Presentation CS595

Yuezhi Che

11/30/2020

Spectre Attacks: Exploiting Speculative Execution

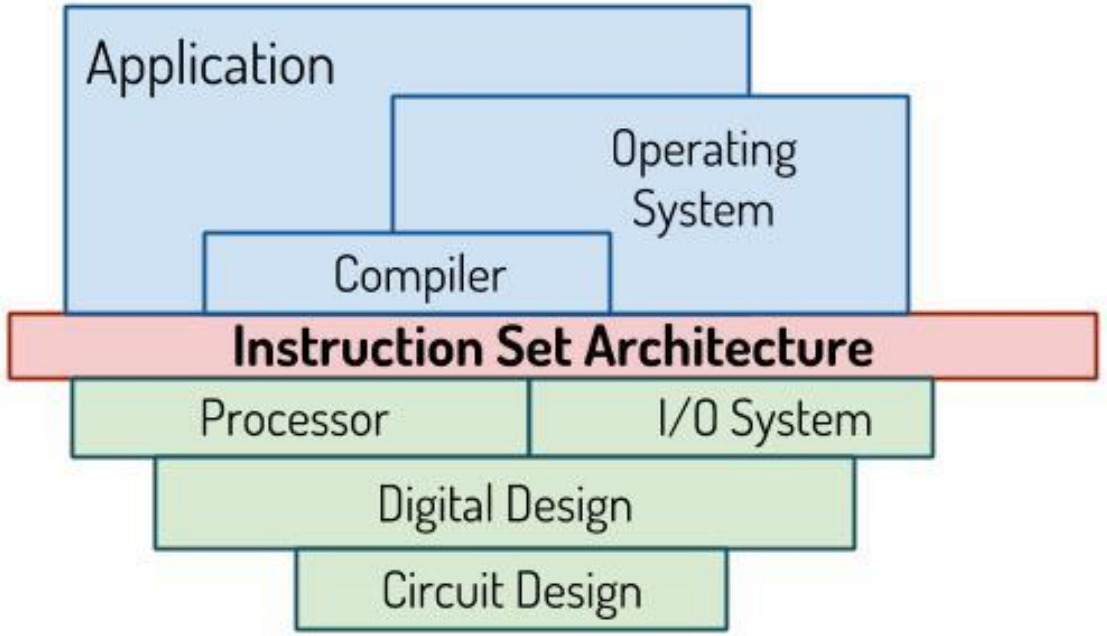
Paul Kocher[1], Jann Horn[2], Anders Fogh[3], Daniel Genkin[4],
Daniel Gruss[5], Werner Haas[6], Mike Hamburg[7], Moritz Lipp[5],
Stefan Mangard[5], Thomas Prescher[6], Michael Schwarz[5], Yuval Yarom[8]
[1] Independent (www.paulkocher.com), [2] Google Project Zero,
[3] G DATA Advanced Analytics, [4] University of Pennsylvania and University of Maryland,
[5] Graz University of Technology, [6] Cyberus Technology,
[7] Rambus, Cryptography Research Division, [8] University of Adelaide and Data61

