Abstract—This paper studies information flow caused by speculation mechanisms in hardware and software. The Spectre attack shows that there are practical information flow attacks which use an interaction of dynamic security checks, speculative evaluation and cache timing. Previous formal models of program execution are designed to capture computer architecture, rather than micro-architecture, and so do not capture attacks such as Spectre. In this paper, we propose a model based on pomsets which is designed to model speculative evaluation. The model is abstract with respect to specific micro-architectural features, such as caches and pipelines, yet is powerful enough to express known attacks such as Spectre and PRIME+ABORT, and verify their countermeasures. The model also allows for the prediction of new information flow attacks. We derive two such attacks, which exploit compiler optimizations, and validate these experimentally against gcc and clang.

I. INTRODUCTION

This paper is about some of the lies we tell when we talk about programs.

An example lie (or to be more formal, a “leaky abstraction”) is the order of reads and writes in a program. We pretend that these happen in the order specified by the program text, for example we think of the program \((x := 0; x := 1; y := 2)\) as having three sequentially ordered write events:

\[
\begin{align*}
W x 0 & \quad W x 1 & \quad W y 2 \\
\end{align*}
\]

However, due to optimizations in hardware or compilers, instructions may be reordered, resulting in executions where the accesses of \(x\) and \(y\) are independent, and the hardware or compiler is free to reorder them:

\[
\begin{align*}
W x 0 & \quad W x 1 & \quad W y 2 \\
\end{align*}
\]

Instruction reordering optimizations are not problematic as long as they are not visible to user code, that is if programs are sequentially consistent. Unfortunately, multi-threaded programs can often observe reorderings. For example running the above writing thread concurrently with an observing thread \((\text{if } (y) \{ z := x \})\) can result in a sequentially inconsistent execution (where we highlight the matching write for each read):

Writing thread:
\[
\begin{align*}
W x 0 & \quad W x 1 & \quad W y 2 \\
\end{align*}
\]

Observing thread:
\[
\begin{align*}
R y 2 & \quad R x 0 & \quad W z 0 \\
\end{align*}
\]

To improve instruction throughput, hardware will often evaluate branches speculatively, and roll back any failed speculations. For example, hardware might incorrectly speculate that \(x\) is nonzero, speculatively execute a write to \(y\), but then roll it back and execute a write to \(z\):

\[
\begin{align*}
R x 0 & \quad W z 1 \\
\end{align*}
\]

Speculation is intended only to be visible at the microarchitectural level, but as Spectre shows, this abstraction is leaky, and in a way that allows side-channel attacks to be mounted.

Instruction reordering and speculative evaluation are similar leaky abstractions. Both were intended originally not to be visible to user code, but both abstractions have leaked. This opens some possible areas of investigation:

- Using ideas from relaxed memory for speculation. There is a significant literature showing how to build models of...
relaxed memory, for use in validating compilers, or proving correctness of programs. Less formally, they provide programmers with a way to visualize and communicate the behavior of their systems. Inspired by these models, we give a compositional model of program execution that includes speculation (§III and §IV) and show how it can be used to model known attacks (§V) on branch prediction [23] and transactional memory [10, 12].

- **Mounting attacks against speculation on relaxed memory.** Spectre shows how a leaky abstraction allows for the construction of side-channels which bypass dynamic security checks. Inspired by these attacks, we show how to mount information flow attacks against compiler optimizations, both against the model (§VII) and against existing compilers (§VIII). Fortunately, we were only able to mount the attacks against ahead-of-time compilers (where optimizations require secrets to be known at compile-time) and not just-in-time compilers (which can optimize based on run-time secrets). With the addition of shared-memory concurrency to JavaScript [14, §24.2], the attacks described in this paper might become feasible.

Readers who wish to focus on the impact of the model can skip to §V on first reading, referring to prior sections as needed.

**Acknowledgments:** We would like to thank the anonymous referees, and the paper shepherd Frank Piessens, whose comments helped greatly improve this paper. Jagadeesan and Riely are supported by National Science Foundation CCR-1617175.

## II. Related Work

Information flow provides a formal foundation for end-to-end security. Informally, a program is secure if there is no observable dependency of low-security outputs on high-security inputs. The precise formalization of this intuitive idea has been the topic of extensive research [38], encompassing a variety of language features such as non-determinism [46], concurrency [39], reactivity [43], and probability [17]. The static and dynamic enforcement of these definitions in general purpose languages [32] has influenced language design and implementation.

A key parameter in defining information flow is the observational power of the attacker model. Whereas the classical input-output behavior is often an adequate foundation, it has long been known [26, 6] that side-channels that leak information arise from other observables such as execution time and power consumption [47, 15]. This approach has also been pursued to develop model-checking techniques for Spectre-like attacks [41]. Like our work, [41] recognizes the role played by adapting techniques from relaxed memory.

In this paper, we adopt the opposite approach, attempting to understand Spectre-like attacks as abstractly as possible and thus to reveal the “essence” of Spectre. We develop a novel model of speculative evaluation and show that it is sufficient to both capture known attacks and predict new attacks. Our model is defined at the language level, rather than the hardware level; thus, we do not model micro-architectural details such as caches or timing.

Relaxed memory models [40, 29, 17, 48, 19, 21] allow speculative execution to varying degrees. Relaxed execution is known to affect the validity of information flow analyses [30, 43]. In these models, a valid execution is defined with reference to other possible executions of the program. These models are not, however, designed for modeling Spectre-style attacks on speculation. For example all of these models will consider the straight-line code:

\[
r := x; s := \text{SECRET}; a[r] := 1
\]

to be the same as the conditional code:

\[
r := x; s := \text{SECRET};
\]

\[
\text{if } (r == s) \{ a[s] := 1 \} \text{ else } \{ a[r] := 1 \}
\]

and indeed an optimizing compiler might choose to rewrite either of these programs to be the other.

An attacker can mount a Spectre-style attack on the conditional code, for example by setting \( x \) to be 0, flushing the cache, executing the program, then using timing effects to determine if \( a[1] \) is in the cache. If it is, then \( \text{SECRET} \) must have been 1. This attack is not possible against the straight-line code, and so any model trying to capture Spectre must distinguish them.

Most definitions of non-interference will say that in both programs, there is no observable dependency of the low-security outputs (\( a \)) on the high-security inputs (\( \text{SECRET} \)) and so both programs are safe. The only existing models of non-interference which capture this information flow are ones such as [47] which model micro-architectural features such as caching and timing.

In our model, the straight-line and conditional programs are not equated, since the conditional code has the execution:

\[
\begin{array}{c}
R x 0 \\
W a[0] 1 \\
W a[1] 1
\end{array}
\]

which is not matched in the straight-line code. Indeed, from an information-flow perspective, this refined treatment of dependencies in conditionals identifies a novel distinguishing feature of our model, namely that the traditional conditional is a self-composition operator in the sense of [38].

Static analyses such as the Smith-Volpano type system [39] will reject the conditional program, due to \( a[s] := 1 \), in which a
III. Model

Our model is based on partially ordered multisets \([16, 50]\) ("pomsets"), whose labels are given by read and write actions. These can be visualized as a graph where the edges indicate dependencies, for example \((r:= x; y:= 1; z:= r + 1)\) has an execution modeled by the pomset:

![Pomset Diagram]

The edge from \((R \times 1)\) to \((W \times 2)\) indicates a data dependency. Since there is no dependency between \((W \times 1)\) and \((W \times 2)\), the write actions may take place in either order. Such reorderings may arise in hardware (for example, caching) or in the compiler (for example, instruction reordering).

The novel aspect of the model is that events have preconditions, which give the thread-local view of memory. These are used in giving the semantics of conditionals and transactions, modeling failed branch prediction and aborted transactions. For example, the program

\[
\begin{cases}
  \text{if } (x) \{ y := 1; z := 1 \} & \text{else } \{ y := 2; z := 1 \}
\end{cases}
\]

has an execution:

![Execution Diagram]

The edges from \((R \times 1)\) to \((W \times 1)\) and \((W \times 2)\) indicate control dependencies. The presence of a crossed out \((W \times 2)\) indicates an event with an unsatisfiable precondition, modeling an unsuccessful speculation. Since the \((W \times 1)\) action is performed on both branches of the conditional, there is no control dependency from \((R \times 1)\).

We give the semantics of a program as a set of pomsets with event labels of the form \((\phi \mid a)\), where \(\phi\) is the event’s precondition (such as \(M = v\)) and \(a\) is the event’s action (such as \(W \times v\)). For example, the semantics of the program \((x:= M)\) includes the case where \(M\) is \(v\), which is written to \(x\), and is captured by the one-event pomset:

\[
M = v \mid W \times v
\]

We make few requirements of the logic of preconditions, save that it includes equalities between expressions, is closed under substitution, and supports a notion of implication.

