The Linley Group

MICROPROCESSOR report

Insightful Analysis of Processor Technology

UPMEM NAILS ROWHAMMER

French Company Offers Defense Against DRAM Vulnerability

By Tom R. Halfhill (June 21, 2021)

Although human memory is notoriously faulty, computer memory requires perfection. We hardly notice a few wayward synapses, but a single-bit error in DRAM can crash a program or even a whole computer. Error-correction codes (ECC) protect servers and other mission-critical systems from random "soft errors" that flip a DRAM bit cell from one to zero or vice versa, but larger errors remain a problem. In recent years, a deliberate attack called RowHammer is playing havoc with DRAM chips and the computers that rely on them.

First documented in 2014, RowHammer deliberately flips bits by rapidly and repeatedly accessing specific DRAM rows. Although it's unable to control the flips to write malicious code into memory, it can overwhelm ECC protection, crashing the affected program or forcing the entire system to reboot. In its simplest form, RowHammer mounts a denial-of-service (DoS) attack. In more-sophisticated assaults, it can trigger a fault that gives the attacker elevated system privileges or access to another user's virtual partition on a shared server. In other words, it's potentially catastrophic.

Various countermeasures have been only somewhat effective or costly in lost performance and power. Now, a French startup, Grenoble-based Upmem, claims to have a defense that's economical and completely effective. It has patented the technique and is offering it to DRAM manufacturers as licensable intellectual property (IP). The catch is that the solution, called Silver Bullet, requires modification of future DRAM-chip designs. The modifications are minimal but can't be added to existing DRAMs.

Upmem is a small company previously known for introducing new DRAMs that integrate data-processing units for in-memory computing (see *MPR 8/16/19,* "Upmem Embeds Processors in DRAM"). Silver Bullet is a separate project that doesn't require Upmem's special DRAMs (which, in their first-generation designs, implement a different technique less suited to new DRAM technologies). Nor does it require the industry to modify memory controllers, create new DDR protocols, revise operating systems, or adopt nonstandard manufacturing technology. If DRAM makers license Silver Bullet, their new chips could be available in less than a year.

Every Problem Looks Like a Hammer

RowHammer works by activating a row of bit cells at an unnaturally high rate. Each cell has one transistor paired with a capacitor, and DRAM chips arrange these cells in tightly packed rows and columns organized in banks. By

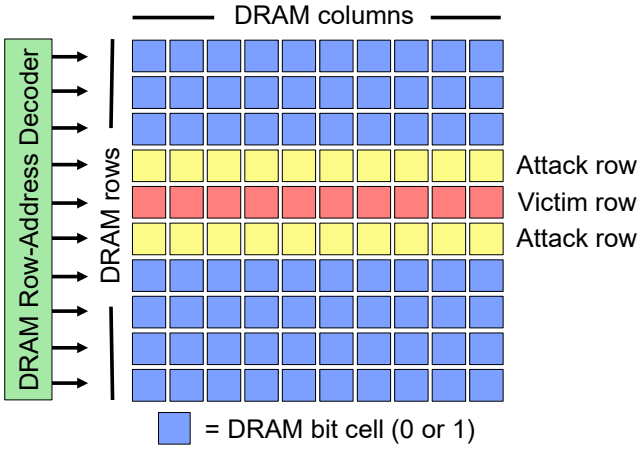

Figure 1. How RowHammer corrupts DRAM. The attack repeatedly activates a specific bit-cell row (yellow) in a DRAM chip, causing electromagnetic effects that randomly flip the bits in a neighboring row (blue). Double-sided attacks hit both sides of the victim row. The strongest attacks have a "blast radius" that corrupts additional rows beyond the victim row.

"hammering" a specific row, the attack induces cross-coupling electromagnetic effects that can randomly flip the bits in a neighboring row. Essentially, RowHammer triggers the same type of soft errors that magnetic fields and cosmic rays can cause accidentally, but it's nonrandom in frequency and location.

Although a malicious program can target a particular row for hammering, it's unable to control exactly how the bits flip in the neighboring row, so the attacker can't write specific data into the DRAM. But by randomly overwriting data at a particular address, the attacker can target a specific program (or even the OS) that uses that address. Thus, RowHammer is limited to DoS aggravation unless it's reinforced by another attack that exploits the vulnerability for different purposes.

Nevertheless, even a crude DoS attack can cripple a data center, cryptocurrency mine, digital-currency exchange, or motor-vehicle owner who refuses to pay the ransom. Rebooting several times a day is no small task. Note that the recent DarkSide ransomware attack on Colonial Pipeline that caused gasoline shortages in the US didn't immobilize the embedded systems controlling the fuel pipelines; instead, it encrypted critical data on the company's business systems, interfering with customer billing.

RowHammer is doubly dangerous because it needn't infect the target computer with sophisticated malware. Although hammering a specific row of DRAM bit cells would seem to require malicious code running close to the metal, experimenters have proved that even high-level interpreted JavaScript running in a web browser can also do the dirty work.

