A Systematic Evaluation of Transient Execution Attacks and Defenses

Claudio Canella (@cc0x1f)$^1$, Jo Van Bulck$^2$, Michael Schwarz$^1$, Moritz Lipp$^1$, Benjamin von Berg$^1$, Philipp Ortner$^1$, Frank Piessens$^2$, Dmitry Evtyushkin, Daniel Gruss$^1$

August 14, 2019

$^1$ Graz University of Technology, $^2$ imec-DistriNet, KU Leuven, $^3$ College of William and Mary
• Clear up naming confusion
Motivation

- Clear up naming confusion
- Systematic analysis shows new variants
Motivation

• Clear up naming confusion
• Systematic analysis shows new variants
• Show defenses cost performance and do not fully work
Motivation

- Clear up **naming confusion**
- Systematic analysis shows **new variants**
- Show defenses **cost performance and do not fully work**
- **Gadget prevalence in Linux kernel**
• CPU uses data in out-of-order execution before permission check
• CPU uses data in out-of-order execution before permission check
• Meltdown can read any kernel address
• CPU uses data in out-of-order execution before permission check
• Meltdown can read any kernel address
• Physical memory is usually mapped in kernel
• CPU uses data in out-of-order execution before permission check
• Meltdown can read any kernel address
• Physical memory is usually mapped in kernel
→ Read arbitrary memory
Problem Solved?

- Meltdown *fully mitigated* in software
• Meltdown fully mitigated in software
• Problem seemed to be solved
• Meltdown *fully mitigated* in software
• Problem *seemed* to be solved
• No attack surface left
Problem Solved?

- Meltdown **fully mitigated** in software
- Problem **seemed** to be solved
- No attack surface left
- That is what everyone thought
Meltdown is a whole category of vulnerabilities
Meltdown is a whole category of vulnerabilities
Not only the user-accessible check
• User/Supervisor bit defines in which privilege level the page can be accessed
Meltdown Variants

Pagefault
Meltdown Variants

Pagefault \rightarrow \text{Meltdown-US}
Meltdown Variants

Meltdown Variants

Pagefault → Meltdown-US → Meltdown-US-L1
Pagefault → Meltdown-P → Meltdown-US-L3
Pagefault → Meltdown-RW → Meltdown-US-LFB
Pagefault → Meltdown-PK

Meltdown Variants

Pagefault

- Meltdown-US
- Meltdown-P
- Meltdown-RW
- Meltdown-PK
- Meltdown-XD
- Meltdown-SM

- Meltdown-US-L1
- Meltdown-US-L3
- Meltdown-US-LFB
operation \#n
Meltdown Root Cause

operation \#n

data

time
Meltdown Root Cause

Operation #n

Data

Data dependency

Operation #n+2

time

Meltdown Root Cause

operation \#n

exception
data
data dependency
operation \#n+2

possibly architectural

time

transient execution

Meltdown Root Cause

- Operation \#n
- Retire
- Exception
- Data dependency
- Operation \#n+2
- Transient execution
- Possibly architectural
- Time

Meltdown Root Cause

Operation \( \#n \) retire

Data dependency

Operation \( \#n+2 \)

Possibly architectural transient execution

Time

Exception

Meltdown
Meltdown Root Cause

operation \#n

exception

raise

Meltdown

data dependency

operation \#n+2

transient execution

possibly architectural
time

Transient cause?
Meltdown Tree

Transien cause?

Meltdown-type

Meltdown Tree

Transient cause?

Meltdown-type

- Meltdown-NM
- Meltdown-AC
- Meltdown-DE
- Meltdown-PF
- Meltdown-UD
- Meltdown-SS
- Meltdown-BR
- Meltdown-GP

