Tecniche di Autenticazione

Indice

- Tecniche di autenticazione e multi-factor authentication
- Protocolli di autenticazione
- Gestione delle password e dei certificati
- Modelli e tecniche per autorizzazione e controllo dell’accesso
- Privileged Identity and Access Management (PAM)
- Cenni sulla segregazione e segmentazione delle reti

Indice

- Tecniche di autenticazione e multi-factor authentication
- Protocolli di autenticazione
- Gestione delle password e dei certificati.
- Modelli e tecniche per autorizzazione e controllo dell’accesso
- Privileged Identity and Access Management (PAM)
- Cenni sulla segregazione e segmentazione delle reti

Autenticazione

- Verifica della **identità** di individui o applicazioni che **chiedono** l'**accesso** a un sistema informatico
- Il soggetto che ha richiesto l'accesso dichiara la sua identità e il sistema deve **provarne** l'**autenticità**
- E' l'atto che consente di stabilire un legame di **fiducia** fra il sistema e il soggetto che ha chiesto l'accesso

Definizione NIST

Autenticazione

- Verifica della **identità** di individui o applicazioni che **chiedono** l'**accesso** a un sistema informatico
- Il soggetto che ha richiesto l'accesso dichiara la sua identità e il sistema deve **provarne** l'**autenticità**
- E' l'atto che consente di stabilire un legame di **fiducia** fra il sistema e il soggetto che ha chiesto l'accesso

Definizione NIST

Autenticazione

- Verifica della **identità** di individui o applicazioni che **chiedono** l'**accesso** a un sistema informatico
- Il soggetto che ha richiesto l'accesso dichiara la sua identità e il sistema deve **provarne** l'**autenticità**
- E' l'atto che consente di stabilire un legame di **fiducia** fra il sistema e il soggetto che ha chiesto l'accesso

Definizione NIST

Identità e fattori di autenticazione

- Qualcosa che si **conosce**
  un segreto, come una parola d'ordine, un codice, ecc.
- Qualcosa che si **possiede**
  tessera, chiave, ecc.
- Qualcosa che ci **caratterizza** come individuo
  impronta digitale, volto, altri tratti biometrici

- Autenticazione multifattore
  ad es., tessera + codice

Identità e fattori di autenticazione

- Qualcosa che si **conosce**
  un segreto, come una parola d'ordine, un codice, ecc.
- Qualcosa che si **possiede**
  tessera, chiave, ecc.
- Qualcosa che ci **caratterizza** come individuo
  impronta digitale, volto, altri tratti biometrici

- Autenticazione multifattore
  ad es., tessera + codice

Identità e fattori di autenticazione

- Qualcosa che si **conosce**
  un segreto, come una parola d'ordine, un codice, ecc.
- Qualcosa che si **possiede**
  tessera, chiave, ecc.
- Qualcosa che ci **caratterizza** come individuo
  impronta digitale, volto, altri tratti biometrici

- Autenticazione multifattore
  ad es., tessera + codice

Identità e fattori di autenticazione

- Qualcosa che si **conosce**
  un segreto, come una parola d'ordine, un codice, ecc.
- Qualcosa che si **possiede**
  tessera, chiave, ecc.
- Qualcosa che ci **caratterizza** come individuo
  impronta digitale, volto, altri tratti biometrici

- Autenticazione multifattore
  ad es., tessera + codice

Sicurezza dei fattori di autenticazione

- Si può valutare in base al modello del rischio (*threat model*) STRIDE proposto da Microsoft

Spoofing	Falsificazione
Tampering	Manomissione
Repudiation	Disconoscimento
Information Disclosure	Rivelazione di segreti
Denial of Service	Blocco del servizio
Elevation of Privilege	Aumento di privilegi

Sicurezza dei fattori di autenticazione

- Si può valutare in base al modello del rischio (*threat model*) STRIDE proposto da Microsoft

Spoofing	Falsificazione
Tampering	Manomissione
Repudiation	Disconoscimento
Information Disclosure	Rivelazione di segreti
Denial of Service	Blocco del servizio
Elevation of Privilege	Aumento di privilegi

