starting 2019

SafeBet: Memory capabilities to enable safe, aggressive speculation in processors

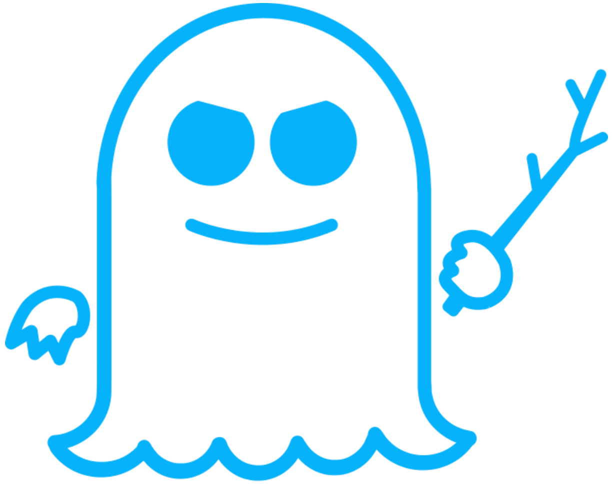
Simon Moore, Jonathan Woodruff, Robert Watson

RISE Annual Conference, London

14th November 2018

UNIVERSITY OF CAMBRIDGE
Computer Science and Technology

Motivation: new speculative execution attacks



SPECTRE

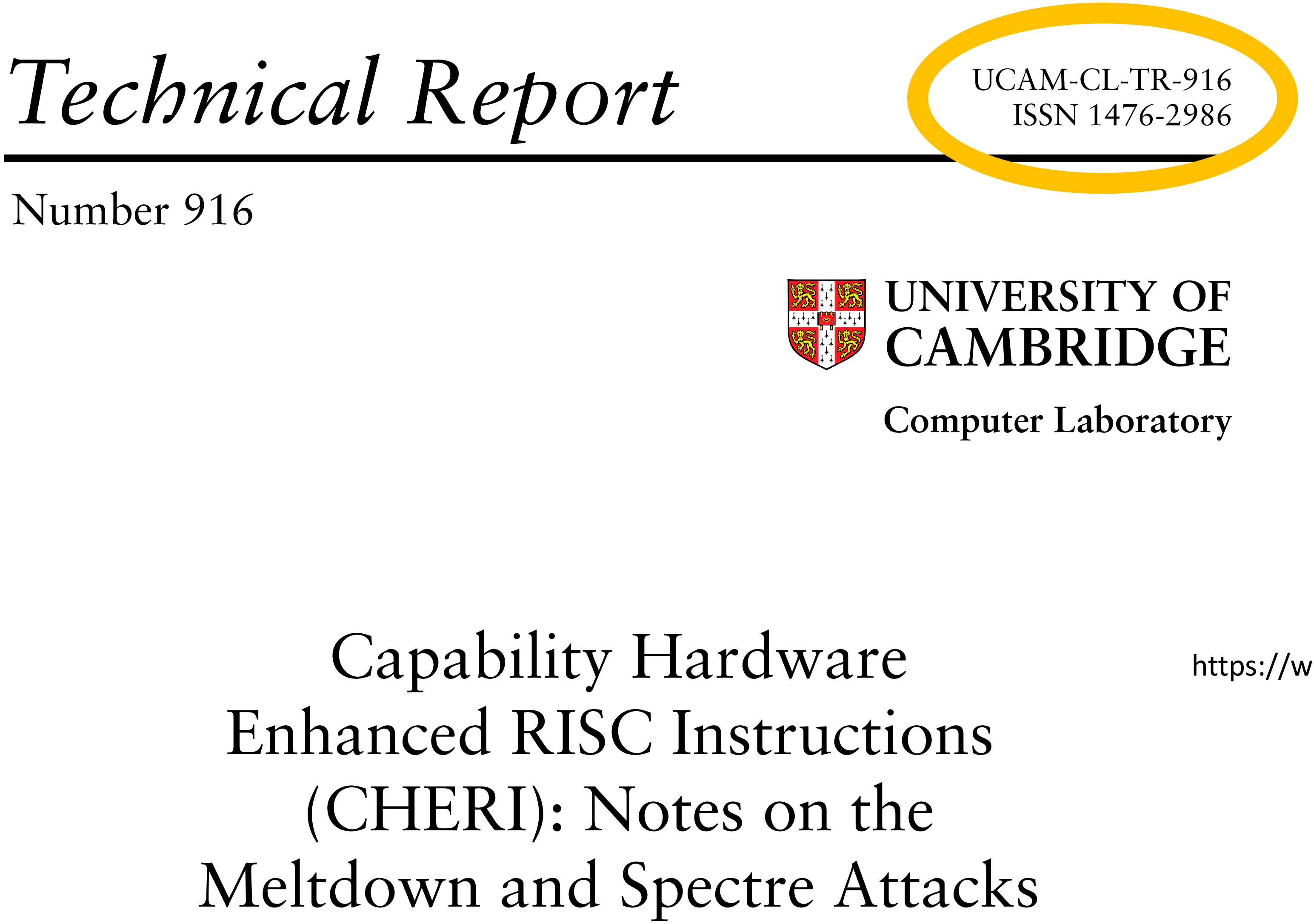
MELTDOWN

FORESHADOW

TLBLEED

All speculatively execute code that that leek secret information via a side-channel

Computer architecture definitely can help



Technical Report

UCAM-CL-TR-916
ISSN 1476-2986

Number 916

UNIVERSITY OF
CAMBRIDGE

Computer Laboratory

Capability Hardware
Enhanced RISC Instructions
(CHERI): Notes on the
Meltdown and Spectre Attacks

URL for technical report:

https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-916.pdf

Approach

project web page

- Ensure that the processor has more semantic knowledge of the code executed
  - Builds on ideas from CHERI: safe pointers and low-cost compartmentalisation
- Method:
  - Develop "RISCy" core illustrating speculative execution attacks
  - Measure vulnerabilities
  - Verify key security mitigations

open source processor, verification engine and other results

- Example mitigations for more secure "RISCy" processor design:
  - No speculative memory access causes a cache miss if its address is illegal in the current context
  - Branch predictions must only be based on state derived from that instruction
  - Dereference of speculated capability pointers is not allowed