Fault type

Meltdown-US
- Meltdown-US-L1
- Meltdown-US-L3
- Meltdown-US-LFB

- Meltdown-P
- Meltdown-RW
- Meltdown-PK
- Meltdown-XD
- Meltdown-SM
- Meltdown-MPX
- Meltdown-BND
• Spectre is a second class of transient execution attack
Spectre is a second class of transient execution attack
Instead of faults, exploit control (or data) flow predictions
operation \#n
operation \#n

prediction

time
Spectre Root Cause

operation \#n

prediction

predict CF/DF

operation \#n+2

time

Spectre Root Cause

operation \#n

prediction

operation \#n+2

possibly architectural

transient execution

time

Spectre Root Cause

operation #n

retire

prediction

predict
CF/DF

operation #n+2

possibly architectural

transient execution

time

Spectre Root Cause

Operation #n

Prediction

Operation #n+2

Flush pipeline on wrong prediction

Predict CF/DF

Possibly architectural transient execution

time
Spectre Root Cause

operation \#n

prediction

operation \#n+2

possibly architectural

transient execution

flush pipeline on wrong prediction

time
• Many predictors in modern CPUs
Many predictors in modern CPUs
- Branch taken/not taken (PHT)
Many predictors in modern CPUs
- Branch taken/not taken (PHT)
- Call/Jump destination (BTB)
Many predictors in modern CPUs
- Branch taken/not taken (PHT)
- Call/Jump destination (BTB)
- Function return destination (RSB)
• Many predictors in modern CPUs
  • Branch taken/not taken (PHT)
  • Call/Jump destination (BTB)
  • Function return destination (RSB)
  • Load matches previous store (STL)
Many predictors in modern CPUs
  - Branch taken/not taken (PHT)
  - Call/Jump destination (BTB)
  - Function return destination (RSB)
  - Load matches previous store (STL)

Most are even shared among processes
Spectre Mistraining

same address space/
in place

Victim

branch
Spectre Mistraining

same address space/
out of place

same address space/
in place

Victim

Congruent branch

Address collision

Victim branch

Spectre Mistraining

- Same address space, out of place
- Same address space, in place

Victim

Congruent branch

Address collision

Victim branch

Shared Branch Prediction State

Spectre Mistraining

Victim

same address space/
out of place

Congruent
branch

Address
collision

Victim
branch

Attacker

same address space/
in place

Shared Branch Prediction State

Spectre Mistraining

same address space/
out of place

same address space/
in place

Congruent branch

Address collision

Victim

Attacker

Shadow branch

cross address space/
in place

Shared Branch Prediction State

Spectre Mistraining

same address space/out of place

Victim

Congruent branch

Address collision

Victim branch

Attacker

 Congruent branch

Address collision

Shadow branch

Shared Branch Prediction State

cross address space/out of place

cross address space/in place

Transient cause?
Spectre Variants

Transient cause?

Spectre-type

prediction

Transient
cause?
Spectre Variants

Transient cause?

microarchitectural buffer

Spectre-type

Spectre-PHT

Spectre-BTB

Spectre-RSB

Spectre-STL

Spectre Variants

Transient cause?

Spectre-type

- Spectre-PHT
  - Cross-address-space
  - Same-address-space
- Spectre-BTB
  - Cross-address-space
  - Same-address-space
- Spectre-RSB
  - Cross-address-space
  - Same-address-space
- Spectre-STL
  - Cross-address-space
  - Same-address-space

microarchitectural buffer

prediction

Spectre Variants

Spectre-type

- Spectre-PHT
- Spectre-BTB
- Spectre-RSB
- Spectre-STL

Transient cause?

microarchitectural buffer

mistraining strategy

Cross-address-space
- Spectre-PHT
- Spectre-BTB
- Spectre-RSB
- Spectre-STL

Same-address-space
- Spectre-PHT
- Spectre-BTB
- Spectre-RSB
- Spectre-STL

in-place (IP) vs., out-of-place (OP)

PHT-CA-IP
PHT-CA-OP
PHT-SA-IP
PHT-SA-OP

BTB-CA-IP
BTB-CA-OP
BTB-SA-IP
BTB-SA-OP

RSB-CA-IP
RSB-CA-OP
RSB-SA-IP
RSB-SA-OP

prediction

• Spectre is **not a bug**
Spectre Fix

- Spectre is not a bug
- It is an useful optimization
Spectre Fix

- Spectre is not a bug
- It is an useful optimization
→ Cannot simply fix it (as with Meltdown)
• Spectre is not a bug
• It is an useful optimization
→ Cannot simply fix it (as with Meltdown)
• Workarounds for critical code parts
Spectre defenses in 3 categories:

