CISPA
HELMHOLTZ CENTER FOR INFORMATION SECURITY

Hammulator

Simulate Now – Exploit Later

Fabian Thomas, Lukas Gerlach and Michael Schwarz

DRAMSec 2023 | June 15, 2023

Why simulate Rowhammer?

- Templating memory for Rowhammer exploits can take hours
- Exploits often unstable
- No possibility to test mitigations against attacks

Solution: Simulating Rowhammer deterministically for rapid prototyping

Problem: No open-source Rowhammer simulator yet

1 Hammulator: Simulate Now – Exploit Later

Authors

Fabian Thomas
PhD Student
fth0mas
fabianthomas.de

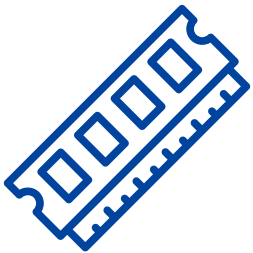
Lukas Gerlach
PhD Student
____salmon____

Michael Schwarz
Faculty
misc0110
misc0110.net

Background: gem5

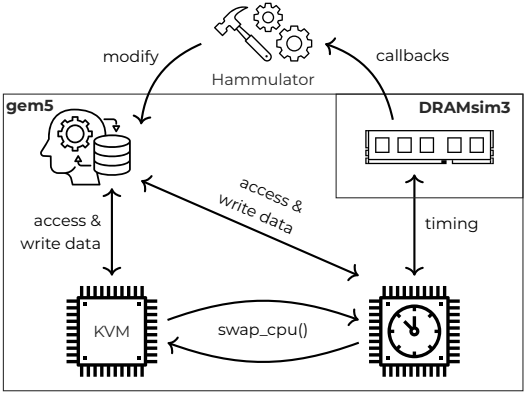
- Modular open-source system and processor simulator
- Supports both syscall emulation and full-system emulation
- **Advanced features:** checkpointing and CPU swapping

Background: DRAMsim3



- Cycle-accurate DRAM simulator
- Easily modifable
- Can be attached to gem5 for timing

Hammulator Architecture



- gem5 does system simulation
- DRAMsim3 for DRAM timing
- Hammulator receives callbacks from gem5/DRAMsim3 and modifies the host memory
- KVM for fast simulation (CPU swapping)

Simulated Effects

- (Mostly) deterministic
- Bit flips start to occur at DRAM-specific hammer count threshold
- Log of hammer count scales linearly with log of number of bit flips
- Up to 5 bit flips in a quadword
- Hammering from non-neighbor rows (distance >1)

Attacks

- Both full-system and syscall emulation possible
- Templating memory can take hours
- Google Project Zero privilege escalation exploit on PT, no templating needed, 1–2 min (200 MB memory, full-system emulation)
- RSA encryption corruption POC (~2 min, syscall emulation)

Attack Showcase

Defenses

- PARA (Probabilistic Adjacent Row Activation), effective in Hammulator with configuration proposed by Kim et al.
- Panopticon-like countermeasure that refreshes neighbors of aggressor rows based on threshold

Limitations & Future Work

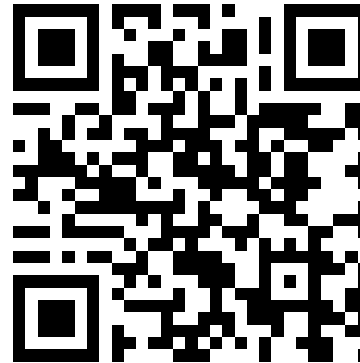
- Data-dependence & effects discovered in Half-Double not simulated
- Achievable with extensions and fine-tuned configurations
- Further studies of mitigations in Hammulator

Thank you!

CISPA
HELMHOLTZ CENTER FOR INFORMATION SECURITY

Hammulator

Simulate Now – Exploit Later



https://github.com/cispa/hammulator

Fabian Thomas, Lukas Gerlach and Michael Schwarz

DRAMSec 2023 | June 15, 2023