The semantics is defined compositionally. As an example, we show how to construct one of the pomsets in \([r:= y; x:= r + 1]\). First, \([x:= r + 1]\) contains the pomset:

\[
r = 1 \mid W \times 2
\]

Next, we perform the substitution of \(r\) with 1 in every precondition, to get that \([x:= r + 1][1/r]\) contains the pomset:

\[
1 = 1 \mid W \times 2
\]

and since \((1 = 1)\) is a tautology, we elide it:

\[
W \times 2
\]

This substitution is performed in defining \([r:= y; x:= r + 1]\), which contains the pomset:

![Pomset Diagram]

\[
R \times 1 \rightarrow W \times 2
\]

There is an ordering \((R \times 1) < (W \times 2)\) (represented pictorially as an arrow) because the precondition \((r = 1)\) depends on \(r\). If the precondition was independent of \(r\) then there would be no ordering, for example \([r:= y; x:= r + 1 - r]\) contains the pomset:

![Pomset Diagram]

\[
R \times 1 \rightarrow W \times 1
\]

since the precondition \((r + 1 - r = 1)\) is independent of \(r\).

The main novelty of our semantics is the use of preconditions, which allow us to provide an unusual model of conditionals. In most models, an execution of \([\text{if} (M) \{ C \} \text{ else } \{ D \}]\) would either be given by an execution from \([C]\) or from \([D]\), but not both. In our semantics, a pomset in \([\text{if} (M) \{ C \} \text{ else } \{ D \}]\) may include both a pomset from \([C]\) and a pomset from \([D]\). For example, \([\text{if} (M) \{ x:= 1 \} \text{ else } \{ x:= 2 \}]\) contains:

\[
M \neq 0 \mid W \times 1 \quad M = 0 \mid W \times 2
\]

that is we have behavior from both branches of execution.

Moreover, two events representing the same action on both sides of a conditional can be merged, producing a single event. The precondition of the merged event is the disjunction of the preconditions of the original events. For example

\[
\begin{cases}
  \text{if } (M) \{ x:= 1; y:= 3 \} & \text{else } \{ x:= 2; y:= 3 \}
\end{cases}
\]

contains:

\[
(M \neq 0) \lor (M = 0) \mid W \times 3
\]

and since \((M \neq 0) \lor (M = 0)\) is a tautology, this is:

\[
M \neq 0 \mid W \times 1 \quad M = 0 \mid W \times 2 \quad W \times 3
\]

Combining this model of conditionals with the previously discussed model of memory using substitutions gives that

\[
\begin{cases}
  \text{if } (z) \{ x:= 1; y:= 3 \} & \text{else } \{ x:= 2; y:= 3 \}
\end{cases}
\]

contains:

\[
R \times 1 \leftarrow \not{1} \neq 0 \mid W \times 1 \quad 1 = 0 \mid W \times 2 \quad W \times 3
\]

and we visualize unsatisfiable preconditions as crossed out:

![Pomset Diagram]

Note that this semantics captures control dependencies such as \((R \times 1) < (W \times 1)\), independencies such as \((R \times 1) \not< (W \times 3)\), and failed speculations such as the crossed out \((W \times 2)\).
In summary, the features we need of the underlying data model are:

- **actions**, which may read or write memory locations, and
- **preconditions**, which are closed under substitution.

In rest of this section we make data models precise and define pomsets. In the next section we give the semantics of a simple imperative language as sets of pomsets.

**A. Data models**

A **data model** consists of:

- a set of **memory locations** $X$, ranged over by $x$ and $y$,
- a set of **registers** $R$, ranged over by $r$ and $s$,
- a set of **values** $V$, ranged over by $v$ and $w$,
- a set of **expressions** $E$, ranged over by $M$ and $N$,
- a set of **logical formulae** $\Phi$, ranged over by $\phi$ and $\psi$, and
- a set of **actions** $A$, ranged over by $a$ and $b$,

such that:

- values include at least the constants 0 and 1,
- expressions include at least registers and values,
- expressions are closed under substitutions of the form $M[N/r]$,
- formulae include at least true, false, and equalities of the form $(M = N)$ and $(x = N)$,
- formulae are closed under negation, conjunction, disjunction,
- formulae are closed under substitutions of the form $\phi[x/r]$ or $\phi[N/x]$,
- there is a relation $\vdash$ between formulae, and
- there are partial functions $Rd$ and $Wr : A \to (X \times V)$.

We shall say $a$ **reads** $v$ from $x$ whenever $Rd(a) = (x, v)$, and $a$ **writes** $v$ to $x$ whenever $Wr(a) = (x, v)$. We shall say $\phi$ implies $\psi$ whenever $\phi \vdash \psi$, $\phi$ is a tautology whenever true $\vdash \phi$, $\phi$ is unsatisfiable whenever $\phi \vdash \false$, and $\phi$ is independent of $x$ whenever $\phi \vdash \phi[v/x]$. In examples, the actions are of the form $(R.x.v)$, which reads $v$ from $x$, and $(W.x.v)$, which writes $v$ to $x$.

**B. 3-valued pomsets**

Recall the definition of a pomset from [16]:

**Definition III.1.** A pomset $(E, \leq, \lambda)$ with alphabet $\Sigma$ is a partial order $(E, \leq)$ together with $\lambda : E \to \Sigma$.

Going forward, we fix the alphabet $\Sigma = (\Phi \times A)$. We will write $\phi[a]$ for the pair $(\phi, a)$. We will write a crossed-out $(\phi, a)$ when $\phi$ is a tautology, and write a crossed-out $(\phi, a)$ when $\phi$ is unsatisfiable. We lift terminology from logical formulae and actions to events, for example if $\lambda(e) = (\phi[a])$ then we say $e$ is unsatisfiable whenever $\phi$ is unsatisfiable, $e$ writes $v$ to $x$ whenever $a$ writes $v$ to $x$, and so forth. We visualize a pomset as a graph where the nodes are drawn from $E$, each node $e$ is labeled with $\lambda(e)$, and an edge $d \to e$ corresponds to an ordering $d \leq e$. For example:

![Diagram of a pomset example]

is a visualization of the pomset where:

$$E = \{0, 1, 2\}$$

$$\lambda(0) = (\true, R.x)$$

$$\lambda(1) = (\false, W.y)$$

We are building a compositional semantics of shared memory concurrency, which means we require a notion of when a read has a matching write. This is a property we require of closed programs, but not of open programs. For example a program whose semantics includes:

![Diagram of program semantics example]

may be put in parallel with another program which writes 0 to $x$. If the program is closed with respect to $x$ though, such an execution cannot exist, so we need each read of $x$ to have a matching write. This is captured by defining when $e$ reads $x$ from $d$ [2]. A preliminary definition (which, as we shall see, needs to be strengthened) is:

- $d < e$,
- $e$ implies $d$,
- $d$ writes $v$ to $x$, and $e$ reads $v$ from $x$, and
- there is no $d < c < e$ such that $c$ writes to $x$.

Unfortunately by itself, this is not enough. The problem is the final clause saying that there does not exist an $x$-blocking event $e$ between $d$ and $e$. Unfortunately, concurrency can turn events that were not $x$-blockers into an $x$-blocker, even if the new thread does not mention $x$. We give an example to show this in Appendix [3]. This is a problem in that it means the preliminary model violates scope extrusion [31], in that we can find programs $C$ and $D$ such that $[[\var x; (C || D)]]$ is not the same as $[[\var x; C] || D]$, even if $D$ does not mention $x$.

There are a number of ways this can be addressed; for example, in models such as [6] the reads-from relation is taken as a primitive. In this paper, we propose 3-valued pomsets as a solution. These are pomsets in which, in addition to positive statements ($d < e$) (interpreted as $e$ depends on $d$), we also have negative statements ($d \nleq e$) (interpreted as $e$ cannot depend on $d$).

**Definition III.2.** A 3-valued pomset $(E, \leq, \nleq, \lambda)$ is a pomset $(E, \leq, \lambda)$ together with $\nleq \subseteq (E \times E)$ such that:

- if $d \leq e$ then $e \nleq d$,
- if $d \leq e$ and $d \nleq e$ then $d = e$,
- if $c \geq d \nleq e$ or $c \nleq d \geq e$ then $c \nleq e$.

Structures similar to 3-valued pomsets have come up in many guises, for example rough sets [34] or ultrametrics over $\{0, 1/2, 1\}$. They correspond to axioms A1–A3 of Lamport’s system executions [25]. They are the notion of pomset given by interpreting $d \leq e$ in a 3-valued logic [42].

In diagrams, we visualize $(e \nleq d)$ as a dashed arrow from $d$ to $e$ (note the change of direction). We refer to edges introduced by $(d < e)$ as strong edges and by $(e \nleq d)$ as weak edges. For readability, we often highlig

![Diagram of pomset example with 3-valued semantics]
the reads-from edges as well. For example one execution of $(x:=0; x:=1) \sqcup (x:=x+1)$ is:

$$\text{W}x0 \rightarrow \text{W}x1 \rightarrow \text{R}x1 \rightarrow \text{W}x2$$

We strengthen the definition of reads-from to require not just that no blocker exists, but that any candidate blocker must either have $d \not< c$ or $c \not< e$. This ensures that any further concurrency cannot turn a non-blocker into a blocker.

