Istituto Tecnico Industriale "G. Ferraris"

Classe 4D - Sistemi e Reti / Educazione Civica

Elaborato finale

Traccia 3: Identità digitale, autenticazione e fiducia nelle reti

Studente: Capuzzo Nicolò

Anno scolastico 2024/2025

Approfondimento sui Metodi di Autenticazione Digitale

Introduzione all'Autenticazione Digitale

Nel contesto attuale, l'autenticazione digitale è diventata un pilastro fondamentale per la sicurezza informatica di individui, aziende e istituzioni. Ogni giorno, milioni di persone accedono a servizi online – dalla scuola al lavoro, fino alle piattaforme di e-commerce – e la verifica dell'identità è il primo passo per garantire la protezione dei dati personali e delle transazioni.

I principali metodi di autenticazione

L'autenticazione digitale si basa su diversi metodi, che possono essere combinati tra loro per aumentare il livello di sicurezza. I metodi più diffusi sono:

- **Autenticazione basata su password**
- **Autenticazione biometrica**
- **Autenticazione tramite certificato**
- **Autenticazione a due o più fattori (2FA/MFA)**
- **Autenticazione tramite token**
- **Autenticazione federata (SSO, OpenID Connect)**
- **Passkey e autenticazione passwordless**

Autenticazione basata su password

È il metodo più tradizionale e ancora oggi il più diffuso. Consiste nell'inserire una combinazione di nome utente e password per accedere a un servizio. Le password dovrebbero essere lunghe, complesse e uniche per ogni account, ma spesso gli utenti tendono a riutilizzare le stesse password o a sceglierne di troppo semplici, aumentando il rischio di furto di credenziali. Per questo motivo, molte organizzazioni stanno passando a sistemi più sicuri.

Autenticazione biometrica

L'autenticazione biometrica utilizza caratteristiche fisiche o comportamentali uniche dell'individuo per verificarne l'identità. Tra i metodi più comuni troviamo:

- **Impronta digitale:** Il sistema confronta l'impronta dell'utente con quella registrata in precedenza. È uno dei sistemi più intuitivi e diffusi, grazie anche alla presenza di sensori sugli smartphone di ultima generazione.
- **Riconoscimento facciale:** Analizza i tratti del volto dell'utente. È comodo, ma può avere limiti in caso di gemelli, foto o cambiamenti nell'aspetto.
- **Scanner dell'iride o della retina:** Utilizza i pattern unici presenti nell'occhio. È molto sicuro, ma meno diffuso per via dei costi e della necessità di dispositivi specifici.
- **Riconoscimento vocale:** Analizza il timbro e le caratteristiche della voce.

La biometria è sempre più utilizzata non solo da aziende e aeroporti, ma anche nella vita quotidiana, ad esempio per sbloccare lo smartphone o autorizzare pagamenti digitali.

Autenticazione tramite certificato digitale

Questa modalità utilizza certificati digitali, che rappresentano una sorta di "passaporto elettronico" rilasciato da un'autorità di certificazione. Il certificato contiene una chiave pubblica e la firma digitale dell'autorità, garantendo che l'identità dell'utente sia stata verificata. È molto usata in ambito aziendale e nella Pubblica Amministrazione, ad esempio per accedere a servizi tramite la Carta d'Identità Elettronica o la firma digitale.

Autenticazione a due o più fattori (2FA/MFA)

Per aumentare la sicurezza, spesso si combinano due o più metodi di autenticazione. Ad esempio, oltre alla password, si richiede un codice temporaneo inviato via SMS o generato da un'app, oppure una verifica biometrica. L'autenticazione a più fattori (MFA) è oggi considerata una best practice per proteggere gli account da accessi non autorizzati

Autenticazione tramite token

I token sono dispositivi fisici o virtuali che generano codici temporanei (TOTP) validi solo per pochi secondi. L'utente deve inserire questo codice insieme alla password per accedere al servizio. I token possono essere hardware (come le chiavette delle banche) o software (app per smartphone).

Autenticazione federata: SSO, OAuth e OpenID Connect

L'autenticazione federata permette di accedere a più servizi utilizzando un solo set di credenziali. Ad esempio, grazie al Single Sign-On (SSO) o a protocolli come OpenID Connect e OAuth 2.0, è possibile usare l'account Google o Facebook per autenticarsi su altri siti, senza dover creare nuove password ogni volta. Questo sistema semplifica la vita agli utenti e riduce il rischio di password deboli..

Passkey e autenticazione passwordless

Le passkey sono un nuovo metodo di autenticazione che elimina completamente la necessità di password. Si basano su dati biometrici o chiavi crittografiche memorizzate su dispositivi sicuri, come smartphone o computer. L'utente si autentica con l'impronta digitale o il volto, e il sistema verifica la sua identità senza mai trasmettere la password.

L'evoluzione dell'identità digitale e la gestione centralizzata

Identity Management System (IMS)

Con la crescita esponenziale dei servizi digitali, la gestione delle identità è diventata sempre più complessa. Le aziende e le istituzioni utilizzano sistemi di Identity Management (IMS) per creare, gestire e proteggere le identità digitali degli utenti Questi sistemi permettono di:

-Automatizzare la creazione e la cancellazione degli account
-Gestire i permessi di accesso in base al ruolo dell'utente
-Integrare la verifica biometrica o documentale (KYC)
-Monitorare e registrare tutte le attività per garantire la compliance alle normative

I sistemi più avanzati offrono dashboard intuitive, reportistica dettagliata e la possibilità di integrare diversi servizi (Active Directory, Google Workspace, ecc.) da un'unica console

Blockchain e identità digitale

Una delle innovazioni più interessanti degli ultimi anni è l'uso della blockchain per la gestione dell'identità digitale. Grazie alla sua natura decentralizzata e immutabile, la blockchain permette di certificare in modo sicuro e trasparente i dati di identità. Un esempio è il Soulbound Token, che lega in modo permanente un'identità digitale a una transazione sulla blockchain, rendendo impossibile la falsificazione o la perdita dei dati.

