Intel svela Tunable Replica Circuit per una maggiore protezione contro alcune minacce fisiche

https://www.hwupgrade.it/i/n/intel-core-hx-adl_720.jpg,

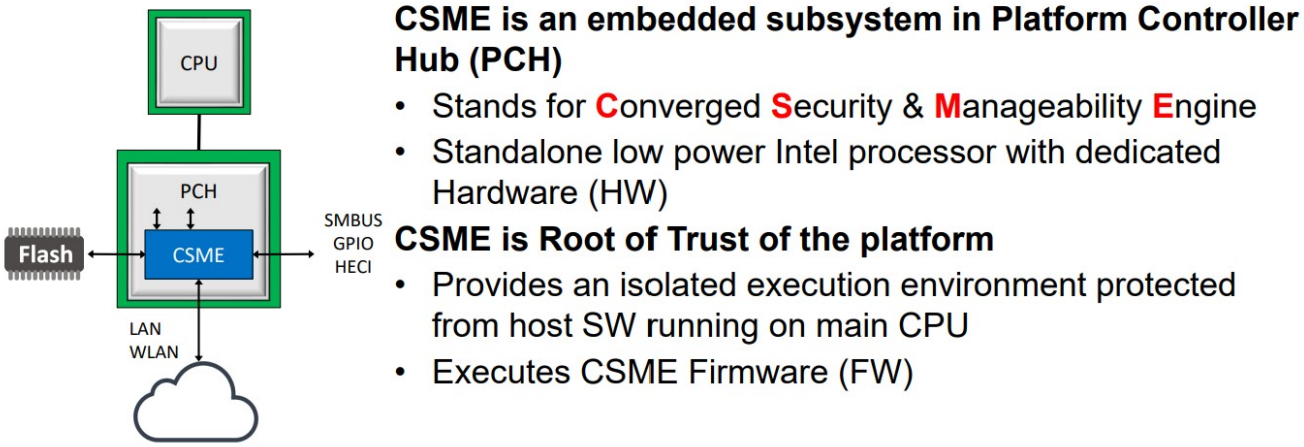
Intel applica un Tunable Replica Circuit per proteggere i sistemi da determinati tipi di attacco fisico di fault injection. L'azienda ne ha parlato durante la Black Hat USA 2022, svelando di averlo integrato sulle piattaforma per i Core di 12a generazione.

di Manolo De Agostini pubblicata il **11 Agosto 2022**, alle **20:01** nel canale Sicurezza

Intel

Nel corso della Black Hat USA 2022, **Intel** ha presentato una ricerca intitolata "*Fault-Injection Detection Circuits: Design, Calibration, Validation and Tuning*" in cui ha discusso i dettagli di **una nuova tecnica** che integra le misure di mitigazione degli attacchi fisici di fault injection già presenti a livello software.

L'azienda statunitense è andata a **integrare della logica chiamata Tunable Replica Circuit (TRC) all'interno del chipset** che accompagna il processore. Tale protezione contro la fault injection si affida a **sensori per rilevare in modo esplicito anomalie nella temporizzazione dei circuiti** che si verificano a seguito di un attacco. Il TRC è stato integrato per la prima volta sulle piattaforme destinate ai processori Intel Core di 12a generazione.



Il TRC **aggiunge la tecnologia di rilevamento della fault injection all'Intel Converged Security and Management Engine (Intel CSME)** ed è progettato per rilevare gli attacchi fisici non invasivi sui pin che forniscono clock e tensione. Il TRC è anche progettato per rilevare le fault injection di tipo elettromagnetico.

"La protezione dei software viene rinforzata grazie alla virtualizzazione, agli stack canaries e all'autenticazione del

codice prima dell'esecuzione", ha affermato Daniel Nemiroff, Senior Principal Engineer di Intel. "Questo ha spinto i malintenzionati a volgere la loro attenzione verso attacchi fisici delle piattaforme informatiche. Uno degli strumenti preferiti sono gli attacchi fault injection attraverso glitch di tensione, clock e radiazioni elettromagnetiche che causano **errori di temporizzazione del circuito e possono consentire l'esecuzione di istruzioni dannose e la potenziale esfiltrazione di dati segreti**".

Il Tunable Replica Circuit è stato **originariamente sviluppato dagli Intel Labs** per monitorare variazioni dinamiche quali come abbassamenti di tensione, cali di temperatura e invecchiamento nei circuiti con l'obiettivo di migliorare le prestazioni e l'efficienza energetica. Con l'evolversi delle nuove tecnologie, evolvono anche le loro applicazioni.

"Modificando la configurazione del monitoraggio e costruendo l'infrastruttura per sfruttare la sensibilità del TRC rispetto agli attacchi di fault injection, il circuito è stato ottimizzato per le applicazioni di sicurezza", ha commentato Carlos Tokunaga, principal engineer di Intel Labs, spiegando l'approccio di ricerca.

- The TRC is integrated into the system agent partition of CSME.
- The CSME-TRC monitors the power and clock coming into CSME, to help protect all portions of CSME from an attack.
- When the TRC detects a glitch, it invokes countermeasures that result in a CSME reset. The rest of the SoC is not impacted.
- The TRC is on the same reset line as all CSME HW, and if CSME is on, the TRC is monitoring this power.
- If CSME is power-gated, the TRC is also power-gated.

Intel Labs, iSTARE-PASCAL (Physical Attack and Side Channel Analysis Lab) e il Client Computing Group di Intel hanno collaborato per testare il TRC in diversi scenari di sicurezza. Insieme, i tre gruppi hanno dimostrato che **il TRC può essere calibrato al punto in cui tali violazioni di tempistica possono essere ricondotte a un attacco.**

Il TRC di Intel è in grado di segnalare un attacco **quando rileva un errore di temporizzazione dovuto a un glitch di tensione, clock, temperatura o elettromagnetico**. Poiché il TRC è calibrato per segnalare gli errori che si verificano a livelli di tensione al di fuori dell'intervallo operativo nominale del CSME, qualsiasi condizione di errore segnalata indica che i dati potrebbero essere danneggiati e rende attive le appropriate operazioni di mitigazione per garantire l'integrità dei dati.

Intel ha applicato il TRC al Platform Controller Hub (PCH), il chipset del sistema, isolato dalla CPU, al cui interno troviamo Intel CSME. "**L'aspetto più importante per la produzione di questo tipo di sensore hardware è la calibrazione**. Calibrato con una sensibilità troppo elevata, il sensore rileverebbe i normali cali di tensione del carico di lavoro come falsi positivi. I falsi positivi potrebbero causare instabilità della piattaforma, comportando un onere aggiuntivo per i responsabili della sicurezza informatica. **Per evitare falsi positivi, Intel ha sviluppato un flusso di calibrazione basato su feedback**", spiega l'azienda.

Anche ridurre al minimo i falsi negativi è importante, quindi il ciclo di feedback si affida ai risultati dei test falsi positivi e falsi negativi, insieme ai dati sui margini del sensore hardware. Ciò indica quanto il sensore è vicino al rilevamento di un problema tecnico e la precisione delle bande di protezione.

Read More