**Definition III.3.** In a 3-valued pomset, $e$ can read $x$ from $d$ whenever:

- $d < e$,
- $e$ implies $d$,
- $d$ writes $v$ to $x$, and $e$ reads $v$ from $x$, and
- if $c$ writes to $x$ then either $d \not< c$ or $c \not< e$.

One of the requirements of closed programs is that every read event reads from a write event.

In the remainder of the paper, we drop the prefix “3-valued”, referring to 3-valued pomsets simply as pomsets.

**IV. SEMANTICS OF PROGRAMS**

In Figure 1 we give the semantics of a simple shared-memory concurrent language as sets of pomsets. Each pomset $P \in \llbracket C \rrbracket$ represents a single execution of $C$. We do not expect $\llbracket C \rrbracket$ to be prefixed closed; thus, one may view each $P \in \llbracket C \rrbracket$ as a completed execution. However, the sets of pomsets given by our semantics are closed with respect to augmentation, which may create additional order and strengthening preconditions:

**Definition IV.1.** $P'$ is an augmentation of $P$ if $E' = E$, $e \leq d$ implies $e \leq' d$, $e \not< d$ implies $e \not< d$, and if $\lambda(e) = (\psi \mid b)$ then $\lambda'(e) = (\psi' \mid b)$ where $\psi'$ implies $\psi$.

We give the semantics using combinators over sets of pomsets, defined in Appendix A. Using $P$ to range over sets of pomsets, these are:

- **restriction** $\nu x.P$, which filters $P$ to include only pomsets where every event that reads from $x$ can read from some $d$, following Definition III.3 and where no precondition can depend on $x$,
- **guarding** $\phi \triangleright P$, which filters $P$, keeping pomsets whose events have preconditions that imply $\phi$,
- **substitution** $P[M/x]$, which replaces $x$ with $M$ in every precondition of $P$,
- **composition** $P_1 \parallel P_2$, which unions pomsets from $P_1$ and $P_2$, allowing events to be merged, and
- **prefixing** $a \rightarrow P$, which adds an event with action $a$ to pomsets in $P$, ordering $a$ before any $e$ whose predicate depends on the value read by $a$.

These operations are similar to those from models of concurrency such as [8], but adapted here to the setting of speculative evaluation.

Restriction and guarding filter the set of pomsets; we have $(\nu x.P) \subseteq P$ and $(\phi \triangleright P) \subseteq P$. Substitution updates the preconditions in a pomset, thus we expect the number of pomsets to be unchanged; in addition, the number of events in each of the pomsets is unchanged. The most interesting operators are composition and prefixing, which create larger pomsets from smaller ones.

Composition is used in giving the semantics for conditionals and concurrency. $P_1 \parallel P_2$ contains the union of pomsets from $P_1$ and $P_2$, allowing overlap as long as they agree on actions. For example, if $P_1$ and $P_2$ contain:

$$\phi \mid a \rightarrow \psi_1 \mid b \quad \psi_2 \mid b \rightarrow \chi \mid c$$

then $P_1 \parallel P_2$ contains:

$$\phi \mid a \rightarrow \psi_1 \lor \psi_2 \mid b \rightarrow \chi \mid c$$

Prefixing is used in giving the semantics of reads and writes. $a \rightarrow P$ adds a new event $c$ with action $a$ to each pomset in $P$. As in the definition of parallel composition, the definition allows the new event to overlap with events in $P$ as long as they agree on the action.

If $c$ writes to a location that is also written by $e$ in $P$, then prefixing introduces weak order between them: $c \not< e$. This ensures that these writes cannot be given the reverse order in an augmentation.

If $c$ reads from a location that occurs in the predicate of $e$, then prefixing introduces order from $c$ to any $e$ whose predicate depends on $x$. For example, if $a$ and $b$ write to the same location, $a$ reads $v$ from $x$, $\psi$ is independent of $x$, and $P$ contains:

$$\psi \mid b \rightarrow \chi \mid c$$

then $a \rightarrow P$ contains:

$$\phi \mid a \rightarrow \psi \mid b \rightarrow \chi[\psi' \mid b] \mid c$$

In the remainder of this section, we give examples to explain the semantics, concentrating on reads and conditionals. Security-relevant examples begin in §V.

**A. Sequential memory accesses**

In the semantics of memory, there are two very different ways memory can be accessed: sequentially or concurrently. These are modeled differently, since hardware and compilers give very different guarantees about their behavior. In the semantics of $\llbracket r := x; C \rrbracket$, given in Figure 1 these are found on left and right sides of the union operation. In this section, we discuss the sequential semantics, $\llbracket C \rrbracket[x/r]$, leaving the concurrent semantics to §IV-B.

Consider the program $(x:=0; y:=x+1)$. One execution of this program is where the write to $y$ uses the sequential value of $x$, which is 0:

$$\text{W}x0 \rightarrow \text{W}y1$$

To see how this execution is modeled, we first expand out the syntax sugar to get the program $(x:=0; r:=x; y:=r+1; \text{skip})$. Now $\llbracket \text{skip} \rrbracket$ is just $\{\}$, and $\llbracket y:=r+1; \text{skip} \rrbracket$ includes:

$$(r+1 = 1) \triangleright (\text{W} y1 \rightarrow \llbracket \text{skip} \rrbracket[1/y])$$
which contains the pomset:

\[
\text{\{ skip \} } = \{ 0 \}
\]
\[
\text{\{ \( x := M; C \) \} } = \cup_\varphi ( (M = v) \triangleright (W \ x \ v) ) \rightarrow \text{\{ C\}[M/x]}
\]
\[
\text{\{ \( r := x; C \) \} } = \text{\{ C\}[x/r] } \cup \cup_\varphi (R \ x \ v ) \rightarrow \text{\{ C\}[x/r]}
\]
\[
\text{\{ \text{if} (M) \{ C \} \text{ else } \{ D \} \} } = ( (M \neq 0) \triangleright \text{\{ C\} } ) \lor ( (M = 0) \triangleright \text{\{ D\} } )
\]
\[
\text{\{ \text{var} \ x; C \} } = \nu x. \text{\{ C\}}
\]

Fig. 1. Semantics of a concurrent shared-memory language

To see how this execution is modeled, we first expand out the syntax sugar to get the program \((x:=1; \text{skip} \mid r:=x; y:=r+1; \text{skip})\). As before, \(\text{\{ y:=r+1; \text{skip} \} }\) includes:

\[
(r + 1 = 2) \triangleright (W \ y \ 2) \rightarrow \text{\{ skip\}[2/y]}
\]

which contains the pomset:

\[
(x + 1 = 1 \mid W \ y \ 1)
\]

expressing that this program can write 1 to y, as long as the precondition \(r + 1 = 1\) is satisfied. Now \(\text{\{ r:=x; y:=r+1; \text{skip} \} }\) has two cases, the sequential case (which does not introduce a read action) and the concurrent case (which does).

For the moment, we are interested in the sequential case:

\[
\text{\{ y:=r+1; \text{skip} \}[x/r]}
\]

which contains the pomset:

\[
(x + 1 = 1 \mid W \ y \ 1)
\]

In this pomset, the precondition is \((x + 1 = 1)\), which specifies a property of the thread-local value of \(x\). Finally \(\text{\{ x:=0; r:=x; y:=r+1; \text{skip} \} }\) includes:

\[
(0 = 0) \triangleright (W \ x \ 0) \rightarrow \text{\{ r:=x; y:=r+1; \text{skip} \}[0/x]}
\]

which contains the pomset:

\[
0 = 0 \mid W \ x \ 0 \quad 0 = 0 \land 0 + 1 = 1 \mid W \ y \ 1
\]

all of whose preconditions are tautologies, so this has the expected behavior:

\[
W \ x \ 0 \quad W \ y \ 1
\]

There is no dependency between \(W \ x \ 0\) and \(W \ y \ 1\), since \((0 = 0 \land 0 + 1 = 1)\) is independent of \(x\).

This example demonstrates how preconditions capture the sequential semantics of memory. In an execution containing an event with label \((\phi \mid a)\), one way the precondition \(\phi\) can be discharged is by an assignment \(x := M\), which performs a substitution \(M/x\). This is a variant of the Hoare semantics of assignment [18], where if \(C\) has precondition \(\phi\) then \(x := M; C\) has precondition \(\phi[M/x]\).

B. Concurrent memory accesses

We now turn to the case of concurrent accesses to memory. Consider the program \((x:=1 \mid y:=x+1)\). In executions of this program, it is possible for the second thread to perform a concurrent read of \(x\):

\[
W x 1 \quad R x 1 \quad W y 2
\]

and so \(\text{\{ x:=1; \text{skip} \mid r:=x; y:=r+1; \text{skip} \} }\) includes:

\[
W x 1 \quad R x 1 \quad W y 2
\]

as expected, including a reads-from dependency \((W \ x \ 1) < (R \ x \ 1)\).