Sicurezza dei fattori di autenticazione

- Si può valutare in base al modello del rischio (*threat model*) STRIDE proposto da Microsoft

Spoofing	Falsificazione
Tampering	Manomissione
Repudiation	Disconoscimento
Information Disclosure	Rivelazione di segreti
Denial of Service	Blocco del servizio
Elevation of Privilege	Aumento di privilegi

Sicurezza dei fattori di autenticazione

- Si può valutare in base al modello del rischio (*threat model*) STRIDE proposto da Microsoft

Spoofing	Falsificazione
Tampering	Manomissione
Repudiation	Disconoscimento
Information Disclosure	Rivelazione di segreti
Denial of Service	Blocco del servizio
Elevation of Privilege	Aumento di privilegi

Sicurezza dei fattori di autenticazione

- Si può valutare in base al modello del rischio (*threat model*) STRIDE proposto da Microsoft

Spoofing	Falsificazione
Tampering	Manomissione
Repudiation	Disconoscimento
Information Disclosure	Rivelazione di segreti
Denial of Service	Blocco del servizio
Elevation of Privilege	Aumento di privilegi

Sicurezza dei fattori di autenticazione

- Si può valutare in base al modello del rischio (*threat model*) STRIDE proposto da Microsoft

Spoofing	Falsificazione
Tampering	Manomissione
Repudiation	Disconoscimento
Information Disclosure	Rivelazione di segreti
Denial of Service	Blocco del servizio
Elevation of Privilege	Aumento di privilegi

Sicurezza dei fattori di autenticazione

- Si può valutare in base al modello del rischio (*threat model*) STRIDE proposto da Microsoft

- **S**poofing
- **T**ampering
- **R**epudiation
- **I**nformation Disclosure
- **D**enial of Service
- **E**levation of Privilege

- Falsificazione
- Manomissione
- Disconoscimento
- Rivelazione di segreti
- Blocco del servizio
- Aumento di privilegi

Sicurezza autenticazione

Pericoli

- Spoofing
- Tampering
- Repudiation
- Information Disclosure
- Denial of Service
- Elevation of Privilege

Esempio

- Furto di identità
- Mascheramento
- Prove per tentativi

Sicurezza autenticazione

Pericoli

- Spoofing
- Tampering
- Repudiation
- Information Disclosure
- Denial of Service
- Elevation of Privilege

Esempio

- Modifica del fattore memorizzato sul sistema informatico

Sicurezza autenticazione

Pericoli

- Spoofing
- Tampering
- Repudiation
- Information Disclosure
- Denial of Service
- Elevation of Privilege

Esempio

- Negare di aver effettuato tentativi di autenticazione

Sicurezza autenticazione

Pericoli

- Spoofing
- Tampering
- Repudiation
- Information Disclosure
- Denial of Service
- Elevation of Privilege

Esempio

- Memorizzazione non protetta del fattore di autenticazione
  - fisica
  - Digitale
- Intercettazione

Sicurezza autenticazione

Pericoli

- Spoofing
- Tampering
- Repudiation
- Information Disclosure
- Denial of Service
- Elevation of Privilege

Esempio

- Blocco autenticazione di soggetti legittimi

Sicurezza autenticazione

Pericoli

- Spoofing
- Tampering
- Repudiation
- Information Disclosure
- Denial of Service
- Elevation of Privilege

