CENG311 - Video Assignment 2

Ahmet Kurt 290201034

January 5, 2025

1. What is RowHammer, and how does it exploit modern DRAM technology?

RowHammer is a serious defect in modern DRAM design that occurs when a particular memory row, known as the ”aggressor row,” is repeatedly accessed. This results in unintentional changes to the values of neighboring rows, known as ”victim rows.” This problem occurs because neighboring cells are disrupted by electrical disturbances caused by the forceful activation. The physical isolation between cells in DRAM chips deteriorates with increasing density and size, making them increasingly vulnerable to these disruptions. RowHammer draws attention to the difficulties in preserving dependability as technology advances.

Key technical aspects that make this vulnerability possible:

1. **High-frequency access patterns:** Aggressively reading or writing to one row can disturb adjacent rows.
2. **Inadequate design isolation:** There are not enough safeguards against cross-row interference in modern DRAM chips.
3. **Dense cell packing:** Interference is increased when memory cells are packed closer together.
4. **Scaling issues:** Charge instability and leakage are more likely to occur in smaller DRAM cells.

2. What are the implications and mitigation strategies for RowHammer?

Real-world risks posed by RowHammer:

System security and data integrity may be jeopardized by the vulnerability. An attacker could purposefully flip memory bits, for instance, to obtain unauthorized access to privileged areas or tamper with important data. These attacks jeopardize system dependability, compromise memory architectural isolation, and have the ability to leak private data, including encryption keys.

Mitigation techniques:

1. **Improved hardware design:** This is a long-term solution. DRAM design can be revised.
2. **Error correction codes (ECC):** Provides limited protection against errors, but is costly.
3. **Frequent memory refreshing:** Frequent refreshing can be a good solution, but it increases energy usage and cost.
4. **Physical Isolation:** Shortens the window for disturbances but increases energy usage and performance costs.
5. **Row relocation:** Moving the row to a new secure area to prevent access to vulnerable areas.
6. **Access control:** Solutions like BlockHammer prevent excessive intervention. They do this by limiting the rate of repeated activations.

3. Challenging parts of the talk:

One of the hardest parts for me was understanding how to balance security and performance in real systems. I didn't have enough technical knowledge to understand this very well.

A question for the speaker:

1. RowHammer seems pretty technical. Do you have any suggestions for a better understanding of this topic? What roadmap did you take to better understand this topic?
   Why? I want to know how to approach this topic as a beginner and build a solid understanding.
2. With the popularity of AI chips, what are some of the risks for RowHammer vulnerabilities in this type of hardware? How can AI chip designs be made more protective to these types of attacks?
   Why? I am curious about the risks and security measures in artificial intelligence systems.