Sicurezza Documentale a.a. 2017/2018

DOCENTI: DOTT.SSA VALERIA FIONDA

DOTT. GIUSEPPE PIRRÒ

Sistemi di Autenticazione

Modi di autenticarsi

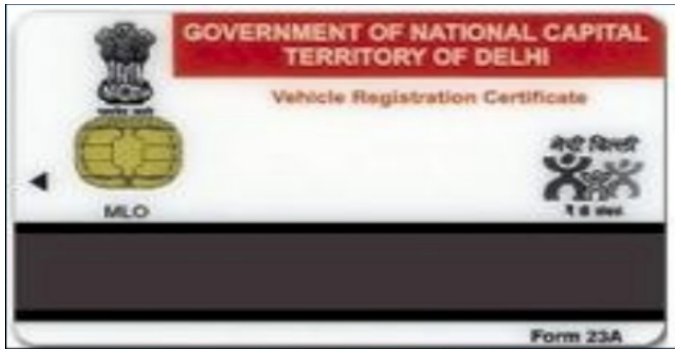
- Qualcosa che conisci:
  - Ad esempio una password, un Personal Identification Number (PIN), la risposta ad un insieme di domande preconfezionate.
- Qualcosa che possiedi:
  - Ad esempio schede elettroniche, smart cards o chiavi fisiche.
  - Questo tipo di identificatori vengono chiamati *token*.
-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

Autenticazione tramite token

- I token sono oggetti che l'utente possiede con lo scopo di autenticarlo
- Si dividono in tre categorie:
  - Memory Cards
  - Smart Cards
  - USB Dongle

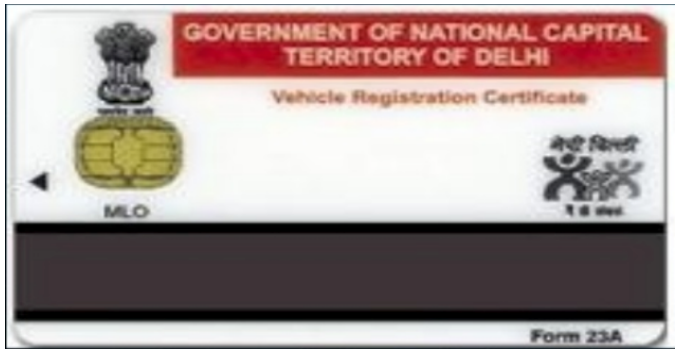
Autenticazione tramite token – Memory Cards

- Le memory cards possono immagazzinare ma non processare dati
  - Un tipo comune di memory card sono le carte bancarie con la banda magnetica sul retro
  - La banda magnetica può memorizzare un codice segreto che può essere letto
- Per l'autenticazione sono generalmente associati all'utilizzo di una password o PIN



Autenticazione tramite token – Memory Cards

- Se combinate con l'utilizzo di una password o PIN forniscono un grado di sicurezza molto maggiore della sola password
- Contro:
  - Richiede l'utilizzo di appositi lettori → costo
  - Perdita del token → l'utente perde la possibilità di accedere al sistema
  - Insoddisfazione dell'utente



Autenticazione tramite token – Smart Cards

- Le smart cards possono sia immagazzinare che processare dati
- Una tipica smart card include tre tipi di memoria:
  - ROM: memorizza i dati che non cambiano durante la vota della carta (ad esempio, il numero della carta e dell'utente).
  - EEPROM: memorizza dati e programmi (ad esempio, il protocollo che la carta può eseguire).
  - RAM: memorizza dati temporanei generati mentre le applicazioni sono in esecuzione.

Autenticazione tramite token – Smart Cards

- Il protocollo di autenticazione che utilizzano può essere:
  - Statico → L'utente si autentica al token, il token autentica l'utente al computer
  - Password generate dinamicamente → Il token genera dinamicamente e periodicamente una password. Questa pasword è utilizzata per l'aqutenticazione nel computer. Il token e il computer devono essere mantenuti sincronizzati.
  - Challenge-response → Il computer genera una *challenge* (sequenza di caratteri random). Il token genera una *response* sulla base della challenge.

