PENGUIN BOOKS

MYSTERY & CRIME

THE CODE
THAT NEVER RAN

MYSTERY & CRIME

CRAIG DISSELKOEN   ALAN JEFFREY
RADHA JAGADEESAN   JAMES RIELY

COMPLETE   UNABRIDGED

A classic locked-room mystery.
Eve was in the false branch of a
conditional the whole time,
how could she do it?

Overview

The Code That
Never Ran:
Modeling Attacks
on Speculative
Evaluation

Craig Disselkoen,
Radha Jagadeesan,
Alan Jeffrey,
James Riely

Why? Spectre!

Craig Disselkoen,
Radha Jagadeesan,
Alan Jeffrey,
James Riely

Why? Spectre!

The Code That
Never Ran:
Modeling Attacks
on Speculative
Evaluation

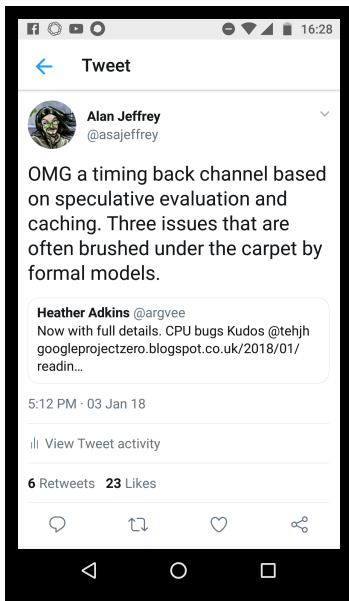Craig Disselkoen,
Radha Jagadeesan,
Alan Jeffrey,
James Riely

Attacks bypass dynamic
security checks:

```
if (canReadSecret) {
  doStuffWith(SECRET);
}
```

Information flow from
SECRET even though
canReadSecret is false.

Most formal models ignore
code in branches that
aren't taken.

Models that include speculation?

The Code That
Never Ran:
Modeling Attacks
on Speculative
Evaluation

Craig Disselkoen,
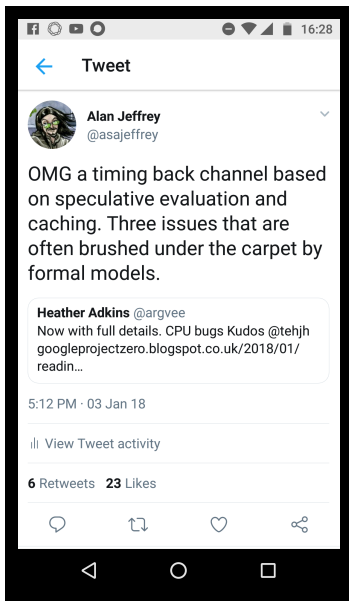Radha Jagadeesan,
Alan Jeffrey,
James Riely

Introduction

Model

Examples

Attacks

Experiments

Conclusions

There are some models that include speculation
relaxed memory models:

- ► *The Java Memory Model*
  Manson, Pugh and Adve, 2005.

- ► *Generative Operational Semantics for Relaxed Memory Models*
  Jagadeesan, Pitcher and Riely, 2010.

- ► *A promising semantics for relaxed-memory concurrency*
  Kang, Hur, Lahav, Vafeiadis and Dreyer, 2017.

Models that include speculation?

The Code That
Never Ran:
Modeling Attacks
on Speculative
Evaluation

Craig Disselkoen,
Radha Jagadeesan,
Alan Jeffrey,
James Riely

Introduction

Model

Examples

Attacks

Experiments

Conclusions

There are some models that include speculation
relaxed memory models:

- *The Java Memory Model*
  Manson, Pugh and Adve, 2005.

- *Generative Operational Semantics for Relaxed Memory Models*
  Jagadeesan, Pitcher and Riely, 2010.

- *A promising semantics for relaxed-memory concurrency*
  Kang, Hur, Lahav, Vafeiadis and Dreyer, 2017.

Question: is there a simple model similar to those of relaxed
memory, that can model speculation?

Information flow attacks on speculation

Craig Disselkoen,
Radha Jagadeesan,
Alan Jeffrey,
James Riely

Speculation happens in many places:

- *Speculation in hardware* (branch prediction,...)

- *Transactions* (transactional memory,...)

- *Relaxed memory* (compiler optimizations,...)

Information flow attacks on speculation

The Code That
Never Ran:
Modeling Attacks
on Speculative
Evaluation

Craig Disselkoen,
Radha Jagadeesan,
Alan Jeffrey,
James Riely

Introduction

Model

Examples

Attacks

Experiments

Conclusions

Speculation happens in many places:

▶ *Speculation in hardware* (branch prediction,...)
  Attacked by Spectre (Kocher *et al.* 2019).