This example demonstrates how read and write events capture the concurrent semantics of memory. In an execution containing an event with label \((R \ x \ v)\), if the execution is \(x\)-closed, then there must be an event it reads from, for example one labeled \((W \ x \ v)\).

C. Control dependencies

Conditionals introduce control dependencies, for example consider the program:

\[
r := z ; \text{ if } (r) \{ x := 1 \} \text{ else } \{ y := 2 \}
\]

This includes executions in which the false branch is taken:
and ones where the true branch is taken:

\[
\begin{array}{c}
R \rightarrow 0 & W x 1 & W x 2
\end{array}
\]

In both cases, we record the actions in the branch that was not taken. This is a novel feature of this model, and is intended to capture speculative evaluation. In §VI-A we will show how this model captures Spectre-like information flow attacks, once the attacker is provided with the ability to observe such speculations.

To see how these executions are modeled, consider the semantics of \([x := 1; \text{skip}]\), which contains any pomset of the form:

\[
\phi | W x 1
\]

in particular it contains:

\[
r \neq 0 | W x 1
\]

Similarly \([y := 2; \text{skip}]\) contains:

\[
r = 0 | W y 2
\]

and so \([^if(r) \{ x := 1; \text{skip} \} \text{else} \{ y := 2; \text{skip} \}^\]

contains:

\[
r \neq 0 | W x 1 \quad r = 0 | W y 2
\]

Now, the semantics of concurrent read performs substitutions, for example:

\[
R \rightarrow 0 \neq 0 | W x 1 \quad 0 = 0 | W y 2
\]

which gives the required pomset:

\[
\begin{array}{c}
R \rightarrow 0 & W x 1 & W y 2
\end{array}
\]

Note that the precondition \(r = 0\) is dependent on \(r\), and so there is a dependency \((R \rightarrow 0) < (W y 2)\), modeling the control dependency introduced by the conditional.

### D. Control independencies

In most models of control dependencies, the dependency relation is syntactic, based on whether the action occurs syntactically inside a conditional. In contrast, the notion in this model is semantic: if an action can occur on both sides of a conditional, there is no control dependency. Consider a variant of the example from §IV-C

\[
r := z; if(r) \{ x := 1 \} \text{else} \{ x := 1 \}
\]

This has the expected execution in which the control dependencies exist:

\[
R \rightarrow 0 & W x 1 & W x 2
\]

but it also has an execution in which the two writes of 1 to \(x\) are merged, resulting in no dependency:

\[
R \rightarrow 0 & W x 1 & W x 2
\]

To see how this arises, consider the definition of \([^if(r) \{ x := 1; \text{skip} \} \text{else} \{ x := 1; \text{skip} \}^\]

\[
\begin{array}{c}
P_1 \parallel P_2 \text{ where } P_1 = (r \neq 0) \triangleright \{x := 1; \text{skip}\} & P_2 = (r = 0) \triangleright \{x := 1; \text{skip}\}
\end{array}
\]

Now, one pomset in \(P_1\) is:

\[
r \neq 0 | W x 1
\]

that is \(P_1\) where:

\[
E_1 = \{e\} \quad \lambda_1(e) = (r \neq 0, W x 1)
\]

and similarly, one pomset in \(P_2\) is:

\[
r = 0 | W x 1
\]

that is \(P_2\) where:

\[
E_2 = \{e\} \quad \lambda_2(e) = (r = 0, W x 1)
\]

Crucially, in the definition of \(P_1 \parallel P_2\) there is no requirement that \(E_1\) and \(E_2\) are disjoint, and in this case they overlap at \(e\). As a result, one pomset in \(P_1 \parallel P_2\) is \(P_0\) where:

\[
E_0 = \{e\} \quad \lambda_0(e) = (r \neq 0 \lor r = 0, W x 1)
\]

that is:

\[
W x 1
\]

Note that this pomset has no precondition dependent on \(r\), since \((r \neq 0 \lor r = 0)\) does not depend on \(r\), which is why we end up with an execution without a control dependency:

\[
R \rightarrow 0 \quad W x 1
\]

This semantics captures compiler optimizations which may, for example, merge code executed on both branches of a conditional, or hoist constant assignments out of loops.

We can now see the counterintuitive behavior of conditionals in the presence of control dependencies. There are programs such as \(\text{if}(z) \{ x := 1 \} \text{else} \{ x := 1 \}\) with executions in which \((W x 1)\) is independent of \((R \rightarrow 0)\):

\[
R \rightarrow 1 \quad W x 1
\]

while programs such as \(\text{if}(z) \{ x := 1 \} \text{else} \{ y := 2 \}\) only have executions in which \((W x 1)\) is dependent on \((R \rightarrow 0)\):

\[
R \rightarrow 1 \quad W x 1 \quad W x 2
\]

These programs have executions with different dependency relations, depending only on conditional branches that were not taken. In §VI-A we shall see that this has security implications, since relaxed memory can observe dependency.
V. ATTACKS ON SPECULATIVE EXECUTION

In this section, we show how known attacks on speculative execution can be modeled. In §V-A we discuss Spectre. In §V-B we describe speculation barriers for defense against Spectre. In §V-C we discuss attacks on transactions.

In each attack, there is a high-security variable SECRET, and the goal of the attacker is to learn one bit of information from SECRET. The Spectre and PRIME+ABORT attacks exploit optimizations in hardware, and so can be mounted against a dynamic SECRET.

A. Spectre

We give a simplified model of Spectre attacks, ignoring the details of cache timing. In this model, we extend programs with the ability to tell whether a memory location has been touched (in practice this is implemented using timing attacks on the cache). For example, we can model Spectre by:

```
var a; if (canRead(SECRET)) { a[SECRET] := 1 }
else if (touched a[0]) { x := 0 }
else if (touched a[1]) { x := 1 }
```

This is a low-security program, which is attempting to discover the value of a high-security variable SECRET. The low-security program is allowed to attempt to escalate its privileges by checking that it is allowed to read a high-security variable:

```
if (canRead(SECRET)) { code allowed to read SECRET }
else { code not allowed to read SECRET }
```

In this case, canRead(SECRET) is false, so the fallback code is executed. Unfortunately, the encoded code is speculatively evaluated, which allows information to leak by testing for which memory locations have been touched.

Attacks may realize the abstract notions in various ways. For example, in variant 1 of Spectre, the dynamic security check is implemented as an array bounds check.

We model the touched test by introducing a new action (T x), and defining:

```
[[if (touched x) { C } else { D }]]
= ((T x) \rightarrow [[C]]) \cup [[D]]
```

Implementations of touched use cache timing, but their success can be modeled without needing to be precise about such microarchitectural details:

- if λ(e) = (ϕ \mid T x) then there is d \triangleright e where d reads or writes x.

Note that there is no requirement that d be satisfiable, and indeed Spectre has the execution:

```
\begin{array}{c}
  R \text{SECRET} 1 \quad \text{W} \quad \text{H} 1 \quad T \ a[1] \quad W x 1
\end{array}
```

but (assuming a successful implementation of touched) not:

```
\begin{array}{c}
  R \text{SECRET} 0 \quad \text{W} \quad \text{H} 1 \quad T \ a[1] \quad W x 1
\end{array}
```

Thus, the attacker has managed to leak the value of a high-security location to a low-security one: if (W x 1) is observed, the SECRET must have been 1.

This shows how our model of speculation can express the way in which Spectre-like attacks bypass dynamic security checks, without giving a treatment of microarchitecture.

B. Speculation barriers

The ability to model Spectre is useful, but really we would like to model defenses against such attacks, and provide some confidence in the correctness of the defense. One such defense which fits naturally in our model is speculation barriers, which prevent code from being speculatively executed. For example, we could introduce such a barrier, and require that a barrier is introduced on each security check:

```
if (canRead(SECRET)) { barrier; \cdots } else { \cdots }
```

To model barriers, we introduce a new action \text{barrier} and define:

```
[[\text{barrier}; C]] = \{\emptyset\} \cup ((\text{SB}) \rightarrow [[C]])
```

Implementations of \text{barrier} make use of hardware barriers which halt speculative execution until all instructions up to the barrier have been retired. Such barriers are successful when:

- if λ(e) = (ϕ \mid \text{SB}) then ϕ is satisfiable.

