Sicurezza Documentale a.a. 2017/2018

DOCENTI: DOTT.SSA VALERIA FIONDA

DOTT. GIUSEPPE PIRRÒ

Sistemi di Autenticazione

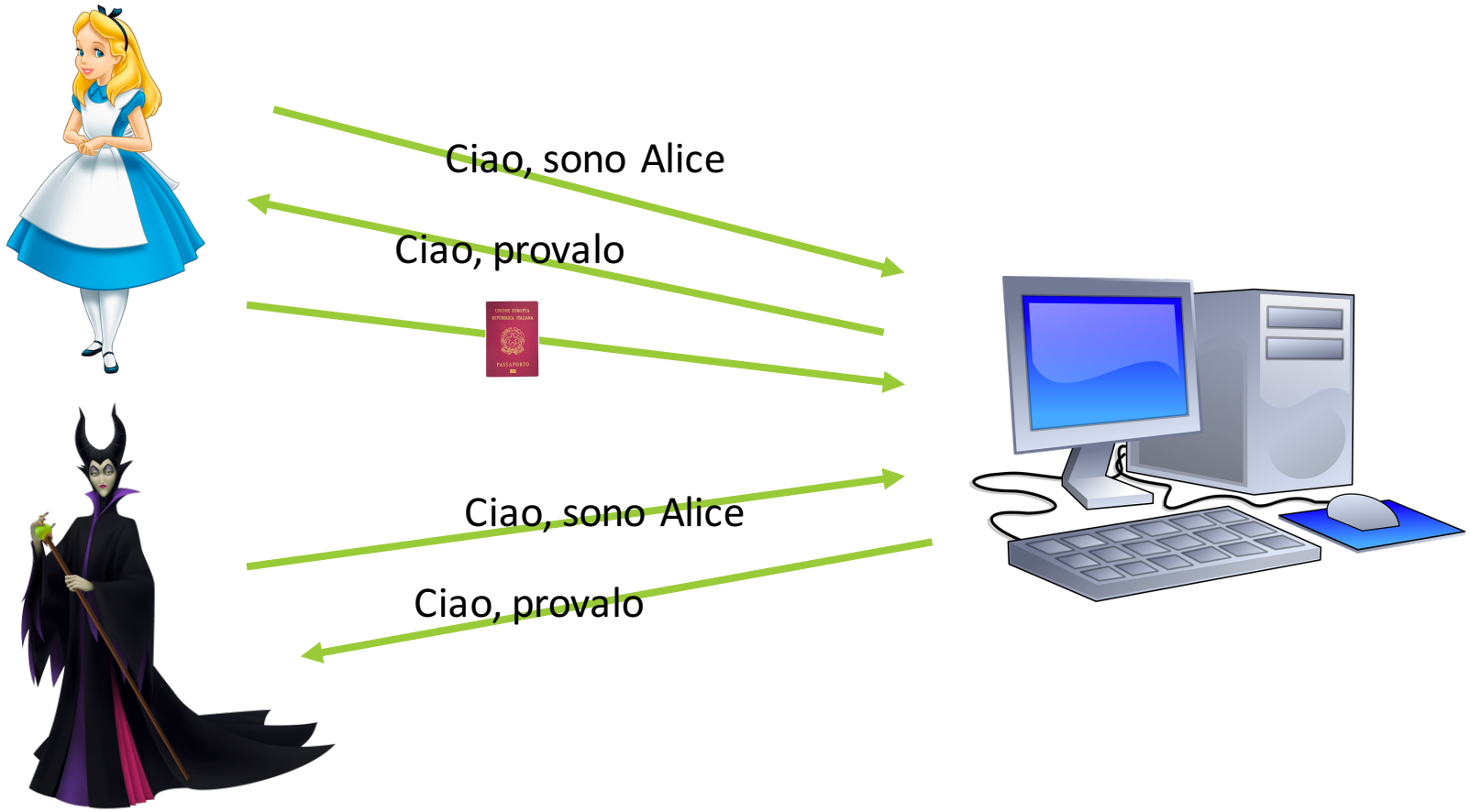
Tipi di servizio

- Servizi senza autenticazione :
  - proteggere i server (ftp, http...) rendendo disponibile solo le informazioni desiderate e niente altro.
- Servizi con autenticazione :
  - l'utente che desidera informazioni deve farsi riconoscere e il server deve decidere se è autorizzato ad avere ciò che chiede.

Processo di autenticazione

Identificazione + verifica

Processo di autenticazione



Modi di autenticarsi

- Qualcosa che conisci:
  - Ad esempio una password, un Personal Identification Number (PIN), la risposta ad un insieme di domande preconfezionate.
- Qualcosa che possiedi:
  - Ad esempio schede elettroniche, smart cards o chiavi fisiche.
  - Questo tipo di identificatori vengono chiamati *token*.
- Qualcosa che sei:
  - Biometrica statica: ad esempio impronte digitali, retina o riconoscimento facciale.
  - Biometrica dinamica: ad esempio pattern vocali, riconoscimento della scrittura.

