FONDAZIONE BRUNO KESSLER
MAGAZINE

Verso l’identità digitale europea

22 Maggio 2023

I ricercatori del Centro per la Cybersecurity di FBK Giada Sciarretta e Amir Sharif sono stati invitati a partecipare, tramite il Dipartimento per la Trasformazione Digitale, a collaborare sul tavolo dell’Expert Group eIDAS per l’elaborazione delle specifiche dell’EUDI Wallet.

Il Centro FBK-Cybersecurity propone soluzioni per affrontare le sfide poste dai rischi emergenti e per cogliere le opportunità generate dallo sviluppo di infrastrutture per la gestione dell’identità digitale, fattore abilitante per la fruizione sicura e rispettosa della privacy dei servizi online offerti ai cittadini da aziende e istituzioni pubbliche.

Lo sviluppo di infrastrutture per la gestione dell’identità digitale porta numerosi **vantaggi**, i più importanti dei quali sono i seguenti:

- fornire agli utenti un’esperienza di identificazione ed autenticazione comune a tutti quei servizi che utilizzano la stessa infrastruttura di gestione dell’identità digitale;
- dare la possibilità
    - a chi offre servizi di focalizzarsi sullo sviluppo di nuove funzionalità e applicazioni senza doversi occupare della base degli utenti e
    - agli sviluppatori dell’infrastruttura di identità digitale di concentrarsi sulla gestione del ciclo di vita degli utenti permettendo di ottimizzare gli investimenti in termini di budget e competenze sia per i gestori dei servizi che dell’identità digitale.

Insieme ai vantaggi, la gestione dell’identità digitale porta con sé una serie di rischi come ad esempio:

- **insicurezza**—una vulnerabilità dell’infrastruttura può avere conseguenze catastrofiche se sfruttata in un attacco che permette, ad esempio, l’esfiltrazione di dati personali che possono successivamente essere usati come base di partenza per furti di identità e
- **mancanza di privacy**—la gestione dei dati da parte dell’infrastruttura deve tenere in massima considerazione la privacy degli utenti poiché tali dati, se non adeguatamente protetti, potrebbero essere usati per attività di profilazione su larga scala supportando il modello di mass surveillance con conseguenze fortemente negative per i diritti fondamentali e la libertà delle persone.

Obiettivo e attività di ricerca del Centro FBK per la Cybersecurity

Diventa quindi fondamentale progettare, sviluppare e implementare le infrastrutture per l'identità digitale in modo tale da garantire sicurezza e privacy. A tal fine, il **Centro per la Cybersecurity di FBK** sviluppa metodologie applicabili durante tutto il ciclo di sviluppo delle infrastrutture per la gestione dell'identità digitale supportate da strumenti automatici per l'analisi e la valutazione dei rischi di sicurezza e privacy. L'uso di strumenti automatici permette di valutare, velocemente e in maniera tracciabile, diverse alternative sin dal concepimento dell'infrastruttura e in seguito passare a vagliare diverse architetture e protocolli crittografici per lo scambio dei dati fino ad eseguire test di sicurezza esaustivi sull'infrastruttura in produzione. Tutto questo sarebbe impossibile senza la componente automatica che permette anche di tracciare in maniera precisa e verificabile le scelte di progetto, sviluppo, implementazione e configurazione fatte per rendere maggiormente trasparente l'infrastruttura finale semplificando processi di audit da parte di vari stakeholder includendo esperti nominati dalle associazioni in difesa dei diritti di cittadini e consumatori nonché delle autorità di controllo nazionale (come ad esempio ACN o **AgID**) o internazionali (come la **Commissione Europea**).

Attività di innovazione del Centro FBK per la Cybersecurity.