For example, a successful implementation of barriers disallows the execution of Spectre:

```
\begin{array}{c}
  R \text{SECRET} 1 \quad \text{W} \quad \text{H} 1 \quad T \ a[1] \quad W x 1
\end{array}
```

One might expect that this is a successful (albeit expensive) defense against Spectre, but it is not, unless the compiler is aware that barrier cannot be lifted out of a conditional. An unaware compiler might perform common subexpression elimination on barriers, allowing the attacker to introduce a barrier to fool a compiler into optimizing the safe:

```
if (canRead(SECRET)) { \text{barrier}; \cdots } else { \text{barrier}; \cdots }
```

into the unsafe:

```
\text{barrier}; if (canRead(SECRET)) { \cdots } else { \cdots }
```

To model the requirement that barriers are not moved past conditions, we make them \text{unmergeable}: SB events on different arms of a conditional cannot be merged. With this requirement, we can show that barriers act as a defense against Spectre by first showing that [[D]] has the same successful executions as:

```
[[if (canRead(SECRET)) { \text{barrier}; C } else { D }]]
```

and then showing that the semantics which only looks at successful executions is \text{compositional}: if [[D]] has the same successful executions as [[D′]] then [[C[D′]]] has the same successful executions as [[C[D]]] for any “program with a hole” C•. Compositional reasoning is what fails when SB is mergeable, as shown by the attack against a compiler which blindly performs common subexpression elimination.

To realize a speculation barrier in microarchitecture, it is likely sufficient for the barrier to stop any further speculation until the barrier is known to succeed. There is experimental evidence that Intel’s mfence instruction has the effect of a speculation barrier in some contexts [41 §VII-D].
C. Transactions

We present a model of transactional memory that is sufficient to capture PRIME+ABORT attacks. We make several simplifying assumptions: transactions are serializable, strongly isolated, and only abort due to cache conflicts.

The action \((B \ v)\) represents the begin of a transaction with id \(v\), and \((C \ v)\) represents the corresponding commit. We model a language in which transactions have explicit identifiers (which we elide in examples) and abort handlers (which we elide when they are empty):

\[
\begin{align*}
\text{begin } v; E; \text{onabort } v \{ D \} & = (B \ v) \rightarrow (\{ E \} \cup (\text{false } \triangleright \{ E \} \parallel \{ D \})) \\
\text{commit } v; D & = (C \ v) \rightarrow \{ D \}
\end{align*}
\]

The semantics of a transaction has two cases: a committed case (executing only the transaction body) and an aborted case (executing both the body and the recovery code, where the body is marked unsatisfiable). For example, two executions of \((\text{begin; } x := 1; x := 2; \text{commit}; \text{onabort } \{ y := 1 \})\) are:

\[
\begin{align*}
B & \xrightarrow{Wx1} Wx2 \xrightarrow{W1} C \\
B & \xrightarrow{Wx1} Wx2 \xrightarrow{Wy1} W1
\end{align*}
\]

At top level, we require that pomsets be serializable, as defined below.

Definition V.1. We say that event \(c\) matches \(b\) if \(\lambda(c) = (C \ v)\) and \(\lambda(b) = (B \ v)\). We say that begin event \(b\) begins \(e\) if \(b \leq e\) and there is no intervening matching commit; in this case \(e\) belongs to \(b\). We say that commit event \(c\) commits \(e\) if \(e \leq c\) and there is no intervening matching begin.

Definition V.2. A pomset is serializable if:

1) no two begins have the same id,
2) every commit follows the matching begin,
3) \(\leq\) totally orders tautological begins and commits,
4) if \(b\) begins \(e\), but not \(d\), and \(d \leq e\) then \(d \leq b\),
5) if \(c\) ends \(e\), but not \(d\), and \(e \leq d\) then \(c \leq d\),
6) if \(e\) and \(d\) belong to \(b\) and read the same location, then both read the same value, and
7) if \(e\) belongs to \(b\), then \(e\) implies some matching \(c\) that ends \(e\).


\[
\begin{align*}
\begin{array}{c}
B \xrightarrow{Wx0} Wx1 \xrightarrow{C} Rx0 \\
B \xrightarrow{Wx0} Wx1 \xrightarrow{Wy1} W1
\end{array}
\end{align*}
\]

In order to model PRIME+ABORT, we need a mechanism for modeling why a transaction aborts, as this can be used as a back channel. We model a simple form of concurrent transaction, which aborts when it encounters a memory conflict—this is similar to the treatment of touched in §V-A.

Definition V.3. A commit event \(c\) matching \(b\) aborts due to memory conflict if there is some \(e\) ended by \(c\), and some tautological \(b \triangleright d \triangleright c\) that does not belong to \(b\) such that \(e\) and \(d\) touch the same location.

The attack requires an honest agent whose access pattern depends upon a secret. Such an honest agent is:

\[
a[\text{SECRET}] := 1
\]

Then the attacker program

\[
\text{begin; } a[1] := 0; r := \text{commit; onabort } \{ x := 1 \}
\]

can write 1 to \(x\) if the \text{SECRET} is 1, in which case the following execution is possible.

\[
\begin{align*}
\begin{array}{c}
W[1] \xrightarrow{a[1]} B \xrightarrow{Wx0} Wx1 \\
W[1] \xrightarrow{Wx1}
\end{array}
\end{align*}
\]

If the attacker knows that commits only abort due to memory conflicts, then this attack is an information flow, since the memory conflict only happens when the \text{SECRET} is 1.

The attacker code here must have write access to the high security variable \(a\). Such a “write up” is allowed by secrecy analyses such as the Smith-Volpano type system [39], which is meant to guarantee noninterference.

If we require that the attacker and honest agent access disjoint locations in memory, then we must include a bit of microarchitecture to model the attack. Suppose that the set of locations \(A\) is partitioned into cache sets and update Definition V.3 so that the commit event aborts due to memory conflict if \(e\) and \(d\) touch locations in the same cache set.

PRIME+ABORT exploits an honest agent whose cache-set access pattern depends upon a secret. If \(a[0]\) and \(a[1]\) belong to separate cache sets, then such an honest agent is, as before:

\[
a[\text{SECRET}] := 1
\]

The attack relies on discovery of some \(y\) which belongs to the cache-set of \(a[1]\). Then the attack can be written as:

\[
\text{begin; } y := 0; r := \text{commit; onabort } \{ x := 1 \}
\]

As before, if the attacker knows that commits only abort due to memory conflicts, then there is an information flow, since the memory conflict only happens when the \text{SECRET} is 1.
This style of attack can be thwarted by requiring that the honest agent and attack code access disjoint cache sets. This approach is pursued in [22].

Another defense is to require a speculation barrier at the beginning of each transaction. This would have the effect, however, of undermining any optimistic execution strategy for transactions: the transaction would only be able to begin when it is known that its commit will succeed.

VI. ATTACKS ON COMPILER OPTIMIZATIONS

In this section, we model two attacks on compiler optimizations. The first attack exploits reordering allowed by relaxed memory which can result in unexpected hardware capabilities, which have to be modeled by adding checks to try to learn a SECRET.

As in the previous section, the goal of the attacker is to learn one bit of information from the high-security SECRET. The attacks on compiler optimizations require the SECRET to be known to the compiler, for example a static SECRET or a JIT compiler.

To defend against these attacks it is sufficient to require a traditional memory fence after each security check: compilers do not reorder instructions over fences.

A. Relaxed memory orders

Consider an attacker program, again using dynamic security checks to try to learn a SECRET. Whereas Spectre uses hardware capabilities, which have to be modeled by adding extra capabilities to the language, this new attacker works by exploiting relaxed memory which can result in unexpected information flows. The attacker program is:

\[
\begin{align*}
\text{var } x &:= 0; \text{var } y := 0; \\
y &:= x \mid \text{if } (y == 0) \{ x := 1 \} \\
&\quad\text{else if } (\text{canRead(SECRET)}) \{ x := \text{SECRET} \} \\
&\quad\text{else } \{ x := 1; z := 1 \}
\end{align*}
\]

In the case where SECRET is 2, this has many executions, one of which is:

\[
\begin{align*}
W_x 0 & \quad W_y 0 \\
R_x 0 & \quad W_y 0 \\
& \quad W_x 1 \\
R_y 1 & \quad W_x 1 \\
& \quad W_z 1
\end{align*}
\]

but there are no executions which exhibit (W z 1), since any attempt to do so produces a cycle, since the value written to x has a control dependency on the value read from y:

\[
\begin{align*}
W_x 0 & \quad W_y 0 \\
R_x 1 & \quad W_y 1 \\
& \quad W_x 1 \\
R_y 1 & \quad W_x 1 \\
& \quad W_z 1
\end{align*}
\]

In the case where SECRET is 1, there is an execution:

\[
\begin{align*}
W_x 0 & \quad W_y 0 \\
R_x 1 & \quad W_y 1 \\
& \quad W_x 1 \\
& \quad W_z 1
\end{align*}
\]

Note that in this case, there is no dependency from (R y 1) to (W x 1). This lack of dependency makes the execution possible. Thus, if the attacker sees an execution with (W z 1), they can conclude that SECRET is 1, which is an information flow attack.

