ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

System Security Group
Prof. Dr. Srdjan Čapkun

Thesis Project Description

Exploiting MLC NAND Flash Chip Error Characteristics

Introduction

Multi-Level-Cell (MLC) NAND Flash Memories allow to achieve higher bit density for the same chip area compared to Single-Level-Cell (SLC) and are therefore commonly used nowadays in most commercially available SSDs. However, compared to SLC memories, they are highly susceptible to write and read interference [1], which can impact their reliability. To function correctly under these technological limitations, MLC SSDs use data scrambling to reduce the interference effects and Error Correction Codes (ECC) to correct the remaining bit errors. Despite these mitigations, as shown in [1], theoretically there exist enough interference to be still able to produce arbitrary bit flips.

Project Description

While errors are known to be present on MLC NAND Flash chips, it has not been studied yet whether any bit flip can be caused by an unprivileged attacker that has only read and write permissions to an MLC SSD. To understand the error characteristics of these devices, in this thesis, we will first try to bypass all the protection mechanisms that reduce and mask the error behaviors at the chip level: ECC and scrambling. ECC is generally performed by the SSD controller, and in order to bypass it, we will observe the error behavior of chips directly, that is by issuing commands directly to them through a special infrastructure that can read raw NAND flash chips.

Depending on the chip model, scrambling is sometimes implemented on-chip and transparently from the commands issued to it, hence bypassing the SSD controller will not also disable the scrambling. Therefore, to fully characterize the errors of the chips under study, the scrambling will be reversed by issuing commands out of specification with a custom infrastructure. The project is composed of three main tasks: 1) reverse engineering the on-chip scrambling mechanism, 2) understanding whether and how an unprivileged user can construct bit patterns that exploit various scramblers, and 3) studying the errors statistics under different levels of interference conditions.

Tasks

- Familiarize with the SSD hardware and NAND flash chip architecture
- Study error behavior under normal utilization conditions
- Reverse engineer the scrambling
- Study error behavior under maximum interference conditions
- Project report
- Final presentation

Supervisors

Ivan Puddu CNB F 103.1 ivan.puddu@inf.ethz.ch

References

[1] Yu Cai, Saugata Ghose, Yixin Luo, Ken Mai, Onur Mutlu, and Erich F Haratsch. Vulnerabilities in mlc nand flash memory programming: experimental analysis, exploits, and mitigation techniques. In *2017 IEEE International Symposium on High-Performance Computer Architecture (HPCA)*, pages 49–60. IEEE, 2017.