CLAUDIO BEGGIATO

ATTACCHI SIDE-CHANNEL

Minaccia e protezione per la sicurezza crittografica in ambito Difesa

Gli attacchi side-channel rappresentano una minaccia silenziosa ma estremamente efficace per i dispositivi crittografici impiegati nella difesa e nella protezione delle informazioni sensibili, rendendo indispensabile un rafforzamento delle capacità nazionali di sicurezza

Audible sintesi articolo

Gli attacchi side-channel (SCA) sono una delle minacce emergenti più gravi nel campo della sicurezza informatica, in particolare per i dispositivi crittografici utilizzati in ambito militare e per la protezione delle informazioni sensibili. A differenza degli attacchi tradizionali che mirano a sfruttare vulnerabilità nel software o nell'hardware, gli attacchi side-channel si basano sull'osservazione di effetti collaterali generati dal sistema stesso, come il consumo di energia, i tempi di esecuzione o le emissioni elettromagnetiche. Questi segnali secondari possono rivelare informazioni vitali, come le chiavi di cifratura, compromettendo gravemente la sicurezza dei dati.

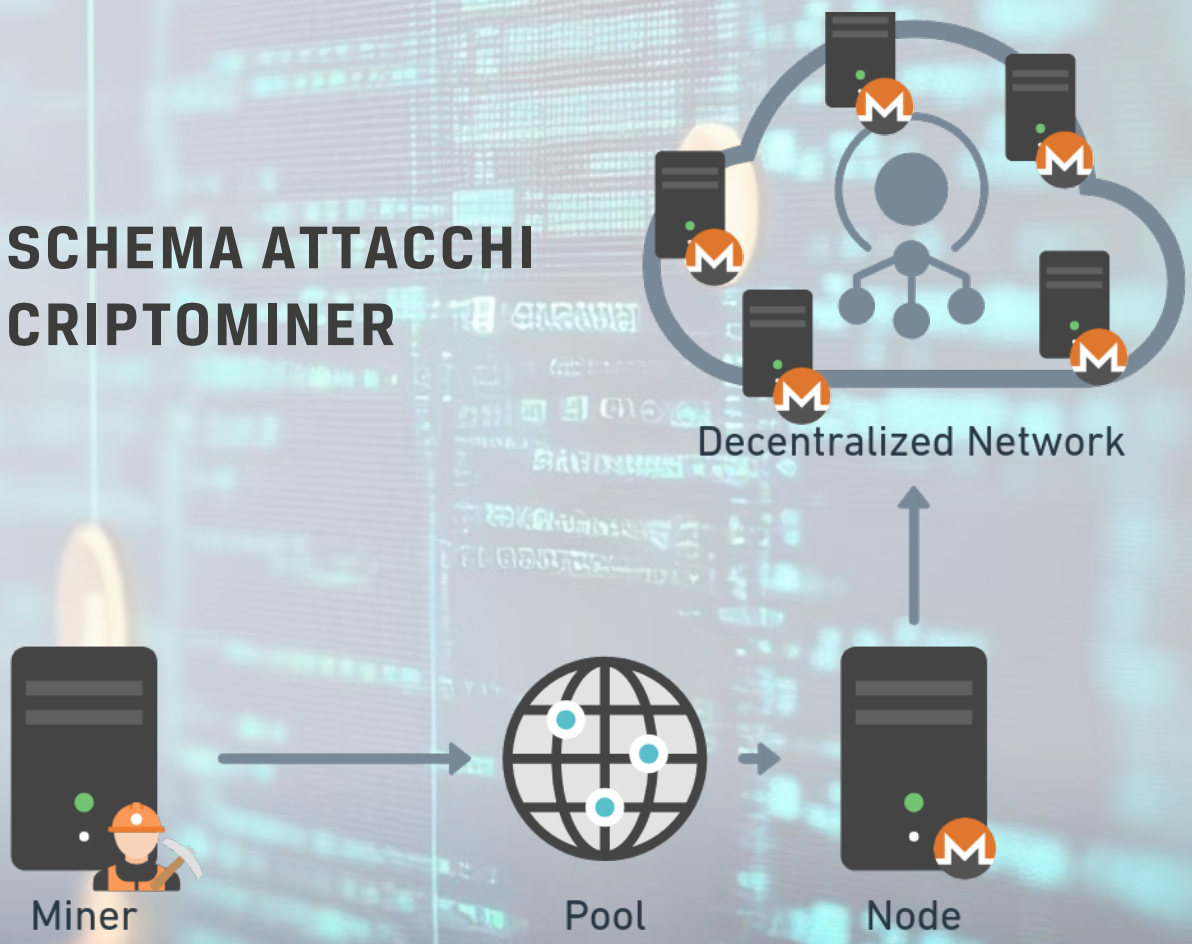
In un attacco side-channel, l'aggressore non agisce direttamente sul codice del programma, ma osserva il comportamento fisico del dispositivo che esegue il programma stesso. Tra gli attacchi più comuni troviamo:

