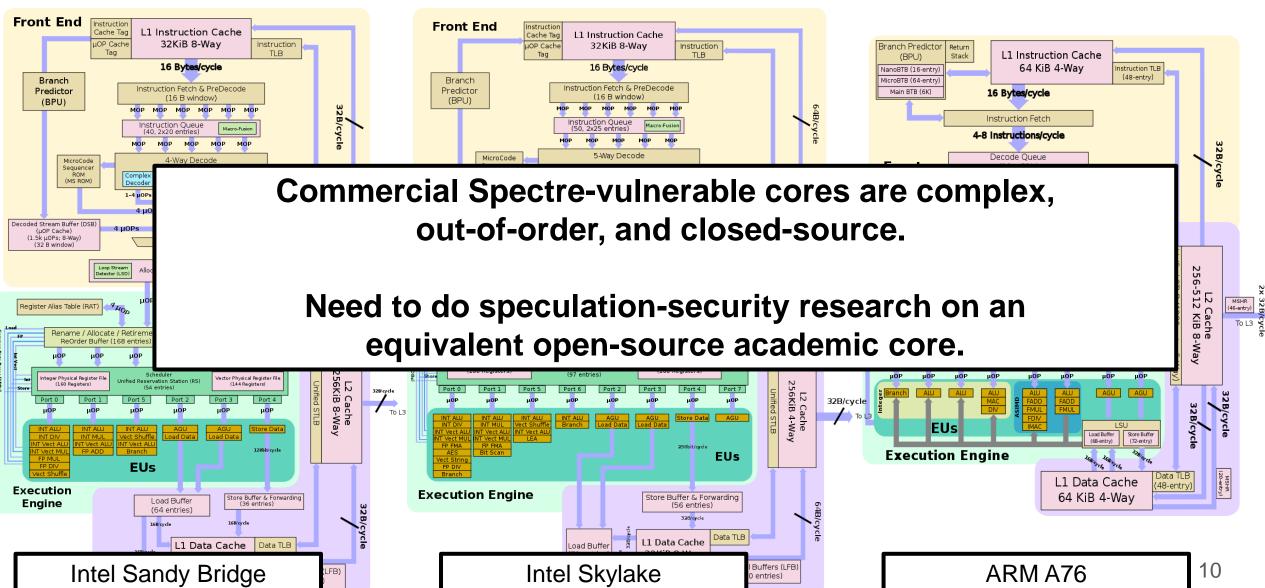


- 1. Think of new security mitigation/exploit
- 2. Use open-source RTL to start implementation
- 3. Quickly iterate through design development with easy, fast, and free tooling
- 4. Open-source work and have others scrutinize or use your work

Modern Microarchitectures







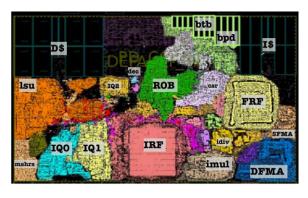
BOOM: The Berkeley Out-of-Order Machine

BOOM Overview

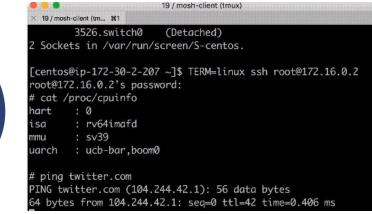




- Open-source, out-of-order, superscalar RISC-V core
- Runs RISC-V ISA RV64GC
- Linux-capable boots Fedora + Buildroot
- Silicon-proven taped out
- ~18K LoC of open-source Chisel RTL
- Highly parameterizable and configurable
- Full integration with Rocket Chip, FireSim, HAMMER









