Rajat Sethi

CPSC 8580

**Paper Summary 11 - Leveraging EM Side-Channel Information to Detect Rowhammer Attacks**

In computer engineering, data is often managed in the computer’s dynamic random-access memory (DRAM) for efficient access. This data is stored in the form of bits, 0s and 1s represented by a cell’s voltage level. A collection of those cells is called a bank, stored as a 2D array with rows and columns. Using that knowledge, the research team discusses rowhammer attacks, the act of using adjacent rows to flip bits in some arbitrary row at the hardware level. This paper’s contribution is finding a defense against this particular attack by developing a new way to detect this attack’s existence in a system.

The key novelty of this paper is the use of EM-emanations to determine rowhammer attacks. In any computation, the DRAM will emit a number of energy sources, like heat. In addition, they also emit some electromagnetic (EM) waves when the electric charge changes. Using these EM frequencies, the computer can look for irregularities in the cell’s charge and act accordingly. Rowhammer attacks often require intense and precise electrical surges through a multi-stage process. If the computer can notice the pattern of these phases, then it can stop the rowhammer attack.

The main weakness of this paper is how precise everything has to be. A rowhammer attack may occur in different manners between different architectures. This includes DRAM type (DDR3 vs. DDR4) or device type (Desktop vs. Mobile) or manufacturer (Dell vs. Lenovo). In other words, this type of defense will have to be configured on a case-by-case basis, rather than a standard “cure-all” like in regular software attacks.

In future works, the team will have to look at many more hardware models to have a complete defense. It is great that the team was able to lay the groundwork for these endeavors, so I hope that other researchers will check the effects and preventions of rowhammer attacks in other devices.