- **C1** Mitigating or reducing the accuracy of covert channels
- **C2** Mitigating or aborting speculation
- **C3** Ensuring secret data cannot be reached
Many countermeasures only consider the cache to get data...
Many countermeasures only consider the cache to get data...
...but there are other possibilities, e.g.,
• Many countermeasures only consider the cache to get data...
• ...but there are other possibilities, e.g.,
  • Port contention (SMoTherSpectre)
• Many countermeasures *only consider the cache* to get data...
• ...but there are other possibilities, e.g.,
  • Port contention (SMoTherSpectre)
  • AVX (NetSpectre)
Many countermeasures only consider the cache to get data...

...but there are other possibilities, e.g.,

- Port contention (SMoTherSpectre)
- AVX (NetSpectre)

Cache is just the easiest
### Spectre Defenses: Microarchitectural Target

<table>
<thead>
<tr>
<th>Defense</th>
<th>Cache</th>
<th>TLB</th>
<th>BTB</th>
<th>BHB</th>
<th>PHT</th>
<th>RSB</th>
<th>AVX</th>
<th>FPU</th>
<th>Execution Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microarchitectural Element</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Category:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>C1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>C2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>C3</td>
</tr>
</tbody>
</table>

Considers element (●), partially considers it/same technique possible (○), or does not consider it (○).
## Spectre Defenses: Microarchitectural Target

<table>
<thead>
<tr>
<th>Defense</th>
<th>InvisSpec</th>
<th>SafeSpec</th>
<th>DAWG</th>
<th>Taint Tracking</th>
<th>Timer Reduction</th>
<th>Retpoline</th>
<th>SLH</th>
<th>YSNB</th>
<th>IBRS</th>
<th>STIPB</th>
<th>IBPP</th>
<th>Serialization</th>
<th>Sloth</th>
<th>SSBD</th>
<th>SSBB</th>
<th>Poison Value</th>
<th>Index Masking</th>
<th>Site Isolation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microarchitectural Element</td>
<td>Cache</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>TLB</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>BTB</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>BHB</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>PHT</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>RSB</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>AVX</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>FPU</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Execution Ports</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Category:

- **C1**: Considers element (●), partially considers it/same technique possible (○), or does not consider it (⊙).
- **C2**: Additional considerations.
- **C3**: Advanced or experimental categories.

### Spectre Defenses: Microarchitectural Target

<table>
<thead>
<tr>
<th>Defense</th>
<th>InvisSpec</th>
<th>SafeSpec</th>
<th>DAWG</th>
<th>Taint Tracking</th>
<th>Timer Reduction</th>
<th>RSB Stuffing</th>
<th>Retpoline</th>
<th>SLH</th>
<th>YSNB</th>
<th>IBRS</th>
<th>STIPB</th>
<th>IBPB</th>
<th>Serialization</th>
<th>Sloth</th>
<th>SSBD</th>
<th>SSBB</th>
<th>Poison Value</th>
<th>Index Masking</th>
<th>Site Isolation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cache</td>
<td>● ● ●</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TLB</td>
<td>● ● ○</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BTB</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BHB</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PHT</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RSB</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AVX</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FPU</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Execution Ports</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Microarchitectural Element
- Cache
- TLB
- BTB
- BHB
- PHT
- RSB
- AVX
- FPU

#### Category:
- **C1**
- **C2**
- **C3**

Considers element (●), partially considers it/same technique possible (○), or does not consider it (○).
## Spectre Defenses: Microarchitectural Target

