Simulating cold boot attacks in the gem5 simulator
Loïc France

To cite this version:
Loïc France. Simulating cold boot attacks in the gem5 simulator. CryptArchi 2023 - 19th International Workshops on Cryptographic architectures embedded in logic devices, Jun 2023, Cantabria, Spain. lirmm-04209526

HAL Id: lirmm-04209526
https://hal-lirmm.ccsd.cnrs.fr/lirmm-04209526
Submitted on 18 Sep 2023

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L’archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d’enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.
Simulating cold boot attacks in the gem5 simulator

Loïc FRANCE
Supervised by Pascal BENOIT & Florent BRUGUIER
The ARCHISEC project

Goal:
Simulate microarchitecture to find weaknesses and develop appropriate protections.

ARCHI-SEC
micro-ARCHitectural SECurity
gem5: Architecture simulator

- CPU type
- Number of cores
- Cache levels and sizes
- Main memory size
- Other modules
- ...

System

CPU

Cache Memories

Main memory

- Graph with bar charts and data
Use simulators to create protections

Simulator

Protection

ATTACK

Bar chart
Previous work: Rowhammer

Integration of memory corruption from **Rowhammer** attacks (corruption of the memory induced by memory accesses)
DRAM data persistence

- Charged capacitor: 1
- Empty capacitor: 0
- Charge time: 64ms
Cold-Boot attack

Principle: recover persistent information from the memory after turning off the victim system
Cold-Boot attack

Principle: recover persistent information from the memory after turning off.
Cold-Boot protections

• Detect temperature changes and wipe memory
  ➢ Not always possible

• Store sensitive data outside RAM
  ➢ Usually only for encryption keys, not for all sensitive data

• Gluing the memory on the motherboard
  ➢ Limits the system, does not prevent booting aggressor OS on victim device

• Full-memory encryption
  ➢ Performance issues, need modifications on the OS and/or the hardware

• Memory Scrambling
  ➢ Only makes extracting data slower
Cold-Boot protections

• Detect temperature changes and wipe memory

• Store sensitive data outside RAM

• Gluing the memory on the motherboard
  J. A. Halderman et al., "Lest we remember: cold-boot attacks on encryption keys," ACM SS 2008

• Full-memory encryption

• Memory Scrambling
  S.F. Yitbarek et al., “Cold Boot Attacks are Still Hot: Security Analysis of Memory Scramblers in Modern Processors,” HPCA 2017
Cold-Boot attacks on NV RAM

Non-volatile → does not need cooling, data persist for a very long time after shut down

⇒ make attacks easier to execute
Cold-Boot simulation

Simulator
Victim system

secret

checkpoint
Demo

```c
int main() {
    char buffer[] = "secret: cryptarchi2023";
    // ...
    return 0;
}
```

```c
int main() {
    int index = find(RAM2, "secret", RAM2_SIZE);
    if (index >= 0) {
        printf("found @ 0x%x\n", index);
        dump(&RAM2[index-64]), 128);
    } else {
        puts("not found\n");
        return 0;
    }
}
```

```
> gem5.opt [...] --kernel=victim.elf --checkpoint-at-end

```
Developing countermeasures
Thank you! Questions?

Loïc France
[loic.france@lirmm.fr]
References


Loïc France
[loic.france@lirmm.fr]