J. Bachrach, et. al. 2012. Chisel: constructing hardware in a scala embedded language. In DAC.

K. Asanovic, et. al. 2016. The Rocket Chip Generator. Technical Report.

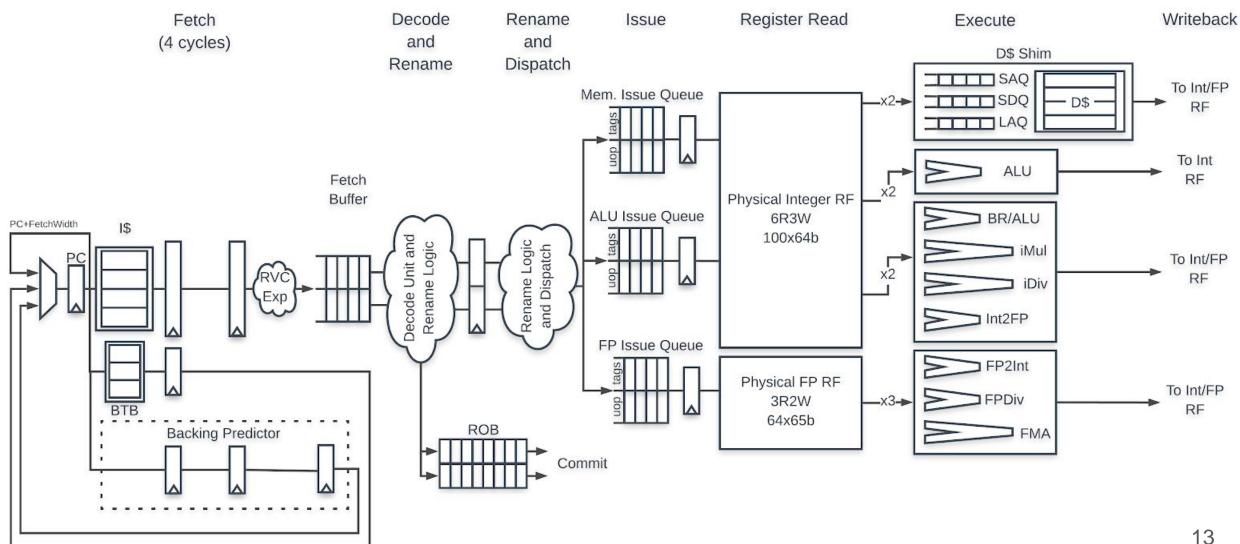
S. Karandikar, et. al. 2018. FireSim: FPGA-accelerated cycle-exact scale-out system simulation in the public cloud. In ISCA.

E. Wang, et. al. 2018. Hammer: Enabling Reusable Physical Design. In WOSET.

BOOM Microarchitecture







Replicating Spectre Attacks

Spectre v1 Overview





Speculation:

- Performance-seeking behavior of modern processors
- Execute instructions before we know they will commit

Side-channel:

- Microarchitectural state which holds interacts with program execution
- Caches, TLBs, power...

Typical Spectre attack:

- 1. Setup processor to misspeculate in victim code (e.g. train branch predictors)
- 2. Misspeculation leaks secret into a side channel
- Attacker recovers secret from side channel

Spectre v1 Example





16

Steps:

- 1. Access *if* statement multiple times correctly (predict *if* to fall-through)
- 2. Give $x > array1_sz$
- 3. Predict the *if* to be true and bring in secret and array2 value
- 4. Use the time difference between cached and uncached lines to determine secret
- 5. Repeat!

```
if (x < array1_sz):
     secret = array1[x]
     out = array2[secret * amount]
    before
                             after
     array2
                              array2
                            addresses
   addresses
                   all
    0*amount
                             0*amount
              uncached
                                        cached
    1*amount
                             1*amount
                             2*amount
    2*amount
                             3*amount
    3*amount
    4*amount
                             4*amount
```

Components Needed – With BOOM?