<table>
<thead>
<tr>
<th>Defense</th>
<th>InvisSpec</th>
<th>SafeSpec</th>
<th>DAWG</th>
<th>Taint Tracking</th>
<th>Timer Reduction</th>
<th>RSB Stuffing</th>
<th>Retpoline</th>
<th>SLH</th>
<th>YSNB</th>
<th>IBRS</th>
<th>STIPB</th>
<th>IBPP</th>
<th>Serialization</th>
<th>Sloth</th>
<th>SSBD</th>
<th>SSBB</th>
<th>Poison Value</th>
<th>Index Masking</th>
<th>Site Isolation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cache</td>
<td>● ● ● ● 0</td>
<td>0 0 0 0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TLB</td>
<td>0 ● ● 0</td>
<td>0 0 0 0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BTB</td>
<td>0 0 0 0</td>
<td>0 0 0 0</td>
<td>●</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BHB</td>
<td>0 0 0 0</td>
<td>0 0 0 0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PHT</td>
<td>0 0 0 0</td>
<td>0 0 0 0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RSB</td>
<td>0 0 0 0</td>
<td>0 0 0 0</td>
<td>●</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AVX</td>
<td>0 0 0 0</td>
<td>0 0 0 0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FPU</td>
<td>0 0 0 0</td>
<td>0 0 0 0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Execution Ports</td>
<td>0 0 0 0</td>
<td>0 0 0 0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Category:**
- **C1**: Considers element (●), partially considers it/same technique possible (○), or does not consider it (○).
- **C2**: Considers element (●), partially considers it/same technique possible (○), or does not consider it (○).
- **C3**: Considers element (●), partially considers it/same technique possible (○), or does not consider it (○).

## Spectre: Defense Analysis

<table>
<thead>
<tr>
<th>Attack</th>
<th>Defense</th>
</tr>
</thead>
</table>
| Intel  | Spectre-PHT  
Spectre-BTB  
Spectre-RSB  
Spectre-STL |
| ARM    | Spectre-PHT  
Spectre-BTB  
Spectre-RSB  
Spectre-STL |
| AMD    | Spectre-PHT  
Spectre-BTB  
Spectre-RSB  
Spectre-STL |

Symbols show if an attack is mitigated (●), partially mitigated (○), not mitigated (□), theoretically mitigated (■), theoretically impeded (□), not theoretically impeded (■), or out of scope (○).
<table>
<thead>
<tr>
<th>Attack</th>
<th>Defense</th>
<th>InvisiSpec</th>
<th>SafeSpec</th>
<th>DAVG</th>
<th>RSB Stuffing</th>
<th>Retpoline</th>
<th>Poison Value</th>
<th>Index Masking</th>
<th>Site Isolation</th>
<th>SLH</th>
<th>YSNB</th>
<th>IBRS</th>
<th>STIPB</th>
<th>IBPB</th>
<th>Serialization</th>
<th>Taint Tracking</th>
<th>Timer Reduction</th>
<th>Sloth</th>
<th>SSBD/SSBB</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intel</td>
<td>Spectre-PHT</td>
<td>●</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Spectre-BTB</td>
<td>●</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Spectre-RSB</td>
<td>●</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Spectre-STL</td>
<td>●</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ARM</td>
<td>Spectre-PHT</td>
<td>●</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Spectre-BTB</td>
<td>●</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Spectre-RSB</td>
<td>●</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Spectre-STL</td>
<td>●</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AMD</td>
<td>Spectre-PHT</td>
<td>●</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Spectre-BTB</td>
<td>●</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Spectre-RSB</td>
<td>●</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Spectre-STL</td>
<td>●</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Symbols show if an attack is mitigated (●), partially mitigated (○), not mitigated (□), theoretically mitigated ( ■), theoretically impeded (□ ), not theoretically impeded (□ ), or out of scope (△).
## Spectre: Defense Analysis

<table>
<thead>
<tr>
<th>Attack</th>
<th>Defense</th>
<th>Intel</th>
<th>ARM</th>
<th>AMD</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Spectre-PHT</td>
<td>Spectre-PHT</td>
<td>Spectre-PHT</td>
</tr>
<tr>
<td></td>
<td></td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Spectre-BTB</td>
<td>Spectre-BTB</td>
<td>Spectre-BTB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Spectre-RSB</td>
<td>Spectre-RSB</td>
<td>Spectre-RSB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Spectre-STL</td>
<td>Spectre-STL</td>
<td>Spectre-STL</td>
</tr>
<tr>
<td></td>
<td></td>
<td>○</td>
<td>○</td>
<td>●</td>
</tr>
</tbody>
</table>

