2023 Design, Automation & Test in Europe Conference (DATE 2023)

Warm-Boot Attack on Modern DRAMs

1st Yichen Jiang
Electrical and Computer Engineering
University of Florida
Gainesville, FL, USA
yichen.jiang@ufl.edu

2nd Shuo Wang
Electrical and Computer Engineering
University of Florida
Gainesville, FL, USA
shuo.wang@ece.ufl.edu

3rd Renato Figueiredo
Electrical and Computer Engineering
University of Florida
Gainesville, FL, USA
renato@ece.ufl.edu

4th Yier Jin
Electrical and Computer Engineering
University of Florida
Gainesville, FL, USA
yier.jin@ece.ufl.edu

***Abstract*—Memory plays a critical role in storing almost all computation data for various applications, including those with sensitive data such as bank transactions and critical business management. As a result, protecting memory security from attackers with physical access is ultimately important. Various memory attacks have been proposed, among which "cold boot" and RowHammer are two leading examples. DRAM manufacturers have deployed a series of protection mechanisms to counter these attacks. Even with the latest protection techniques, DRAM may still be vulnerable to attackers with physical access. In this paper, we proposed a novel "warm boot" attack which utilizes external power supplies to bypass the existing protection mechanisms and steal the data from the modern SODIMM DDR4 memory. The proposed "warm boot" attack is applied to various DRAM chips from different brands. Based on our experiments, the "warm boot" attack can achieve as high as 94% data recovery rate from SODIMM DDR4 memory.**

I. Introduction

DRAM stores critical information from the operating system, e.g. file system data structures, as well as user-sensitive data. Directly accessing the data from the DRAM creates security threats to data safety. However, an implicit underlying assumption has been that, since DRAM memory is volatile, non-encrypted data stored there is lost upon power-off; thus, data privacy techniques have focused on securing data in persistent storage. While recent work proves that there is a short window of time where DRAM memory still holds data even as power is removed, which can be potentially exploited by a malicious user with physical access to DRAM [1], [2].

As a result, physical access to the DRAM still imposes potential threats against the data security stores inside the DRAM. To demonstrate that more protection methods are needed for DRAM data security, in the paper, we propose a new DRAM attack, named warm boot attack. The warm boot attack is a physical memory disclosure attack on removable SODIMM DDR4 DRAM. The warm boot attack utilizes an external power supply to extend the data retention time when the DRAM device is disconnected from the DIMM slot. In our experiments, we have demonstrated the feasibility of this attack in hardware platforms and shown the ability to steal secrets from a victim device. As demonstrated in our experimentation, the proposed method can achieve up to 94% data recovery We then expanded our experiments to various DRAMs from different vendors, demonstrating that the warm-boot attack applies to almost all SODIMM DDR4 memory.

The overall contributions of this paper are as follows:

- A new warm-boot attack mechanism and procedure are proposed, which utilize an external power supply to implement a memory disclosure attack on modern DRAMs.
- Detailed experiments are performed on DRAMs from different vendors to validate that the proposed warm-boot attack can be successfully applied to almost all modern DRAMs.

The rest of the paper is organized as follows. Section II briefly reviews the famous cold boot attack. Section III presents the proposed novel warm-boot attack. Experimental setup and results on a prototype are presented and summarized in Section IV. Finally, Section V concludes the paper.

II. Background

A. Cold Boot Attack

Halderman et al. [3] proposed cold-boot attacks to steal data stored inside modern DRAMs. The code-boot attack is based on the fact that the voltages on the capacitors inside DRAM can remain for a short time at low temperatures after the power is off. As long as the voltage remains, the data can be correctly stored inside the DRAM. The cold-boot attack uses liquid nitrogen to cool down the DRAM, which allows the DRAM to keep data for a short period despite the disconnection from a power supply. Sensitive data can then be retrieved from an external USB device once the system is rebooted.

III. Warm Boot Attack

A. Proposed Attack Procedure

In this paper, we studied the possibility of using an external power supply attached to the DRAM sticks when removing them from a platform to prevent data loss so the data can be retrieved later. Based on this, we have developed a technique to implement and evaluate the proposed approach. We use two platforms: the victim platform (holding secret data), and the

978-3-9819263-7-8/DATE23/© 2023 EDAA

Table I: Data remaining rate of warm boot attack

Brand	Vdd&Vss	Vdd&Vss&Vtt	All connected
Micron-1	*11%*	*24%*	*24%*
Micron-2	*11%*	*24%*	*24%*
ATECH	*54%*	*72%*	*72%*
Samsung	*1%*	*12%*	*12%*
Hynix	*38%*	*59%*	*59%*
TimeTec	*62%*	*76%*	*76%*

attack platform (from which the secret data is to be stolen). And the proposed procedure is listed as follows:

- Power on the victim platform and write data to DRAM.
- Connect the DRAM to an external power supply and turn on the power supply before removing the DRAM from the slot on the victim platform.
- Plug the DRAM into the attack platform and read the secret data.

