JumpSwitches: Restoring the Performance of Indirect Branches In the Era of Spectre

Nadav Amit, Fred Jacobs, Michael Wei

July 2019

Spectre: Speculative Execution Vulnerabilities

-=[R3]

R1=R2

OS kernel

Speculative Execution CPU Vulnerabilities

CALL *R10

branch predictor

OS kernel

Speculative Execution CPU Vulnerabilities

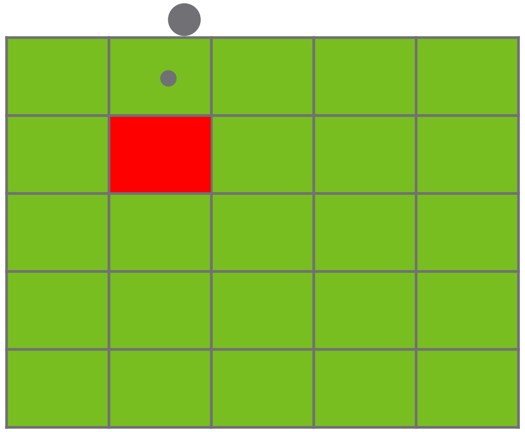
CALL *R10

branch predictor

R9 = [uptr + R8]

R8 *= 64

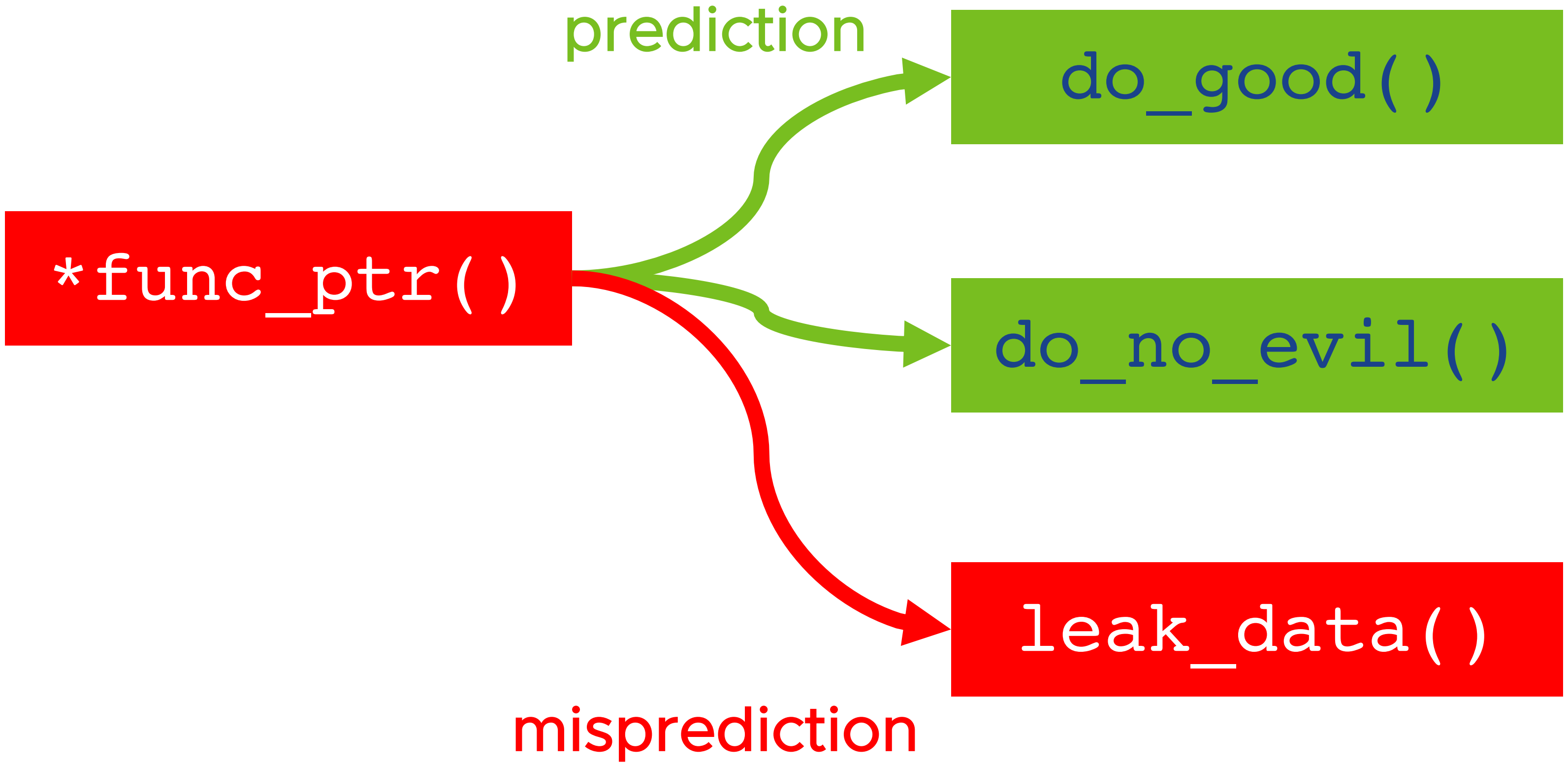
R8=*secret



CPU cache

OS kernel

Spectre v2 – Unrestricted Indirect Branch Speculation



prediction

*func_ptr()

do_good()

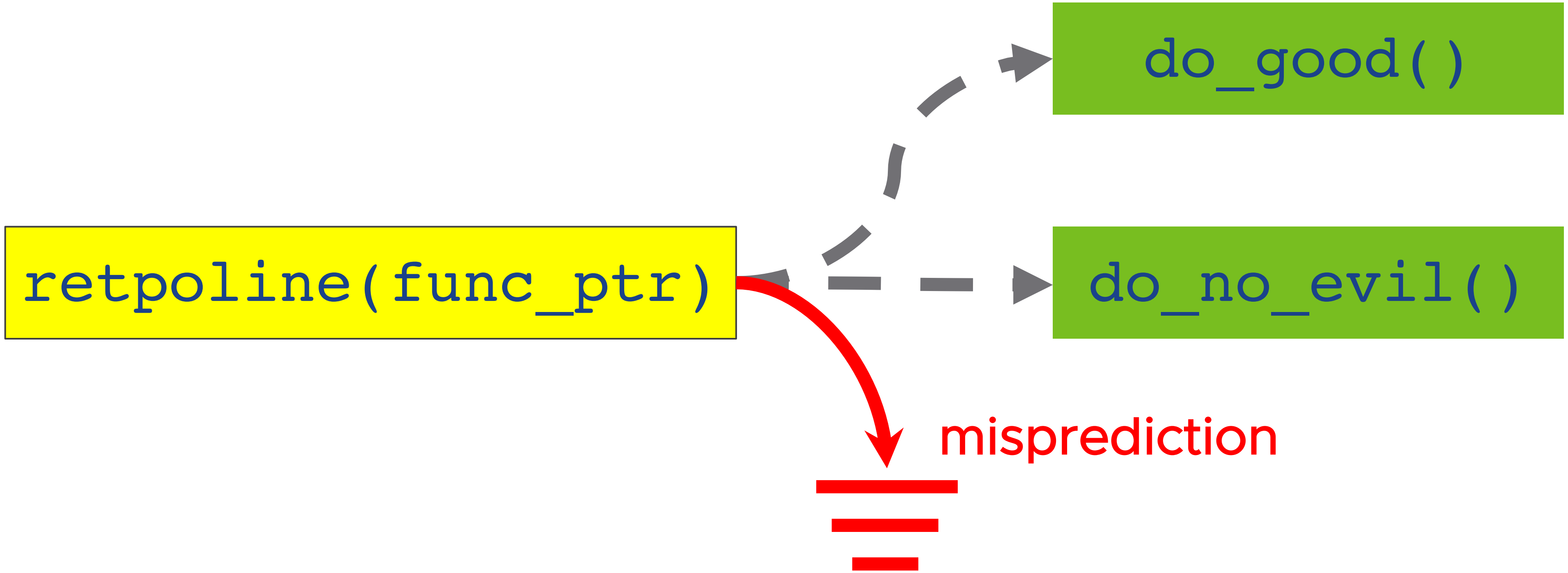
do_no_evil()

leak_data()

misprediction

©2019 VMware, Inc.