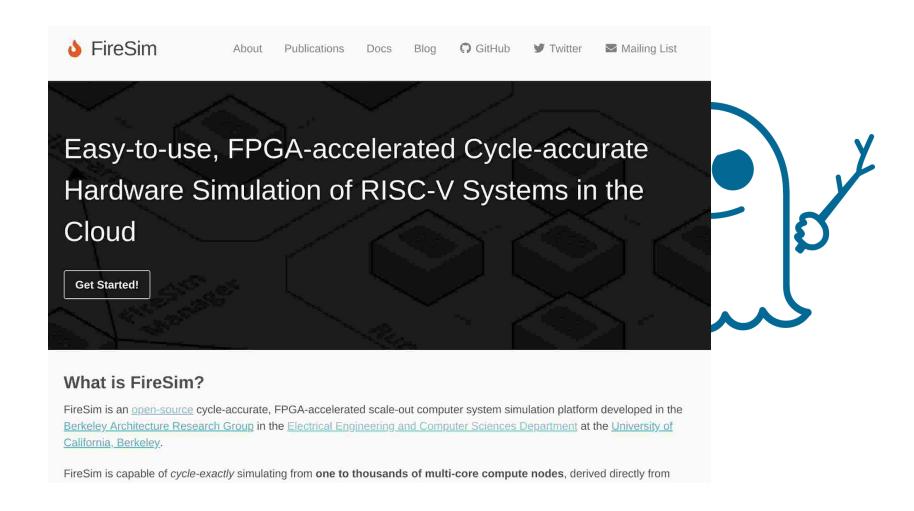
- Branch Prediction
 - Set associative BTB and GShare branch predictors
- Speculative Execution
 - Out-of-order execution and branch kill masks for speculative execution
- Caching
 - L1 data cache and a outer memory set to the latency of an L2 cache
- Cache Manipulation
 - Custom-made L1 data cache clflush

BOOM provides all the elements to replicate Spectre!