Because each new generation of DRAM manufacturing technology packs the cells more tightly, RowHammer becomes more dangerous with time. The minimum "hammer count"—the smallest number of row activations that can flip the bits in a neighboring row—keeps falling. As Figure 1 shows, attackers can also reduce the hammer count by activating both rows alongside the victim row.

Some attacks are intense enough to corrupt additional rows beyond the victim row, an expansion called the *blast radius*. In some of the latest DRAM chips, engineers have observed a two-row radius. Although the bit errors gradually taper off in rows further from the victim row, the blast radius may expand as each new DRAM generation crowds the rows of smaller transistors more closely.

A Refreshing Solution

Despite years of effort, DRAMs remain vulnerable. Typical countermeasures are merely mitigations that reduce the risk or the negative effects. Usually, they strengthen data integrity by increasing the DRAM refresh rate and by adding attack-mitigation logic to the DRAM, but clever attacks can dodge these defenses.

Dynamic RAM must frequently recharge the capacitor in each cell to preserve its binary value, so refreshing them more often maintains a stronger charge that resists corruption. Among the drawbacks are higher power consumption and sometimes lower performance if the extra refresh cycles interfere with data operations.

JEDEC, the industry-standards body for solid-state memory, has a standing committee and a Google-chaired forum of major companies working on the problem. The committee recently published two RowHammer papers (see the "For More Information" box). One JEDEC countermeasure is Refresh Management (RFM), which was added to the DDR5, LPDDR4/4X, LPDDR5, HBM3, and GDDR6 protocols. RFM can raise the refresh rate but can't identify the specific bit-cell rows that are under attack and therefore need refreshing. JEDEC's recommended countermeasures for DRAM protocols lacking RFM are even less effective. Generally, any changes to memory protocols have wider implications than modifying DRAMs, because they affect memory controllers, processors, and system software.

Silver Bullet works with or without RFM and employs faster refreshing, too. The difference is it counters RowHammer's targeted attacks by mounting a narrow defense. Instead of raising the refresh rate for the whole chip or a large region, it focuses on the subbank containing the victim row. Simply put, the added logic monitors row activations throughout the chip and springs into action only when it detects a suspicious number characteristic of hammering. Then it boosts the refresh rate for that subbank to a level that foils the attack. This approach minimizes power and performance penalties. The power savings vary greatly but could be 50% or more relative to the less effective alternatives.

Configurable design parameters can adapt Silver Bullet for different subbank sizes, hammer-count thresholds, and refresh rates. These parameters also prepare Silver Bullet for future DRAMs built in denser technologies. Because it resides in the DRAM chip, it requires neither firmware nor OS revisions, and it's invisible to software. Consequently, however, it can't identify the program causing the attack or even warn that an attack is happening. System administrators must find and remove the malware using other means. In addition, some legitimate programs have been known to inadvertently mimic RowHammer behavior.

DRAM Must Change

Silver Bullet's downside is that it requires new DRAMs. But the changes are on the design side, not in manufacturing, so it's compatible with existing and future DRAM processes. The only changes are a small amount of logic that counts the row activations, stores this data in a table, and boosts the refresh rate for the victim subbank when the hammer count exceeds a configurable threshold.

DRAM chips already have flexible refreshing and the ability to refresh particular banks or subbanks to repair soft errors. What they lack is the ability to detect a relentless RowHammer attack and to concentrate a higher refresh rate on a subbank verging on multibit errors. According to

Upmem, Silver Bullet can resist attacks that expand the blast radius to six or more rows—far wider than any attack yet observed.

In theory, Silver Bullet's hammer-count table can reside in either the DRAMs or the memory controller, but the latter alternative is more difficult, as current controllers lack visibility into the DRAM's physical topology. Although a controller-based-table would be compatible with existing DDR protocols, it requires a standard row mapping, which in turn requires DRAM makers to agree on a limited number of topologies. These modifications would enable Silver Bullet to convert a logical DDR row index into a physical index. Convincing DRAM makers to add the hammer-count logic should be easier than convincing them to adopt new topologies and mapping schemes.

Upmem's US patent on Silver Bullet (10,885,966-B1) describes the table's structure and operation but not its physical implementation. Currently, the company is asking DRAM makers to store the table in a new SRAM block instead of in DRAM. Again, the latter alternative is technically feasible but has problems; namely, a DRAM table could itself be vulnerable to a RowHammer attack. For now, Upmem prefers SRAM that's completely invisible to software—and, unlike dynamic RAM, needs no refreshing.

Table Size Is Configurable

The table size varies with the number of rows per subbank and the hammer-count threshold that triggers a refresh. Subbanks can range from 2 rows to 4,096; more rows require fewer table entries and thus a smaller table, but the higher refresh rate will spread over a larger region. To date, the lowest hammer count observed to corrupt neighboring cells is 4,800 activations per row in a double-sided attack, for a total of 9,600 activations.