Current Solution: Retpolines



every indirect branch is mispredicted

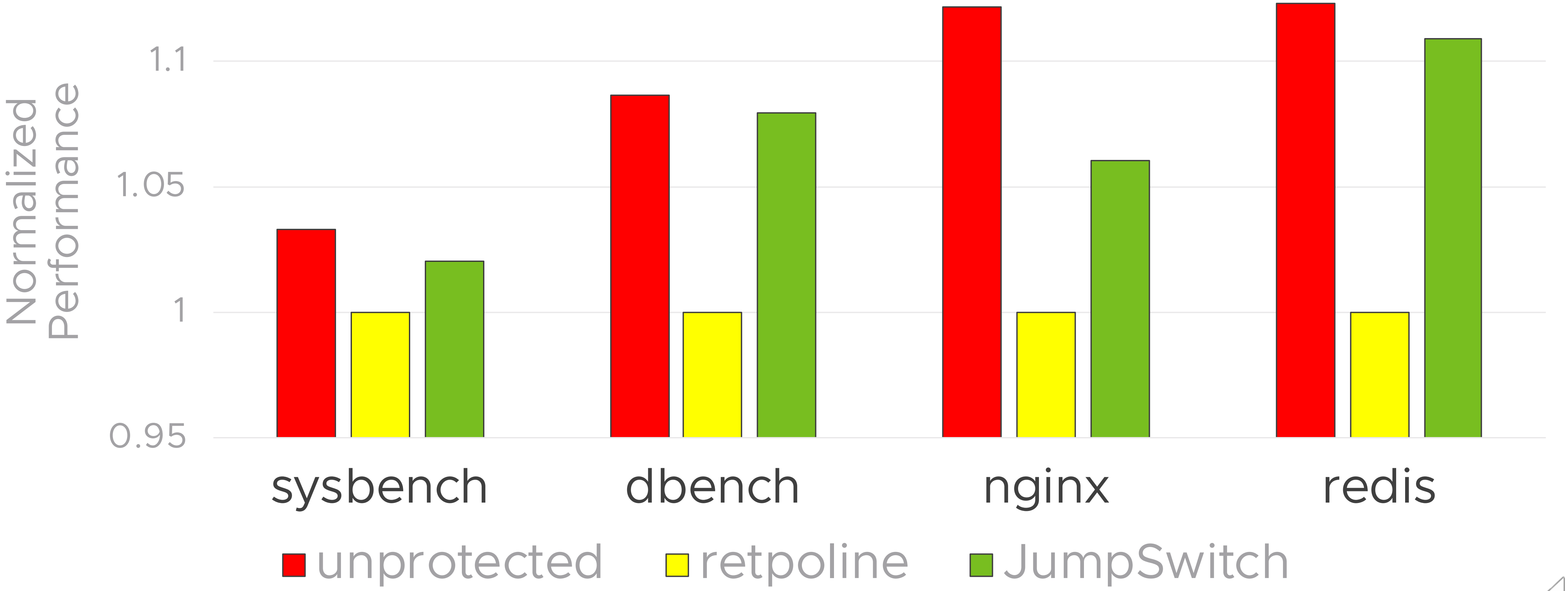
JumpSwitches

Dynamic indirect branch promotion

Mechanisms to reduce Retpoline overheads by:

- Learning targets on the fly
- Binary rewriting the targets
- Supporting multiple hot targets
- and per-context targets

Macro-Benchmarks on Linux



Security #1: Kernel

Today at 5:10, Track II