HORIZON 2020

Robust and Efficient Approaches to Evaluating Side Channel and Fault Attack Resilience

Risultati in breve

Nuovi strumenti aiutano a proteggere i dispositivi integrati

I semplici microprocessori dei computer possono essere manomessi. I produttori sviluppano protezioni, ma valutare equamente le difese è complesso.

ECONOMIA DIGITALE

SICUREZZA

© Hamik, Shutterstock

I cosiddetti dispositivi integrati sono semplici microprocessori per computer, progettati per una singola funzione, incorporati all'interno di comuni prodotti. Tra gli esempi si annoverano gli smart chip delle carte di credito, o il chip nelle chiavi dell'auto che permette lo sblocco a distanza di un veicolo specifico.

Sebbene tali dispositivi utilizzino la crittografia, sono hackerabili. La decrittazione convenzionale (delle e-mail intercettate, ad esempio) si basa sull'analisi dei messaggi inviati e ricevuti, rendendo difficile la derivazione diretta della chiave di crittografia. Nonostante ciò, con un chip incorporato, l'hacker ha accesso fisico al dispositivo. Dati alcuni input e output, la misurazione della quantità di energia consumata durante l'elaborazione alla fine può rivelare la chiave crittografica.

Questi attacchi si chiamano attacchi del canale laterale. Dagli anni Novanta, l'industria delle smart card bancarie ha sviluppato numerose contromisure che non

rivelano chiavi crittografiche.

Il problema è che tali contromisure sono difficili da valutare. Non esiste un consenso sui metodi più adatti e finora non è stato possibile confrontare le varie valutazioni. Le valutazioni sono in genere complesse (perché gli attacchi sono sempre più sofisticati) e molto intense dal punto di vista dei calcoli, il che significa costose.

Migliore protezione

Il progetto REASSURE, finanziato dall'UE, ha sviluppato metodi migliori per valutare le contromisure contro l'hackeraggio dei dispositivi integrati. I dispositivi dell'Internet delle cose (IoT) sono ora obiettivi primari degli attacchi; tuttavia, i produttori di IoT non dispongono delle competenze e delle attrezzature necessarie per valutare le contromisure. Per aiutare i produttori, il progetto ha sviluppato strumenti di controllo automatico del codice per gli sviluppatori di IoT. I ricercatori hanno anche fornito una serie di strumenti software aggiuntivi, supportati dalla formazione.

Gli ingegneri hanno sviluppato strumenti specifici per le aziende che sviluppano dispositivi integrati e relative contromisure. Le aziende devono poter valutare internamente l'efficacia delle loro contromisure. Successivamente, l'azienda si reca in un laboratorio di valutazione, che valuterà in modo indipendente la resistenza del dispositivo agli attacchi del canale laterale. «Poiché questa valutazione esterna è costosa», spiega il dottor Francois Koeune, coordinatore del progetto, «è nell'interesse di entrambe le parti renderla il più efficace possibile».

I nuovi strumenti sono più affidabili dei precedenti metodi di valutazione e hanno maggiori probabilità di trovare i punti deboli. Gli strumenti aiutano anche il laboratorio indipendente a mantenere la certificazione per condurre tali valutazioni.

Miglioramento delle prestazioni

I partner industriali hanno implementato gli strumenti sviluppati durante il progetto, spesso arrivando a un significativo miglioramento. Nei casi migliori, gli strumenti hanno ridotto di 10 volte il numero di tracce necessarie per l'analisi e di 16 volte la potenza di calcolo necessaria. I nuovi strumenti hanno anche aiutato le rivalutazioni del prodotto necessarie dopo ogni debolezza di sicurezza rilevata. Utilizzando gli strumenti, un partner è stato in grado di saltare la metà dei test abituali senza originare alcuna perdita di sicurezza. Infine, gli strumenti si sono dimostrati più completi e nel 10 % dei casi di convalida interna hanno individuato violazioni della sicurezza non rilevabili in precedenza.

«Inoltre, uno standard ISO in questo settore è entrato nella fase di revisione durante

il nostro progetto», aggiunge Koeune. «Abbiamo pubblicato documenti che evidenziano quelli che riteniamo essere i punti deboli più rilevanti di questo standard». L'International Standards Organisation lo ha riconosciuto e aprirà lo standard per la revisione. Gli strumenti di REASSURE, oltre alla formazione per il loro utilizzo, rappresentano un importante sviluppo nella messa in sicurezza di questi dispositivi onnipresenti.

Parole chiave

REASSURE | strumenti | contromisure | dispositivi integrati | protezione | valutazione | hackeraggio | attacco del canale laterale

Scopri altri articoli nello stesso settore di applicazione

Strumenti digitali intelligenti aiutano l'industria alimentare europea ad affrontare gli elevati costi energetici

31 Maggio 2022

Proteggere i sistemi elettrici ed energetici dell'Europa

24 Febbraio 2023

Il GPS/GNSS basato su cloud traccia le posizioni utilizzando una quantità minima di energia

20 Gennaio 2023

Le comunità energetiche traggono vantaggi dalla flessibilità

14 Ottobre 2022

Informazioni relative al progetto

REASSURE

ID dell'accordo di sovvenzione: 731591

Sito web del progetto

DOI
10.3030/731591

Progetto chiuso

Data della firma CE
27 Novembre 2016

Data di avvio
1 Gennaio 2017

Data di completamento
31 Marzo 2020

Finanziato da
INDUSTRIAL LEADERSHIP - Leadership in enabling and industrial technologies - Information and Communication Technologies (ICT)

Costo totale
€ 3 528 635,00

Contributo UE
€ 3 478 747,50

Coordinato da
UNIVERSITE CATHOLIQUE DE LOUVAIN
Belgium

Ultimo aggiornamento: 7 Settembre 2020