This attack is not just an artifact of the model, since the same behavior can be exhibited by compiler optimizations. Consider the program fragment:

\[
\begin{align*}
\text{if } (y == 0) \{ x := 1 \} \\
\text{else if } (\text{canRead(SECRET)}) \{ x := \text{SECRET} \} \\
\text{else } \{ x := 1; z := 1 \}
\end{align*}
\]

In the case where SECRET is a constant 1, the compiler can inline it and lift the assignment to x out of the if statement:

\[
\begin{align*}
x := 1; \text{if } (y == 0) \{ \} \\
\text{else if } (\text{canRead(SECRET)}) \{ \} \\
\text{else } \{ z := 1 \}
\end{align*}
\]

After this optimization, a sequentially consistent execution exhibits (W z 1). We discuss the practicality of this attack further in §VII.

B. Dead store elimination

A common compiler optimization is dead store elimination, in which writes are omitted if they will be overwritten by a subsequent write later in the same thread. We can model eliminated writes by ones with an unsatisfiable precondition. For example, one execution of (x := 1; z := 2) || (r := x) is:

\[
\begin{align*}
W_x 0 & \quad W_y 0 \\
R_x 0 & \quad W_y 0 \\
& \quad W_x 2 \\
R_y 1 & \quad W_x 2 \\
& \quad R_z 1
\end{align*}
\]

Recall that for any satisfiable e, if e reads x from d then d is satisfiable. This means that, although we can eliminate (W x 1) we cannot eliminate (W x 2).

One heuristic that a compiler might adopt is to only eliminate writes that are guaranteed to be followed by another write to the same variable. This can be formalized by saying that a write event d is eliminable if there is a tautology e \nless d which writes to the same location. A model of dead store elimination is one where, in every pomset, every eliminable event is unsatisfiable. This model includes the example above.

Note that if dead store elimination is always performed, then there is an information flow attack similar to the one in §VI-A. Consider the program:

\[
\begin{align*}
y &:= x \mid x := 1; \\
\text{if } (\text{canRead(SECRET)}) \{ \text{if } (\text{SECRET}) \{ x := 2 \} \} \\
\text{else } \{ x := 2 \}
\end{align*}
\]
In the case that $\text{SECRET}$ is 0, there is an execution:

$$\xrightarrow{R \ x_1} \xrightarrow{W \ y_1} \xrightarrow{W \ x_1} \xrightarrow{\phi} \xrightarrow{W \ x_2}$$

where $\phi$ is $(\neg \text{canRead(SECRET)})$, which is not a tautology, and so the $(W \ x_1)$ event is not eliminated. In the case that $\text{SECRET}$ is not 0, the matching execution is:

$$\xrightarrow{R \ x_2} \xrightarrow{W \ y_2} \xrightarrow{W \ x_1} \xrightarrow{\neg \phi} \xrightarrow{W \ x_2}$$

Now the $(W \ x_2)$ event is a guaranteed write, so the $(W \ x_1)$ event is eliminated, and so cannot be read. In the case that the attacker can rely on dead store elimination taking place, this is an information flow: if the attacker observes $x$ to be 1, then they know $\text{SECRET}$ is 0. We return to this attack in §VII.

VII. EXPERIMENTS

One theme of this paper is that optimizations not typically part of formal abstractions can result in information flow leaks. This is typified by the Spectre attack, which leverages speculative execution, a hardware optimization. §VI-A and §VI-B presented other attacks along the same line, which leverage compiler optimizations. These attacks also, unlike Spectre, do not rely on timing side channels, or indeed timers of any kind, bypassing many common Spectre mitigations [24, 45].

In this section we present implementations of the attacks described in §VI-A and §VI-B in both cases exploiting compiler optimizations to construct an information flow attack. We demonstrate the efficacy of our proof-of-concept attacks against the clang and gcc C compilers. All of our experiments are performed on a Debian 9 machine with an Intel i7-6500U processor and 8 GB RAM; we test against gcc 6.3.0 and clang 3.8.

A. Attacker model

As explained in Section IV our model expresses a variety of attacks with differing attacker models. The Spectre (§VI-A) and PRIME+ABORT (§V) attacks exploit optimizations in hardware, and so can be mounted against a dynamic $\text{SECRET}$. Our model captures this appropriately. In contrast, the attacks from §VI-A and §VI-B leverage compiler optimizations and require the $\text{SECRET}$ to be known to the compiler, for example a static $\text{SECRET}$ for a JIT compiler. As our experimental section is devoted to these latter (novel) attacks, we discuss the attacker model for these attacks in more detail.

In the attacker model for the compiler-optimization attacks, we assume that there is a $\text{SECRET}$ hardcoded into an application; for instance, $\text{SECRET}$ may be an API key. This $\text{SECRET}$ is known at compile time, but may not be accessed except behind a security check. Since the attacker is running with low security privileges, the security check always fails, so the attacker can only access the $\text{SECRET}$ in dead code. The attacker’s goal is to learn the value of the $\text{SECRET}$.

As a running hypothetical example, suppose there is a library that contains a hardcoded $\text{SECRET}$:

```c
static const uint $\text{SECRET} = 0x1234;
static volatile bool $\text{canReadSecret} = false;
```

The attacker is not allowed to write to $\text{canReadSecret}$ or read from $\text{SECRET}$ except after performing an $\text{if(canReadSecret)}$ check.

This is not necessarily a realistic attacker model, since in most cases secrets are only known at run time rather than compile time, which means that the attacks presented in this section are more proof-of-concepts rather than immediately exploitable vulnerabilities. However, the mechanisms we use are novel and could potentially be applied in other contexts. For instance, many real-world contexts allow untrusted or third-party entities to write code in a scripting language which is then compiled alongside and integrated into a larger application, often using a just-in-time (JIT) compiler. JavaScript code from third-party websites running in a browser is a common example of this. Although we consider only attacks using C code against a C compiler, one could imagine a similar attack using JavaScript against browser JIT compilers, where the compiler may have access to interesting secrets such as the browser’s cookie store, and may be able to optimize based on those secrets. We plan to explore JavaScript attacks of this type as future work.

B. Load-store reordering attack

We begin by examining the attack in §VI-A in more detail. We show that by exploiting compiler optimizations which perform load-store reordering, an attacker can learn the value of a compile-time $\text{SECRET}$ despite only being allowed to use it inside dead code. We verified that this attack succeeds against gcc version 6.3.0.

The form of the attack presented in §VI-A works in theory, but in practice, just because a compiler is allowed to perform a load-store reordering doesn’t mean that it will. We found that gcc and clang chose to read $y$ into a register first (before writing to $x$), regardless of the value of $\text{SECRET}$. However, using a similar program we were able to coax gcc to emit a different ordering of the read of $y$ and the write of $x$ depending on the value of a $\text{SECRET}$:

```c
var x:= 0; var y:= 0;
y:= x || x:= 1;
if (canReadSecret) { x:= $\text{SECRET}$
  if (y > 0) { z:= 0 } else { z:= 1 }
}
```

Figure 2 shows the assembly output of gcc on this program in the cases where $\text{SECRET}$ is 0 and 1 respectively. In the case that $\text{SECRET}$ is 1, gcc removes the $\text{if}$ statement entirely, and moves the read of $y$ above the write of $x$. However, when $\text{SECRET}$ is 0, the $\text{if}$ statement must remain intact, and gcc does not move the read of $y$. This means that if $\text{SECRET}$ is 1, the second thread will always read $y==0$ and always assign $z==1$. However, if $\text{SECRET}$ is 0, it is possible that the first thread may observe $x==1$ and write $y==1$ in time for the second thread to observe $y==1$ and thus assign $z==0$. In this way, we leverage compiler load-store reordering to learn the value of a compile-time $\text{SECRET}$. 
We extend this attack to leak a secret consisting of an arbitrary number N of bits. To do this, we compile N copies of the test function, each performing a boolean test on a single bit of SECRET. So that the bit value is constant at compile time, we must compile a separate function for each bit, rather than execute the same code repeatedly in a loop.

We make three additional tweaks to improve the reliability, so that the attacker can confidently infer the value of SECRET based on the observed value of z. First, rather than performing \( y := x \) only once in the forwarding thread, we perform \( y := x \) continuously in a loop. This maximizes the probability that, once \( x := 1 \) occurs in the main thread, y will be immediately assigned 1 by the forwarding thread and the main thread will be able to read \( y == 1 \).

Second, we wish to lengthen the timing window between \( x := 1 \) and the read of \( y \) in the main thread (in the case where SECRET is 0 and the read of \( y \) remains below 0). However, we wish to do this in a way that does not block the reordering of the read of \( y \) upwards in the case where SECRET is 1. We do this by inserting many copies of the line

\[
\text{if} \left( \text{canReadSecret} \right) \{ x := \text{SECRET} \}
\]

instead of just one. In the case where SECRET is 0, this results in many reads of canReadSecret and many conditional jumps, which in practice creates a timing window for the forwarding thread to perform \( y := x \). However, in the case where SECRET is 1, all of these inserted lines can be removed just as a single copy could be. In practice, we found that inserting too many copies of the line prevents gcc from reordering the read of \( y \) above the write to \( x \) as desired; inserting 30 copies was sufficient to create a timing window while still allowing the desired reordering.