Esempio

- Mancata restrizione all'accesso a privilegi di amministratore di sistema

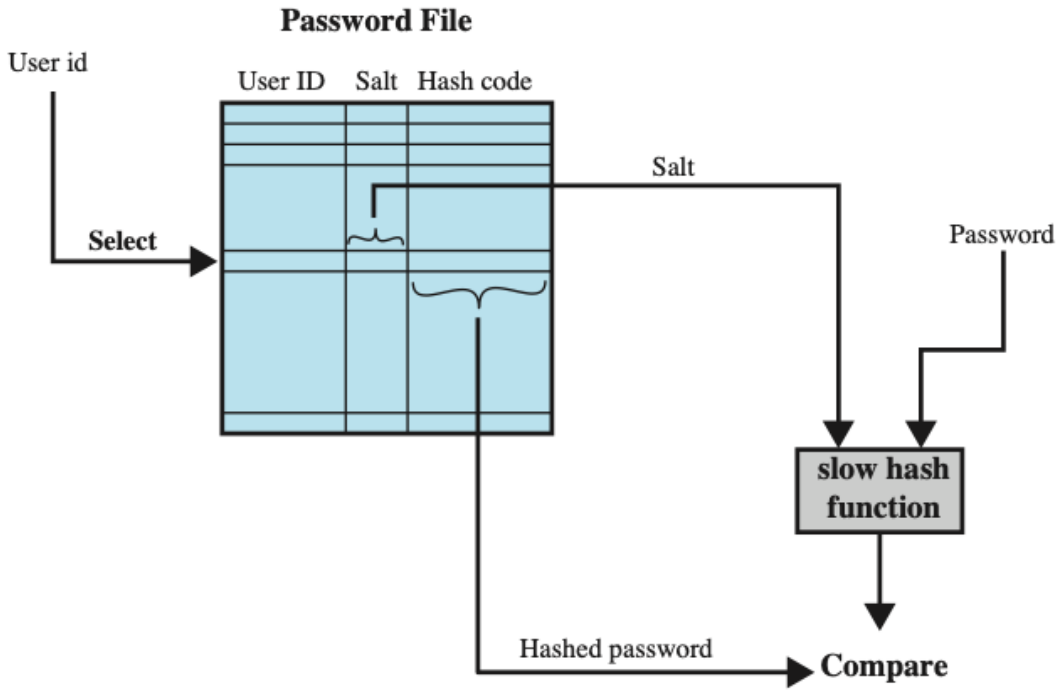
Memorizzazione del fattore di autenticazione sul sistema

- È un **segreto condiviso** fra il soggetto e il sistema
- La tecnica di **memorizzazione sul sistema** deve ridurre il rischio di
  - esposizione del fattore di autenticazione in caso di furto del supporto di memorizzazione
  - accettazione di fattori diversi da quelli impostati in fase di configurazione

Autenticazione con dispositivo fisico

- È un oggetto che deve essere custodito dal soggetto
- Basato sul paradigma chiave-serratura
  - il dispositivo deve agire come una *chiave*
- Accoppiamento basato su circuiti elettronici o codici

Autenticazione con parola d'ordine



- *Salt*
  stringa di bit casuale
- Si memorizza hash crittografico della combinazione fra parola chiave e salt

Attacchi a sistemi basati su parola d'ordine

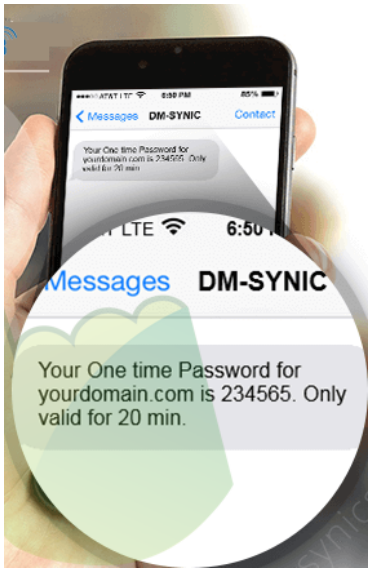
- Attacchi a sistemi di crittografia deboli
- Attacchi *a forza bruta* che consentono innumerevoli tentativi di autenticazione in sequenza
- Attacchi basati su dizionari e regole euristiche
- Attacchi basati sulla possibilità di indovinare la parola chiave più probabile per un dato soggetto

OTP – One-Time Password

- Un codice è generato in modo casuale e può essere utilizzato una sola volta
  - di solito è valido per un periodo di tempo molto limitato
- Il codice può essere generato dal soggetto o inviato dal sistema utilizzando un canale separato di comunicazione (out-of-band)

