Practical evaluation of RowHammer on an Embedded System (AISEC)

RowHammer is a powerful fault injection technique, launched from software, to inject bitfaults into DRAM. Over the last decade, RowHammer was shown to threaten DRAMs. Vendors reacted and deployed countermeasures, which lead to the believe that the problem was solved. However, in the last years, research showed that RowHammer is still threatened by a more sophisticated technique, called Many-sided RowHammer.

In this work, we aim to create bitfaults inside the LPDDR4 of an embedded system by using the Many-Sided RowHammer technique. Therefore, we will port an existing RowHammer tool to our target embedded architecture. We will then evaluate, whether successful Many-sided RowHammer attack is possible on our targetted embedded platform, and which are the necessary parameters. Finally, we want evaluate how an attacker may use the particular achieved fault model.

Prerequisites

The following skills are valuable for the execution of the project:
* Good knowledge of programming in C
* Basic experience with assembly programming
* Basic experience with embedded Linux (e.g., Buildroot, Yocto, Raspbian, etc.)
* Basic knowledge about memory hierarchies and DRAM structure

Contact

If you are interested in this particular HiWi position, please send an email with
* a short CV,
* a short cover letter, and
* your last grading sheet.

Kilian Zinnecker, kilian.zinnecker@aisec.fraunhofer.de

Advisors

Georg Sigl
Kilian Zinnecker (Fraunhofer AISEC)