Spectre v1 Running on FireSim







```
HE LE YES HAVE BOOK THE WORLD
REMODES NOT THE EXPLORATE THE BASE FROM THE
BLANKER LIVER : TO FRENCH --- DASK For FRENCH
BLMDORTSIM | THRESTEE --- SMARL THRESTEE'S
BARDORLESHE BAPARENE --> DADB(THENETAL)
DOMESTING RESOURCES -++ DAMESTABLES
Avision time: - electrical --- management
ALBOOD CHAIL RESIDENCE --- DASKER WIND LLD
NAMES OF TAXABLE PART OF TAXAB
mumbertier: wermicht --- matelenetatis)
matter (ide: Signite2) \longrightarrow Mate(Signite22)
0x800001364: 38613623 --- MASK 18863923)
Execos(1500) Taccount --- MASA(tuccos(1))
0x800001300c1.wt3022797.-++ 2x580x0x12227963
8x80001264; 56450702 ---- BASK(5A490790)
6480001364; ALDRESS -> MARANTEN
sting but "secret" alrey
executions: wastern and furnit goessile; amount of biles, bythe i
                                                                                                                     Second assess(3) amount of Mrs.( 5/560
execution (country) who for an execution amount of Mins. Type
                                                                                                                     (second source)) around of Notic 17100
tamous (f) who first good () amount of intelligities
                                                                                                                     becaled (priess) ) amount of Mrts.( 1/10)
buildODSACO: wantible of a First gueroubble amount of Indical Types
                                                                                                                     hecard guess() present of Nytal 27300
$4800050041 extensió silv Parah puestoso amente of hiteatido/dol
                                                                                                                      second material) around an Syruc 1/100
bobbbs(525): wanto(a) in't Puralt guesade) amount of hites for 60
                                                                                                                     Decirod guess() Amount of MVILC 2/980
momentals; waster +h- forst generals amount of hitse William
                                                                                                                     pecand gomes (T) imposed of title ( 2/18)
formobilities: woodern who figure guernists amount of Mirai, 1950)
                                                                                                                     become minutely precent of Althur 27000.
                                                                                                                                                 3 second of filtra: 2/16/91/wide Simulation Status & 5605 46-12-1937/30.89446
Namico 1975; washiri with Pirty guardest arrests of hitse Scholl 1
                                                                                                                    necovid mensi.
scatteriology; wanted who Pictor question amount of Initial th/Sen-
bellows1524; wanted to An Pictor question amount of Initial Security
                                                                                                                                                                                                 This worklout's outpot, is facated inc.
                                                                                                                      second mental arount of Witt 17800.
                                                                                                                                                                                                 mana/castca_Pf.resbridgstay/results_warkings/(btth-81-12--25-06-24-atopt-detrest_detail
                                                                                                                     second games (f.) amount of filts(-2/16).
fe8000352bc eact(r) viv. Porst gusse(r) wearn of https://d/id/
                                                                                                                      second electric prount of Vital 2/167
                                                                                                                                                                                                 Titles right in large by Lincolned time:
second querial 3 amount of Mytat 2/400
                                                                                                                     pecsed gomes(*) sessent of title( 3/18)
SHROOKSSDET WARREST A NO. FIRST GURRACTO AMOUNT AF MARKE BYRD
                                                                                                                      necond assessible ensures of balls 3/161
GABOOKSSM': wante(3) w/w Picraft guelou(3) amount of Mitral Wildle
                                                                                                                     percent guests in mount of hitse TVBS.
execonditions wantout you factor question amount of Miller Wildo
                                                                                                                      second games(") weeket of this 2/MI
                                                                                                                                                                                                Instance St., 250,368 J. 21 ( TerMinsted: Falue
firmitte (531: western) +5x Firsh greeners amount of Mitral $550)
                                                                                                                      ORON SatW To travers Classes become
BARROOKSEC: MARKE [2] MIN. Plant goods(2) amount of MAILENANG
                                                                                                                     becalled games (WE amount of https: (2/18))
(#80001533); earth(i) ele filrat pares(ii) weamt of htts:(ib/100)
                                                                                                                      parant status I wasnet of Mits. 1/300
BuildOEDSS4; word(1) = " First purso(1) amount of M(1)(10/10)
                                                                                                                     second guess(/1 arount of hits); 2/181
GARGETS IN HARTON WAS FIRST GRADE (II) AMOUNT OF MUSICIPATE
                                                                                                                                                                                                 second gonos(5) anount of fits: 2/16)
SHROOMERSON: wanter of rafe thank govern(-) amount of MALL SAND
                                                                                                                      second numeral 3 second of Mittal 3/300.
EMBODESSET: MANDEES HIT FIRST QUARTED HORSES OF BUESL SYSDE
                                                                                                                     pecand goessial amount of Vital 2/187
                                                                                                                                                                                                 Inchese Mr. 200,588 J. St. C. Selr seast-petrost-deck | Ste number; Sin-
tadooriscii: eantori nin Piret queent) atendi sil MitsEllivido
                                                                                                                      potent games at amount of hitsel 2018)
                                                                                                                                                                                                  Selection (Size) want (a) why Pirsh goesaled amount of Mitsi Syleti
                                                                                                                     percent puressi (i) amount of http://dillin
EXECUTION: VEHICLES HIS Plant guerrico amount of hitel $750
                                                                                                                     necond plans () amount of Nite 2/300
                                                                                                                                                                                                 TOTAL CONTRACTOR OF THE PARTY O
field008152h: esett(x) =0= forst gates(x) searet of MALLES/360
                                                                                                                     second manual/s lescent of Attnl 7/140
Bulli00350x; want(5):+0+ First queso(6) amount of BUEN. T/II01
                                                                                                                                                                                               1/3 imitences are critic tenestry.
                                                                                                                     person guest() amount of MVtx( T/380)
                                                                                                                                                                                                the street attance over attill, comment
Building State: weekless with Phrist (weekles) who are of buttering the
                                                                                                                     second goess() amount of MitsE 7/500
BARROSCOURT MANERAL HOW From E- recorded amount of MARKE BISED | control doubtle amount of MARKE INTER-
* O'D meanings of the last in the
                                                                                                                                                                                                                                                                                                                            THE R. LEWIS CO., LANSING, MICH.
```

Implementing a Speculation Buffer

Protecting Data Caches



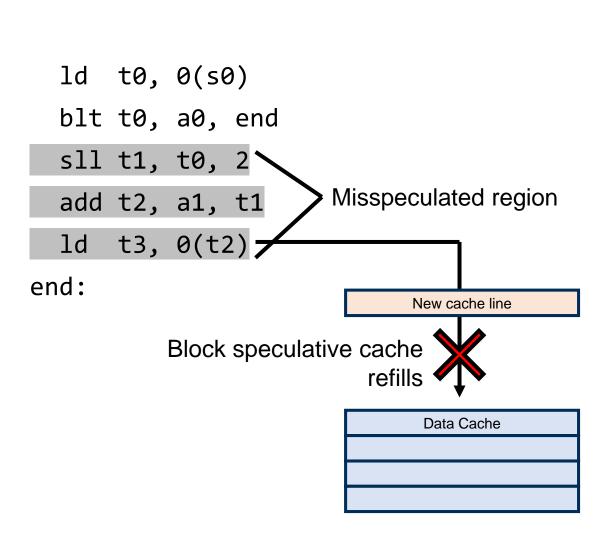


Problem: Load refills are not subject to architectural guarantees

 Misspeculated loads leave sideeffects, creating a side-channel

Solution: Treat the data cache as an architectural structure

- Only alter the cache state when instructions commit
- Implement a working prototype in BOOM RTL