Autenticazione tramite token – USB Dongle

- Stessa funzionalità delle smart cards

Autenticazione biometrica

- L'uso di caratteristiche biometriche rappresenta di fatto la forma più antica di riconoscimento:
  - Volto
  - Voce
  - Forma della mano
  - Retina
  - Impronta
  - Firma
- Una grandezza biometrica è descritta come una caratteristica fisiologica o comportamentale che possa essere misurata e successivamente identificata al fine di attestare l'identità di una persona (o più in generale di un essere vivente).

Autenticazione biometrica

- Nel 1882 Alphonse Bertillon (1853-1914), capo del servizio di identificazione della polizia di Parigi, introdusse un nuovo sistema di misurazione corporea studiato appositamente per l'identificazione dei criminali. Queste misure erano studiate in modo tale che, in teoria, potessero identificare univocamente ogni persona e non cambiassero durante il corso della vita adulta






Il caso di Will e di William West

- Due uomini imprigionati nel penitenziario di LeavenWorth (Kansas) avevano misure molto simili secondo il sistema di Bertillon. William rilasciato nel 1901, Will imprigionato nel 1903.

Will West's Bertillon Measurements
178.5; 187.0; 91.2; 19.7; 15.8; 14.8; 6.6; 28.2; 12.3; 9.7

William West's Bertillon Measurements
177.5; 188.0; 91.3; 19.8; 15.9; 14.8; 6.5; 27.5; 12.2; 9.6

Autenticazione biometrica

- Alla fine del XIX secolo, nel suo lavoro sull'ereditarietà, Galton criticò il sistema di Bertillon dal punto di vista statistico. Nel 1892 introdusse la nozione di minuzia e suggerì un primo sistema di classificazione di impronte molto elementare.
- Nel 1893, l'Home Ministry Office, UK, riconobbe che non esistono due individui con la stessa impronta. Presto molti dei maggiori dipartimenti di polizia cominciarono a "schedare" le impronte dei criminali. Molti studi rigorosi furono finanziati e furono sviluppati metodi scientifici per il confronto visivo di impronte.

Autenticazione biometrica

- Con il termine “riconoscimento biometrico” si fa di solito riferimento all’uso di caratteristiche fisiologiche o comportamentali distintive per il riconoscimento automatico di individui.
  - Fisiologiche
    - Impronta, mano, iride, retina, volto, dna
  - Comportamentli
    - Firma, voce

