Investigadores del Georgia Institute of Technology y de la Purdue University han mostrado en otro estudio que las garantías de seguridad que ofrece Intel Software Guard eXtensions (SGX) pueden ser eludidas en sistemas DDR4, permitiendo la desencriptación pasiva de datos sensibles.

SGX es una característica de hardware presente en procesadores Intel para servidores que permite ejecutar aplicaciones dentro de un Entorno de Ejecución Confiable (TEE). Su función es aislar código y recursos de confianza dentro de lo que se denomina enclaves, impidiendo que atacantes vean su memoria o estado de CPU.

Con ello, el mecanismo pretende mantener la confidencialidad de los datos incluso si el sistema operativo subyacente ha sido alterado o comprometido. No obstante, los hallazgos más recientes evidencian las limitaciones de SGX.

«Demostramos que es posible construir un dispositivo para inspeccionar físicamente todo el tráfico de memoria de un equipo de forma económica y sencilla, usando herramientas eléctricas básicas y equipamiento adquirible por internet,» explicaron los investigadores. *«Con nuestro interposer contra el mecanismo de atestación de SGX, logramos extraer la clave secreta de atestación SGX de una máquina que se encontraba en estado plenamente confiable, vulnerando así la seguridad de SGX.»*

Al igual que el ataque Battering RAM divulgado recientemente por investigadores de KU Leuven y la University of Birmingham, el método ahora descrito —apodado WireTap— utiliza un interposer colocado entre la CPU y el módulo de memoria para observar los datos que fluyen entre ambos. Ese interposer puede ser introducido por un actor malintencionado mediante un ataque a la cadena de suministro o un compromiso físico.

En esencia, el ataque físico explota el uso por parte de Intel de cifrado determinista para orquestar una recuperación completa de claves contra el Quoting Enclave (QE) de SGX, lo que hace posible extraer una clave de firma ECDSA capaz de firmar informes arbitrarios de enclaves SGX.

Dicho de otra manera, un atacante puede aprovechar la naturaleza determinista del cifrado de memoria para construir una especie de oráculo que rompa la seguridad del código criptográfico de tiempo constante.

«Hemos logrado extraer claves de atestación, que son el mecanismo principal para verificar si un código está ejecutándose bajo SGX,» afirmaron los investigadores. *«Esto permite a cualquier atacante hacerse pasar por hardware SGX legítimo, mientras en realidad ejecuta código de forma expuesta y mira dentro de tus datos.»*

«Como dos caras de la misma moneda, WireTap y Battering RAM exploran propiedades complementarias del cifrado determinista. Mientras WireTap se centra principalmente en vulnerar la confidencialidad, Battering RAM se enfoca sobre todo en la integridad. El resultado es el mismo; no obstante, tanto SGX como SEV son fáciles de romper usando interposición de memoria.»

Si bien Battering RAM es un ataque de bajo coste que puede montarse con equipos por debajo de los 50 USD, el montaje de WireTap sale aproximadamente por 1,000 USD, incluyendo el analizador lógico.

En un escenario hipotético de ataque dirigido a despliegues de blockchain protegidos por SGX —como Phala Network, Secret Network, Crust Network e IntegriTEE— el estudio concluye que WireTap podría utilizarse para debilitar las garantías de confidencialidad e integridad, permitiendo a atacantes revelar transacciones privadas o apropiarse de recompensas de forma ilegítima.

En respuesta, Intel indicó que la explotación está fuera del alcance de su modelo de amenazas, ya que asume un adversario con acceso físico directo al hardware y un interposer en el bus de memoria. En ausencia de un «parche», recomiendan operar los servidores en entornos físicamente seguros y emplear proveedores de nube que ofrezcan seguridad física independiente.

«Tales ataques están fuera del perímetro de protección ofrecido por el cifrado de memoria

basado en Advanced Encryption Standard-XEX-based Tweaked Codebook Mode with Ciphertext Stealing (AES-XTS),» dijo el fabricante. *«Dado que ofrece protección limitada de confidencialidad, y no proporciona integridad ni protección anti-repetición frente a atacantes con capacidades físicas, Intel no planea asignar un CVE.»*