Finally, we redundantly execute the entire attack several times, noting the value of \( z \) in each case. We note that if \( y \) of the redundant runs produces a value of \( z == 0 \) for a particular bit position, then we can be certain that the corresponding bit of SECRET must be 0, as it implies the read of \( y \) was not reordered upwards in that particular function. On the other hand, the more runs that produce a value of \( z == 1 \) for a particular bit position, the more certain we can be that the read of \( y \) was reordered above the \( x := 1 \) assignment, and SECRET is 1.

Figure 3 gives the performance results for this attack against gcc version 6.3.0. The attack can sustain hundreds of thousands of bits per second leaked with near-perfect accuracy, or millions of bits per second with error rates of a few percent. This means that an attacker can leak a 2048-bit secret with near-perfect accuracy in under 10 ms. Note that this bandwidth assumes that all copies of the attack function are already compiled; the cost of compilation is not included here.

C. Dead store elimination attack

In this section we return to the attack in §VI-B based on dead store elimination. We show that in our attacker model (given in §VII-A), the attacker is able to exploit dead store elimination to again learn the value of a compile-time SECRET despite only being allowed to use it inside dead code. This attack is even more efficient than the attack on load-store reordering, and further, we were able to demonstrate its effectiveness against both gcc and clang.

We start from the simple form of the attack presented in §VI-B and extend it to leak a secret consisting of an arbitrary number of bits, in the same way that we extended the load-store reordering attack. We make three additional tweaks to improve the reliability so that the attacker can confidently infer the value of SECRET. Two of them follow exactly the same pattern as the reliability tweaks for the load-store reordering attack in §VII-B — continuously forwarding \( x \) to \( y \) in the forwarding thread, and running the entire attack multiple times. The remaining tweak is again motivated by increasing the timing window in which the forwarding can happen, but differs in some details from the implementation in §VII-B.

To increase the timing window, we insert additional time-consuming computation immediately following the \( x := 1 \) operation in the main thread. This increases the likelihood that the listening thread will be able to observe \( x := 1 \) (unless the
We have tried where possible to abstract away from the micro-architectural details that enable attackers to exploit speculation, while still trying to capture the “essence” of Spectre. There are trade-offs with any such abstraction, as higher-level abstractions make program behavior easier to understand and reason about, but at the cost of ignoring potential attacks. One software developer’s useful abstraction is another’s ignoring the difficult issues.

As a concrete instance, one feature of Spectre we have glossed over is the ability of the attacker to influence speculation, for example by training the branch predictor or influencing the contents of caches. We expect that such attacker influence could be modeled using a mechanism similar to the speculation barriers of §V-B, but under the control of the attacker rather than the honest agents.

The paper’s primary focus is not weak memory, and the model of relaxed memory used in this paper is deliberately simplified, compared for example to C11 [7][8]. Nonetheless, we believe that the model developed in the paper has promise as a semantics for relaxed memory. Our model appears to be the first in the literature that both validates all of the JMM causality test cases and also forbids thin air behavior; the most prominent existing models are either too permissive [9][10][11] or too conservative [10]. In separate work, we are exploring the usual properties of weak memory, such as comparisons with sequentially consistent models, optimization soundness, or compilation soundness. While our model of transactions shows the flexibility of our model, in this future work, we will include known features of hardware, including locks, fences, and read-modify-write instructions. This development is not core to the basic findings of this paper.

The design space for transactions is very rich [13]. We have only presented one design choice, and it remains to be seen how other design choices could be adopted. For example, we have chosen not to distinguish commits that are aborted due to transaction failure from commits which are aborted for other reasons, such as failed speculation.

In future work, it would be interesting to see if full-abstraction results for pomsets [36] can be extended to 3-valued pomsets.

One interesting feature of this model is that (in the language of [35]) it is a per-candidate execution model, in that the correctness of an execution only requires looking at that one execution, not at others. This is explicit in memory models such as [19][21] in which “alternative futures” are explored, in a style reminiscent of Abramsky’s bisimulation as a testing equivalence [1]. Models of information flow are similar, in that they require comparing different runs to test for the presence of dependencies [11]. In contrast, the model presented here explicitly captures dependency in the pomset order, and models multiple runs by giving the semantics of if in terms of a concurrent semantics of both branches. In the parlance of information flow [3], the humble conditional suffices to construct a composition operator to detect information flow in the presence of speculation.

<table>
<thead>
<tr>
<th>Redundancy</th>
<th>Bandwidth (bits/s)</th>
<th>Bitwise Acc</th>
<th>Per-run Acc</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1.19 million</td>
<td>99.991%</td>
<td>95.6%</td>
</tr>
<tr>
<td>2</td>
<td>597 thousand</td>
<td>99.99986%</td>
<td>99.7%</td>
</tr>
<tr>
<td>3</td>
<td>397 thousand</td>
<td>100.0%</td>
<td>100.0%</td>
</tr>
</tbody>
</table>

Fig. 4. Performance results for the dead store elimination attack on clang when leaking a 2048-bit secret. Terms are the same as defined in the caption for Figure 5.

<table>
<thead>
<tr>
<th>Stall amount</th>
<th>10</th>
<th>100</th>
<th>500</th>
</tr>
</thead>
<tbody>
<tr>
<td>Redundancy 1</td>
<td>2.54 million</td>
<td>1.54 million</td>
<td>584 thousand</td>
</tr>
<tr>
<td>Redundancy 2</td>
<td>1.24 million</td>
<td>774 thousand</td>
<td>295 thousand</td>
</tr>
<tr>
<td>Redundancy 3</td>
<td>841 thousand</td>
<td>521 thousand</td>
<td>201 thousand</td>
</tr>
<tr>
<td>Redundancy 4</td>
<td>620 thousand</td>
<td>387 thousand</td>
<td>145 thousand</td>
</tr>
</tbody>
</table>

Fig. 5. Performance results for the dead store elimination attack on gcc when leaking a 2048-bit secret. Rows give different values of ‘redundancy’ (as defined in previous figures), while columns give amounts of stall time immediately following the $x:=1$ write (as measured in loop iterations). Each table cell gives the leak bandwidth in bits/sec, followed by the bitwise accuracy.

$x:=1$ write was eliminated). Inserting this computation should be done without interfering with the dead store elimination process itself, so that the compiler will continue to eliminate the $x:=1$ write if and only if SECRET was 1. For gcc, we have a fair amount of freedom with the time-consuming computation — for instance, we can use an arbitrarily long loop. In fact, we can perform a further optimization by monitoring the value of the variable $y$ (written to by the listening thread) and breaking out of the loop early if we see that the listening thread has already observed $x == 1$. However, with clang, we cannot use a loop at all — the time-consuming computation must be branch-free and, furthermore, must not consist of too many instructions. Nonetheless, we find that even with these restrictions, we are able to construct a reliable and fast attack against both clang and gcc.

Performance results for the dead store elimination attack against clang are given in Figure 4 and against gcc are given in Figure 5. Both attacks are faster than the load-store-reordering attack from §VII-B when comparing settings which give the same accuracy. In particular, the attack on gcc can leak a 2048-bit cryptographic key with perfect accuracy (in our tests) in about 2 ms.

VIII. CONCLUSIONS AND FUTURE WORK

In this paper, we have presented a model of speculative evaluation and shown that it captures non-trivial properties of speculations produced by hardware, compiler optimizations, and transactions. These properties include information flow attacks: in the case of hardware and transactions this is modeling known attacks [23][12], but in the case of compiler optimizations the attacks are new, and were discovered as a direct result of developing the model. We have experimentally validated that the attacks can be carried out against gcc and clang, though only against secrets known at compile time.

clang and gcc.


Appendix

A. Operations on sets of pomsets

Here we give the formal definitions for the operations described at the beginning of §IV.

In order to model speculation barriers in §V-B, we partition the actions into mergeable and unmergeable.

In transactional memory, begin and commit actions are memory fences: that is, they are a barrier to reordering memory accesses. To capture this (and other memory barriers), we introduce a connective to model such barriers.

Let $R$ be a relation on sets of pomsets.

Definition A.1. Let $a \to \P$ be the set $\P'$ where $\P' \in \P$ whenever there is $P \in \P$ such that:

- $E' = E \cup \{c\}$,
- if $d \leq e$ then $d \preceq' e$,
- if $d \not\leq e$ then $d \not\preceq' e$,
- if $c \in E$ then $c$ is mergeable,
- $X'(c) = (\phi, a)$, and
- if $\lambda(e) = (\psi \mid b)$ then $X'(e) = (\psi' \mid b)$, where:
  - $c \prec e$ whenever $a$ is an acquire or $b$ is a release,
  - if $a$ is an acquire then $\psi$ is independent of every $y$,
  - if $a$ and $b$ both touch the same location and one is a write, then $c \not\prec e$, and


The first constraint ensures that events are ordered before a release and after an acquire. The second constraint ensures that thread-local reads do not cross acquire fences.