Silver Bullet avoids periodically resetting the hammer counter. In theory, resets might help identify the aggressor program by reducing the time window in which an attack operates and thereby reducing the number of possible aggressors. But periodic resets complicate the counter logic, and identifying aggressors gets more difficult as more rows come under attack. (Multiple rows can be hammered simultaneously.) Also, Upmem says identifying the aggressor would require substantial OS revisions.

Chip designers can configure Silver Bullet's hammer-count threshold to as few as 213 activations, so it adapts to future process technologies whose smaller cells are more susceptible to lower counts. In existing and near-future processes, the 9,600-activation threshold should be sufficient. Upmem says the resulting SRAM table will be 256KB for a 16Gbit DRAM. The control logic is negligible.

Although the table is puny, the physical implementation is somewhat larger than one might expect. A six-transistor SRAM cell fabricated in a logic process is about 20x larger than a DRAM cell fabricated in a similar-size DRAM process. But these SRAMs will be fabricated in DRAM technology, which is much less area efficient for SRAM and logic. To be overly conservative, Upmem estimates the SRAM cells may be upwards of 200x larger than the DRAM cells. Even so, a 16Gbit die grows by only about 0.6%. The company says this cost is much smaller than for other mitigations that are less effective, consume more power, and impair performance.

Upmem won't produce a test chip to prove Silver Bullet's mettle. Doing so is expensive and, claims the company, unnecessary. Instead, Upmem commissioned a 40-page mathematical analysis coauthored with Professor Onur Mutlu and a team from ETH Zurich, one of Europe's top-rated computer-science universities. This document describes Silver Bullet in detail and calculates its effectiveness when configured with various parameters. It's written for engineers with a deep understanding of DRAMs and RowHammer. The paper's conclusion is that Silver Bullet should prove effective when implemented correctly.

Permanent Solution Seems Inevitable

Any solution that requires chipmakers to modify their future designs, no matter how minor the changes, is a major undertaking. In recent years, AMD and Intel have redesigned their x86 processors to resist Spectre attacks on their branch-prediction and speculative-execution logic. RowHammer is a similar low-level hardware attack not easily fixed in software.

Whereas Spectre mainly afflicts two chipmakers, RowHammer mainly afflicts three: Samsung, SK Hynix, and

For More Information

Upmem is offering Silver Bullet to DRAM manufacturers as licensable IP for undisclosed fees and royalties. For more information, access *www.upmem.com/technology*.

The company commissioned a mathematical analysis of its solution: "Silver Bullet Security Analysis," by Abdullah Giray Yağlıkçı, Jeremie S. Kim, Fabrice Devaux, and Onur Mutlu; access *arxiv.org/abs/2106.07084*.

US patent 10,885,966-B1 (January 5, 2021) describes Silver Bullet. Patent application 2021/0012832 (January 14, 2021) describes a RowHammer-resistant DRAM with in-memory processing. Essentially, it combines Silver Bullet with Upmem's previously disclosed special DRAMs (see *MPR 8/16/19,* "Upmem Embeds Processors in DRAM").

In March, the JC-42 committee of the JEDEC Solid-State Technology Association published two RowHammer papers: "Near-Term DRAM Level Rowhammer Mitigation" (*JEP300-1*, March 2021) and "System Level Rowhammer Mitigation" (*JEP301-1*, March 2021). Both are free downloads with JEDEC registration.

Semiconductor Engineering recently published an article describing the difficulty of testing DRAM chips for RowHammer vulnerability; access *semiengineering.com/is-there-a-practical-test-for-rowhammer-vulnerability*.

Micron, which together own about 95% of the DRAM market. It's a small potential-customer base for Upmem. If one of them chooses to license Silver Bullet, however, the others may have to follow or risk losing sales to customers that need mission-critical memory. To offset the royalties, a DRAM maker could charge a premium for Silver Bullet chips, much as ECC-protected memory costs more now.

Ideally, Upmem would have a prototype chip that verifiably defeats RowHammer in real-world lab tests. But fabricating one is much costlier for the small company than it is for a DRAM manufacturer, which has to spin test chips for new designs anyway. Until then, double-checking Upmem's lengthy mathematical analysis will keep the engineers busy. The principle is solid; the variables are Silver Bullet's ability to detect activations exceeding tolerable thresholds and to respond quickly enough to prevent corruption.

Ultimately, the three leading DRAM makers will judge Silver Bullet. No one else can evaluate such a complex cost-benefit equation. Winning even one manufacturer would give Upmem greater leverage with the others. But because steadily shrinking DRAM cells make random soft errors more likely as well, Silver Bullet or a similar solution seems inevitable. ♦

To subscribe to *Microprocessor Report,* access www.linleygroup.com/mpr or phone us at 408-270-3772.