Sicurezza, rischi e best practice

I rischi dell'identità digitale

L'identità digitale, se non protetta adeguatamente, può essere oggetto di furto, truffe e attacchi informatici. Secondo recenti rapporti, l'81% dei data breach è causato da credenziali trafugate o troppo deboli. I settori più colpiti sono la Pubblica Amministrazione, la sanità e il settore finanziario, ma nessuno è davvero al sicuro.

Come proteggere l'identità digitale

Per difendersi dai rischi, è importante adottare alcune best practice:

- Utilizzare password lunghe, complesse e diverse per ogni servizio
- Attivare sempre l'autenticazione a due o più fattori
- Non condividere mai le proprie credenziali
- Aggiornare regolarmente i software e le app
- Prestare attenzione ai tentativi di phishing e alle email sospette
- Utilizzare password manager per gestire in modo sicuro le proprie credenziali

Le aziende, oltre a formare il personale, dovrebbero implementare sistemi di monitoraggio, backup e ripristino delle identità digitali, e adottare tecnologie avanzate come la crittografia e la blockchain per rafforzare la sicurezza.

Il ciclo di vita dell'identità digitale

Il processo di gestione dell'identità digitale si articola in tre fasi principali:

1. **Creazione:** L'utente fornisce i propri dati personali a un identity provider, che li verifica tramite documenti o riconoscimento biometrico.
2. **Verifica:** L'autorità controlla l'autenticità dei dati e assegna all'utente un profilo digitale con credenziali univoche.
3. **Utilizzo:** L'utente accede ai servizi online tramite le credenziali fornite, che possono essere password, PIN, impronta digitale, riconoscimento facciale, ecc.

Ogni fase deve essere protetta da sistemi di sicurezza avanzati per evitare furti o manipolazioni.

Implicazioni sociali ed etiche

L'uso diffuso dell'identità digitale solleva importanti questioni etiche e sociali. Da un lato, permette una maggiore inclusione digitale e semplifica l'accesso ai servizi, dall'altro può creare nuove forme di esclusione per chi non ha accesso alle tecnologie o non possiede le competenze necessarie. È fondamentale garantire che i sistemi siano accessibili a tutti e che la privacy degli utenti sia sempre rispettata.

Le tecnologie biometriche, in particolare, pongono problemi legati alla raccolta e conservazione di dati estremamente sensibili. È necessario che le aziende e le istituzioni adottino politiche trasparenti e rispettino le normative sulla protezione dei dati personali (come il GDPR)

Riferimenti espliciti agli standard del settore

La PKI e il sistema SPID si basano su standard internazionali riconosciuti quali:

- X.509: standard per i certificati digitali.
- RFC 5280: profilo per i certificati X.509.
- eIDAS Regulation (EU) 910/2014: regolamento europeo per l'identificazione elettronica e i servizi fiduciari.
- ISO/IEC 27001: standard per la gestione della sicurezza delle informazioni.
- NIST SP 800-63: linee guida per l'autenticazione digitale e la gestione delle identità.

Questi standard garantiscono interoperabilità, sicurezza e conformità legale a livello europeo e internazionale

Caso studio reale: Implementazione della PKI nella federazione SPID italiana

La federazione SPID, gestita da AgID, è un caso concreto di applicazione della PKI per l'identità digitale. Dal 2016, SPID ha consentito a milioni di cittadini italiani di accedere in modo sicuro ai servizi pubblici online.

Fonti attendibili:

-Documento ufficiale AgID "Infrastruttura PKI Agid della federazione SPID" (2020)

-Rapporto annuale AgID sullo stato di SPID (2023)

-Studi di settore come quelli di Namirial e Entrust sulle soluzioni PKI in Italia

La federazione SPID ha dimostrato come una PKI ben progettata possa garantire sicurezza, scalabilità e facilità d'uso, integrando più Identity Provider e servizi pubblici e privati.

Analisi critica delle soluzioni proposte

Vantaggi:

-Sicurezza elevata: la gerarchia PKI e l'uso di chiavi crittografiche garantiscono autenticazione forte e protezione dei dati.

.

-Interoperabilità: grazie agli standard internazionali, SPID funziona con molteplici servizi e provider.

-Flessibilità: diversi livelli di sicurezza permettono di adattare l'autenticazione alle esigenze dell'utente e del servizio.

-Non ripudiabilità: le firme digitali garantiscono l'integrità e l'autenticità delle transazioni.

Limiti:

-Complessità tecnica: la gestione della PKI richiede infrastrutture e competenze elevate.

-Dipendenza da infrastrutture centrali: la sicurezza si basa sulla protezione della Root CA, che rappresenta un punto critico.

- Accessibilità: l'uso di smart card o dispositivi NFC può essere limitante per utenti con minori competenze tecnologiche o senza dispositivi adeguati.

-Costi di gestione: mantenere e aggiornare la PKI può essere oneroso per le istituzioni.

.

Conclusioni

L’identità digitale è ormai parte integrante della nostra vita quotidiana. La sua gestione richiede attenzione, consapevolezza e l’adozione di tecnologie avanzate per garantire sicurezza e privacy. Solo attraverso una combinazione di metodi di autenticazione robusti, sistemi di gestione centralizzati e un approccio etico e inclusivo, sarà possibile sfruttare appieno i vantaggi della trasformazione digitale, riducendo al minimo i rischi.