Spectre attack

- Vulnerabilities in modern computers

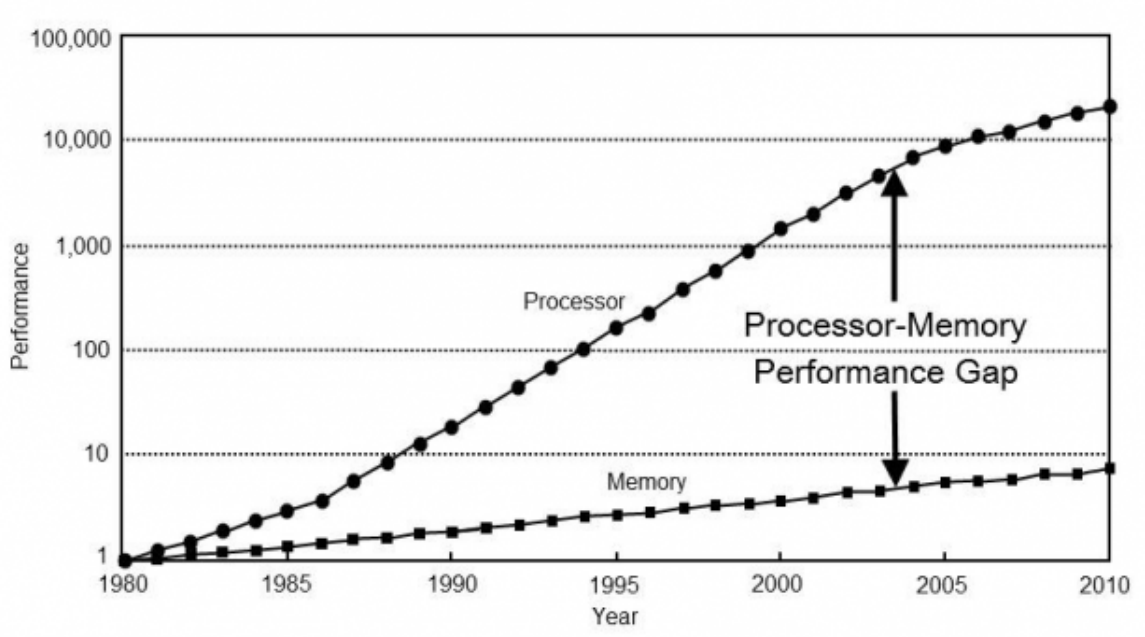
Background: *Computer architecture*

- Instruction set architecture (ISA)
- Execution order
  - In-order
  - Out-of-order
  - Re-order buffer (ROB)



Background: *To boost CPU performance*

- Improve hardware
- Design optimization
  - **Speculative execution**
- Memory hierarchy
  - CPU-memory
  - Caches



Spectre attack overview

- Conditional branch example
  - array1 = [1,2]
  - array2 = [x, y, z ……]
  - x is input under the attacker's control

```
if (x < array1_size)
    y = array2[array1[x] * 4096];
```