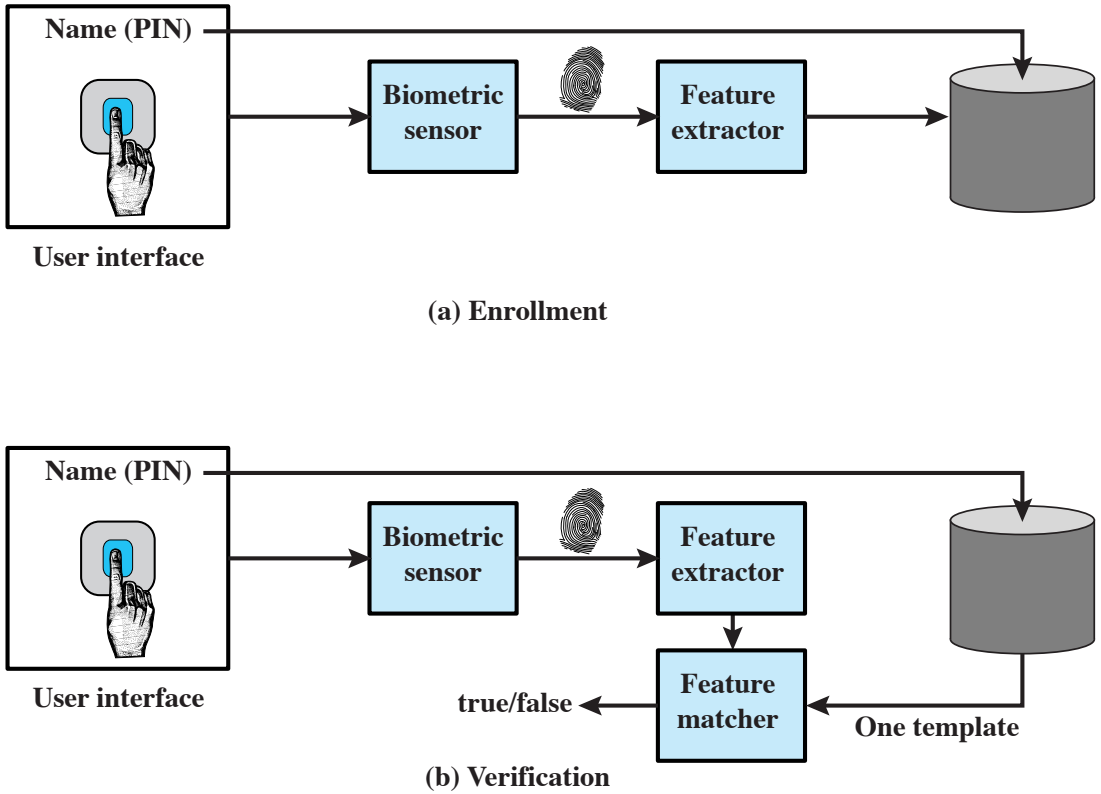
Autenticazione biometrica - vantaggi

- Le password o i token utilizzati per l'identificazione sono metodi di autenticazione "innaturali"
  - Non possono attestare con sicurezza l'identità della persona, ma semplicemente garantire che l'utente sia a conoscenza di qualcosa o la possegga.
- Le caratteristiche biometriche sono un metodo di autenticazione "naturale"
  - Le caratteristiche biometriche non possono essere perse, prestate, rubate o dimenticate
  - L'utente deve "semplicemente" presentarsi di persona
  - Le caratteristiche biometriche garantiscono la presenza della persona, in quanto risulta molto difficile per un individuo falsificare le caratteristiche fisiche di qualcun altro.