Password-based authentication

- Il più usato sistema di difesa contro le intrusioni
  - Sistemi multi-utente
  - Sistemi di rete
  - Siti di e-commerce sul Web
- User name o ID+password:
  - Il sistema confronta la password con quella corrispondente all'utente conservata nel sistema.
  - Il sistema conserva le password degli utenti in un file di passwords.

Password-based authentication

- La password serve ad autenticare l'ID
- L'ID serve a mettere in sicurezza i dati nei seguenti modi:
  - Determina se l'utente ha il diritto di accedere al sistema.
  - Determina i privilegi di cui gode l'utente nel sistema (ad esempio, se può modificare i file o può solo leggerli).
  - Gli ID sono utilizzati dagli utenti che creano un file per stabilire chi vi può accedere.

Le vulnerabilità delle password

- I sistemi che utilizzano sistemi di autenticazione basati su password di solito memorizzano le password in un dizionario indicizzato tramite l'ID utente.

Attacco al dizionario offline

- Tipicamente meccanismi di controllo degli accessi vengono utilizzati per proteggere il dizionario delle password
- È possibile che I sistemi di controllo vengano bypassati
- L'attacker ottiene il dizionario delle password

- Contromisure
  - Protezione del dizionario delle password
  - Misure di intrusion detection
  - Veloce riemissione delle password compromesse

Il dizionario delle password

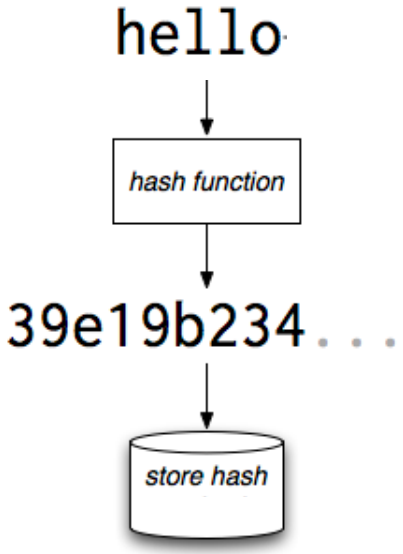
- Password in chiaro

```
john:automobile
mary:balloon
joe:wepntkas
```

- Semplice implementazione
- Rischioso
  - Tutti gli utenti sono compromessi se vengono effettuati accessi non autorizzati al file delle password

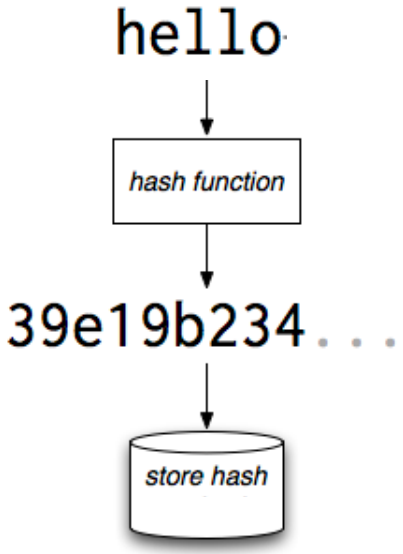
Il dizionario delle password

- Le password di solito non sono memorizzate e non viaggiano in chiaro ma opportunamente codificate (criptate)
  - Di solito si effettua un hashing delle password



Il dizionario delle password

- La funzione di hash è una funzione matematica che trasforma una stringa (sequenza di caratteri) di lunghezza arbitraria in una stringa di lunghezza fissa



