HORIZON 2020

KEEPING YOUR CONNECTED SMART DEVICES PROTECTED AGAINST HACKERS AND CYBER ATTACKS

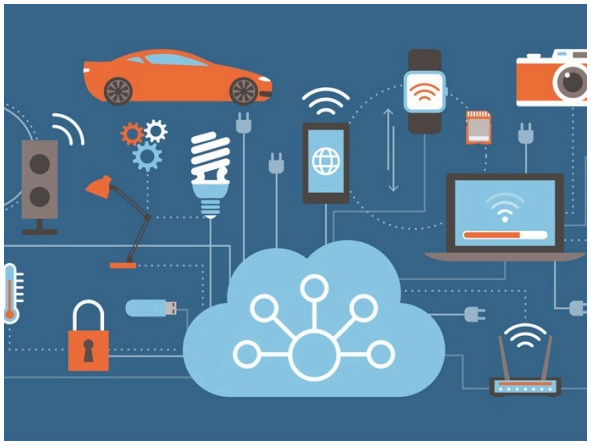
Risultati in breve

Dispositivi IoT protetti rimuovendo le credenziali statiche

Milioni di dispositivi dell'Internet delle cose (IoT) di vecchia concezione possono ora essere messi in sicurezza. La soluzione costruisce un guscio di sicurezza a 3 livelli, elimina le password fisse ed esegue il software di crittografia e autenticazione anche su semplici chip. L'auto-riparazione basata sull'intelligenza artificiale mantiene i sistemi IoT affidabili e sicuri.

ECONOMIA DIGITALE

SICUREZZA



© elenabsl, Shutterstock

L'IoT non è un internet a parte, ma significa invece corsie di internet su cui semplici dispositivi condividono i dati. Tra gli esempi di questi dispositivi vi sono le apparecchiature di fabbrica intelligenti, i tracciatori di inventario wireless, gli elettrodomestici intelligenti e gli scanner biometrici per la sicurezza informatica.

La connessione di tali dispositivi a Internet ha creato enormi e imprevedibili vulnerabilità legate alla sicurezza. I dispositivi IoT sono notoriamente vulnerabili alla pirateria informatica. Oltre a una lunga lista di vulnerabilità condivise con i server web, questi dispositivi soffrono anche di una scarsa autenticazione del dispositivo, dove le unità hackerate possono hackerare altri dispositivi. Questo problema si chiama computer zombie e porta

comunemente a impedire l'accesso al servizio. Un secondo grande punto debole dei dispositivi IoT è che sono troppo semplici da usare a livello informatico per eseguire un software di difesa dotato di crittografia. Fino a poco tempo fa, tali dispositivi non avevano essenzialmente alcuna protezione.

Gli attacchi costano alla società

Quasi la metà delle aziende che si occupano di dispositivi IoT ha subito gravi violazioni della sicurezza che hanno inciso sulle entrate. Poiché tali violazioni causano ormai oltre 5 000 miliardi di euro di perdite annuali, il settore IT ha iniziato a prendere sul serio il problema. Inoltre, la Commissione europea ha emanato il regolamento generale sulla protezione dei dati (GDPR) che, a partire dal 2018, ha iniziato a imporre pesanti multe alle aziende non conformi. Tuttavia, il raggiungimento di una reale sicurezza richiederà più di un semplice deterrente pecuniario.

Il progetto ELIoT Pro, finanziato dall'UE, ha sviluppato una soluzione affidabile, sostituendo un punto debole cruciale dell'IoT, quello delle password fisse, con una password monouso utilizzata nel protocollo di autenticazione degli amministratori di sistema dell'IoT, anche in caso di autenticazione e crittografia da dispositivo a dispositivo. Questi protocolli sono inoltre progettati per essere molto leggeri dal punto di vista informatico, adatti anche per dispositivi IoT semplici.

Addio alle credenziali statiche

«Le password e qualsiasi altra credenziale statica come la biometria, se non gestite correttamente, sono vulnerabilità ben note e ampiamente sfruttate», spiega il coordinatore del progetto Jack Wolosewicz. «L'ottanta per cento di tutti gli attacchi informatici si basa sullo sfruttamento di queste credenziali». Per evitare questo, il team del progetto ha eliminato la necessità di tali credenziali e la vulnerabilità associata, sostituendole invece con token di transazione monouso che scadono entro 200 millisecondi. Senza password gli hacker non hanno nulla da rubare. In questo modo si neutralizzano i rischi di attacchi di phishing o gli attacchi «man in the middle». Solo in questo modo si elimina l'80 % di tutte le minacce nelle comunicazioni uomo-macchina, come quelle tra un amministratore di sistema e i pannelli di controllo IoT.

Il protocollo di cifratura del progetto elimina il restante 20 % di minacce. Il protocollo fornisce una forte crittografia che riesce comunque a funzionare su dispositivi molto semplici. Ciò si ottiene utilizzando una soluzione software che assicura la trasmissione dei dati e l'autenticazione dei dispositivi per le comunicazioni tra macchina e macchina.

Un altro aspetto del sistema ELIoT Pro è l'auto-riparazione, ottenuta attraverso

l’analisi predittiva dell’intelligenza artificiale. In questo modo, il sistema è in grado di rilevare attività anomale, compresi gli attacchi informatici, ed è anche in grado di anticipare i guasti del dispositivo o del sistema.

«Il concetto di ELIoT Pro lo rende una soluzione universale per il networking dell’IoT», aggiunge Wolosewicz, «indipendentemente dal settore. Il nostro sistema viene utilizzato nelle applicazioni industriali dell’IoT, negli edifici intelligenti, nelle case intelligenti e nelle città intelligenti. Non esiste una soluzione all-inclusive paragonabile alla nostra». Il team del progetto ha quindi concluso accordi con le principali aziende di ciascuno di questi settori. In seguito, i ricercatori cercheranno di ottenere un maggior numero di accordi di questo tipo, lavorando al tempo stesso al ramo vendite e commercializzazione del progetto.

Parole chiave

ELIoT Pro | IoT | crittografia | password | credenziali statiche | sicurezza | Internet delle cose | password monouso | token di transazione | intelligenza artificiale | autoguarigione

Scopri altri articoli nello stesso settore di applicazione

Combattere gli incendi boschivi in modo integrato

6 Agosto 2024

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

31 Maggio 2022

Rafforzare la sicurezza informatica contro le minacce emergenti nelle città intelligenti

31 Gennaio 2025

Edifici stampati in 3D prossimi alla realizzazione

30 Marzo 2020

Informazioni relative al progetto

ELIoT Pro

ID dell’accordo di sovvenzione: 822641

Sito web del progetto

DOI
10.3030/822641

Progetto chiuso

Data della firma CE
13 Settembre 2018

Data di avvio
1 Giugno 2018

Data di completamento
31 Maggio 2020

Finanziato da
INDUSTRIAL LEADERSHIP - Innovation In SMEs

Costo totale
€ 2 827 625,00

Contributo UE
€ 1 979 337,50

Coordinato da
CYBERUS LABS
Poland

Ultimo aggiornamento: 30 Ottobre 2020

Permalink: https://cordis.europa.eu/article/id/422562-iot-devices-secured-by-removing-static-credentials/it