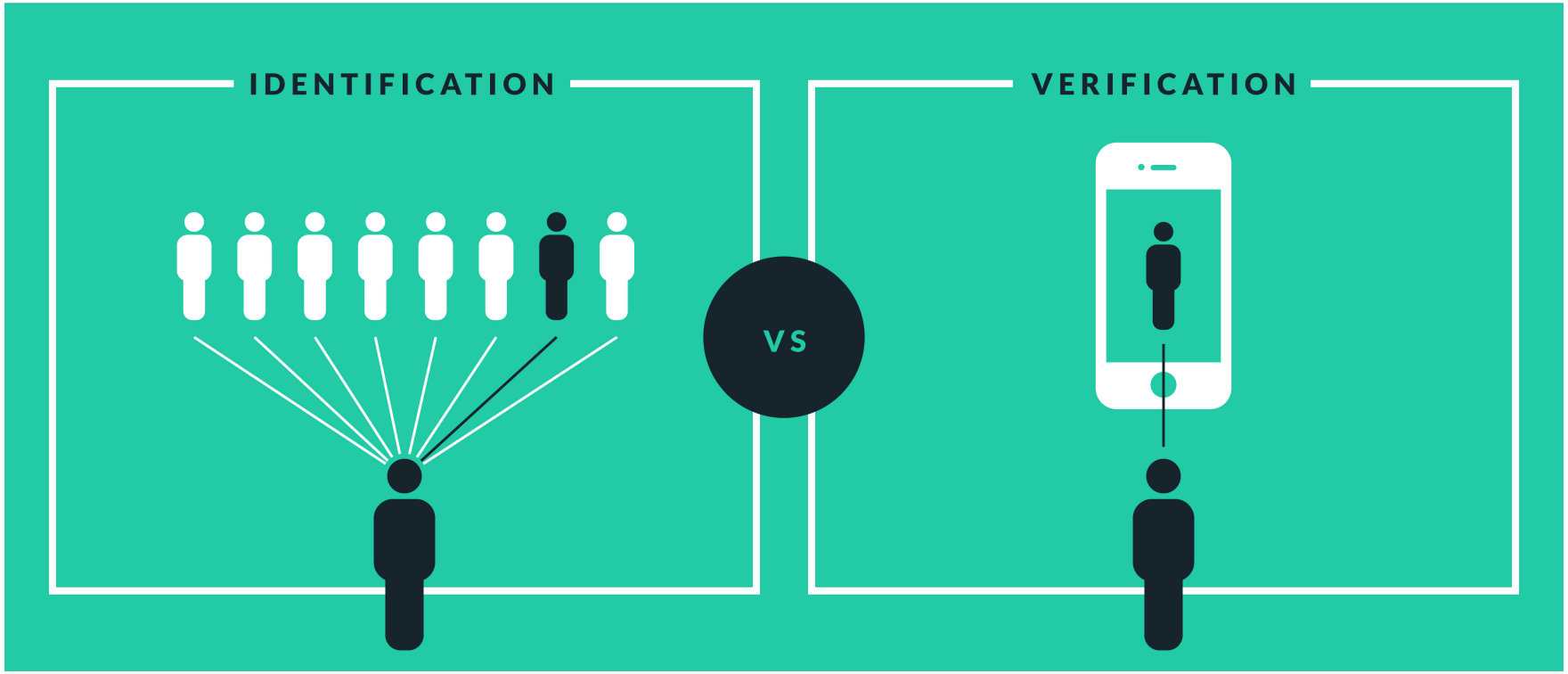
Autenticazione biometrica - svantaggi

- Non garantiscono un’accuratezza del 100%
- Esistono utenti che non possono utilizzare alcune tecnologie
- Le caratteristiche possono mutare nel tempo
- I dispositivi biometrici, in alcune circostanze, possono non essere affidabili

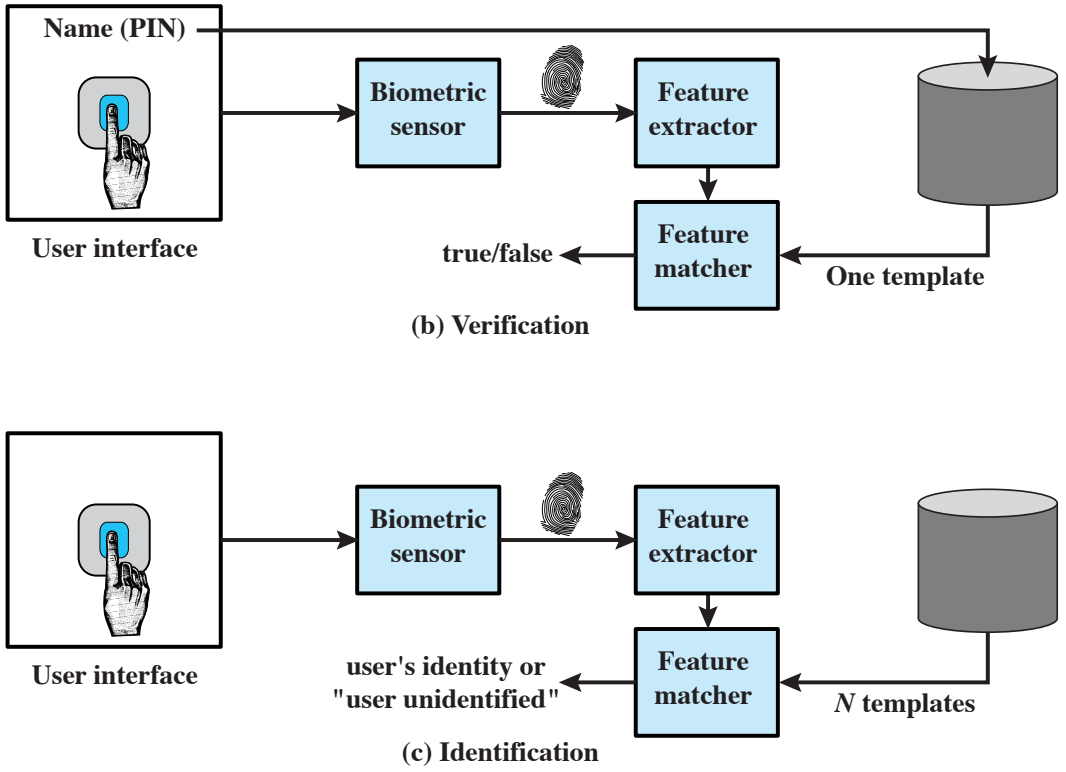
Autenticazione biometrica - funzionamento