▶ *Transactions* (transactional memory,...)
  Attacked by Prime+Abort (Disselokoen *et al.* 2017).

▶ *Relaxed memory* (compiler optimizations,...)
  No known attacks.

Question: are there information flow attacks against
compiler optimizations?

Contributions

- ▶ A simple compositional model.
- ▶ Examples.
- ▶ Attacks (including a new attack on relaxed memory).
- ▶ Experiments (testing practicality of new attacks).

Pomsets

C11-style models are based on *events*
with *labels* (e.g. $(R\,x\,3)$ or $(W\,x\,3)$)
and *relations* (e.g. happens-before or reads-from).

Craig Disselkoen,
Radha Jagadeesan,
Alan Jeffrey,
James Riely

Pomsets

The Code That
Never Ran:
Modeling Attacks
on Speculative
Evaluation

Craig Disselkoen,
Radha Jagadeesan,
Alan Jeffrey,
James Riely

Introduction

Model

Examples

Attacks

Experiments

Conclusions

C11-style models are based on *events*
with *labels* (e.g. $(R\,x\,3)$ or $(W\,x\,3)$)
and *relations* (e.g. happens-before or reads-from).

Simplest such is *partially ordered multisets* (Gisher, 1988).

Only one relation, a partial order modelling dependency

Pomsets

The Code That
Never Ran:
Modeling Attacks
on Speculative
Evaluation

Craig Disselkoen,
Radha Jagadeesan,
Alan Jeffrey,
James Riely

Introduction

Model

Examples

Attacks

Experiments

Conclusions

C11-style models are based on *events*
with *labels* (e.g. (R x 3) or (W x 3))
and *relations* (e.g. happens-before or reads-from).

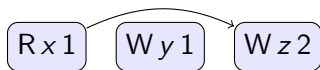Simplest such is *partially ordered multisets* (Gisher, 1988).

Only one relation, a partial order modelling dependency, e.g.
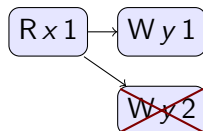
$$\boxed{\text{R}\,x\,1} \quad \boxed{\text{W}\,y\,1} \longrightarrow \boxed{\text{W}\,z\,2}$$

is an execution of ($r := x$; $y := 1$; $z := r + 1$).

Pomsets

The Code That
Never Ran:
Modeling Attacks
on Speculative
Evaluation

Craig Disselkoen,
Radha Jagadeesan,
Alan Jeffrey,
James Riely

Introduction

Model

Examples

Attacks

Experiments

Conclusions

C11-style models are based on *events*
with *labels* (e.g. (R x 3) or (W x 3))
and *relations* (e.g. happens-before or reads-from).

Simplest such is *partially ordered multisets* (Gisher, 1988).

Only one relation, a partial order modelling dependency, e.g.

is an execution of (if (x) { y := 1 } else { y := 2 }).

Compositional pomset model

Craig Disselkoen,
Radha Jagadeesan,
Alan Jeffrey,
James Riely

First off, straight-line code.

Compositional pomset model

First off, straight-line code.

New idea: put preconditions on events

Craig Disselkoen,
Radha Jagadeesan,
Alan Jeffrey,
James Riely

Compositional pomset model

Craig Disselkoen,
Radha Jagadeesan,
Alan Jeffrey,
James Riely

First off, straight-line code.

New idea: put preconditions on events, e.g.

$$\boxed{r = 1 \mid \mathsf{W}\,z\,2}$$

is an execution of ($z := r + 1$).

Compositional pomset model

The Code That
Never Ran:
Modeling Attacks
on Speculative
Evaluation

Craig Disselkoen,
Radha Jagadeesan,
Alan Jeffrey,
James Riely

Introduction

Model

Examples

Attacks

Experiments

Conclusions

First off, straight-line code.

New idea: put preconditions on events, e.g.

$$\boxed{\mathsf{W}\,y\,1} \quad \boxed{r = 1 \mid \mathsf{W}\,z\,2}$$

is an execution of ($y := 1; z := r + 1$).

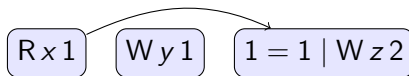*Note*: no dependency because r does not depend on $y := 1$.

Compositional pomset model

The Code That
Never Ran:
Modeling Attacks
on Speculative
Evaluation

Craig Disselkoen,
Radha Jagadeesan,
Alan Jeffrey,
James Riely

Introduction

Model

Examples

Attacks

Experiments

Conclusions

First off, straight-line code.

