10 - User Authentication

Password-based authentication

le falle di sicurezza non lasciano tracce
Impossibile dimostrare la propria innocenza se qualcuno usa in modo corretto la tua identità
c'è sempre la possibilità che la password possa essere indovinata:

- Sia P la **probabilità che una password venga indovinata** (bruteforce) durante un intervallo di tempo T
- sia G il rateo di domande per unità di tempo.
- Sia N lo **spazio dei caratteri della password**
- $P = \frac{(G \times T)}{N}$
- Modi per ridurre P
  - Ridurre T: obbligare il cambio password dopo un dato tempo
  - Ridurre G: abbassare il rateo di guess artificialmente
  - Aumentare N: password più lunghe e complesse

Attacchi online
Sistema usato per verificare la correttezza delle guesses

- Normalmente è inevitabile se i sistemi devono essere accessibili online
  Difese:
- ridurre il rateo di guess, aggiungere un delay ogni guess.
- limitare il numero di tentativi non corretti
- riportare date/time location dell'ultimo login avvenuto con successo

Attacchi offline
Si basa su una lista pre-costruita di password
Deve avere accesso alla password salvata in qualche modo

Password encryption
Può essere basato su una one way hash function
Il file della password può contenere i **digests** della password e non il cleartext
Durante il login viene generato il digest della password e comparato con il valore salvato nel file.

Dictionary attack

Ottenere una copia dei file che contengono le password criptate (digests)
Avere un file contenente una lista di parole comuni (dizionario)

- Per ogni parola w nel dizionario si calcoli il suo digest $f(w)$ e lo si compari con il digest della password
- Tutte le corrispondenze sono le password indovinate
- Può essere più sofisticato trasformando w (permutazioni, al contrario, etc.)

Difese:

- Limitare l'acesso ai file contenenti le password tramite l'OS
- Non è possibile ridurre il rate di guess
- Si può artificialmente rallentare la one-way hash function che viene usata per generare il digest
- Salting della password per prevenire attacchi globali
- Shadow della password: password criptata contenente altre informazioni criptate (es: nome, email...)

Salting

Quando l'utente U usa una password P, il sistema salva per l'utente U due quantità S e Q

- S è il salting ovvero un numero generato casualmente dove l'utente salva la password
- Q è il digest ottenuto tramite $f(P|S)$ dove S è una one-way hash function
- Solo S e Q(non P) sono salvate nel file assieme allo username U
  Quando l'utente U vuole autenticarsi deve identificarsi come U fornendo la password P:
- il sistema legge S e Q, associati con U

- concatena S con P e applica f per ottenere Q^*
- Compara Q^* con Q
- se $Q^* = Q$ allora l'autenticazione ha avuto successo
  Se l'attaccante riesce a leggere il file password, esso ottiene solo S e Q ma **non** è in grado di ricavare P

La stessa password ha diverse versioni criptate (digests) che dipendono dal salt
Il salting della password previene diversi attacchi (es il problema che molti utenti usano le stesse password per più siti)

Login spoofing

- Un utente malintenzionato crea un pagina di login falsa.
- Attende che l'utente vittima faccia il login con le proprie credenziali
- Salva il login/password
- Mostra un messaggio di errore (login errato)
- Avvia il **vero** programma o reindirizza alla vera pagina di login
- La vittima crede di aver scritto male la password e ritenta l'inserimento che stavolta avviene con successo.

Una difesa generica si basa sulla **mutua autenticazione**:

- l'utente autentica se stesso al server
- il server autentica se stesso all'utente
- Basato su tecniche crittografiche come firme digitali e certificati

Phishing

Incarnazione moderna del login spoofing

- Il phisher prova a ottenere informazioni in maniera flaudolenta come password e i dettagli delle carte di creddito.
- Normalmente viene eseguito tramite mail o messaggi ma possono usare anche telefoni.
- Si basa spesso su social engineering

Keylogger

Programma che può registrare password, e dati sensibili inseriti.
Spyware keylogger sono usati anche per capire le abitudini su internet
I keylogger sono spesso software ma possono anche essere hardware

Difese:

- spyware detection removal programs
- firewall per bloccare il traffico in uscita
- tastiere virtuali

Packet sniffing

il packet sniffer è un software che è in grado di analizzare il traffico sulla rete a cui è connesso
Cerca di identificare pacchetti contenenti password che vengono inviate in chiaro d protocolli poco sicuri come telnet, rlogin o ftp.
Salva i dati catturati localmente o li invia a un server.

Difese:
basate su tecniche di crittografia per offuscare le password

- Richiede che le password non vengano **mai** mandate in chiaro tramite la rete
- richiedono one-time passwords

Autenticazione basata su "something you are"

Conosciuta come biometrica:

- impronta digitale
- riconoscimento vocale
- retina

- viso
  Richiede hardware specializzato
  Il metodo biometrico scelto deve minimizzare i falsi negativi o falsi positivi

Proprietà desiderate per l'autenticazione biometrica:

- Universalità: tutti possono possederlo
- Unicità: due persone differenti non devono avere le stesse caratteristiche
- Permanenza: le caratteristiche non possono essere alterabili o cambiare con il tempo
- Acquisibile: facile da acquisire

Si possono usare anche sistemi di autenticazione basato su determinate azioni:

- keystroke authentication: intervallo di pressione dei tasti, pressione, durata, posizione del click
- Velocità accelerazione e pressione della penna.