Autenticazione

Esistono diversi tipi di autenticazione come;

- **Persona-persona**, basata sull'incontro tra i due soggetti;
- **Utente-computer**, certamente la più comune, è utilizzata dall'utente per accedere ad un computer;
- **Computer-computer**, utilizzato per accedere ad un computer remoto, per esempio per accedere ad un sito Web;
- **Utente-utente**, tipo di autenticazione rara, ma fattibile.

Autenticazione utente-computer

Relativamente al tipo di autenticazione **utente-computer**, possiamo notare una successiva distinzione:

- Basata su **conoscenza di segreti** prestabiliti e precondivisi, per esempio *password* e *pin*;
- Basata su **possesso di dispositivi magnetici o elettronici**, per esempio *carte magnetiche*, *smart-card* e *smart-token*;
- Basata su **biometria** di caratteristiche fisiche dell'utente, per esempio *impronte* ed *iride*.

Autenticazione basata sulla conoscenza di segreti

Il tipo di autenticazione basato sulla **conoscenza di segreti** si basa sull'implementazione di una password. Esistono 4 tipologie di **rischio** per una password:

- **Guessing**, ovvero indovinare la password stessa. Legate al concetto di *guessing*, esistono i seguenti attacchi:

    - Attacco **standard**, attacchi con una matrice sociale basati sulle parole maggiormente legate all'utente stesso (e.g. *hobby*, *nomi parenti*, *compleanno*, *indirizzi*);
    - Attacco **dizionario**, per cui vengono provate tutte le parole presenti all'interno di un dizionario, talvolta arricchendo il tutto con regole che ricalcano possibili scelte dell'utente (e.g. *parola al contrario,* 0 *al posto di "o",* 1 *al posto di "i"*);
    - Attacco **bruteforce**, per cui vengono provate *esaustivamente* tutte le parole costruibili in un dato vocabolario. Abbiamo notato, grazie ai *mini-challenge*, che una password di 8 caratteri è una soglia realistica.

    Quali sono le contro misure rispetto quest'ultimi 3 attacchi? Esistono 3 diverse misure per gli attacchi descritti, ovvero:

    - **Controllo sulla password**, attraverso cui il sistema controlla che la password non sia banale (e.g. *lunghezza*).
    - **Controllo sul numero inserimenti**, secondo cui il sistema limita i tentativi di login per cui pena è il blocco del dispositivo (e.g. *dispositivo mobile*).
    - **Uso di CAPTCHA** (acronimo di "*Completely Automated Public Turing Test To Tell Computers and Humans Apart*") è essenzialmente un *turing-test* in grado di riconoscere l'umano dalla macchina ed informare la macchina rispetto questa informazione. Rispetto il captcha, esiste un recente algoritmo basato su Google Street View viola il 99% delle captcha alfanumeriche.

    Si noti che spesso, in alcuni dispositivi, vengono adottate una combinazione di quest'ultime misure.

- **Snooping**, quindi indovinare la password *sbirciando*;

- **Spoofing**, ossia scoprire la password tramite un falso (e.g. *fake-login*);

- **Sniffing**, ovvero scoprire la password a partire da un *intercettazione*;

Chiaramente per trovare la giusta password è necessario *bilanciare mnemocità e complessità* di quest'ultima. A partire da questo, esistono le seguenti **implicazioni**:

- Non usare parole del dizionario;
- Usare almeno 8 caratteri;
- Non usare la stessa password per autenticazioni diverse, altrimenti una sola compromissione comprometterebbe altri sistemi.

Tuttavia, potrebbe risultare difficile ricordare tutte le nostre password, motivo per cui nascono dei sistemi cui scopo è conservare al meglio tutte le nostre password (e.g. *all'interno del browser*).

Autenticazione basata sul possesso

Attraverso questo secondo tipo di autenticazione, l'*obiettivo* è quello di convalidare l'identità dell'utente a partire possesso di un determinato oggetto, tipicamente *magnetico* o *elettronico*, che può memorizzare un informazione sensibile;
• Informazione su carta magnetica interamente leggibile;
• Informazione su carta elettronica leggibile coerentemente con interfaccia funzionale;
Oggetti più diffusi per questo scopo sono le *smart-card* e *smart-token*.
Uno *smart-token*, a differenza di una *smart-card*, ha un interfaccia di *I/O utente*, mentre una *smart-card* ha *I/O macchina*; inoltre, uno smart token può avere un pulsante o una tastiera per immettere il pin.

Autenticazione basata sulla biometria

Attraverso questo terzo tipo di autenticazione, l'*obiettivo* è quello di convalidare l'identità dell'utente a partire possesso di una determinata **caratteristica personale ed univoca**.
Si basa sull'assunzione della natura che ognuno di noi possegga caratteristiche fisiche univoche, per esempio rispetto le impronte digitali. Si noti che lo stesso non è vero rispetto le caratteristiche comportamentali, le quali possono non essere uniche.

L'autenticazione basata sulla biometria è **meno accurata** rispetto i precedenti due modi, basati sul possesso e conoscenza.

Se una lettera è un concetto e può essere rappresentato facilmente secondo un banale codice ASCII, un impronta digitale non può essere inteso come un concetto bensì come un *oggetto reale*, il quale deve essere dicretizzato secondo determinate scelte.
Un impronta digitale viene rappresentata secondo il campionamento delle minuzie (i.e. i punti di biforcazione) all'interno dell'impronta.
Chiaramente un dito all'interno

Sappiamo che due campioni biometrici non sono mai uguali, motivo per cui alla registrazione dell'impronta dobbiamo registrare più di una volta quest'ultima, creando un template: una "*media*" del campionamento per la nostra impronta.
L'autenticazione avviene a partire dal confronto tra l'impronta "*live*" ed il *template*; tuttavia, se il solo cambio di un bit all'interno dell'hash di una stringa di bit fa sì che il codice risultato sia completamente diverso, il riconoscimento dell'impronta digitale prevede una **tolleranza** rispetto l'impronta live presentata, il che rende evidente la poca fiscalità del riconoscimento. Il motivo è dato dal fatto che ogni campione biometrico è diverso dall'altro e non esiste un modo per rappresentare un campione biometrico in modo inattaccabile. Questa fiscalità è presente all'interno dell'autenticazione per conoscenza di una password.

Perchè l'autenticazione basata sulla **biometria è sempre accompagnata da una password**? Essenzialmente per i seguenti tre motivi:

- Rappresentare un campione biometrico può essere imprecisa, altalenante;
- Non è possibile modificare un informazione biometrica, il che rende questa meno robusta;
- Un impronta viene "*lasciata*" dappertutto al nostro tocco di un oggetto.

> Soluzione al terzo problema soprastante potrebbe essere "*Finger Vein*", un sistema sensoristico che riconosce lo schema dei capillari sanguigni all'interno del polpastrello.

> Possiamo classificare le impronte digitali secondo tre tipologie: (i) **loop**, la più diffusa fra le tre, (ii) **arch**, la meno diffusa e (iii) **whorl**, la seconda più diffusa dopo loop.