Citadel

Side-Channel-Resistant Enclaves with Secure Shared Memory on a Speculative Out-of-Order Processor.

Jules Drean    Miguel Gomez-Garcia    Thomas Bourgeat    Srini Devadas
Everyone loves enclaves!!

Idea:
Hardened Process with Strong Isolation and Integrity Properties

Set Up:
Remote User

Existing Platforms:
Intel SGX & TDX
Arm TrustZone & CCA
AMD SEV
Komodo
Hector-V
CURE
Keystone
OpenTEE
...
But they are broken...

- Hardware vendors are not addressing the problem
- Most academic proposals are limited to software changes

*Side channels are often considered out of the threat model...*
Let's fix it!

Citadel

- Hardware / Software co-design for usable enclave
- Secure against transient execution attacks
- Practical mechanism for secure shared memory
- End-to-end hardware and software implementation
- Fully open source
Overview

Hardware
RISC-V out-of-order multicore processor running on FPGA
Uses MI6 hardware mechanism for strong microarchitectural isolation

Software
- Secure Bootloader
- Security Monitor
- Linux Kernel Module
Enclaves from Linux processes
End-to-end Attestation protocol
15K TCB

Secure Shared Memory
Simple problem with many pitfalls
Speculation on shared memory enables transient execution attacks
Blocking speculation through uncacheable memory is insecure

End-to-End applications:
- Secure crypto library
- MicroPython runtime

---

[0] RiskyOO: Composable building blocks to open up processor design. Zhang S, Wright A, Bourgeat T, Arvind A. In MICRO 2018. IEEE.
Citadel

- Hardware / Software co-design for usable enclave
- Secure against transient execution attacks
- Practical mechanism for secure shared memory
- End-to-end hardware and software implementation
- Fully open source