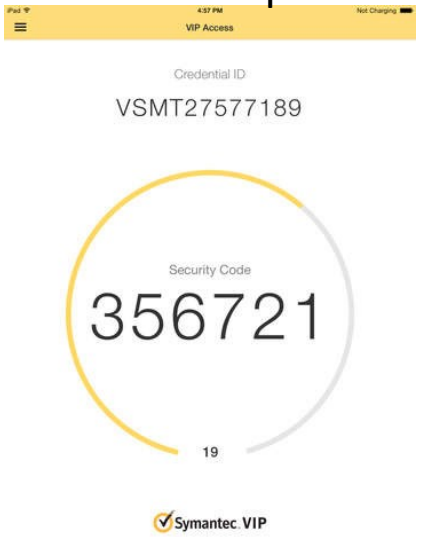
OTP – One-Time Password

OTP via SMS



OTP con generatore fisico

OTP con applicazione vincolata a uno smartphone



Biometrie

- Utilizzati principalmente per ridurre il rischio di attacchi di tipo *spoofing*
- Svantaggi
  - costo delle apparecchiature
  - costo della fase di *enrollment* (acquisizione biometria)
  - accettazione da parte dei soggetti
  - *liveness detection* per individuare accessi con falsi biometrici

Biometrie

Volto per controllo passaporto

Verifica dell’iride

Falsi biometrici

Challenge-response

- Il soggetto registra nel sistema **più valori** di uno stesso fattore di autenticazione
  - Ad es., un insieme di parole-chiave diverse, impronte digitali di più dita, ecc.
- Per ogni richiesta di accesso il sistema **chiede a caso** uno dei valori memorizzati o una particolare sequenza

Requisiti di sicurezza per autenticazione

- Requisiti di base
  - Identificare i diversi soggetti che devono essere autenticati
    - Persone fisiche, processi, sistemi, ecc.
  - Definire procedure per acquisire in modo certo i dati di autenticazione dei soggetti

- Vulnerabilità sistemi di autenticazione

Autenticazione multi-fattore

- Per mitigare i rischi legati a autenticazione con un solo fattore
- Possono essere usati in modo congiunto
  - Ad es., tessera di riconoscimento + codice
- Possono essere usati in cascata
  - Ad es., parola chiave + OTP

Autenticazione multi-fattore

- Per mitigare i rischi legati a autenticazione con un solo fattore
- Possono essere usati in modo congiunto
  - Ad es., tessera di riconoscimento + codice
- Possono essere usati in cascata
  - Ad es., parola chiave + OTP

Autenticazione multi-fattore

- Per mitigare i rischi legati a autenticazione con un solo fattore
- Possono essere usati in modo congiunto
  - Ad es., tessera di riconoscimento + codice
- Possono essere usati in cascata
  - Ad es., parola chiave + OTP

Autenticazione multi-fattore

- Le combinazioni dei fattori devono tener conto di
  - usabilità della soluzione
  - capacità di riduzione progressiva del rischio
- Esempio: accesso *forte* a servizi bancari (SCA – Strong Customer Authentication)
  - Primo fattore: nome utente + password
  - Secondo fattore: associato allo smartphone
- Direttiva EU PSD2

Autenticazione multi-fattore

- Le combinazioni dei fattori devono tener conto di
  - usabilità della soluzione
  - capacità di riduzione progressiva del rischio
- Esempio: accesso *forte* a servizi bancari (SCA – Strong Customer Authentication)
  - Primo fattore: nome utente + password
  - Secondo fattore: associato allo smartphone
- Direttiva EU PSD2

Approfondimento 1: Autenticazione: NIST SP 800-63-3

- Identity proofing establishes that a subject is who they claim to be. Digital authentication is the process of determining the validity of one or more authenticators used to claim a digital identity. Authentication establishes that a subject attempting to access a digital service is in control of the technologies used to authenticate. Successful authentication provides reasonable risk-based assurances that the subject accessing the service today is the same as that which previously accessed the service.
- Digital identity is the unique representation of a subject engaged in an online transaction. A digital identity is always unique in the context of a digital service, but does not necessarily need to uniquely identify the subject in all contexts. In other words, accessing a digital service may not mean that the subject's real-life identity is known

