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

Gli informatici hanno dimostrato come sia possibile rendere vulnerabili le unità di elaborazione centrale (CPU) Intel agli attacchi, manomettendo la tensione operativa dei processori.

ECONOMIA DIGITALE

© metamorworks, Shutterstock

Nell'ottica di soddisfare la crescente esigenza di prestazioni ed efficienza, risulta fondamentale ottimizzare le CPU dei computer e regolarne la frequenza e la tensione in base alle necessità. Invece di consumare energia ininterrottamente, cosa che produce troppo calore, come nei centri di elaborazione dati e fa scaricare la batteria troppo velocemente, come accade nei dispositivi mobili, i chip sono programmati per utilizzare solo la potenza necessaria al loro processore per eseguire un'operazione specifica. In una procedura nota come «sottotensione» o «sovratensione» e attraverso interfacce software privilegiate, i sistemi moderni possono funzionare correttamente in presenza di specifiche condizioni di esercizio. Molti processori, compresi i diffusissimi esemplari della serie Intel Core, si basano su questa tecnologia. Ma come si possono proteggere i dati quando l'aggressore si serve di mezzi fisici per compromettere la sicurezza dei microprocessori del computer?

Parzialmente supportato dai progetti FutureTPM e SOPHIA, finanziati dall'UE, un team di scienziati ha dimostrato che queste interfacce software possono essere sfruttate per indebolire la sicurezza del sistema. In un documento di ricerca, spiegano come siano riusciti a minare l'integrità della Intel Software Guard Extensions (SGX), una serie di codici di istruzioni relative alla sicurezza incorporata

nelle CPU dei moderni processori Intel. SGX contribuisce a difendere i calcoli sensibili all'interno di cosiddette «enclave», il cui contenuto è protetto e non può essere modificato dall'esterno, nemmeno in presenza dei più avanzati tipi di malware.

Manomettere la tensione

Gli stessi scienziati sono riusciti a dimostrare come sia possibile violare la sicurezza controllando la tensione durante l'esecuzione di calcoli interni all'enclave. «Si tratta dell'attacco Plundervolt, in cui un avversario software privilegiato abusa di un'interfaccia di ridimensionamento della tensione Intel Core per compromettere l'integrità dei calcoli interni all'enclave Intel SGX». Inoltre, aggiungono: «Plundervolt controlla attentamente la tensione di alimentazione del processore durante un calcolo interno all'enclave, provocando errori prevedibili nel pacchetto del processore. Di conseguenza, nemmeno la tecnologia di cifratura/autenticazione della memoria di Intel SGX può fornire una protezione efficace da Plundervolt».

Gli scienziati hanno concluso che la loro ricerca «offre ulteriori prove a sostegno del fatto che l'esecuzione in enclave può consegnare calcoli sensibili a piattaforme remote inaffidabili, creando nuove e inattese superfici di attacco, che continuano a essere rilevanti e a necessitare di ulteriori approfondimenti».

Come osservato in un comunicato stampa emesso dall'Università di Birmingham, tra i partner del progetto FutureTPM, «Intel ha già risposto a questa minaccia alla sicurezza, rilasciando un aggiornamento dei microcodici volto a mitigare Plundervolt». Citato nello stesso comunicato, l'autore del documento di ricerca David Oswald dell'Università di Birmingham afferma: «Stando alle nostre attuali conoscenze, il difetto che abbiamo scoperto comprometterà esclusivamente la sicurezza delle enclave SGX. Intel ha reagito rapidamente alla minaccia e gli utenti possono ora proteggere le loro enclave SGX scaricando l'aggiornamento fornito da Intel».

Il progetto FutureTPM (Future Proofing the Connected World: A Quantum-Resistant Trusted Platform Module), che ha finanziato la ricerca, si concluderà nel mese di dicembre 2020. Le sue tecnologie TMP (Trusted Platform Module) sono già ampiamente utilizzate. I partner del progetto ritengono che, oltre ai calcoli fidati, il progetto FutureTPM avrà un impatto significativo su altre applicazioni di crittografia in generale. SOPHIA (Securing Software against Physical Attacks), un altro sostenitore del progetto dedicato alla sicurezza Plundervolt, si concentra sull'esecuzione sicura ed efficiente del software in presenza di attacchi fisici. Si occupa di sicurezza hardware, architetture di sistema sicure, implementazioni crittografiche e canali laterali.

Per maggiori informazioni, consultare:
sito web del progetto FutureTPM
progetto SOPHIA

Paesi

Austria

Progetti correlati

Future Proofing the Connected World: A Quantum-Resistant Trusted Platform Module

FutureTPM

7 Settembre 2023

PROGETTO

Securing Software against Physical Attacks

SOPHIA

3 Ottobre 2023

PROGETTO

Articoli correlati

PROGRESSI SCIENTIFICI

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

4 Maggio 2018

Ultimo aggiornamento: 30 Gennaio 2020

Permalink: https://cordis.europa.eu/article/id/413290-how-to-breach-computer-chip-security-by-starving-computers-of-voltage/it