Un approccio proattivo per garantire una sicurezza informatica a lungo termine

Per affrontare la crescente minaccia della sicurezza informatica, i progetti SHARCS e PQCRYPTO, finanziati dall'UE, stanno sviluppando paradigmi, architetture e software di sicurezza necessari per garantire che i nostri sistemi TIC siano sicuri e affidabili.

SICUREZZA

© Shutterstock

Nell'odierno mondo interconnesso, le nostre attività quotidiane dipendono sempre più spesso dalla sicurezza informatica. Spaziando dal settore bancario fino allo shopping online, la telemedicina, la comunicazione mobile, il cloud computing e l'internet delle cose, la società continua a mettere online una crescente quantità di informazioni riservate e private.

Con la minaccia della pirateria informatica in continua evoluzione, è essenziale che il settore pubblico e quello privato adottino un approccio proattivo alla sicurezza informatica. Per poterci riuscire, due progetti finanziati dall'UE, SHARCS e PQCRYPTO, stanno lavorando per sviluppare nuovi paradigmi, architetture e software di sicurezza per accertarsi che i nostri sistemi TIC siano sicuri e affidabili.

Occorrono metodi di crittografia aggiornati

Al giorno d'oggi, la maggior parte delle nostre informazioni in rete è protetta mediante algoritmi a chiave pubblica (RSA), logaritmi discreti su campi finiti o curve ellittiche. In pratica, questi sistemi generalmente forniscono una variazione sufficiente a garantire la sicurezza delle nostre comunicazioni in rete. Ma visto che la società si sta avvicinando all'uso dei grandi computer quantistici, l'applicabilità di questi sistemi

diventerà obsoleta.

Ad esempio, le informazioni riservate come i documenti sanitari e i segreti della sicurezza nazionale devono arrivare con un livello di sicurezza garantito. Tuttavia, quando sono memorizzate su un computer quantistico, l'uso di RSA o della crittografia basata su curve ellittiche non fornirà più protezione dalla pirateria informatica. Con l'UE e i governi nazionali che investono fortemente nello sviluppo dei computer quantistici, i ricercatori di SHARCS e PQCRYPTO avvertono che la società deve agire adesso per prepararsi alle conseguenze della sicurezza informatica legate all'era dell'informatica quantistica.

Flip Feng Shui dimostra i punti deboli

Per mettere in prospettiva la gravità di questa minaccia, gli esperti di pirateria informatica che collaborano con il progetto hanno usato una nuova tecnica di attacco non-software basata su bug per alterare la memoria di macchine virtuali ospitate sul cloud. Questa tecnica, chiamata Flip Feng Shui (FFS), consente all'aggressore di noleggiare una macchina virtuale sullo stesso host della vittima, permettendogli di decodificare le chiavi della macchina virtuale o di installare un malware senza essere notato. Con questo attacco, i pirati informatici possono non solo vedere e far trapelare dei dati, ma possono anche modificare i dati usando un errore nell'hardware. Di conseguenza, al server può essere ordinato di installare un software maligno e indesiderato e di consentire l'accesso a utenti non autorizzati.

In un attacco FFS, i ricercatori hanno ottenuto l'accesso alle macchine virtuali dell'host indebolendo le chiavi pubbliche OpenSSH con un solo bit. In un altro attacco, i ricercatori hanno modificato le impostazioni dell'applicazione di gestione software apt apportando dei cambiamenti marginali all'URL dove una apt scarica il software. Da qui, il server potrebbe installare un malware che è stato presentato come un aggiornamento del software.

Mitigare oggi le minacce di domani

Chiaramente, si deve lavorare ancora per garantire la sicurezza delle nostre informazioni online. Mediante questo unico test, i ricercatori hanno confutato l'opinione comune che i capovolgimenti dei bit dell'hardware abbiano un limitato potere pratico. Armati con primitive di comunicazione FFS, i ricercatori sono stati in grado di lanciare un attacco end-to-end incredibilmente potente, persino nella completa assenza di punti deboli nel software.

Per mitigare le minacce come ad esempio FFS e altre, vi è una continua necessità di nuovi metodi di verifica, certificazione dell'hardware e adattamenti delle esigenze software. Per queste ragioni, il progetto SHARCS sta progettando, costruendo e dimostrando delle applicazioni e dei servizi progettati per essere sicuri capaci di

realizzare la sicurezza end-to-end per gli utenti. Allo stesso tempo, il progetto PQCRYPTO sta lavorando a dei sistemi crittografici che sono sicuri non solo per le esigenze di oggi, ma anche contro gli attacchi a lungo termine presentati dai computer quantistici. Assieme, questi progetti forniranno una serie di sistemi ad alta sicurezza in grado di rispondere alle necessità in evoluzione della sicurezza informatica di dispositivi mobili, cloud computing e Internet delle cose.

Per maggiori informazioni, consultare:
Sito web del progetto SHARCS
Sito web del progetto PQCRYPTO

Paesi

Grecia, Paesi Bassi

Progetti correlati

PROGETTO

PQCRYPTO

Post-quantum cryptography for long-term security

7 Settembre 2023

PROGETTO

SHARCS

Secure Hardware-Software Architectures for Robust Computing Systems

5 Settembre 2023

Questo articolo è contenuto in...

RIVISTA RESEARCH*EU

Le applicazioni di Galileo – cosa ci attende

Articoli correlati

PROGRESSI SCIENTIFICI

È possibile prevenire gli attacchi informatici quantistici? Sì, secondo un'iniziativa dell'UE, che mostra anche come

26 Marzo 2020

NUOVI PRODOTTI E TECNOLOGIE

Nuovi strumenti e metodi per proteggere le infrastrutture critiche d'Europa

19 Maggio 2016

Tendenze scientifiche: Il dibattito sulla criptazione

22 Gennaio 2015

Ultimo aggiornamento: 6 Settembre 2016

Permalink: https://cordis.europa.eu/article/id/120147-a-proactive-approach-to-ensuring-longterm-cybersecurity/it