New idea: put preconditions on events, e.g.

$$\boxed{R\,x\,1} \quad \boxed{W\,y\,1} \quad \boxed{1 = 1 \mid W\,z\,2}$$

is an execution of $(r := x;\, y := 1;\, z := r + 1)$.

Note: dependency because r depends on $r := x$.
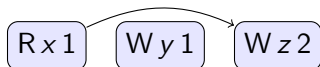*Also note*: performing a substitution $[1/r]$.

Compositional pomset model

The Code That
Never Ran:
Modeling Attacks
on Speculative
Evaluation

Craig Disselkoen,
Radha Jagadeesan,
Alan Jeffrey,
James Riely

Introduction

Model

Examples

Attacks

Experiments

Conclusions

First off, straight-line code.

New idea: put preconditions on events, e.g.

$$\boxed{R\,x\,1} \quad \boxed{W\,y\,1} \quad \boxed{W\,z\,2}$$

is an execution of $(r := x;\ y := 1;\ z := r + 1)$.

Visualize: elide tautologies

Compositional pomset model

Next, conditionals.

The Code That
Never Ran:
Modeling Attacks
on Speculative
Evaluation

Craig Disselkoen,
Radha Jagadeesan,
Alan Jeffrey,
James Riley

Compositional pomset model

Craig Disselkoen,
Radha Jagadeesan,
Alan Jeffrey,
James Riely

Next, conditionals.

New idea: an execution of if $M \{ C \}$ else $\{ D \}$
comes from an execution of C *and* an execution of D

The Code That
Never Ran:
Modeling Attacks
on Speculative
Evaluation

Craig Disselkoen,
Radha Jagadeesan,
Alan Jeffrey,
James Riely

Introduction

Model

Examples

Attacks

Experiments

Conclusions

Compositional pomset model

Next, conditionals.

New idea: an execution of if $M \{ C \}$ else $\{ D \}$
comes from an execution of C *and* an execution of D, e.g.

$$\boxed{r \neq 0 \mid \mathsf{W}\, y\, 1}$$

is an execution of ($\qquad\qquad y := 1 \qquad\qquad$)
when $r \neq 0$

Compositional pomset model

The Code That
Never Ran:
Modeling Attacks
on Speculative
Evaluation

Craig Disselkoen,
Radha Jagadeesan,
Alan Jeffrey,
James Riely

Introduction

Model

Examples

Attacks

Experiments

Conclusions

Next, conditionals.

New idea: an execution of if $M \{ C \}$ else $\{ D \}$
comes from an execution of C *and* an execution of D, e.g.

$$\boxed{r = 0 \mid W y \, 2}$$

is an execution of ($y := 2$)
when $r = 0$

Compositional pomset model

The Code That
Never Ran:
Modeling Attacks
on Speculative
Evaluation

Craig Disselkoen,
Radha Jagadeesan,
Alan Jeffrey,
James Riely

Introduction

Model

Examples

Attacks

Experiments

Conclusions

Next, conditionals.

New idea: an execution of if $M \{ C \}$ else $\{ D \}$
comes from an execution of C *and* an execution of D, e.g.
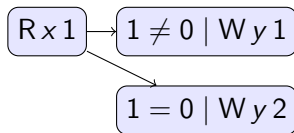
$$\boxed{r \neq 0 \mid W\, y\, 1}$$

$$\boxed{r = 0 \mid W\, y\, 2}$$

is an execution of (if $(r) \{ y := 1 \}$ else $\{ y := 2 \})$

Compositional pomset model

The Code That
Never Ran:
Modeling Attacks
on Speculative
Evaluation

Craig Disselkoen,
Radha Jagadeesan,
Alan Jeffrey,
James Riely

Introduction

Model

Examples

Attacks

Experiments

Conclusions

Next, conditionals.

New idea: an execution of if $M \{ C \}$ else $\{ D \}$
comes from an execution of C *and* an execution of D, e.g.

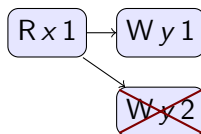is an execution of $(r := x; \text{if } (r) \{ y := 1 \} \text{ else } \{ y := 2 \})$

Compositional pomset model

The Code That
Never Ran:
Modeling Attacks
on Speculative
Evaluation

Craig Disselkoen,
Radha Jagadeesan,
Alan Jeffrey,
James Riely

Introduction

Model

Examples

Attacks

Experiments

Conclusions

Next, conditionals.