The tricky parts of the definition are the named cases, which place requirements on read dependencies. If \( a \) reads \( v \) from \( x \), we have to decide whether \( e \) depends on \( e \) for some \( e \) with old precondition \( \psi \) and new precondition \( \psi' \). The first case [DEPENDENT READ] is that the dependency exists, in which case \( \psi' \) just has to imply \( \psi[v/x] \). The more interesting case is [INDEPENDENT READ], in which case \( \psi' \) has to imply \( \psi[v/x] \) and \( \psi \). This corresponds to a case where \( e \) can be performed with or without \( c \). In particular, if \( \psi \) is independent of \( x \) then we can pick \( \psi' \) to be \( \psi \), and the independent read case will apply.

**Definition A.2.** Let \( P_0 \in (P_1 \parallel P_2) \) whenever there are \( P_1 \in P_1 \) and \( P_2 \in P_2 \) such that:

- \( E_0 = E_1 \cup E_2 \),
- if \( e \leq d \) or \( e \leq 2d \) then \( e \leq 0 \),
- if \( e < _1 d \) or \( e < _2 d \) then \( e \leq 0 \),
- if \( e \in (E_1 \cap E_2) \) then \( e \) is mergeable,
- if \( \lambda_0(e) = \langle \phi_0 | a \rangle \) then either:
  - \( \lambda_1(e) = \langle \phi_1 | a \rangle \) and \( \lambda_2(e) = \langle \phi_2 | a \rangle \) and \( \phi_0 \) implies \( \phi_1 \lor \phi_2 \),
  - \( \lambda_1(e) = \langle \phi_1 | a \rangle \) and \( \phi_0 \) implies \( \phi_1 \), or
  - \( \lambda_2(e) = \langle \phi_2 | a \rangle \) and \( \phi_0 \) implies \( \phi_2 \).

**Definition A.3.** Let \( \mathcal{P}[M/x] \) be the set \( \mathcal{P}' \) where \( P' \in \mathcal{P}' \) whenever there is \( P \in \mathcal{P} \) such that:

- \( E' = E \),
- if \( d \leq e \) then \( d \leq' e \), and
- if \( d \leq e \) then \( d \leq e \), and
- if \( \lambda(e) = \langle \psi | a \rangle \) then \( \lambda'(e) = \langle \psi[M/x] | a \rangle \).

and similarly for \( \mathcal{P}[x/r] \).

**Definition A.4.** Let \( (\phi \sqsupset \mathcal{P}) \) be the subset of \( \mathcal{P} \) such that \( P \in \mathcal{P} \) whenever:

- if \( \lambda(e) = \langle \psi | a \rangle \) then \( \phi \) implies \( \psi \).

**Definition A.5.** A 3-valued pomset is \( x \)-closed if, for every \( e \in E \):

- \( e \) is independent of \( x \), and
- if \( e \) reads from \( x \), then there is a \( d \) such that \( e \) can read \( x \) from \( d \).

The definitions as they stand allow cycles in weak edges. This is necessary for examples such as \( (x := y - 1; x := 1 || y := x - 1; y := 1) \) which has execution:

However, in order to model release/acquire fencing in transactions, we need to ban executions such as:

The problem here is the weak cycle between \((W x 0)\) and \((W x 1)\), which according to **Definition III.3** allows both \((R x 0)\) and \((R x 1)\), even though one of them must be a stale value. This can be addressed by requiring \( \prec \) to form a per-location partial order. This is a form of partial coherence, and can be strengthened to total coherence by requiring \( \prec \) to be a per-location total order.

**Definition A.6.** A 3-valued pomset is partially (resp. totally) \( x \)-coherent if, when restricted to events which touch \( x \), \( \prec \) forms a partial (resp. total) order.

**Definition A.7.** Let \((\nu x \cdot \mathcal{P})\) be the subset of \( \mathcal{P} \) such that \( P \in \mathcal{P} \) whenever \( P \) is \( x \)-closed and partially \( x \)-coherent.

**B. Blockers**

Recall the preliminary definition of reads-from in **III-B** which defined an \( x \)-blocker to be and event \( c \) that writes to \( x \) such that \( d < c < e \). Were we to adopt this definition, then concurrent threads could turn events that were not \( x \)-blockers into an \( x \)-blocker, even if the new thread does not mention \( x \).

To see this, consider the program \((x := 1; y := x || x := z + 1; y := x || (z := 2)} \} \) with execution:

and the program \((z := y; z := y)\) with execution:
If these are placed in parallel, then a possible execution is:

and now the \((W \times 2)\) event is an \(x\)-blocker, so \((R \times 1)\) cannot read from \((W \times 1)\).

In the final definition of reads-from in §III-B we ruled out \(x\)-blockers by requiring that any event \(e\) that writes to \(x\) has either \(d \not< c\) or \(c \not< e\). With this definition, in order for \((R \times 1)\) to read from \((W \times 1)\), we either need \((W \times 1) \not< (W \times 2)\) or \((W \times 2) \not< (R \times 1)\), for example:

then putting this in parallel as before results in:

but this is not a valid 3-valued pomset, since \((W \times 2) < (R \times 1)\) but also \((W \times 2) \not< (R \times 1)\), which is a contradiction.

C. Release/acquire synchronization

We can develop a simple model of release/acquire synchronization using the following actions:
- \((\text{Rel } x v)\), a release action that writes \(v\) to \(x\), and
- \((\text{Acq } x v)\), an acquire action that reads \(v\) from \(x\).

The semantics of programs with releasing write and acquiring read are similar to regular write and read, with \(\text{Rel } x v\) replacing \(W \times v\) and \(\text{Acq } x v\) replacing \(R \times v\):

\[
\begin{align*}
\lfloor \text{rel } x := M; C \rfloor &= \bigcup_v \left( (M = v) \triangleright (\text{Rel } x v) \rightarrow [C][M/x] \right) \\
\lfloor \text{acq } r := x; C \rfloor &= \bigcup_v (\text{Acq } x v) \rightarrow [C][x/r]
\end{align*}
\]

To see the need for the first constraint on prefixing, consider the program:

\[
\text{var } x := 0; \text{var } f := 0; (x := 1; \text{rel } f := 1 \mid \text{acq } r := f; s := x)
\]

This has an execution:

but not:

since \((W \times 0) \not< (W \times 1) < (R \times 0)\), so this pomset does not satisfy the requirements to be \(x\)-closed. If we replace the release with a plain write, then the outcome \((\text{Acq } f 1)\) and \((R \times 0)\) is possible:

since no order is required between \((W \times 1)\) and \((W \times 1)\). Symmetrically, if we replace the acquire of the original program with a plain read, then the outcome \((R \times 1)\) and \((R \times 0)\) is possible.

D. Relaxed memory

In §VI-A we presented an information flow attack on relaxed memory, similar to Spectre in that it relies on speculative evaluation. Unlike Spectre it does not depend on timing attacks, but instead is based on the sensitivity of relaxed memory to data dependencies.

Our model includes concurrent memory accesses, which can introduce concurrent reads-from. Since we are allowing events to be partially ordered, this gives a simple model of relaxed memory. For example an independent read independent write (IRIW) example is:

\[
\begin{align*}
x &:= 0; x := x + 1 \mid y := 0; y := y + 1 \\
\mid r_1 := x; r_2 := y \mid s_1 := y; s_2 := x
\end{align*}
\]

which includes the execution:

This model does not introduce thin-air reads (TAR). For example the TAR pit \((x := y \mid y := x)\) fails to produce a value for \(x\) from thin air since this produces a cycle in \(\leq\), as shown on the left below:

\[
\begin{align*}
\text{Ry 42} & \rightarrow \text{Rx 42} & \text{Ry 1} & \rightarrow \text{Rx 1} \\
\text{Wx 42} & \rightarrow \text{Wy 42} & \text{Wx 1} & \rightarrow \text{Wy 1}
\end{align*}
\]

This cycle can be broken by removing a dependency. For example \((x := y \mid r := x; y := r + 1 - r)\) has the execution on
the right above. Note that \((R x 1) \not\leq (W y 1)\), so this does not introduce a cycle.

Although it is not the primary focus of this paper, our model may be an attractive model of relaxed memory. Many prior models either permit thin-air executions that our model forbids or forbid desirable executions that our model permits.

Pugh [37] developed a set of twenty causality test cases in the process of revising the Java Memory Model (JMM) [29]. Using hand calculation, we have confirmed that our model gives the desired result for all twenty cases, unrolling loops as necessary. Our model also gives the desired results for all of the examples in Batty et al. [5, §4] and all but one in Ševčík [44, §5.3]: redundant-write-after-read-elimination fails for any sensible non-coherent semantics. Our model agrees with the JMM on the “surprising and controversial behaviors” of Manson et al. [29, §8], and thus fails to validate thread inlining.