Approfondimento 2:
Attacchi contro sistemi di autenticazione

Tipo di attacco	Fattore di Autenticazione	Esempio	Mitigazione
Scambio di identità	Parola-chiave	Ipotesi, tentativi	Complessità, limitazione numero tentativi
	Dispositivo fisico	Ipotesi, tentativi	Complessità
	Biometria	Fabbricazione di falsi	Complessità, *liveness detection*
Contro il sistema	Parola-chiave	Furto dell'archivio	Crittografia, protezione da accessi diretti
	Dispositivo fisico	Manomissione	Complessità
	Biometria	Furto dell'archivio	Crittografia, protezione da accessi diretti

Approfondimento 2: Attacchi contro sistemi di autenticazione

Tipo di attacco	Fattore di Autenticazione	Esempio	Mitigazione
Spiare, furto, copia	Parola-chiave	Osservazione fisica (*shoulder surfing*), keylogger	Cura nella custodia della parola-chiave, rifiuto di parole-chiave note, autenticazione multi-fattore
	Dispositivo fisico	Furto, clonazione, contraffazione	Sistemi resistenti alla clonazione e alla contraffazione; autenticazione multi-fattore
	Biometria	Fabbricazione di falsi	Rilevazione di tentativi di copia dal dispositivo di acquisizione; *liveness detection*

Approfondimento 2:
Attacchi contro sistemi di autenticazione

Tipo di attacco	Fattore di Autenticazione	Esempio	Mitigazione
Replica di fattori intercettati	Parola-chiave, dispositivo fisico, biometria	Replica di una parola-chiave, di un codice	Protocolli challenge-response; OTP
Cavalli di Troia	Parola-chiave, dispositivo fisico, biometria	Dispositivo di acquisizione fasullo	Definizione di luoghi e dispositivi autorizzati all'autenticazione
Blocco del sistema	Parola-chiave, dispositivo fisico, biometria	Invio di numerose richieste di autentica-zione che falliscono	Autenticazione multi-fattore con dispositivi fisici

Approfondimento 3:
Direttiva EU PSD2 2015/2366

- (95) La sicurezza dei pagamenti elettronici è fondamentale per garantire la protezione degli utenti e lo sviluppo di un contesto affidabile per il commercio elettronico. Tutti i servizi di pagamento offerti elettronicamente dovrebbero essere prestati in maniera sicura, adottando tecnologie in grado di garantire l'autenticazione sicura dell'utente e di ridurre al massimo il rischio di frode. […] I servizi di pagamento offerti via Internet o tramite altri canali a distanza […] dovrebbero pertanto comportare l'autenticazione delle operazioni attraverso codici dinamici, affinché l'utente sia, in ogni momento, al corrente dell'importo e il beneficiario dell'operazione che l'utente sta autorizzando.
- (96) […] L'uso sicuro di credenziali di sicurezza personalizzate è necessario per limitare i rischi connessi al phishing e ad altre attività fraudolente. Al riguardo, l'utente dovrebbe poter fare affidamento sull'adozione di misure che tutelano la riservatezza e l'integrità delle credenziali di sicurezza personalizzate. Tali misure comprendono di norma sistemi di cifratura basati su dispositivi personali del pagatore, tra cui lettori di carte o telefoni cellulari, o forniti al pagatore dal proprio prestatore di servizi di pagamento di radicamento del conto mediante canali diversi, come SMS o posta elettronica. Le misure, comprendenti normalmente i sistemi di cifratura, che possono dar luogo a codici di autenticazione quali password monouso, sono in grado di potenziare la sicurezza delle operazioni di pagamento. L'uso di tali codici di autenticazione da parte degli utenti dei servizi di pagamento dovrebbe essere considerato compatibile con i relativi obblighi in relazione agli strumenti di pagamento e alle credenziali di sicurezza personalizzate, anche quando sono coinvolti prestatori di servizi di disposizione di ordine di pagamento o prestatori di servizi di informazione sui conti.