New idea: an execution of if $M \{ C \}$ else $\{ D \}$
comes from an execution of C *and* an execution of D, e.g.

is an execution of $(r := x ; \text{if} (r) \{ y := 1 \} \text{else} \{ y := 2 \})$

Visualize: elide tautologies and cross out unsatisfiables

Compositional pomset model

But...

The Code That
Never Ran:
Modeling Attacks
on Speculative
Evaluation

Craig Disselkoen,
Radha Jagadeesan,
Alan Jeffrey,
James Riely

Compositional pomset model

But... any execution of C should be
an execution of if M { C } else { C }

Craig Disselkoen,
Radha Jagadeesan,
Alan Jeffrey,
James Riley

Compositional pomset model

The Code That
Never Ran:
Modeling Attacks
on Speculative
Evaluation

Craig Disselkoen,
Radha Jagadeesan,
Alan Jeffrey,
James Riely
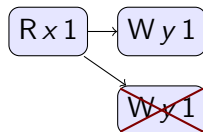
Introduction
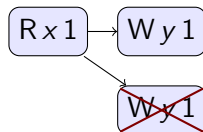
Model

Examples

Attacks

Experiments

Conclusions

But... any execution of C should be
an execution of if $M \{ C \}$ else $\{ C \}$, e.g.

is an execution of (if $x \{ y := 1 \}$ else $\{ y := 1 \}$)

Compositional pomset model

The Code That
Never Ran:
Modeling Attacks
on Speculative
Evaluation

Craig Disselkoen,
Radha Jagadeesan,
Alan Jeffrey,
James Riely

Introduction

Model

Examples

Attacks

Experiments

Conclusions

But... any execution of C should be
an execution of if $M \{ C \}$ else $\{ C \}$, e.g.

$$\boxed{R\,x\,1} \longrightarrow \boxed{W\,y\,1}$$

$$\boxed{W\,y\,1}$$

is an execution of (if $x \{ y := 1 \}$ else $\{ y := 1 \}$), but so is

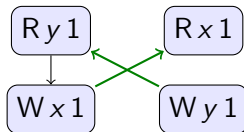$$\boxed{R\,x\,1} \qquad \boxed{W\,y\,1}$$

Compositional pomset model

The Code That
Never Ran:
Modeling Attacks
on Speculative
Evaluation

Craig Disselkoen,
Radha Jagadeesan,
Alan Jeffrey,
James Riely

Introduction

Model

Examples

Attacks

Experiments

Conclusions

But... any execution of C should be
an execution of if $M \{ C \}$ else $\{ C \}$, e.g.

$$\boxed{R\,x\,1} \longrightarrow \boxed{W\,y\,1}$$

$$\xcancel{\boxed{W\,y\,1}}$$

is an execution of (if $x \{ y := 1 \}$ else $\{ y := 1 \}$), but so is

$$\boxed{R\,x\,1} \qquad \boxed{W\,y\,1}$$

New idea: events from different branches can merge.

Compositional pomset model

Lastly, concurrency.

The Code That
Never Ran:
Modeling Attacks
on Speculative
Evaluation

Craig Disselkoen,
Radha Jagadeesan,
Alan Jeffrey,
James Riely

Compositional pomset model

Craig Disselkoen,
Radha Jagadeesan,
Alan Jeffrey,
James Riely

Lastly, concurrency.

Old idea: match reads with matching writes (à la C11)

Compositional pomset model

The Code That
Never Ran:
Modeling Attacks
on Speculative
Evaluation

Craig Disselkoen,
Radha Jagadeesan,
Alan Jeffrey,
James Riely

Introduction

Model

Examples

Attacks

Experiments

Conclusions

Lastly, concurrency.

Old idea: match reads with matching writes (à la C11), e.g.

is an execution of $(x := y \;||\; r := x\,;\, y := 1)$.

Compositional pomset model

Glossed over some details:

- 3-valued pomsets for negative constraints $d \nleq e$,
- sanity conditions on reads-from,
- precise rules for dependency,
- scoping and scope extrusion,
- $\cdots$

All in the paper!

Examples go here

The Code That
Never Ran:
Modeling Attacks
on Speculative
Evaluation

Craig Disselkoen,
Radha Jagadeesan,
Alan Jeffrey,
James Riely

Information flow attacks go here

Implementing the new attacks

The Code That
Never Ran:
Modeling Attacks
on Speculative
Evaluation

Craig Disselkoen,
Radha Jagadeesan,
Alan Jeffrey,
James Riely

Outro goes here

The Code That
Never Ran:
Modeling Attacks
on Speculative
Evaluation

Craig Disselkoen,
Radha Jagadeesan,
Alan Jeffrey,
James Riely