Prior Work





InvisiSpec

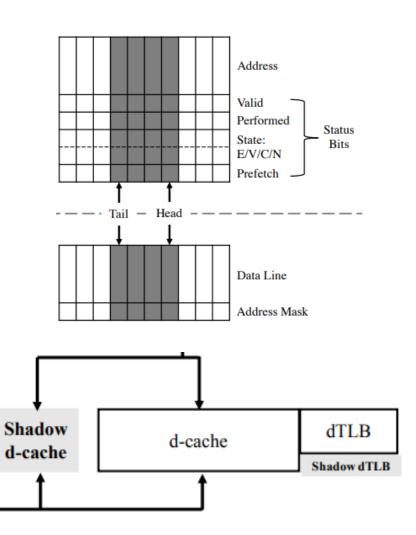
- Per load-queue-entry speculation buffer
- Speculation-aware cache-coherence policy

Safespec

- Speculation-depth sized "shadow structures"
- Protect DCache, ICache, TLBs

BOOM Speculation Buffer:

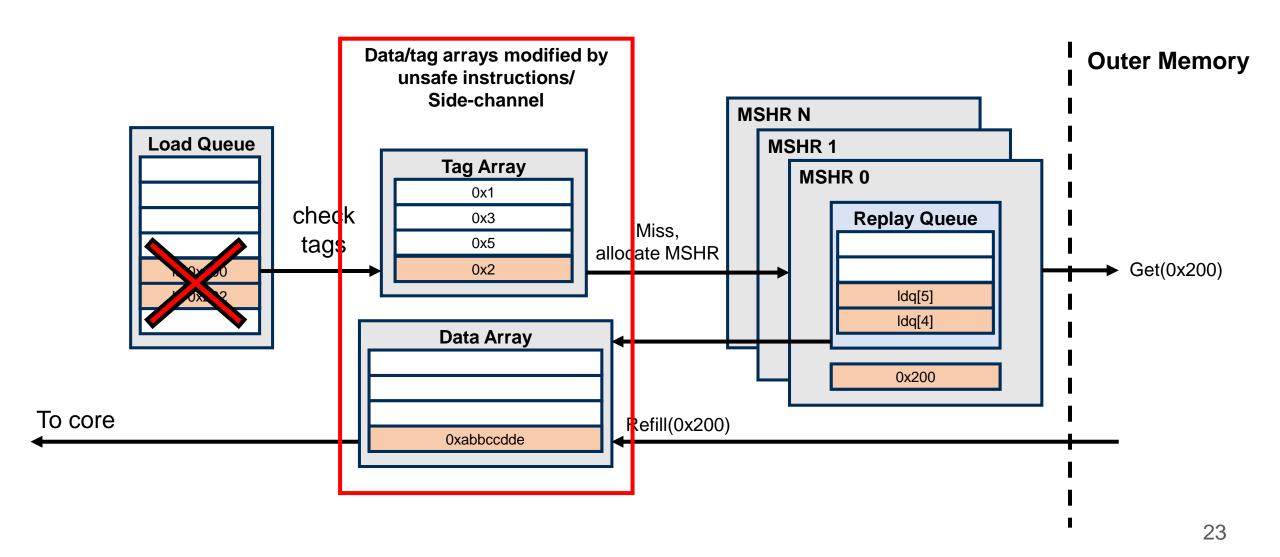
 Hold speculated loads in line-fillbuffers



