Un equipo de investigadores de seguridad de Google demostró otra variante del ataque Rowhammer, que elude todas las defensas actuales para manipular los datos almacenados en la memoria.

Apodada como Half-Double, la nueva técnica de martilleo depende del débil acoplamiento entre dos filas de memoria que no están inmediatamente adyacentes entre sí, pero que se ha eliminado una fila.

> *«A diferencia de TRRespass, que explota los punto ciegos de las defensas dependientes del fabricante, Half-Double es una propiedad intrínseca del sustrato de silicio subyacente»,* dijeron los investigadores.
>
> *«Esto es probablemente una indicación de que el acoplamiento eléctrico responsable de Rowhammer es una propiedad de la distancia, que efectivamente se vuelve más fuerte y de mayor alcance a medida que las geometrías de las celdas se reducen. Se pueden concebir distancias superiores a dos»*, agregaron.

Los ataques de Rowhammer son similares a la ejecución especulativa en que ambos rompen las garantías de seguridad fundamentales hechas por el hardware subyacente. Descubierto en 2014, Rowhammer se refiere a una clase de vulnerabilidades de DRAM en las que los accesos repetidos a una fila de memoria (agresor) pueden inducir una perturbación eléctrica lo suficientemente grande como para voltear bits almacenados en una fila adyacente (victima), lo que permite que el código no confiable escape de su sandbox y tome el control del sistema.

Aunque los fabricantes de DRAM implementaron contramedidas como Target Row Refresh (TRR) para frustrar dichos ataques, las mitigaciones se han limitado a dos vecinos inmediatos

de una fila agresora, excluyendo así las celdas de memoria a una distancia de dos filas. Las protecciones imperfectas significaron que las defensas TRR en las tarjetas DDR4 podrían eludirse para organizar nuevas variantes de ataques Rowhammer como TRRespass y SMASH.

El Rowhammer asistido a distancia dos, también conocido domo Half-Double, ahora se une a esa lista. *«Dadas tres filas consecutivas A, B y C, pudimos atacar a C dirigiendo una gran cantidad de accesos a A, junto con solo un puñado a B»*, explicaron los investigadores. En esta nueva configuración, A es el *«agresor lejano»,* B es el *«agresor cercano»* y C es *«la víctima».*

Google dijo que actualmente está trabajando con el Joint Electron Device Engineering Council (JEDEC), un organismo de estandarización independiente y una organización comercial de ingeniería de semiconductores, junto con otros socios de la industria, para identificar posibles soluciones para las vulnerabilidades de Rowhammer.

> *«Para evaluar la efectividad de una mitigación a nivel de SoC, un proveedor de DRAM debería probar una combinación de distancias de martilleo en lugar de solo probar a distancias individuales. En otras palabras, martillar una sola fila o un par de filas intercaladas en el medio crudo no mostrará este efecto. En cambio, los pares de filas en uno o ambos lados de la víctima prevista deben martillarse»*, dijeron los investigadores.