Falle nella sicurezza informatica mostrano che più veloce non significa necessariamente migliore

Alcuni ricercatori hanno scoperto bug nella sicurezza vecchi di 20 anni nei chip di CPU, mettendo in evidenza la necessità di computer più sicuri.

© Production Perig, Shutterstock

Nella corsa verso computer dalle prestazioni migliori, la tradizionale polarizzazione dei fabbricanti sulla velocità è avvenuta a spese della sicurezza. A evidenziare quanto siano realmente vulnerabili i computer di oggi, due falle fondamentali nella sicurezza sono state recentemente scoperte nei processori. Chiamate Meltdown e Spectre, le falle potrebbero consentire agli utenti di accedere senza autorizzazione ai dati personali memorizzati nella parte più protetta del vostro sistema informatico.

I due bug sono stati trovati in maniera indipendente da quattro differenti gruppi di ricerca, uno dei quali era un team di ricercatori del Politecnico di Graz, in Austria. Supportato dal finanziamento dell'UE per il progetto SOPHIA, il team di Graz ha svolto un ruolo chiave nella scoperta di Meltdown e Spectre.

Un Meltdown, o collasso, del sistema

Entrambi i bug permettono di accedere alle informazioni senza avere l'autorizzazione, ma ottengono questo risultato in modi differenti. Meltdown lo fa superando l'isolamento della memoria, consentendo a programmi malevoli di leggere le parti normalmente non accessibili della memoria di un computer. Questo è reso possibile da una funzionalità chiamata «esecuzione fuori ordine». Per rendere più

veloce un'operazione, «i moderni processori eseguono le operazioni fuori ordine, ovvero guardano avanti e organizzano le operazioni successive per far girare al minimo le unità di esecuzione del processore», hanno spiegato il team di Graz e altri ricercatori in un articolo postato sul sito web della Cornell University Library.

«La causa alla radice di Meltdown», riferiscono gli autori, «è l'hardware. L'attacco è indipendente dal sistema operativo, e non dipende da nessun punto debole nel software.» Tutti i processori Intel che svolgono l'esecuzione fuori ordine vengono colpiti. Fortunatamente, i ricercatori hanno sviluppato delle patch per il software contro Meltdown.

Lo Spectre, o spettro, nel sistema

I processori che effettuano un'esecuzione fuori ordine potrebbero giungere a una diramazione in cui la direzione futura dipende da istruzioni che devono ancora essere eseguite. Per massimizzare le prestazioni, i processori prevedono allora il percorso che verrà probabilmente seguito da un programma ed eseguono anzitempo le istruzioni ivi presenti. A rendere possibili gli attacchi di Spectre è la vulnerabilità insita in questo processo. Spectre consente di rubare i dati dalla memoria di altre applicazioni che girano su una macchina, interrompendo l'isolamento tra di esse.

In uno studio separato a cui hanno partecipato anche i ricercatori di Graz, gli autori descrivono come funziona questa classe di attacchi: «A un livello alto, gli attacchi di Spectre inducono il processore a eseguire in modo speculativo sequenze di istruzioni che non sarebbero state eseguite durante la corretta esecuzione del programma.» Queste operazioni speculative portano alla fuoriuscita di informazioni riservate.

Spectre, essendo più difficile da correggere e non colpendo solo processori Intel, ma anche AMD e ARM, rappresenta un problema più grave per l'industria.

Anche se scoperte solo di recente, le falle esistono dalla metà degli anni novanta. Un pensiero allarmante, dato che queste vulnerabilità avrebbero potuto essere sfruttate per decenni da qualcuno senza che nessuno se ne accorgesse. Stefan Mangard, ricercatore capo per SOPHIA, sottolinea il bisogno di computer più sicuri in una intervista postata sul sito web del Consiglio europeo della ricerca: «Nel contesto odierno, caratterizzato da un numero sempre più elevato di attacchi ai sistemi informatici […], dobbiamo accettare la sicurezza quale primario criterio di progettazione. Mi auguro che la scoperta delle falle Meltdown e Spectre dia il via a un nuovo modo di pensare alla progettazione dei computer.»

SOPHIA (Securing Software against Physical Attacks) sta proseguendo la sua ricerca su dei modi per eseguire il software in modo sicuro ed efficiente in presenza di attacchi fisici su tutti i tipi di dispositivi informatici.

Per maggiori informazioni, consultare:
pagina web del progetto su CORDIS

Paesi

Austria

Progetti correlati

PROGETTO

Securing Software against Physical Attacks

SOPHIA

3 Ottobre 2023

Articoli correlati

NOTIZIE

PROGRESSI SCIENTIFICI

Come violare la sicurezza dei microprocessori riducendo la tensione fornita ai computer

30 Gennaio 2020

Ultimo aggiornamento: 4 Maggio 2018

Permalink: https://cordis.europa.eu/article/id/123337-computer-security-flaws-reveal-faster-isnt-necessarily-better/it