Autenticazione biometrica - funzionamento



Autenticazione biometrica - funzionamento

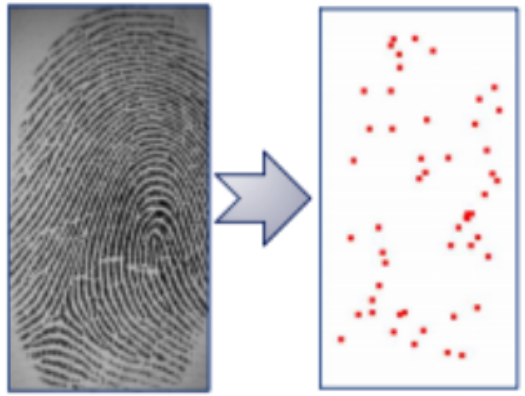


Autenticazione biometrica – positiva e negativa

- Riconoscimento positivo (login su un computer, commercio elettronico):
  - Il sistema stabilisce se la persona è chi dichiara di essere
  - Lo scopo è quello di impedire che più persone utilizzino la stessa identità
  - Modalità verifica o identificazione
- Riconoscimento negativo (servizi sociali):
  - Il sistema stabilisce se la persona è chi nega di essere
  - Lo scopo è quello di evitare che una singola persona utilizzi più identità
  - Sola modalità identificazione

Autenticazione biometrica - template

- Dati caratteristici e codificati ottenuti dalle feature uniche di un esempio biometrico
- Un elemento fondamentale di un sistema biometrico
  - Per il matching si utilizzano i template
  - Template diversi vengono generati ogni volta che un individuo fornisce un esempio biometrico



- Per ciascun individuo sono solitamente memorizzati più template per tenere conto di possibili variazioni della caratteristica biometrica

