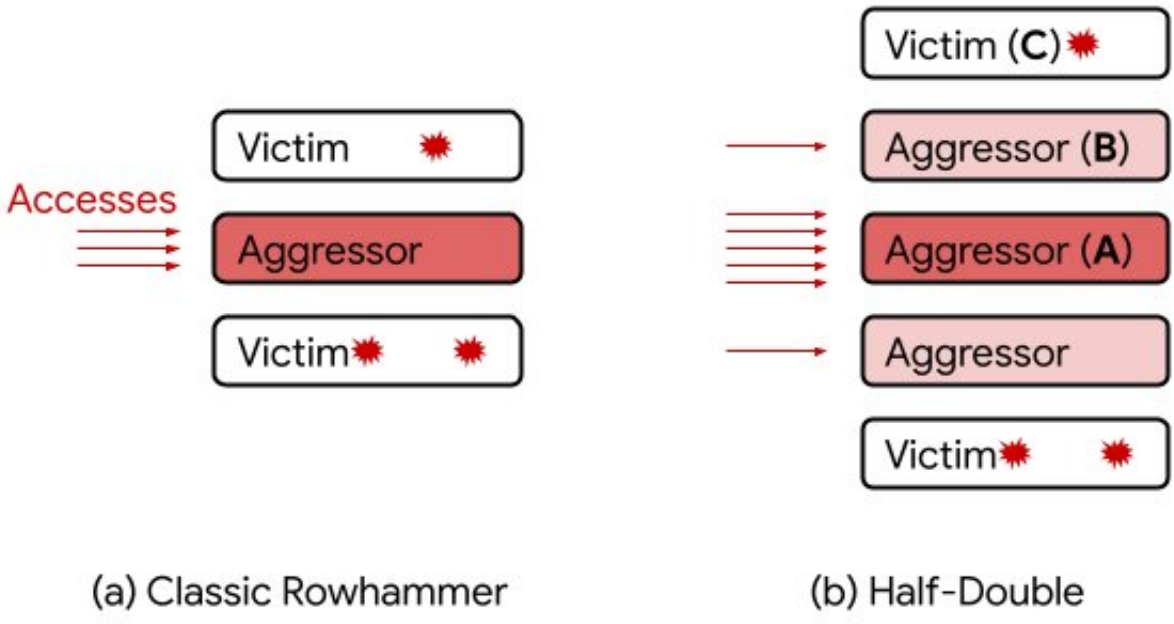
Google announces Half-Double, a new technique used in the Rowhammer DRAM security exploit

June 1 2021, by Sarah Katz



Half-Double function diagram. Credit: Google.com

Google has just revealed the discovery of a new technique used by attackers to take advantage of the Rowhammer security exploit present in Dynamic Random-Access Memory (DRAM). This new strategy involves capitalizing on the issues with some of the newer DRAM chips in the ways memory cells interact with each other.

This DRAM vulnerability works by using access to one address to alter the data stored at various other addresses. Similar to CPU execution vulnerabilities, Rowhammer interferes with the security architecture of the underlying hardware. As the exploit exists within the Silicon material itself, the bug enables potential bypass of both hardware and software protection measures. Such security circumvention can allow untrusted code to escape the sandbox and take over the system.

Having first discovered Rowhammer back in 2014, Google has since taken steps to mitigate this privileged escalation issue by monitoring for frequently accessed addresses. From there, chip manufacturers updated the proprietary logic inside their products accordingly. At first, this solution appeared successful—until 2020, when Google's TRRespass paper displayed the ability to reverse engineer the built-in mitigation systems and hinder defenses by distributing access. In fact, further research showed the potential for exploitation from JavaScript, without even the need to invoke cache-management primitives or system calls.

Perhaps most concerning, Half-Double has shown the unique Rowhammer capability of spreading to rows beyond its adjacent neighbors within the memory chip. This increase in distance likely suggests a growing sophistication of the Rowhammer exploit.

Google has begun collaborating with the independent semiconductor engineering trade organization JEDEC, among others, to try and resolve this Rowhammer threat. For now, Google encourages the multiple possibly impacted industries—from automotive to IoT—to contribute to and support this effort in any way possible.

More information: Qazi, S. et al. "Introducing Half-Double: New Hammering Technique for DRAM Rowhammer Bug." Google Online Security Blog, Google, 25 May 2021, security.googleblog.com/2021/0 … e-new-hammering.html