

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

Creative Commons Attribution-ShareAlike 4.0 Mozilla Research | DePaul University | U. California San Diego

Overview

Introduction Model Examples Attacks Experiments Conclusions The Code That Never Ran: Modeling Attacks on Speculative Evaluation

Craig Disselkoen, Radha Jagadeesan, Alan Jeffrey, James Riely

Introduction

Mode

Examples

Nttacks

 $\mathsf{E} \mathsf{x} \mathsf{p} \mathsf{e} \mathsf{r} \mathsf{i} \mathsf{m} \mathsf{e} \mathsf{n} \mathsf{t} \mathsf{s}$

Why? Spectre!



The Code That Never Ran: Modeling Attacks on Speculative Evaluation

Craig Disselkoen, Radha Jagadeesan, Alan Jeffrey, James Riely

Introduction

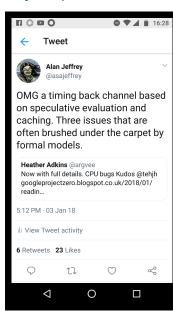
Mode

Examples

Attacks

Experiment:

Why? Spectre!



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.

The Code That Never Ran: Modeling Attacks on Speculative Evaluation

Craig Disselkoen, Radha Jagadeesan, Alan Jeffrey, James Riely

Introduction

Mode

Examples

TILACKS

experiments

Models that include speculation?

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.

The Code That Never Ran: Modeling Attacks on Speculative Evaluation

Craig Disselkoen, Radha Jagadeesan, Alan Jeffrey, James Riely

Introduction

Model

Examples

ttacks

Models that include speculation?

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?

The Code That Never Ran: Modeling Attacks on Speculative Evaluation

Craig Disselkoen, Radha Jagadeesan, Alan Jeffrey, James Riely

Introduction

Model

Examples

illacks

vneriments



Information flow attacks on speculation

Speculation happens in many places:

- Speculation in hardware
 Attacked by Spectre (Kocher et al. 2019).
- Transactions
 Attacked by Prime+Abort (Disselokoen et al. 2017).
- Relaxed memory
 No known attacks.

The Code That Never Ran: Modeling Attacks on Speculative Evaluation

Craig Disselkoen, Radha Jagadeesan, Alan Jeffrey, James Riely

Introduction

Model

Examples

ttacks

Experiments

Information flow attacks on speculation

Speculation happens in many places:

- Speculation in hardware
 Attacked by Spectre (Kocher et al. 2019).
- Transactions
 Attacked by Prime+Abort (Disselokoen et al. 2017).
- Relaxed memory
 No known attacks.

Question: Do all three lead to information flow attacks?

The Code That Never Ran: Modeling Attacks on Speculative Evaluation

Craig Disselkoen, Radha Jagadeesan, Alan Jeffrey, James Riely

Introduction

Model

Examples

Nttacks

Experiments

Contributions

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

The Code That Never Ran: Modeling Attacks on Speculative Evaluation

Craig Disselkoen, Radha Jagadeesan, Alan Jeffrey, James Riely

Introduction

Mod

Examples

Attacks

Experiments

anclusions

Model goes here

The Code That Never Ran: Modeling Attacks on Speculative Evaluation

Craig Disselkoen, Radha Jagadeesan, Alan Jeffrey, James Riely

Introduction

Model

Examples

Attacks

Experiments

Examples go here

The Code That Never Ran: Modeling Attacks on Speculative Evaluation

Craig Disselkoen, Radha Jagadeesan, Alan Jeffrey, James Riely

Introductio

Model

Examples

Attacks

 $\mathsf{E} \mathsf{x} \mathsf{periments}$

Information flow attacks go here

The Code That Never Ran: Modeling Attacks on Speculative Evaluation

Craig Disselkoen, Radha Jagadeesan, Alan Jeffrey, James Riely

Introductio

Model

Examples

Attacks

Experiments

Implementing the new attacks

The Code That Never Ran: Modeling Attacks on Speculative Evaluation

Craig Disselkoen, Radha Jagadeesan, Alan Jeffrey, James Riely

Introduction

Mode

Examples

Attacks

Experiments

Outro goes here

The Code That Never Ran: Modeling Attacks on Speculative Evaluation

Craig Disselkoen, Radha Jagadeesan, Alan Jeffrey, James Riely

Introductio

iviodei

Examples

Attacks

Experiments