Symbols show if an attack is mitigated (●), partially mitigated (○), not mitigated (◇), theoretically mitigated (■), theoretically impeded (□), not theoretically impeded (◇), or out of scope (◇).
## Spectre: Defense Analysis

<table>
<thead>
<tr>
<th>Attack</th>
<th>Intel</th>
<th>ARM</th>
<th>AMD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spectre-PHT</td>
<td><img src="image" alt="Symbol" /></td>
<td><img src="image" alt="Symbol" /></td>
<td><img src="image" alt="Symbol" /></td>
</tr>
<tr>
<td>Spectre-BTB</td>
<td><img src="image" alt="Symbol" /></td>
<td><img src="image" alt="Symbol" /></td>
<td><img src="image" alt="Symbol" /></td>
</tr>
<tr>
<td>Spectre-RSB</td>
<td><img src="image" alt="Symbol" /></td>
<td><img src="image" alt="Symbol" /></td>
<td><img src="image" alt="Symbol" /></td>
</tr>
<tr>
<td>Spectre-STL</td>
<td><img src="image" alt="Symbol" /></td>
<td><img src="image" alt="Symbol" /></td>
<td><img src="image" alt="Symbol" /></td>
</tr>
</tbody>
</table>

Symbols show if an attack is mitigated (●), partially mitigated (○), not mitigated (◇), theoretically mitigated (■), theoretically impeded (□), not theoretically impeded (◇), or out of scope (◇).
Spectre: Defense Analysis

<table>
<thead>
<tr>
<th>Attack</th>
<th>Intel</th>
<th>Defense</th>
<th>ARM</th>
<th>AMD</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>InvisiSpec</td>
<td>RSB Stuffing</td>
<td>RSB Stuffing</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SafeSpec</td>
<td>Poison Value</td>
<td>Poison Value</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DAVG</td>
<td>Index Masking</td>
<td>Index Masking</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Retpoline</td>
<td>Site Isolation</td>
<td>Site Isolation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Poison Value</td>
<td>SLH</td>
<td>SLH</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Index Masking</td>
<td>YSNB</td>
<td>YSNB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Site Isolation</td>
<td>IBRS</td>
<td>IBRS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Serialization</td>
<td>STIPB</td>
<td>STIPB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Taint Tracking</td>
<td>IBPB</td>
<td>IBPB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Timer Reduction</td>
<td>Serialization</td>
<td>Timer Reduction</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Sloth</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>SSBD/SSBB</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Spectre-PHT</td>
<td>●</td>
<td>○</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Spectre-BTB</td>
<td>●</td>
<td>○</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Spectre-RSB</td>
<td>○</td>
<td>○</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Spectre-STL</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>●</td>
</tr>
</tbody>
</table>

Symbols show if an attack is mitigated (●), partially mitigated (○), not mitigated (◇), theoretically mitigated (■), theoretically impeded (□), not theoretically impeded (□), or out of scope (◇).
## Spectre: Defense Analysis

<table>
<thead>
<tr>
<th>Attack</th>
<th>Defense</th>
<th>Intel</th>
<th>ARM</th>
<th>AMD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spectre-PHT</td>
<td></td>
<td>•</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Spectre-BTB</td>
<td></td>
<td>•</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Spectre-RSB</td>
<td></td>
<td>•</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>Spectre-STL</td>
<td></td>
<td>•</td>
<td>•</td>
<td></td>
</tr>
</tbody>
</table>

Symbols show if an attack is mitigated (●), partially mitigated (○), not mitigated (○), theoretically mitigated (■), theoretically impeded (□), not theoretically impeded (□), or out of scope (◇).
## Spectre: Defense Analysis