Life of a Misspeculated Load



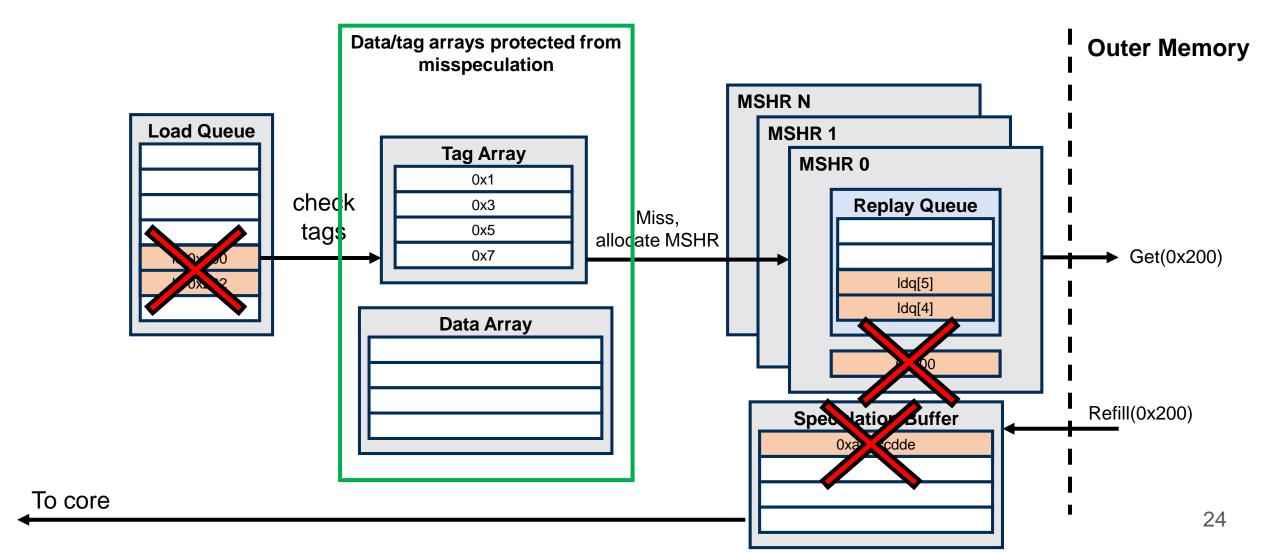




Blocking Misspeculated Loads



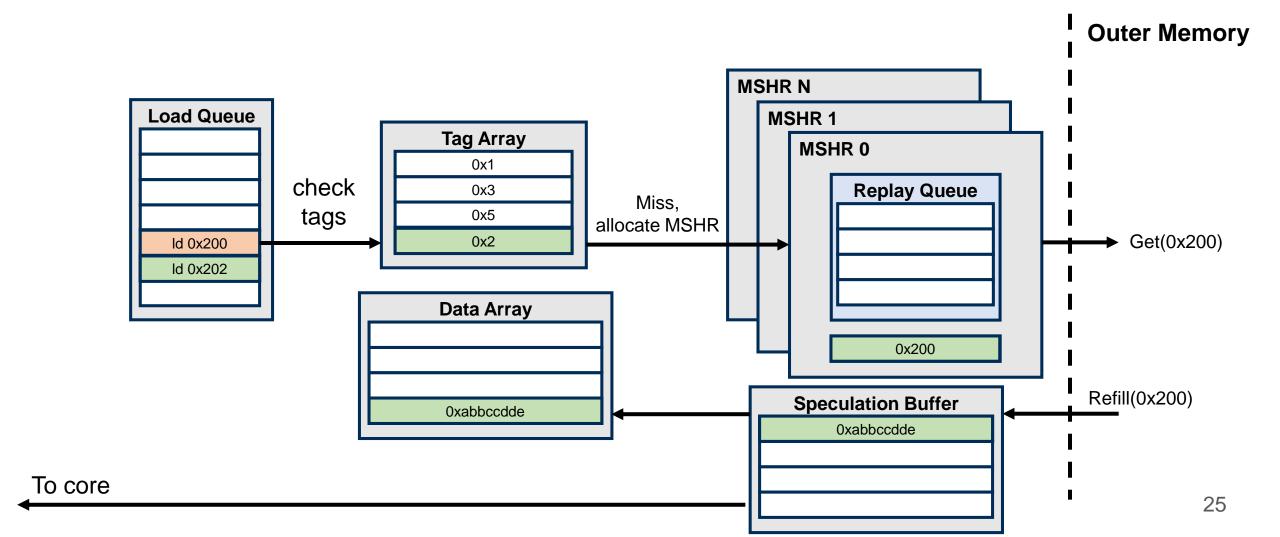




Blocking Misspeculated Loads







Blocking Misspeculated Loads





- Load refills wait in the buffer until one of their misses has committed
- Stall writeback until one of the following occurs
 - A load-miss to that line has committed OR
 - A store-miss hits that line (stores are non-speculative)
- If all load misses to that line were misspeculated, discard it
- Bypass loads out of the load-fill-buffer
 - Subsequent loads "see" the data in the DCache
 - Minimizes performance penalty

