Intel anunció hoy que su característica de seguridad CET experimental estará disponible por primera vez en la siguientes CPU móviles Tiker Lake de la compañía.

Intel ha estado trabajando en CET (Tecnología de Flujo de Control) desde 2016, cuando publicó la primera versión de la especificación CET.

CET trabaja con *«flujo de control»*, un término técnico empleado para describir el orden en que se ejecutan las operaciones dentro de la CPU.

El malware que se ejecuta en un dispositivo puede usar vulnerabilidades en otras aplicaciones para secuestrar su flujo de control e insertar su código malicioso para que se ejecute en el contexto de otra aplicación.

En las futuras CPU móviles Tiger Lake de Intel, CET protegerá el flujo de control por medio de dos nuevos mecanismos de seguridad, a saber, shadow stack y seguimiento indirecto de sucursales.

Shadow stack se refiere a una copia del flujo de control previsto de una aplicación, almacenar la shadow stack en un área segura de la CPU y usarla para garantizar que no se produzcan cambios no autorizados en el orden de ejecución previsto en una aplicación.

Intel afirma que la pila de sombra de CET protegerá a los usuarios de una técnica denominada Programación Orientada al Retorno (ROP), donde el malware abusa de la instrucción RET para agregar su código malicioso al flujo de control de una aplicación legítima.

Por otro lado, el seguimiento indirecto de ramas se refiere a restringir y agregar protecciones adicionales a la capacidad de una aplicación para usar *«tablas de salto»* de la CPU, que son tablas que contienen ubicaciones de memoria utilizadas en el flujo de control de una aplicación.

Intel dice que el rastreo indirecto de sucursales protege contra dos técnicas llamadas

Programación Orientada a Saltos (JOP) y Programación Orientada a Llamadas (COP), donde el malware abusa de las instrucciones JMP o CALL para secuestrar las tablas de salto de una aplicación legítima.

Debido a que Intel publicó la especificación CET en 2016, los fabricantes de software han tenido tiempo de ajustar su código para la primera serie de CPU Intel que lo admitirán.

El soporte CET ya llegó a Glibc, y Microsoft también agregó el soporte CET a Windows Insiders, como una característica llamada Protección de pila forzada por hardware.

Lo que se requiere ahora es que Intel envíe CPU que admitan instrucciones CET, de modo que las aplicaciones y los sistemas operativos puedan activar el soporte y optar por la protección que proporciona CET.

CET fue lanzado hoy para la línea de CPU móviles de Intel que utilizan la microarquitectura Tiger Lake, pero la tecnología también estará disponible en plataformas de escritorio y servidor, dijo Tom Garrison, vicepresidente del Grupo de Computación del Cliente y gerente general de Estrategias e Iniciativas de Seguridad (SSI) en Intel Corporation.