<table>
<thead>
<tr>
<th>Attack</th>
<th>Defense</th>
<th>InvisSpec</th>
<th>SafeSpec</th>
<th>DAVG</th>
<th>RSB Stuffing</th>
<th>Retpoline</th>
<th>Poison Value</th>
<th>Index Masking</th>
<th>Site Isolation</th>
<th>SLH</th>
<th>YSNB</th>
<th>IBRS</th>
<th>ST/PB</th>
<th>IBPB</th>
<th>Serialization</th>
<th>Taint Tracking</th>
<th>Timer Reduction</th>
<th>Sloth</th>
<th>SSBD/SSBB</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intel</td>
<td>Spectre-PHT</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Spectre-BTB</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Spectre-RSB</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Spectre-STL</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td></td>
</tr>
<tr>
<td>ARM</td>
<td>Spectre-PHT</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Spectre-BTB</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Spectre-RSB</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Spectre-STL</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td></td>
</tr>
<tr>
<td>AMD</td>
<td>Spectre-PHT</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Spectre-BTB</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Spectre-RSB</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Spectre-STL</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td></td>
</tr>
</tbody>
</table>

Symbols show if an attack is mitigated (●), partially mitigated (○), not mitigated (○), theoretically mitigated (■), theoretically impeded (□), not theoretically impeded (◇), or out of scope (◇).
# Spectre: Defense Analysis

<table>
<thead>
<tr>
<th>Attack</th>
<th>Defense</th>
<th>InvisSpec</th>
<th>SafeSpec</th>
<th>DAVG</th>
<th>RSB Stuffing</th>
<th>Retpoline</th>
<th>Poison Value</th>
<th>Index Masking</th>
<th>Site Isolation</th>
<th>SLH</th>
<th>YSNB</th>
<th>IBRS</th>
<th>STIPB</th>
<th>IBPB</th>
<th>Serialization</th>
<th>Taint Tracking</th>
<th>Timer Reduction</th>
<th>Sloth</th>
<th>SSBD/SSBB</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Intel</strong></td>
<td>Spectre-PHT</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
</tr>
<tr>
<td></td>
<td>Spectre-BTB</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
</tr>
<tr>
<td></td>
<td>Spectre-RSB</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
</tr>
<tr>
<td></td>
<td>Spectre-STL</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
</tr>
<tr>
<td><strong>ARM</strong></td>
<td>Spectre-PHT</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
</tr>
<tr>
<td></td>
<td>Spectre-BTB</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
</tr>
<tr>
<td></td>
<td>Spectre-RSB</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
</tr>
<tr>
<td></td>
<td>Spectre-STL</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
</tr>
<tr>
<td><strong>AMD</strong></td>
<td>Spectre-PHT</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
</tr>
<tr>
<td></td>
<td>Spectre-BTB</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
</tr>
<tr>
<td></td>
<td>Spectre-RSB</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
</tr>
<tr>
<td></td>
<td>Spectre-STL</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
</tr>
</tbody>
</table>

Symbols show if an attack is mitigated (●), partially mitigated (○), not mitigated (□), theoretically mitigated (■), theoretically impeded (□), not theoretically impeded (□), or out of scope (◇).
## Spectre Mitigating: Performance

<table>
<thead>
<tr>
<th>Defense Evaluation</th>
<th>Penalty</th>
<th>Benchmark</th>
</tr>
</thead>
<tbody>
<tr>
<td>KAISER/KPTI</td>
<td>0–2.6 %</td>
<td>System call rates</td>
</tr>
<tr>
<td>Retpoline</td>
<td>5–10 %</td>
<td>Real-world workload servers</td>
</tr>
<tr>
<td>Site Isolation</td>
<td>10–13 %</td>
<td>Memory overhead</td>
</tr>
<tr>
<td>InvisiSpec</td>
<td>22 %</td>
<td>SPEC</td>
</tr>
<tr>
<td>SafeSpec</td>
<td>-3 %</td>
<td>SPEC on MARSSx86</td>
</tr>
<tr>
<td>DAWG</td>
<td>1–15 %</td>
<td>PARSEC, GAPBS</td>
</tr>
<tr>
<td>SLH</td>
<td>29–36.4 %</td>
<td>Google microbenchmark suite</td>
</tr>
<tr>
<td>YSNB</td>
<td>60 %</td>
<td>Phoenix</td>
</tr>
<tr>
<td>IBRS</td>
<td>20–30 %</td>
<td>Sysbench 1.0.11</td>
</tr>
<tr>
<td>STIBP</td>
<td>30–50 %</td>
<td>Rodinia OpenMP, DaCapo</td>
</tr>
<tr>
<td>Serialization</td>
<td>62–74.8 %</td>
<td>Google microbenchmark suite</td>
</tr>
<tr>
<td>SSBD/SSBB</td>
<td>2–8 %</td>
<td>SYSmark 2018, SPEC integer</td>
</tr>
<tr>
<td>L1TF Mitigations</td>
<td>-3–31 %</td>
<td>SPEC</td>
</tr>
</tbody>
</table>
## Spectre: Linux Kernel Gadget Prevalence