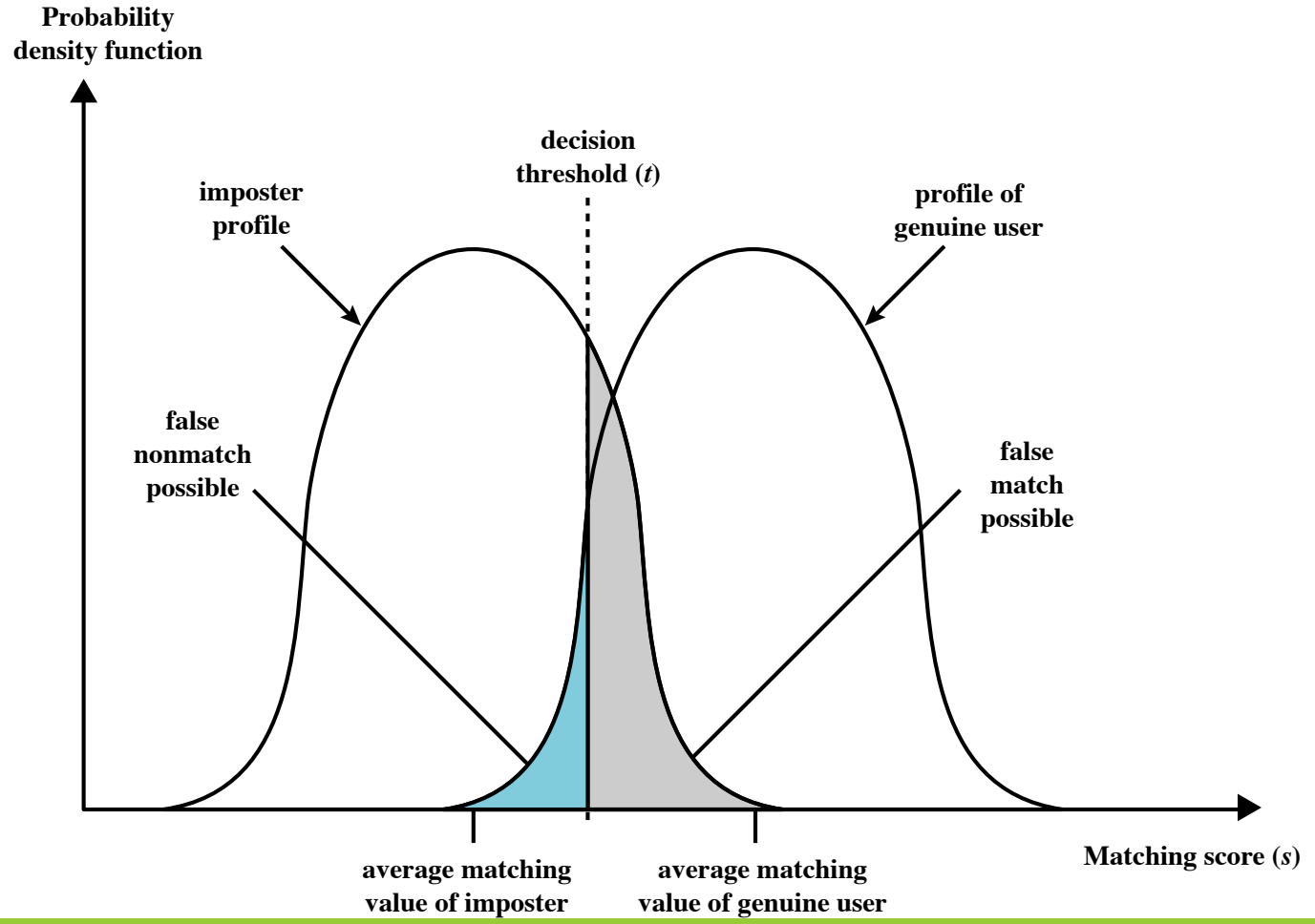
Autenticazione biometrica - accuratezza

- I sistemi biometrici non forniscono un match al 100%
- Il sistema di autenticazione usa un algoritmo per generare un punteggio alla corrispondenza
- Il punteggio è confrontato con una soglia prefissata, per prendere la decisione finale (“match” o “no match”)

