Advanced Networked Agents for Security and Trust Assessment in CPS/IOT Architectures

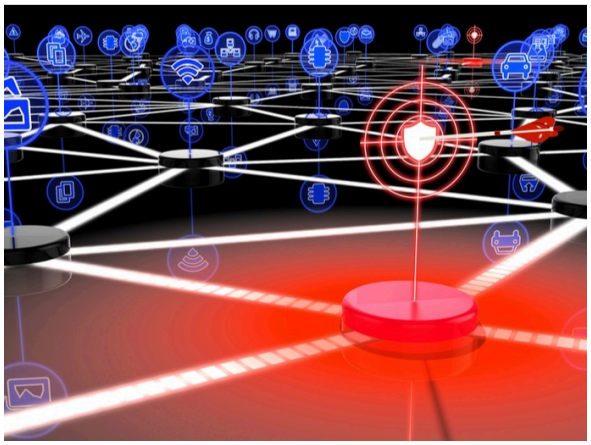
Risultati in breve

Un quadro di riferimento per la privacy e la sicurezza affronta la sicurezza informatica

I sistemi ciberfisici (CPS, Cyber-Physical Systems) basati sull'Internet delle cose (IoT) e sulle architetture di cloud virtualizzate presentano rischi nuovi e inattesi che non possono essere completamente risolti dalle attuali soluzioni di avanguardia. Un'iniziativa dell'UE ha introdotto una soluzione che fornisce la massima sicurezza e fiducia.

ECONOMIA DIGITALE

SICUREZZA



© BeeBright, Shutterstock

Sono richiesti nuovi paradigmi e metodi per costruire sin da subito la sicurezza all'interno di un sistema TIC, per adattarsi alle mutevoli condizioni di sicurezza e ridurre l'esigenza di correggere i difetti successivi alla distribuzione, nonché per fornire garanzie sulla sua sicurezza e affidabilità in ogni momento. Il progetto ANASTACIA ha affrontato queste preoccupazioni attraverso la ricerca, lo sviluppo, la dimostrazione e la convalida di una soluzione olistica che consenta fiducia e sicurezza sin dalla progettazione, per CPS eterogenei, distribuiti e ad evoluzione dinamica.

Affrontare la crescente vulnerabilità delle TIC di oggi

«A tal fine, abbiamo sviluppato un quadro per la sicurezza e la privacy che affronta la complessità delle architetture IoT e la natura diversa dei potenziali attacchi», spiega il coordinatore Stefano Bianchi. Ciò è stato fatto per prendere decisioni autonome utilizzando nuove tecnologie di rete, quali la rete definita dal software (SDN, Software-Defined Networking) e la virtualizzazione delle funzioni di rete (NFV, Network Function Virtualisation), nonché un'attuazione intelligente e dinamica della sicurezza e tecnologie e strumenti di monitoraggio.

Il progetto si è basato sulle funzionalità SDN e NVF per incorporare i prodotti di sicurezza sviluppati e fornire un modo dinamico per distribuirli quando necessario. L'SDN e l'NFV forniscono inoltre una soluzione sicura per CPS e IoT altamente connessi. «Proponendo un quadro conforme alla sicurezza e alla privacy per rendere sicure le complesse architetture CPS e IoT, ANASTACIA abbraccerà numerosi settori e ambiti di applicazione delle TIC di diverso tipo», commenta Bianchi.

Il quadro include un paradigma di sviluppo della sicurezza basato sulla conformità per garantire le migliori prassi e l'uso di componenti e facilitatori della sicurezza, nonché un marchio dinamico di sicurezza e privacy (DSPS, Dynamic Security and Privacy Seal) olistico che combina le normative di sicurezza e privacy quali il regolamento generale sulla protezione dei dati e gli standard ISO con il monitoraggio e la verifica online in tempo reale. Esso comprende inoltre una suite di componenti e facilitatori distribuiti per la fiducia e la sicurezza in grado di orchestrare e sviluppare, in modo dinamico, politiche di sicurezza degli utenti e azioni resilienti con una valutazione del rischio all'interno di architetture CPS e IoT complesse e dinamiche.

Pianificazione, attuazione e strategie di monitoraggio intelligenti nel campo della sicurezza

Le parti interessate coinvolte direttamente dal tema della sicurezza informatica e dagli aspetti di privacy ne beneficeranno. Gli architetti di soluzioni e software, gli analisti e i responsabili di progetto trarranno vantaggio dal paradigma di sviluppo della sicurezza, mentre gli sviluppatori e gli integratori sfrutteranno appieno i componenti e i facilitatori di fiducia e sicurezza distribuiti. Il DSPS sarà sfruttato dai responsabili delle informazioni, dai responsabili della sicurezza e dai responsabili della protezione delle informazioni.

«ANASTACIA ha sviluppato metodologie e strumenti per fornire garanzie appropriate sul fatto che i sistemi TIC sviluppati siano mantenuti sicuri e affidabili e soddisfino le esigenze dei livelli certificati di garanzia, dove la sicurezza è considerata la preoccupazione principale», conclude Bianchi. «In definitiva le soluzioni sono pensate per liberare gli utenti finali dall'onere di controllare in continuazione lo stato di sicurezza e la conformità alla privacy di un'infrastruttura CPS e IoT monitorata»

Il quadro contribuirà inoltre ad aumentare la consapevolezza sulle minacce informatiche e le problematiche di privacy e fornirà soluzioni utilizzabili per mettere in pratica gli approcci metodologici, nonché per incrementare il livello di sicurezza informatica e privacy all'interno del mercato unico digitale dell'UE.

Parole chiave

ANASTACIA | sicurezza | privacy | CPS | IoT | fiducia | sicurezza informatica | SDN | NFV

Scopri altri articoli nello stesso settore di applicazione

Mettere l'Europa in prima linea nella rivoluzione del supercalcolo

4 Maggio 2023

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

31 Maggio 2022

Una soluzione intelligente per superare in astuzia le minacce cibernetiche

20 Luglio 2018

L'applicazione personalizzata basata su IA che insegna le lingue straniere a livello di conversazione

20 Marzo 2020

Informazioni relative al progetto

ANASTACIA

ID dell'accordo di sovvenzione: 731558

Sito web del progetto

DOI
10.3030/731558

Progetto chiuso

Data della firma CE
27 Novembre 2016

Data di avvio
1 Gennaio 2017

Data di completamento
31 Dicembre 2019

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

Costo totale
€ 5 420 208,75

Contributo UE
€ 3 999 208,75

Coordinato da
ALGOWATT SPA
Italy

Ultimo aggiornamento: 7 Agosto 2020