<table>
<thead>
<tr>
<th>Gadget</th>
<th>Example (Spectre-PHT)</th>
<th>#Occurrences</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prefetch</td>
<td>if(i&lt;LEN_A){a[i];}</td>
<td>172</td>
</tr>
<tr>
<td>Compare</td>
<td>if(i&lt;LEN_A){if(a[i]==k){};}</td>
<td>127</td>
</tr>
<tr>
<td>Index</td>
<td>if(i&lt;LEN_A){y = b[a[i]*x];}</td>
<td>0</td>
</tr>
<tr>
<td>Execute</td>
<td>if(i&lt;LEN_A){a<a href="void">i</a>;}</td>
<td>16</td>
</tr>
</tbody>
</table>
You can find our proof-of-concept implementation and classification tree on:

- https://github.com/IAIK/transientfail
- http://transient.fail/
Recap

- Introduced a new naming scheme
- Discovered new attack variants
- Showed that defenses cost too much performance for little effect
- Showed prevalence of gadgets in Linux kernel
Recap

- Introduced a new naming scheme
- Discovered new attack variants
Recap

• Introduced a new naming scheme
• Discovered new attack variants
• Showed that defenses cost too much performance for little effect
Recap

- Introduced a new naming scheme
- Discovered new attack variants
- Showed that defenses cost too much performance for little effect
- Showed prevalence of gadgets in Linux kernel
• Transient Execution Attacks are...
• Transient Execution Attacks are...
  • ...a novel class of attacks
Conclusion

• Transient Execution Attacks are...
  • ...a novel class of attacks
  • ...extremely powerful
Transient Execution Attacks are...
  • ...a novel class of attacks
  • ...extremely powerful
  • ...only at the beginning
Conclusion

- Transient Execution Attacks are...
  - ...a novel class of attacks
  - ...extremely powerful
  - ...only at the beginning

- Many optimizations introduce side channels → now exploitable
A Systematic Evaluation of Transient Execution Attacks and Defenses

Claudio Canella (cc0x1f)\(^1\), Jo Van Bulck\(^2\), Michael Schwarz\(^1\), Moritz Lipp\(^1\), Benjamin von Berg\(^1\), Philipp Ortner\(^1\), Frank Piessens\(^2\), Dmitry Evtyushkin, Daniel Gruss\(^1\)

August 14, 2019

\(^1\) Graz University of Technology, \(^2\) imec-DistriNet, KU Leuven, \(^3\) College of William and Mary
We want to thank our shepherd, Jonathan McCune, for his helpful comments and suggestions that substantially helped in improving the paper. This work has been supported by the Austrian Research Promotion Agency (FFG) via the K-project DeSSnet, which is funded in the context of COMET – Competence Centers for Excellent Technologies by BMVIT, BMWFW, Styria and Carinthia. This work has been supported by the Austrian Research Promotion Agency (FFG) via the project ESPRESSO, which is funded by the province of Styria and the Business Promotion Agencies of Styria and Carinthia. This project has received funding from the European Research Council (ERC) under the European Union’s Horizon 2020 research and innovation programme (grant agreement No 681402). This research received funding from the Research Fund KU Leuven, and Jo Van Bulck is supported by the Research Foundation – Flanders (FWO). Evtyushkin acknowledges the start-up grant from the College of William and Mary. Additional funding was provided by generous gifts from ARM and Intel. Any opinions, findings, and conclusions or recommendations expressed in this paper are those of the authors and do not necessarily reflect the views of the funding parties.