La conferma della rilevanza dei contributi del Centro viene dalle pubblicazioni in conferenze e riviste internazionali di cybersecurity. A completare la validazione delle tecniche sviluppate dal Centro vi sono le numerose attività progettuali di co-progettazione e sviluppo di soluzioni per la gestione dell'identità digitale con varie realtà tra le quali

- il **Poligrafico e Zecca dello Stato (IPZS)** per lo sviluppo di metodologie per la progettazione sicura di infrastrutture per l'autenticazione basate sulla Carta d'Identità Elettronica (CIE) 3.0 (come il bottone ??Entra con CIE?? per accedere ai servizi della Pubblica Amministrazione Italiana) e
- varie organizzazione pubbliche e private all'interno del progetto Europeo ??Large Scale Pilot EUDI Wallet?? POTENTIAL che ha l'obiettivo di costruire la nuova infrastruttura dell'identità digitale Europea in conformità con la nuova versione della regolamentazione **eIDAS 2.0**.

Per il Centro FBK per la Cybersecurity, vi sono due grandi **sfide di ricerca e innovazione**, tra le tante poste dallo sviluppo sicuro di infrastrutture per l'identità digitale, che emergono come particolarmente importanti:

- al fine di integrare meccanismi di autenticazione per la fruizione sicura di servizi sensibili come quelli per i pagamenti o la gestione dei dati sanitari, un pre-requisito fondamentale è minimizzare i rischi cyber in fase di identificazione (anche detta onboarding) durante la quale si verifica che un utente è veramente chi dice di essere e si rilasciano le credenziali che verranno successivamente utilizzate in fase di autenticazione. Data la spinta alla digitalizzazione di molti processi della Pubblica Amministrazione (soprattutto sanitari) e dei privati (come quelli bancari) velocizzata dalla pandemia di COVID-19, anche i processi di identificazione sono stati digitalizzati senza il vincolo della presenza (ad esempio, è possibile creare un conto corrente senza recarsi fisicamente nella filiale di una banca). Questa trasformazione ha portato all'introduzione di nuovi attacchi alle procedure di identificazione da remoto che possono portare al furto di identità con conseguenze potenzialmente catastrofiche per l'utente che ne è vittima. Ad esempio, molti processi usano frammenti video per confrontare il viso della persona che richiede la creazione dell'identità digitale con l'immagine associata al documento di identità presentato: le moderne tecniche di manipolazione delle immagini anche video (ad esempio i deep fake) riescono ad incollare

virtualmente il viso della vittima cui si e sottratto un documento d'identità in maniera dinamica in modo tale da rendere difficile per algoritmi di controllo dell'immagine od un operatore umano reperire tali manipolazioni. Il Centro sta sviluppando tecniche per la rilevazioni di questo tipo di minacce e di altre che possono mettere in pericolo il processo di identificazione, fornendo una classificazione completa delle minacce e delle relative mitigazioni, sviluppando al contempo tecniche automatiche per la valutazione dei rischi in modo tale da aiutare chi sviluppa questi processo a definire la configurazione di mitigazioni che offra il livello desiderato di sicurezza;

- nel breve, medio e lungo termine bisognerà integrare l'infrastruttura per la gestione dell'identità digitale con il crescente e sempre più articolato e complesso ecosistema di servizi e applicazioni offerto dalla **Pubblica Amministrazione Italiana ed Europea** al fine di sfruttare appieno i vantaggi offerti dalla **digitalizzazione dei processi**. Questo deve essere fatto tenendo conto dei diversi livelli di maturazione delle infrastrutture per l'identità digitale presenti nei vari Stati Membri in modo tale da non imporre brusche transizioni ai cittadini. In altre parole, bisognerà capire come gestire il transitorio da infrastrutture basate su un modello centralizzato attualmente disponibili al modello decentralizzato basato su **EUDI Wallet** previsto dalla nuova versione di eIDAS (2.0). In particolare, si dovrà capire se le attuali infrastrutture dovranno essere completamente rimpiazzate a tendere oppure parte di esse (ad esempio quei servizi per il rilascio di attributi certificati come la patente di guida) possano essere mantenute e integrate nelle nuove.

LINK

https://magazine.fbk.eu/it/news/verso-lidentita-digitale-europea/

TAG

- #cybersicurezza

VIDEO COLLEGATI

- https://www.youtube.com/watch?v=-sgJJv9kBao

MEDIA COLLEGATI

- FBK-Cybersecurity: https://www.fbk.eu/it/cybersecurity/

AUTORI

- Giancarlo Sciascia