# Googlers’ Epic Hack Exploits How Memory Leaks Electricity

As Moore’s Law has packed more and more transistors onto a single memory chip, scientists have fretted for years that electric charges that “leak” out from those tiny components might cause unpredictable errors in neighboring semiconductors. But now a team of Google researchers has demonstrated a more unexpected problem with that electromagnetic leakage: hackers can use it to purposefully corrupt portions of some laptops’ memory, and even to bypass the security protections of those computers.

In a [post on its Google Project Zero security blog Monday](http://googleprojectzero.blogspot.de/2015/03/exploiting-dram-rowhammer-bug-to-gain.html), a group of the company’s researchers revealed new hacker exploits that take advantage of what’s known as the “Rowhammer” technique. Here’s how Rowhammer gets its name: In the Dynamic Random Access Memory (DRAM) used in some laptops, a hacker can run a program designed to repeatedly access a certain row of transistors in the computer’s memory, “hammering” it until the charge from that row leaks into the next row of memory. That electromagnetic leakage can cause what’s known as “bit flipping,” in which transistors in the neighboring row of memory have their state reversed, turning ones into zeros or vice versa. And for the first time, the Google researchers have shown that they can use that bit flipping to actually gain unintended levels of control over a victim computer. Their Rowhammer hack can allow a “privilege escalation,” expanding the attacker’s influence beyond a certain fenced-in portion of memory to more sensitive areas.

Google's hack shows a fundamental flaw in basic computer hardware that could be impossible to fully patch in existing vulnerable computers.

“We have shown two ways in which the DRAM rowhammer problem can be exploited to escalate privileges,” the researchers write in their blog post. “History has shown that issues that are thought to be ‘only’ reliability issues often have significant security implications, and the rowhammer problem is a good example of this. Many layers of software security rest on the assumption the contents of memory locations don’t change unless the locations are written to.”

Though the Google researchers’ bit-flipping attack isn’t merely theoretical, it would be far from simple to pull off in practice. The Project Zero team limited their exploit testing to laptops running Linux, and even then found that it only worked on less than half the models of computer they tried. Nonetheless, their hack shows a fundamental flaw in basic computer hardware that could be impossible to fully patch in existing vulnerable computers, and might force computer makers to reconsider the security implications of electromagnetic leakage in memory.

“This is definitely some of the more important security research to come out in years,” says well-known security researcher Dan Kaminsky, who gained fame for finding a critical security flaw in the Internet’s domain name system in 2008. “We think of a computer as deterministic…The moment it isn’t, you have undefined behavior, and in security undefined behavior is redefinable behavior. The [software] developer doesn’t know what the computer’s going to do, but the attacker does.”

 Flickr/ [Dick Thomas Johnson](https://www.flickr.com/photos/31029865@N06/6001342851)

Google didn’t make its researchers available for an interview despite WIRED’s request, and a spokeperson wrote in a statement only that “We’re working closely with hardware manufacturers to help mitigate the issue.”

In their blog post, however, Google researchers write that they first learned of the Rowhammer phenomenon from a [paper published by a team of Intel and Carnegie Mellon University researchers last year](http://users.ece.cmu.edu/~yoonguk/papers/kim-isca14.pdf). ([A response blog post from Cisco security analysts](http://blogs.cisco.com/security/mitigations-available-for-the-dram-row-hammer-vulnerability) traces the findings back earlier, to at least 2012.) That paper showed only that bit flipping was possible through repeatedly accessing a neighboring row of memory; it didn’t attempt to actually turn that technique into a hacker exploit.

“The previous academic paper described this as a possibility,” says Morgan Marquis-Boire, a former Google security researcher who now runs security for First Look Media. “What [Google’s] Project Zero has done is sit down and study this and find the conditions to exploit it in real time, in the real world.”

The first advancement the Google researchers made was to “hammer” memory rows on both sides of the position in memory they targeted—doubling the opportunities for electromagnetic charge to leak from one memory row to the next. The researchers didn’t specify how long they ran their program, but they suggest that their double-Rowhammer technique makes it vastly more effective. “For many machines, double-sided hammering is the only way of producing bit flips in reasonable time,” they write. “We have observed 25+ bits flipped in one row on one particularly fragile machine.”

But the Googlers’ real advancement is in how they used that technique to break into protected portions of a computer’s memory. In one attack, for instance, they write that they were able to gain full administrator control of a Linux operating system. That exploit worked by flipping bits in a so-called “page table” that acts as a table of contents showing where virtual memory addresses map to physical memory. After enough tries, corrupting that map sometimes redirected the attack program to more sensitive portions of memory it wasn’t meant to access. In some cases, it redirected the program to the page table itself, allowing the attacker to then rewrite any portion of memory he or she chose.

“What’s so interesting about Rowhammer: It's a physical world problem.”

In another attack, the Googlers’ Rowhammering allowed them to escape the “sandbox” in Google’s native client, a system used to run code inside a browser with limited privileges. Though Google has since disabled a function of its native client that allowed the attack, the attack nonetheless hinted at the possibility that Rowhammering in the future might allow an attacker to compromise a computer via a malicious website.

The Google researchers didn’t share any of the names of the computers or memory makers whose products were affected by their exploits, or the full details of the success rates of their attacks. They did, however, include a chart of 29 unidentified makes and models of laptops. Of those 29, only 15 were susceptible to bit flipping. For their sandbox escape, they report that only 13 percent of the bit flips their technique created actually made the exploit possible. They offered no information about just how often their Linux operating system privilege escalation attack worked.

The researchers include other important caveats to their technique, too: they admit that their bit flipping would only work on memory that doesn’t have an error correction feature common to many computers’ memory. That feature may explain why their attack didn’t work at all in nearly half of the Linux-running laptops they tested. And they say that a computer under more “memory pressure”—one that’s using more of its memory resources to run programs at the time of attack—might be harder to exploit.

Even so, the Googlers’ work represents an important step in proving that many computers’ DRAM has an inherent physical flaw, and one that can’t be fixed with a mere software patch. The researchers [released a Rowhammer test program](https://github.com/google/rowhammer-test), which allows users to check if their memory is vulnerable to bit flipping. And they suggest that memory makers consider implementing new Rowhammering protections that “refresh” memory after a certain number of accesses to adjacent positions to prevent electromagnetic leakage from causing bit flips.

Still, ex-Googler Marquis-Boire points out that what makes the Rowhammer vulnerability so insidious is that isn’t fundamentally a software issue. And that will make fixing it a much more complex process than the typical software update. “That’s what’s so interesting about Rowhammer: It’s a physical world problem,” he says. “And physical world attacks are always the hardest to patch.”