Software-based Microarchitectural Fault Attack

Jan Kalbantner

Technical Report

RHUL–ISG–2020–4

22 June 2020

Information Security Group
Royal Holloway University of London
Egham, Surrey, TW20 0EX
United Kingdom

Executive Summary

In 1972, James Anderson published a report about technological requirements of computers at the US Airforce. In this report, he presented the following three core principles of information security [7]:

1. Unauthorised information release,
2. Unauthorised information modification,
3. Unauthorised denial of access.

Those three thwart the information security principles of (1) confidentiality, (2) integrity and (3) availability, which every computer system need to ensure at all times. In 2014, researchers from Carnegie Mellon University and Intel Labs [75] found that due to the increased density within DRAM technology, it gets challenging to prevent cell charges from interacting with adjacent cells. Kim et al. [75] found that through rapidly accessing the same row in DRAM, they can corrupt data in adjacent rows and can cause bits to flip artificially. 'Flipping Bits in Memory Without Accessing Them: An Experimental Study of DRAM Disturbance Errors' became the base for future research on the after that named vulnerability '*Rowhammer*'. Afterwards, other researchers found ways to use this vulnerability, amongst other things, to exploit memory management techniques in different environments [112, 132, 133, 138], inject errors in cryptographic protocols [23] and perform privilege escalation attacks [56, 57, 75, 112, 132, 138].

In this dissertation, we provide an overview of recent Rowhammer attacks [26, 41, 57, 75, 83, 88, 112, 116, 132, 133, 138] and countermeasures [20, 28, 49, 71, 133, 136] against these attacks. We structure the Rowhammer attacks into four procedures: (1) preparation, (2) hammering, (3) verification and (4) exploitation. Further, we implement the Phys Feng Shui exploitation technique [132, 133] and evaluate it with an LG Nexus 5 mobile device to show the availability of the analysed Rowhammer attacks.

Dividing Rowhammer attacks into these four categories allowed us a better overview of them when we presented the countermeasures. We looked at eighteen defence mechanisms usable against Rowhammer attacks. Some mechanisms seem to be very potent against single adversarial methods, but the least of the analysed countermeasures can be used for more than one Rowhammer attack. In our analysis, we focused on DMA-based attacks and showed that none of the recent techniques is reliable, practical, secure and usable at the same time. Of the analysed countermeasures only GuardION [133] and a modified version of ANVIL [20] were seen as secure. However, GuardION is only usable against Rowhammer attacks utilising direct memory accesses, and further is, according to Google [134], not a practical concern and was therefore not implemented by them yet. Our implementation of a DMA-based attack on an LG Nexus 5 Android device showed that it is a practical concern. In average, we found exploitable unique bit flips after 473 seconds and it showed that the Phys Feng Shui technique is still a real threat against mobile devices.