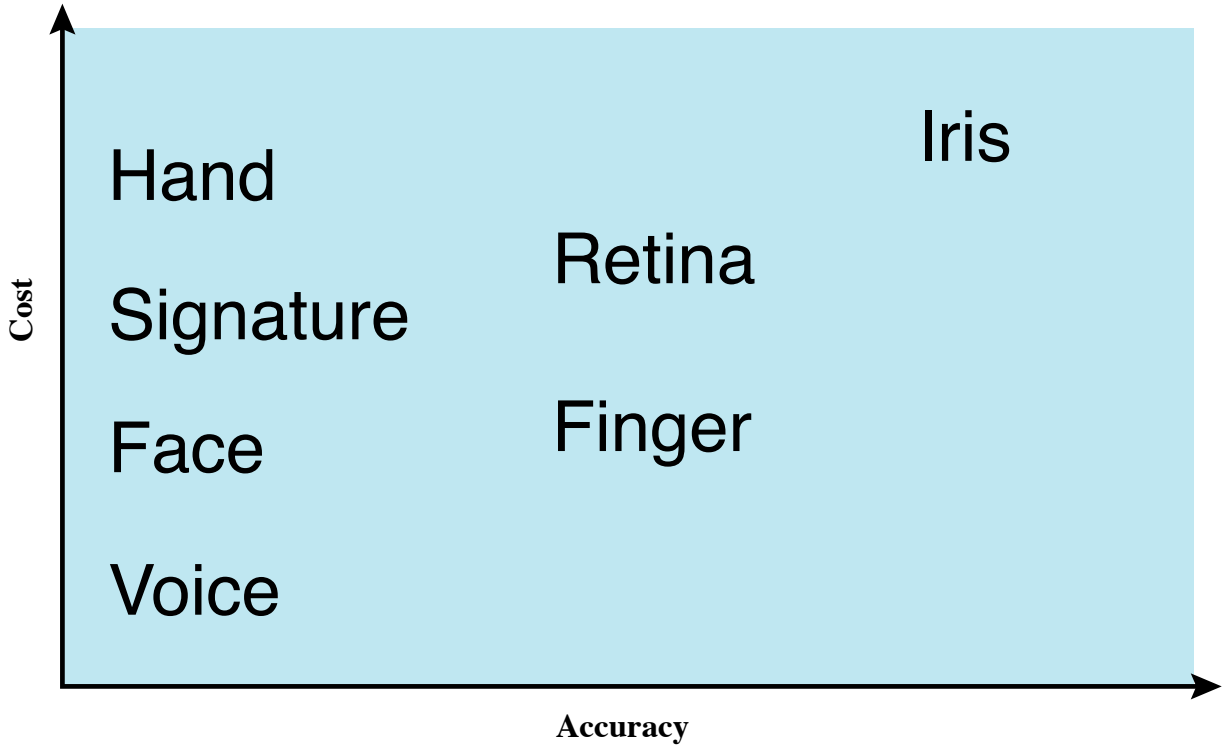
Autenticazione biometrica - accuratezza

- Uno score è detto *genuine* (autentico) se è il risultato del matching di due esempi della stessa caratteristica biometrica di un individuo; è detto *impostor* se nasce dal confronto tra due esempi di individui diversi.
- Uno score *impostor* che supera la soglia prefissata causa una falsa accettazione (*falso postivo*).
  - Falso positivo→ misurazioni biometriche di persone diverse sono erroneamente considerate come appartenenti alla stessa persona
- Uno score *genuine* inferiore alla soglia prefissata determina una falsa reiezione (falso negativo).
  - Falso negativo → misurazioni biometriche della stessa persona sono erroneamente attribuite a persone diverse

Autenticazione biometrica - accuratezza



Autenticazione biometrica - accuratezza



Autenticazione remota

Client	Transmission	Host
U, user	$U \rightarrow$	
	$\leftarrow \{r, h(), f()\}$	random number h(), f(), functions
P' password r', return of r	$f(r', h(P')) \rightarrow$	
	$\leftarrow$ yes/no	if $f(r', h(P')) = f(r, h(P(U)))$ then yes else no

(a) Protocol for a password

Client	Transmission	Host
U, user	$U \rightarrow$	
	$\leftarrow \{ r, h(), f()\}$	r, random number h(), f(), functions
$P' \rightarrow W'$ password to passcode via token r', return of r	$f(r', h(W')) \rightarrow$	
	$\leftarrow$ yes/no	if $f(r', h(W')) = f(r, h(W(U)))$ then yes else no

(b) Protocol for a token

Client	Transmission	Host
U, user	$U \rightarrow$	
	$\leftarrow \{ r, E()\}$	r, random number E(), function
$B' \rightarrow BT'$ biometric D' biometric device r', return of r	$E(r', D', BT') \rightarrow$	$E^{-1}E(r', P', BT') = (r', P', BT')$
	$\leftarrow$ yes/no	if $r' = r$ and $D' = D$ and $BT' = BT(U)$ then yes else no

(c) Protocol for static biometric

Client	Transmission	Host
U, user	$U \rightarrow$	
	$\leftarrow \{ r, x, E()\}$	r, random number x, random sequence challenge E(), function
$B', x' \rightarrow BS'(x')$ r', return of r	$E(r', BS'(x')) \rightarrow$	$E^{-1}E(r', BS'(x')) = (r', BS'(x'))$ extract B' from $BS'(x')$
	$\leftarrow$ yes/no	if $r' = r$ and $x' = x$ and $B' = B(U)$ then yes else no

(d) Protocol for dynamic biometric