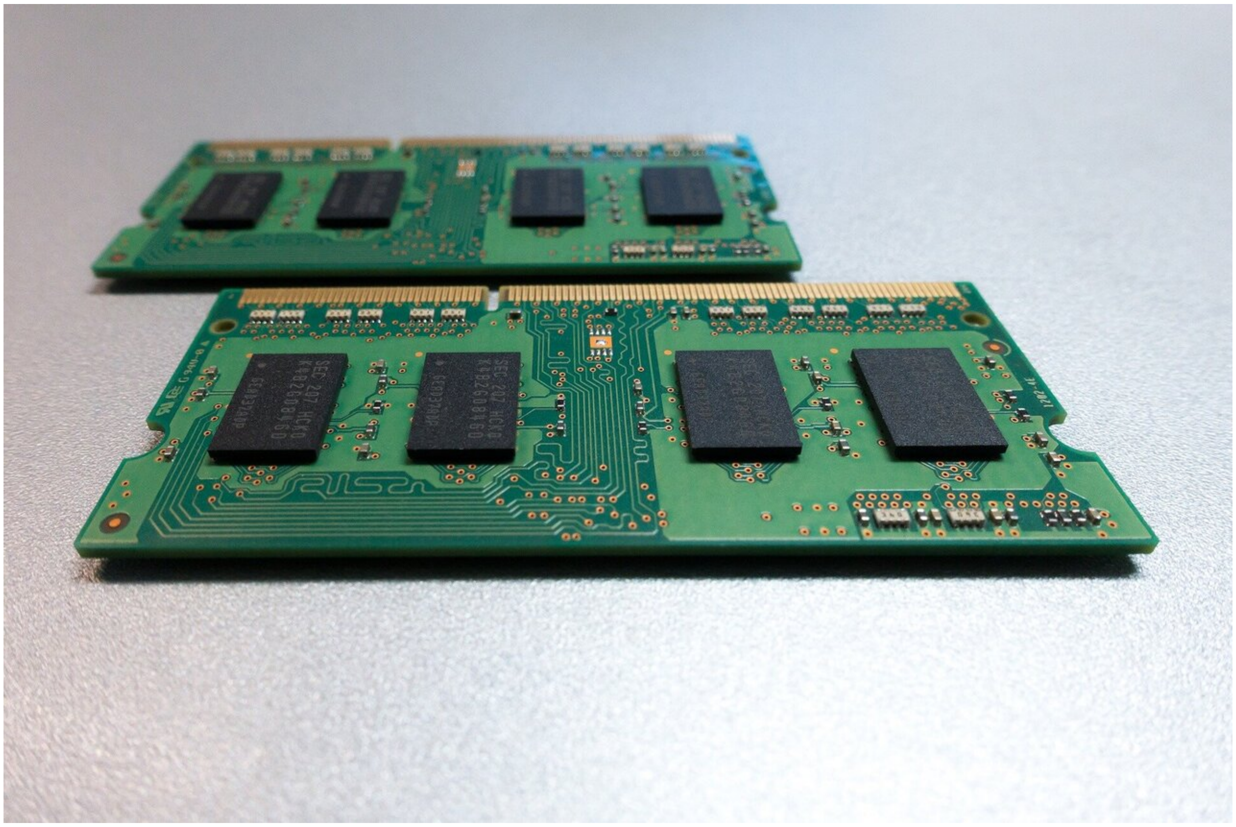
TechXplore

Researchers explore RAMBleed attack in pilfering data

June 15 2019, by Nancy Cohen



Credit: CC0 Public Domain

Do you remember Rowhammer, where an attacker could flip bits in the memory space of other processes?

Dan Goodin in *Ars Technica* reminded readers of the Rowhammer exploit—"Rowhammer attacks work by rapidly accessing—or hammering—physical rows inside vulnerable chips in ways that cause bits in neighboring rows to flip, meaning 1s turn to 0s and vice versa"—and he reminded readers of its evolution.

Over the past four years, he wrote, it has taken on capabilities such as elevating system rights and rooting Android phones. Goodin viewed this new attack as the use of Rowhammer "to extract cryptographic keys or other secrets stored in vulnerable DRAM modules."

Well, it continues to inspire trouble makers in other ways.

An attacker can read out physical memory belonging to other processes in a side-channel attack called RAMBleed. Its name reflects its characteristics: "Due to deficiencies in the memory modules, the RAM bleeds its contents, which we then recover through a side-channel."

"RAMBleed takes Rowhammer in a new direction," said Dan Goodin in *Ars Technica*. "Rather than using bit flips to alter sensitive data, the new technique exploits the hardware bug to extract sensitive data stored in memory regions that are off-limits to attackers."

Computerworld also wanted to draw the distinction between Rowhammer and the more recent discovery. "Unlike Rowhammer, which only allows for data corruption, the newly discovered RAMBleed vulnerability provides a way to grab data such as encryption keys from memory."

A joint team of four researchers with affiliations at University of Michigan, Graz University of Technology and University of Adelaide made the discovery.

The team issued information that covers a Q&A, along with a link to the paper they prepared. The authors will present this paper, "RAMBleed: Reading Bits in Memory Without Accessing Them," at the IEEE Symposium on Security and Privacy next year.

They sought to demonstrate the risk that RAMBleed poses. They presented an end-to end attack against OpenSSH 7.9, allowing an unprivileged attacker to extract the server's 2048-bit RSA private signing key.

The authors said that "a break of this key enables the attacker to masquerade as the server, thereby allowing her to conduct man-in-the-middle (MITM) attacks and decrypt all traffic from the compromised sessions."

What causes RAMBleed? Lucian Constantin in *Computerworld* said the attack was possible because of "a known design issue with modern DRAM chips that has been exploited in the past to modify protected data."

The authors in their paper said that "RAMBleed exploits a physical phenomenon in DRAM DIMMs wherein the likelihood of a Rowhammer induced bit flip depends on the values of the bits immediately above and below it. Bits only flip when the bits both immediately above and below them are in their discharged state." DRAM stands for dynamic random access memory.

How do we view this on the pain scale?

"RAMBleed shifts Rowhammer from being a threat not only to integrity, but confidentiality as well," they stated.

ECC (Error Correcting Code) memory does not prevent RAMBleed, which uses bit flips as a read side channel, and does not require bit flips to be persistent.

"Instead, the attacker merely needs to know that a bit flip occurred; the secret information leaks regardless of whether or not ECC corrects the flip."

As for defense through antivirus software, the team believed it "very unlikely" that any antivirus software currently on the market detects RAMBleed.

So, was RAMBleed ever exploited in the wild? They could not say definitely but they believed it to be unlikely.

Meanwhile, "ordinary" users, Goodin said, need not panic. "RAMBleed requires a fair amount of overhead and at least some luck." Instead, "RAMBleed and the previous attacks it builds on poses a longer-term threat."

The team notified Intel, AMD, OpenSSH, Microsoft, Apple and Red Hat about their findings, said Constantin.

CVE-2019-0174 is the CVE (Common Vulnerabilities and Exposures) number.

What does the team recommend?

"Users can mitigate their risk by upgrading their memory to DDR4 with targeted row refresh (TRR) enabled. While Rowhammer-induced bit flips have been demonstrated on TRR, it is harder to accomplish in practice."

Memory manufacturers, they said, can help mitigate by more rigorously testing for faulty DIMMs.

More information: rambleed.com/
rambleed.com/docs/20190603-rambleed-web.pdf

Citation: Researchers explore RAMBleed attack in pilfering data (2019, June 15) retrieved 19 April 2024 from https://techxplore.com/news/2019-06-explore-rambleed-pilfering.html