- **Timing Attacks**: analizzando i tempi di esecuzione delle operazioni, un attaccante può determinare comportamenti specifici del dispositivo e, in alcuni casi, ricostruire la chiave crittografica;
- **Power Consumption Attacks**: misurando i picchi nel consumo energetico durante le operazioni di calcolo, un attaccante può ottenere informazioni sulle operazioni interne, come quelle legate alla crittografia. Questo tipo di attacco include sia l'analisi a potenza semplice che l'analisi differenziale della potenza (DPA), che offre una maggiore precisione nella ricostruzione delle chiavi;
- **Fault Attacks**: manipolando i parametri fisici del dispositivo, come la tensione o la frequenza di clock, si può costringere il sistema a produrre errori, da cui è possibile dedurre la chiave segreta. Un caso particolare di questo tipo di attacco è il cache attack, che sfrutta il comportamento delle memorie cache per ottenere informazioni riservate.
- **Analisi delle Emissioni Elettromagnetiche e Acustiche**: le onde elettromagnetiche e i suoni emessi da un dispositivo durante operazioni crittografiche possono essere utilizzati per recuperare informazioni sensibili. Ad esempio, studi hanno dimostrato che è possibile estrarre dati da smart card o da dispositivi FPGA ascoltando le loro emissioni acustiche.

Gli SCA come minaccia per la Difesa Nazionale

Nel contesto della difesa, la protezione contro gli attacchi side-channel assume una rilevanza cruciale. I dispositivi crittografici utilizzati per la gestione e la protezione di informazioni sensibili, come smart card, token, e sistemi FPGA (Field Programmable Game Array), sono particolarmente vulnerabili agli SCA. Questi dispositivi sono progettati per garantire la segretezza e l'integrità delle informazioni, ma emettono inevitabilmente segnali collaterali che possono essere sfruttati da un attaccante. Se un

SCHEMA ATTACCHI CRIPTOMINER



IL MASKING È UNA TECNICA CHE CONSISTE NEL NASCONDERE, FILTRARE O PROTEGGERE INFORMAZIONI APPLICANDO UNA MASCHERA AI DATI, IN MODO DA RENDERLI PARZIALMENTE O TOTALMENTE INVISIBILI A CHI NON È AUTORIZZATO

GLI FPGA (FIELD-PROGRAMMABLE GATE ARRAY) SONO CIRCUITI INTEGRATI PROGRAMMABILI CHE PERMETTONO DI REALIZZARE HARDWARE DIGITALE PERSONALIZZATO. A DIFFERENZA DI CPU E GPU, ELABORANO I DATI IN PARALLELO REALE, GARANTENDO LATENZA BASSISSIMA E PRESTAZIONI ELEVATE. SONO UTILIZZATI IN AMBITI CRITICI COME DIFESA, TELECOMUNICAZIONI, INDUSTRIA E AI, DOVE SERVONO AFFIDABILITÀ, VELOCITÀ E CAPACITÀ DI RICONFIGURAZIONE

aggressore riesce a monitorare e analizzare questi segnali, può ottenere l'accesso a chiavi segrete o altre informazioni crittografiche, compromettendo la sicurezza dei dati.

L'adozione di tecniche di protezione avanzate contro gli SCA è fondamentale per la cyber difesa nazionale, soprattutto per la protezione di infrastrutture critiche. Tali tecniche non solo migliorano la sicurezza dei sistemi, ma sono anche essenziali per garantire la superiorità informativa e la disponibilità delle informazioni in contesti di conflitto cibernetico o di guerra elettronica.