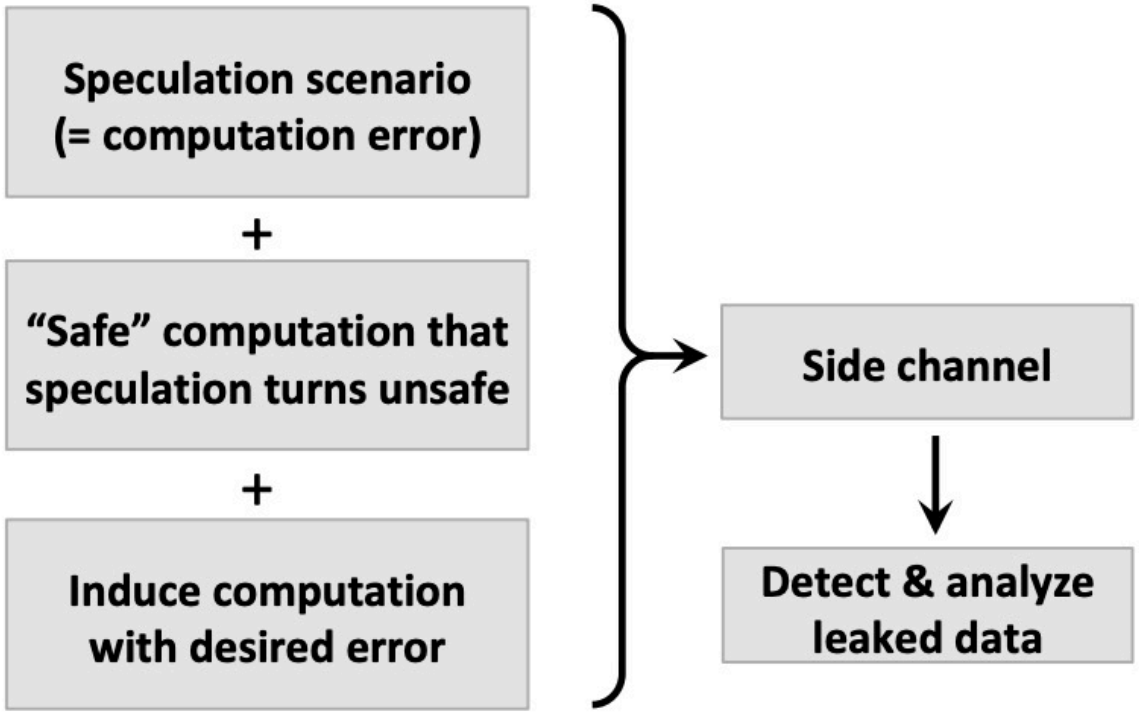
Spectre attack overview

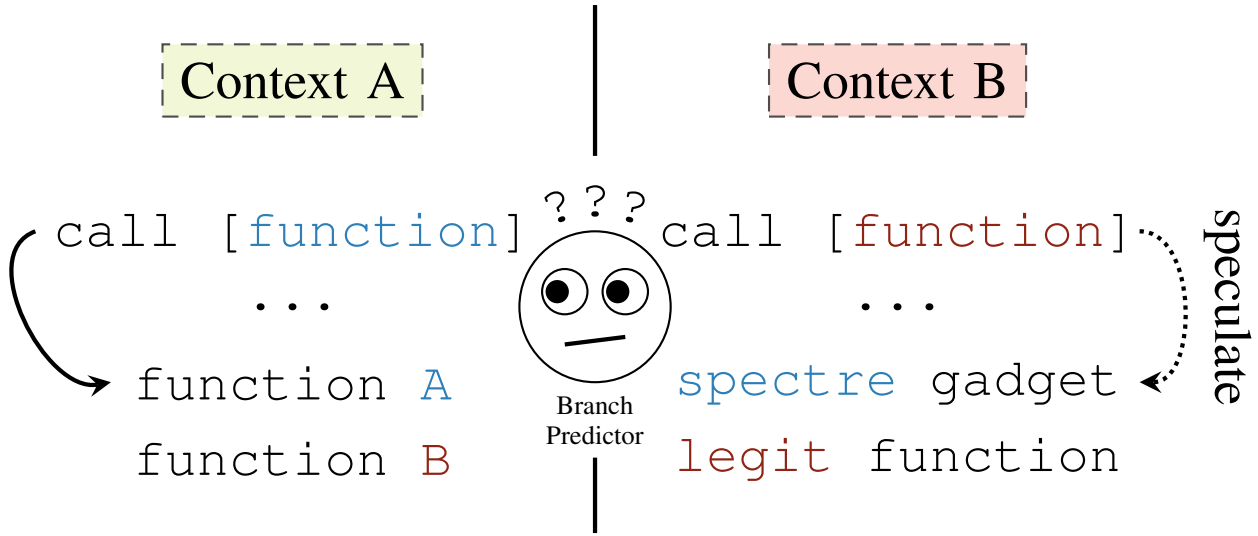
- Attacker read array2[i*4096]
  - Find i=3 is fast
  - array[x] = k has been cached
  - Then secret k =3 is revealed
- Side channel attack

array2[0 * 4096]	
array2[1* 4096]	
array2[2 * 4096]	
array2[3 * 4096]	cached
array2[4 * 4096]	

Spectre attack: Brach prediction

- Attacker can misdirect the prediction





Mitigation options

- Not do speculative execution
  - Trade-off between performance and security
- Preventing access to secret data
  - Add new data dependencies
- Add hardware to hide speculative execution
- Not all speculative loads leak secret

Summary

- Spectre attacks leverage the speculative execution.
- Software security depends on having a clear common understanding between hardware and software.
- Trade-off between security and performance is always a problem.

Thank you