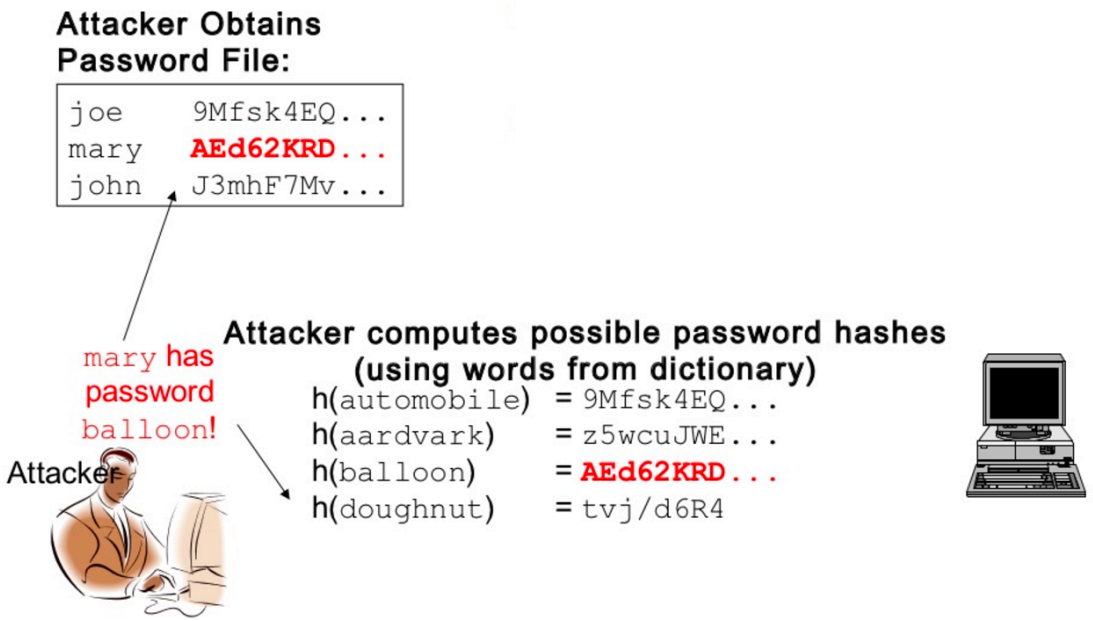
Il dizionario delle password

- La funzione di hash è una funzione matematica che trasforma una stringa (sequenza di caratteri) di lunghezza arbitraria in una stringa di lunghezza fissa

```
john:9Mfsk4EQh+XD2lBcCAvputrIuVbWKqbxPgKla7u67oo=
mary:AEd62KRDHUXW6tp+XazwhTLSUlADWXrinUPbxQEfnsI=
joe:J3mhF7Mv4pnfjcnoHZ1ZrUELjSBJFOo1r6D6fx8tfwU=
```

Password-based authentication

- Le password di solito non sono memorizzate e non viaggiano in chiaro ma opportunamente codificate (criptate)
  - Di solito si effettua un hashing delle password



Attacco al dizionario offline - Contromisure

- Protezione del dizionario delle password
- Misure di intrusion detection
- Veloce riemissione delle password compromesse

Attacco ad un account specifico

- L’attacker cerca di ottenere la password di uno specifico account sottomettendo al sistema delle password che pensa possano essere corrette fino ad indovinare la password.

- Contromisure
  - Meccanismi di blocco degli accounts: un account è bloccato dopo un certo numero di tentativi sbagliati (di solito non più di 5).

Attacco alle password popolari

- Si utilizzano password popolari e si usano per tentare l'accesso utilizzando più di un ID.
  - Sfrutta il fatto che gli utenti di solito scelgono password facili da ricordare.

- Contromisure
  - Proibire all'utente di scegliere password di uso comune
  - Controllare la sorgente delle richieste di autenticazione (l'indirizzo IP)

Indovinare la password di un singolo utente

- L'attacker cerca di carpire informazioni riguardo ad un singolo utente e le usa per cercare di indovinare la sua password
  - Per ricordare la password molti utenti usano informazioni legate alla propria vita personale

- Contromisure
  - Forzare l'utente a scegliere password sicure
    - Minima lunghezza
    - Utilizzo di caratteri speciali
    - Vietare l'utilizzo di informazioni che identifica l'utente
    - Forzare il cambio password ad intervalli regolari

Hijacking (Appropriazione) della workstation

- L’attacker aspetta che una postazione di lavoro venga lasciata incustodita dopo che un utente ha acceduto.

- Contromisure
  - Log out automatico dopo un certo periodo di inattività
  - Schemi di intrusion detection per capire se il comportamento dell’utente è cambiato

Sfruttamento degli errori dell'utente

- Nel caso in cui il sistema assegni automaticamente una password l'utente solitamente la scrive o salva da qualche parte perchè è difficile da ricordare.
- L'attacker può usare tecniche di social engeneering per fare in modo che un utente riveli la password
- Contromisure
  - Intrusion detection
  - Accesso tramite password combinato ad altre tecnica di autenticazione

Sfruttamento dell'uso multiplo delle password

- Se l'utente usa la stessa password in diversi sistemi questa diventa più vulnerabile.
  - Supponete di avere un account google, uno facebook, uno Yahoo!, uno Dropbox e uno presso il servizio A.
  - Avete generato una password robusta di 14 caratteri scelti completamente random e la usate in tutti i suddetti servizi.
  - Se il servizio A memorizza le password in chiaro nel suo dizionario è facile che possa essere compromesso.
  - Se un attacker riesce ad avere accesso al file potrà accedere a tutti I servizi dello stesso utente e non soltanto al servizio A.

Monitoraggio elettronico

- Se le password sono trasmesse in una rete ad un sistema remoto sono vulnerabili se attackers intercettano il messaggio contenete la password
- In questo caso la semplice codifica (criptazione) non è una protezione sufficiente
  - La password criptata è a tutti gli effetti una password