

Master Thesis

Hammering Attacks on FPGA-Based Systems

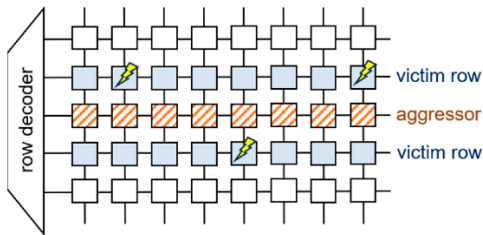


Fig1. Illustrative example of bit flips

```
hammer:
mov (X), %eax // read from address X
mov (Y), %ebx // read from address Y
cflush (X) // flush cache for address X
cflush (Y) // flush cache for address Y
mfence
jmp hammer
```

Fig2. x86 Assembly code for rowhammer attack

Img source: Kim, D.; Park, H.; Yeo, I.; Lee, Y.K.; Kim, Y.; Lee, H.-M.; Kwon, K.-W. Rowhammer Attacks in Dynamic Random-Access Memory and Defense Methods. *Sensors* 2024

Modern FPGA-based systems are increasingly used in security-critical applications, from automotive to cloud acceleration. As these platforms evolve into high-performance, reconfigurable environments, their integration with system memory becomes a critical security vulnerability. **Rowhammer attacks**, where rapid memory access patterns induce bit flips in adjacent rows, represent a significant threat to system integrity. While traditionally studied in the context of CPUs, FPGA-based systems offer unique, low-level control over memory timings and bus cycles that can be exploited for more sophisticated hammering techniques.

This thesis focuses on: implementing hammering-style attacks initiated directly from the FPGA fabric. Unlike standard software-based exploits, the FPGA can bypass typical cache hierarchies and access the memory controller with unusual frequency. The research will investigate how the high degree of parallelism and precise timing control available in FPGAs can be used to bypass

existing protection mechanisms. By gaining direct access to the physical memory interface, the goal is to demonstrate the limits of current hardware defences against specialized, hardware-driven memory corruption.

Tasks of the student

Tasks will vary according to the thesis topic and scope. Tasks of the student might include but are not limited to:

- Selecting a target FPGA platform and configuring the interface between the programmable logic and the memory
- Designing and implementing custom RTL modules to maximize memory row activation rates
- Conducting systematic experiments to identify vulnerable memory addresses and analyzing the collected data

Skills required/beneficial for the thesis

- Experience with VHDL/Verilog and FPGA design suites
- Programming skills (C++, Python)
- A strong interest in hardware security

Skills acquired within the thesis

- Hands-on experience in hardware design
- Expertise in low-level memory architectures
- Work in a research environment

Language

- The collaboration with the colleagues can be in English.

Contact

- Zeynep Demirdag, zeynep.demirdag@kit.edu
- Dr. Hassan Nassar, hassan.nassar@kit.edu