Metodi di protezione contro gli SCA: l'Importanza per la Difesa

La difesa contro gli attacchi side-channel non si limita alla progettazione di dispositivi più resistenti, ma implica anche l'adozione di strategie sistematiche per l'individuazione e la mitigazione delle vulnerabilità. Le principali metodologie di protezione includono:

- Tecniche di Blinding e Randomizzazione: L'uso di metodi come la randomizzazione dei tempi di esecuzione o del consumo energetico rende più difficile per l'attaccante correlare il comportamento del dispositivo alle operazioni crittografiche. Ad esempio, la randomizzazione del clock o l'introdurre ritardi casuali nelle operazioni può confondere gli attaccanti che cercano di analizzare i segnali collaterali.
- Tecniche di "Masking": Un'altra tecnica consiste nell'offuscare i dati sensibili utilizzando operazioni matematiche che nascondono i valori reali. Ciò rende molto più difficile per un attaccante estrarre informazioni dalla potenza o dal tempo di esecuzione delle operazioni.
- Analisi del Consumo Energetico: Alcuni dispositivi utilizzano circuiti speciali per "filtrare" o ridurre i segnali di consumo energetico, impedendo agli attaccanti di raccogliere informazioni utili dai picchi di corrente.
- Protezione delle Memorie e dei Cache: Le operazioni sulle memorie cache sono una delle principali fonti di vulnerabilità negli attacchi side-channel. Tecniche come la gestione sicura della cache e l'isolamento dei dati sensibili durante le operazioni crittografiche possono ridurre significativamente il rischio di attacchi.

In ambito difesa, la protezione contro gli SCA è essenziale per evitare che dati critici, come le chiavi di cifratura, vengano rubati o manipolati da attori malintenzionati. Questi metodi permettono di rafforzare i dispositivi e i sistemi contro tecniche di intrusione sempre più sofisticate, garantendo che le informazioni sensibili rimangano protette anche in presenza di attacchi avanzati.

Il ruolo delle iniziative nazionali nella protezione contro gli SCA

In Italia, la protezione contro gli attacchi side-channel è un tema di crescente importanza per la sicurezza nazionale. Sebbene a livello internazionale esistano numerosi laboratori e centri di ricerca specializzati nella valutazione della sicurezza contro gli SCA, il Paese ha avviato iniziative per sviluppare capacità nazionali in questo campo. In particolare, grazie al supporto di progetti come il Piano Nazionale della Ricerca Militare (PNRM), è stata data priorità allo sviluppo di competenze per la valutazione e la protezione contro le vulnerabilità legate agli SCA.

Tra questi, uno degli sviluppi più significativi è il progetto "SCA SHIELD", che ha come obiettivo quello di creare una piattaforma di test per analizzare la resistenza dei dispositivi crittografici contro gli attacchi side-channel. Questo progetto, supportato da finanziamenti pubblici e da collaborazioni con aziende del settore della difesa, mira a fornire un centro d'eccellenza per la verifica della sicurezza dei dispositivi crittografici, sia a livello hardware che software. La creazione di un'infrastruttura di test avanzata è fondamentale per garantire che i dispositivi utilizzati dalla Difesa e dalle istituzioni sensibili siano sicuri contro minacce di tipo side-channel.

L'importanza delle competenze nazionali per la sicurezza crittografica

L'adozione di metodi di protezione avanzati contro gli attacchi side-channel in ambito difesa non è solo una questione di ricerca e sviluppo, ma anche di capacità operative, infatti la creazione di un centro nazionale per la valutazione della sicurezza permette non solo di migliorare la protezione dei dispositivi esistenti, ma anche di guidare l'industria nazionale nella progettazione di nuovi dispositivi crittografici robusti contro gli SCA.

L'introduzione di tecniche di protezione come la randomizzazione, il masking e la gestione sicura delle memorie non solo potenzia la sicurezza dei dispositivi, ma permette anche di sviluppare standard e linee guida internazionali per la protezione contro gli attacchi side-channel. In questo contesto, l'Italia ha il potenziale di diventare un punto di riferimento per la sicurezza cibernetica avanzata a livello globale, migliorando la protezione delle proprie infrastrutture critiche e delle informazioni sensibili.