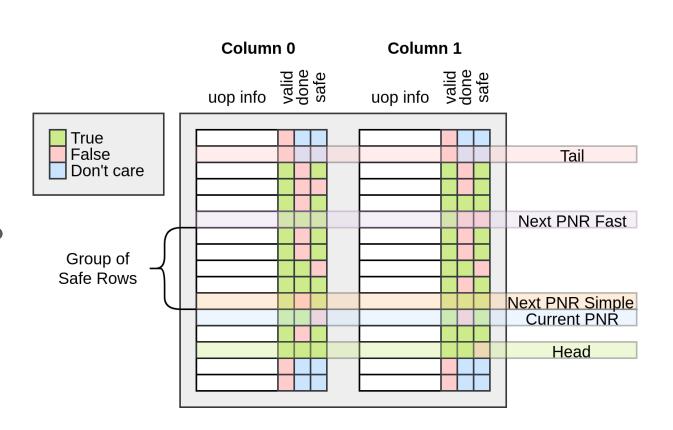
Committing Loads





When to commit load refills to the DCache?

- When the ROB commits the load?
 - Most secure.
 - Huge performance penalty for load misses
- When the load is free from branches?
 - Does not consider exceptions/interrupts
 - Minimal performance penalty
- When the load reaches the point-of-no-return
 - New ROB pointer, tracks instructions which are guaranteed to commit



Speculation Buffer Results





1 month implementation time Microbenchmarks

 Set of assembly routines to test edge cases

Dhrystone results

Original: 2176 dps

• W. Speculation buffer: 2216 dps

Impact: ~2% better IPC

Preliminary physical results in TSMC 45nm

~3% larger area

	<u>Version of BOOM</u>		
<u>Benchmark</u>	<u>Normal</u>	With Speculation Buffer	<u>%</u> Difference
Non-speculative LD misses to same sets	540 cycles	640 cycles	-19%
Non-speculative LD misses to different sets	264 cycles	297 cycles	-11%
MSHR evicted speculative LD misses	48 cycles	67 cycles	-40%
Dhrystone	2176 dps	2216 dps	+2%

Comparison





	InvisiSpec	SafeSpec	BOOM Speculation Buffer
Implementation Platform	Custom GEM5	Marssx86	BOOM RTL
Buffer size	Additional cacheline * load-queue-size	Additional cacheline * speculation depth	Repurposed line-fill- buffers
Commit condition	Wait for branch OR Wait for non-speculative	Wait for branch OR Wait for commit	Wait for point-of-no-return
Physical design feedback	CACTI estimates	CACTI estimates	Trial TSMC 45nm implementation
Protected components	L1D, LLC, multicores	L1D, L1I, TLBs	L1D
Performance impact	-22% performance	+3% performance	+2% performance

Conclusion

Conclusion





Demonstrated application of RISC-V ecosystem towards secure hardware

- Working demonstrations of Spectre attacks on a RISC-V core
- RTL of Spectre mitigation available in an open-source core

Continue improving BOOM security

- Secure other structures: TLBs, ICache, LLC, branch predictors
- Enable secure enclave execution

BOOMv3 Tapeout + More Attacks

- Planning to add Speculation Buffer and CSRs to enable/disable it
- More attacks with different predictors/structures (TAGE, RAS, etc)

Questions?

Thanks CARRV19!

Contact: {abe.gonzalez,bkorpan,jzh,edyounis,krste}@berkeley.edu

Links:

- Core: boom-core.org
- Github: github.com/riscv-boom
- FireSim: fires.im
- HAMMER: github.com/ucb-bar/hammer

Thanks:

- Chris Celio, David Kohlbrenner
- UCB ADEPT Lab