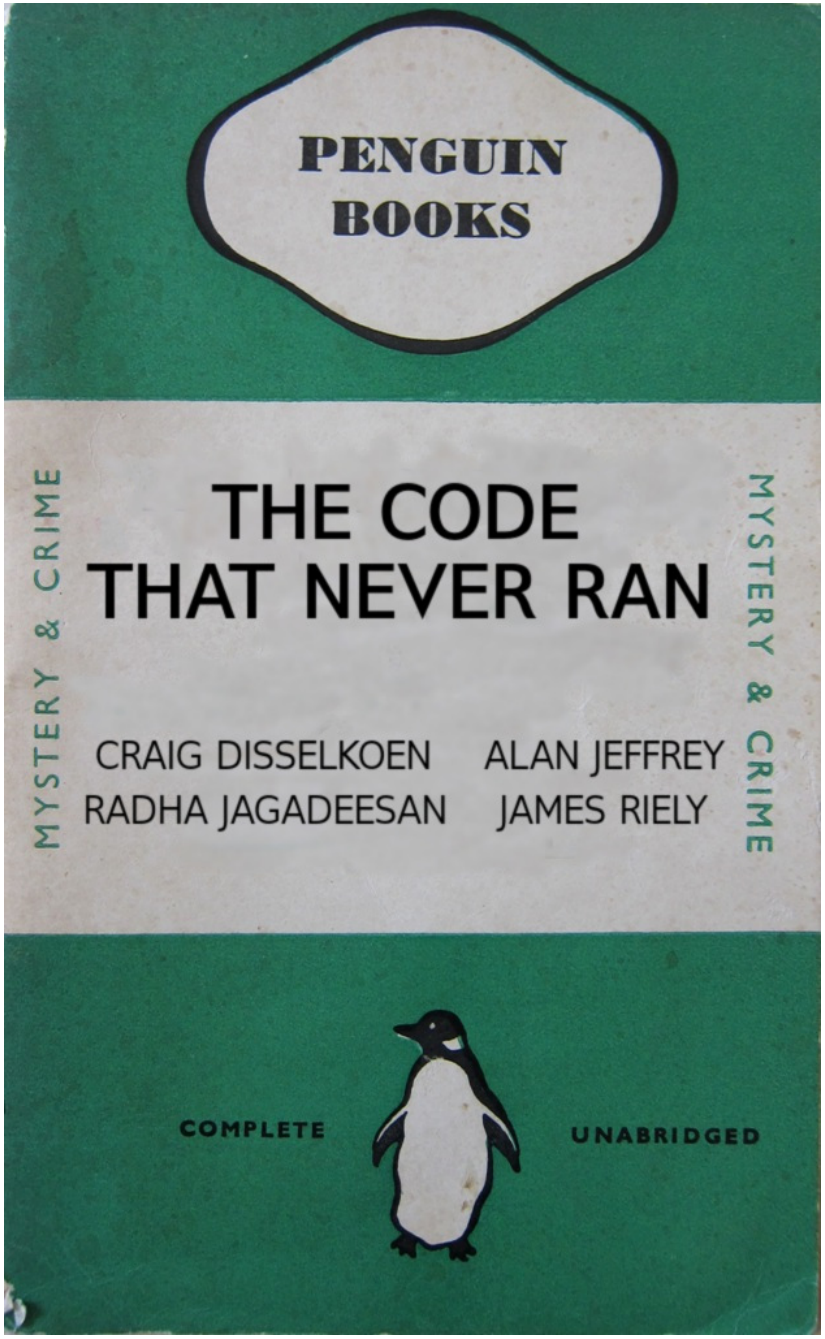


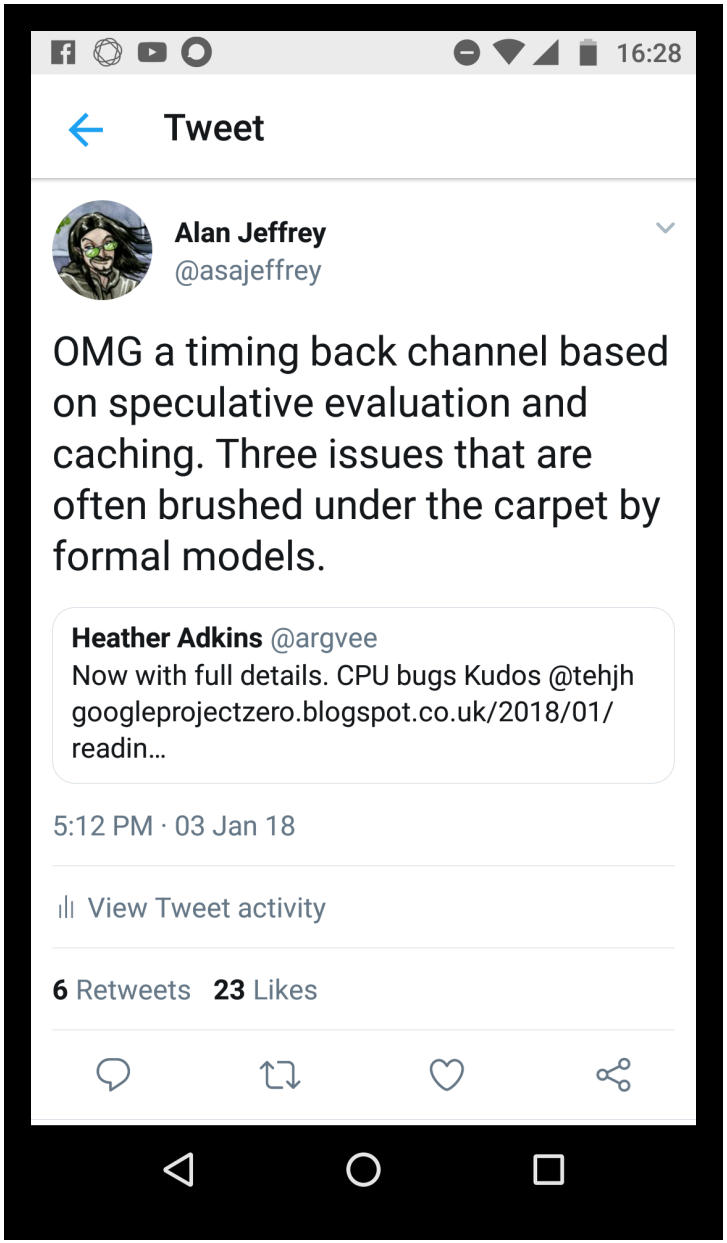
A classic locked-room mystery.
Eve was in the false branch of a conditional the whole time,
how could she do it?

Mozilla Research | DePaul University | U. California San Diego

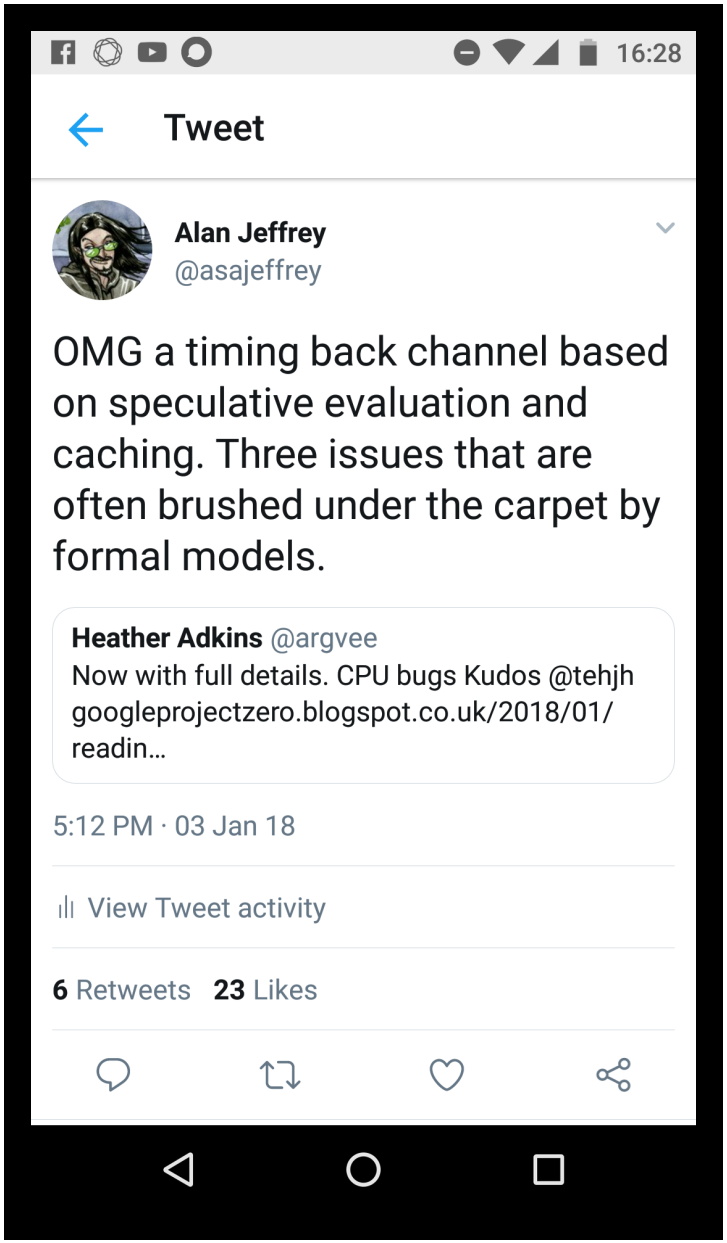
Overview

Introduction
Model
Examples
Attacks
Experiments
Conclusions

Why? Spectre!



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.

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.

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?

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.

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?

Contributions

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

Model goes here

Examples go here

Information flow attacks go here

Implementing the new attacks

Outro goes here