Securing the Internet of Things with a unique microchip fingerprinting technology

Risultati in breve

Metodi di identificazione innovativi proteggono i dispositivi IoT

I dispositivi IoT sono talmente insicuri da minacciare l'intera rete Internet. Ora, milioni di dispositivi legacy possono essere identificati e autenticati individualmente.

ECONOMIA DIGITALE

SICUREZZA

© Blue Planet Studio, Shutterstock

L'Internet delle cose (IoT) si riferisce a semplici dispositivi hardware collegati tramite Internet. Alcuni esempi includono videocamere per campanello, dispositivi di monitoraggio sanitario indossabili, allarmi antincendio e semafori urbani. Secondo alcune stime, il mondo potrebbe disporre di 50 miliardi di tali dispositivi entro il 2025 e di 1 000 miliardi entro il 2030.

Sebbene forniscano servizi convenienti, i dispositivi IoT sono molto insicuri e possono essere facilmente hackerati. I dispositivi hackerati possono essere creati per violare altri dispositivi. Queste situazioni minacciano la reputazione delle aziende e possono causare pericoli reali di vario genere per le persone. La vulnerabilità si verifica perché la memoria e la capacità di elaborazione dei dispositivi sono troppo basse per una sicurezza sofisticata.

La sostituzione di miliardi di dispositivi legacy con hardware aggiornati non è fattibile.

Tuttavia, il progetto INSTET, finanziato dall'UE, ha sviluppato un modo per proteggere i dispositivi IoT che evita tale sostituzione. L'attuale progetto ha migliorato la tecnologia di identificazione dei dispositivi sviluppata in un precedente progetto di studio di fattibilità relativo alla fase 1 dello Strumento per le PMI, recante lo stesso nome. Il nuovo progetto ha confermato il potenziale commerciale del concetto.

Ogni dispositivo viene fisicamente identificato

Il metodo innovativo assegna in primo luogo un identificatore a ogni dispositivo IoT, in base alle sue caratteristiche fisiche uniche. Gli identificatori fisici vengono derivati utilizzando algoritmi speciali che misurano le variazioni casuali generate nel processo di produzione dell'hardware, tramite una funzione fisica non clonabile sviluppata dal progetto: si parla in questo caso di biometria del silicio, che in sostanza rileva le «fingerprint» (impronte digitali) di ogni dispositivo IoT rendendone impossibile la falsificazione.

Una volta che ogni dispositivo è stato fornito di identificatore, questo deve essere autenticato prima di poter procedere a uno scambio sicuro di dati. In caso contrario, non è possibile garantire che i dispositivi stiano comunicando con la parte corretta. La capacità di verificare l'identità del dispositivo è ciò che consente di proteggere i dispositivi IoT semplici.

La funzione fisica non clonabile è una componente del sistema di sicurezza INSTET che migliora l'intero sistema di sicurezza con servizi di sicurezza di alto livello forti e non falsificabili. «Il vantaggio principale è che non è necessario programmare la chiave radice dall'esterno», afferma il coordinatore del progetto, Georgios Selimis. «Questo significa che la chiave rimane sempre all'interno e quindi è sempre al sicuro».

Semplici aggiornamenti del chip

Inoltre, la funzione fisica non clonabile si basa sui circuiti onnipresenti della memoria statica ad accesso casuale (SRAM). «Pertanto, il nostro approccio è scalabile a tutti i dispositivi IoT», aggiunge Selimis, «poiché la SRAM è un componente presente in tutti i microcontrollori, anche quelli a basso costo. Di conseguenza, siamo in grado di aggiornare quei milioni di dispositivi IoT installati sul campo, senza richiedere una riprogettazione dei prodotti». Questa è l'unica soluzione sul mercato in grado di fornire una forte sicurezza basata su hardware utilizzando soltanto software facilmente implementabile su dispositivi IoT con potenza di elaborazione limitata.

Il sistema si rivolge a tre segmenti IoT separati. INSTET Wearables fornisce sicurezza end-to-end (da punto a punto) per i dispositivi indossabili. INSTET Medical supporta il collegamento del software con l'hardware del dispositivo medico. Infine,

INSTET Critical Infrastructures supporta la connettività cloud IoT. I ricercatori hanno creato con successo diverse architetture software per ciascuna applicazione, creando e gestendo inoltre dimostratori per ogni segmento di mercato. Il personale del progetto ha sviluppato analisi di mercato dettagliate e piani di valorizzazione.

Successivamente, il consorzio si concentrerà sullo sviluppo di standard e regolamenti specifici per il mercato e il risultato sarà la chiusura di una delle principali debolezze della sicurezza che interessano i dispositivi IoT.

Parole chiave

INSTET | IoT | sicurezza | Internet delle cose | identificazione del dispositivo | funzione fisica non clonabile | biometria del silicio

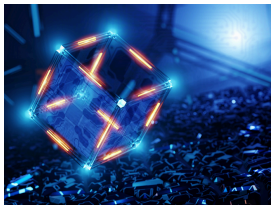
Scopri altri articoli nello stesso settore di applicazione

L'unico limite è il cielo per l'innovazione software flessibile e di facile utilizzo

6 Novembre 2020

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

31 Maggio 2022



Traguardo nell’entanglement di ioni intrappolati a oltre 200 metri di distanza

21 Febbraio 2023

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

20 Gennaio 2023

Informazioni relative al progetto

INSTET

ID dell’accordo di sovvenzione: 811509

Sito web del progetto

DOI
10.3030/811509

Progetto chiuso

Data della firma CE
30 Maggio 2018

Data di avvio
1 Giugno 2018

Data di completamento
31 Maggio 2020

Finanziato da
INDUSTRIAL LEADERSHIP - Innovation In SMEs

Costo totale
€ 2 496 362,50

Contributo UE
€ 1 747 453,75

Coordinato da
INTRINSIC ID BV
Netherlands

Ultimo aggiornamento: 6 Novembre 2020