IV. Preliminary Experiment

A. Proof of Concept

In this section, we exploit the data recovery rate of the warm boot attack. We have found that V_{DD}, V_{SS}, V_{TT}, and V_{PP} pins are important to implement a warm boot attack based on our previous analysis. Thus, we select these pins as candidate pins and exploit these pins to get the best data remaining rate. During the experiments, we also found that all V_{DD} pins are connected togetherinside the DRAM, so do all the V_{SS} pins, hence we only connect single V_{DD} and V_{SS} pins to the external power supply.

In the experiments, we tested DRAMs at room temperature ($25°C$). The attack steps follow the description in Section III. We repeated the above processes with the external power supply connected to different candidate pins. In Table I, we listed all tested results. All tested DRAM brands are in the first column and the "-x" (x is 0,1,2...) labels the same model DRAM but different chips. The rest columns are the data remaining rates when different pins listed in the first row were connected to the extenral power supply. As the results show, the best data remaining rate for warm boot attack is nearly 76% against the Timetec DDR4. Also, we noticed that all DRAMs achieve the best data remaining performance when connecting the V_{TT} pin to the power supply.

B. Exploitation of Remaining Data Pattern

During our experiments, we observed that certain DRAMs exhibit a consistent remaining data pattern after an attack. To exploit the remaining pattern, we selected Micron-1 DDR4 as the testing chip and in Figure 1, we demonstrated a snippet of remaining data (in both hexadecimal and binary format) from Micron-1 DDR4. Each line represents the remaining data recovered from a 4KB space and the addresses of each line are continuous. Next, we select the most repeated value in each column (the column is separated by a comma in the figure) as the remaining data pattern. Following this approach, the remaining data pattern could be efficiently generated. We

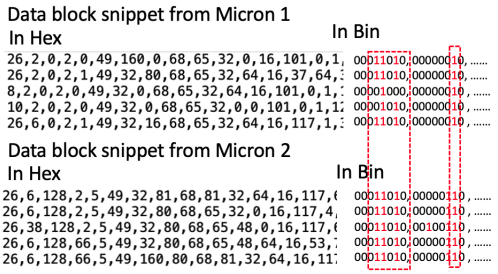

Figure 1: Remaining data generated from two different chips

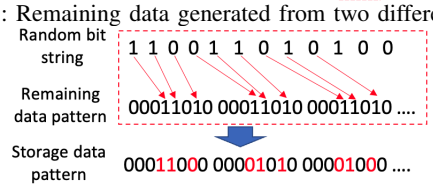

Figure 2: Exploitation of remaining data pattern

repeated the testing steps above for another Micron DDR4 chip, and the results are shown in figure 1. As shown in the figure 1, Micron-2 also has similar remaining data patterns to Micron-1.

Next, we focused on how to utilize the remaining data pattern. In Figure 2, we demonstrated our exploitation technique. We randomly generated a bit string and then we transformed it into a new storage data pattern according to the remaining data pattern. In this step, we assigned the value in a random bit string only to the position where it remains "1" in the remaining data pattern. After the new storage data pattern was generated, we wrote this storage data pattern to the testing DRAM and implemented our warm boot attack on this memory chip. Finally, we read the data back and checked if the original bit string could be recovered from the storage data pattern. As shown by the results, we achieved a significant improvement of the remaining rate up to 94% for Micron DDR4 and 87% for Samsung DDR4.

V. Conclusion

DRAM is an essential component of most modern devices. Physical access to the DRAM poses a high risk to data security which stores inside the DRAM. In our paper, we proposed a new technique that utilizes the external power supply to extend the data remaining time, so the attacker can steal the sensitive data stored inside DRAM. In our experiments, we achieved 76% data remaining rate from the DRAM without any hard technique implemented. Furthermore, we achieved a 94% data recovery rate when we utilized the remaining data pattern. Our proposed attack mechanism was therefore proven practical.

References

[1] J. Liu, B. Jaiyen, Y. Kim, C. Wilkerson, and O. Mutlu, "An experimental study of data retention behavior in modern dram devices: Implications for retention time profiling mechanisms," *ACM SIGARCH Computer Architecture News*, vol. 41, no. 3, pp. 60–71, 2013.

[2] O. Mutlu and J. S. Kim, "Rowhammer: A retrospective," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 39, no. 8, pp. 1555–1571, 2019.

[3] J. A. Halderman, S. D. Schoen, N. Heninger, W. Clarkson, W. Paul, J. A. Calandrino, A. J. Feldman, J. Appelbaum, and E. W. Felten, "Lest we remember: cold-boot attacks on encryption keys," *Communications of the ACM*, vol. 52, no. 5, pp. 91–98, 2009.