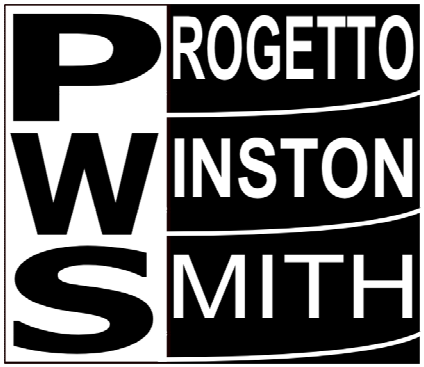
E-Privacy 2004

Firenze, 14 – 15 maggio 2004



Il sottile confine tra privacy e sicurezza: i dispositivi biometrici

Yvette Agostini - yvette@yvetteagostini.it
vodka@s0ftpj.org
Il Progetto Winston Smith
The Freenet Project

Di cosa parleremo ?

- Cosa sono I sistemi biometrici
- identificazione e riconoscimento
- Caratteristiche biometriche
- Indici di accuratezza
- schema di principio e vulnerabilità
- Biometria e privacy
- Bibliografia

Cosa sono I sistemi biometrici

DEFINIZIONE

Un sistema biometrico è un dispositivo che è in grado, in modo **automatizzato**, di **identificare** una **persona** basandosi su caratteristiche di tipo **biologico**

Le caratteristiche di tipo biologico possono essere:

- **fisiologiche**: tendenzialmente statiche, “di forma”
- **comportamentali**: relative a come l’individuo esegue determinate azioni

Identificazione

L’identificazione è il processo che consente di risalire all’identità di una persona esaminando una “impronta” biometrica calcolata a partire dalle caratteristiche biometriche dell’individuo

Esempio: il sistema di identificazione basato su parametri del volto, in test da parte della Polizia Ferroviaria alla Stazione Termini di Roma

(http://www.weekit.it/weekit/unico/art006004038993.jsp)

Riconoscimento

Il riconoscimento prevede che l'identità della persona sia nota a priori e l'impronta biometrica viene confrontata con il modello precedentemente immagazzinato. Se questi due template si discostano troppo, allora la persona viene respinta.

Il riconoscimento è la metodologia di funzionamento che ci interessa più da vicino (maniglie biometriche, videoriconoscimento, ecc)

Requisiti delle caratteristiche biometriche

Quando una caratteristica biologica è usabile in biometria?

- E' **universale**: tutti la possiedono
- E' **unica**: non esistono due persone con la stessa caratteristica
- E' **permanente**, ovvero non varia nel tempo
- E' **misurabile**, cioe' e' facile da misurare correttamente

Requisiti delle tecniche di misurazione

Quali caratteristiche deve avere il sistema di misurazione delle caratteristiche biometriche?

- performance in termini di accuratezza
- accettabilità, cioè deve essere gradito a chi deve sottoporsi a misurazione
- sicurezza, in termini di elevata difficoltà a essere ingannato

Caratteristiche fisiologiche

Caratteristiche fisiologiche:

- impronte digitali
- forma della mano
- forma del volto
- vari parametri dell'occhio
- DNA

Caratteristiche comportamentali

Caratteristiche comportamentali:

- dinamica della firma
- dinamica della digitazione a tastiera
- emissione vocale

Indici di accuratezza: FAR e FRR

FRR = False Rejection Rate

percentuale di utenti autorizzati che vengono erroneamente respinti = probabilità di non riconoscere chi è autorizzato

FAR = False Acceptance Rate

percentuale di utenti non autorizzati che vengono erroneamente accettati = probabilità di accettare chi non è autorizzato

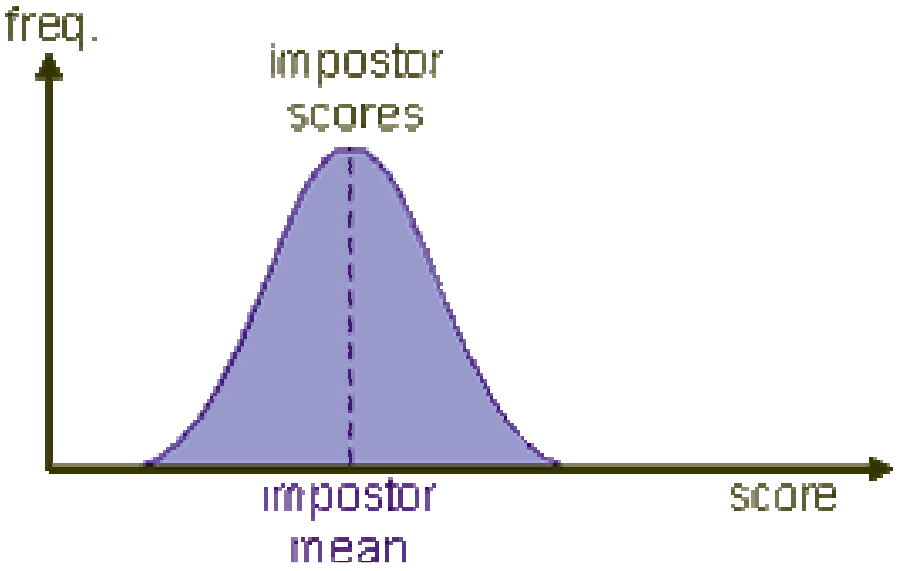
Più si è selettivi e più aumenta la probabilità che una persona autorizzata sia respinta e viceversa

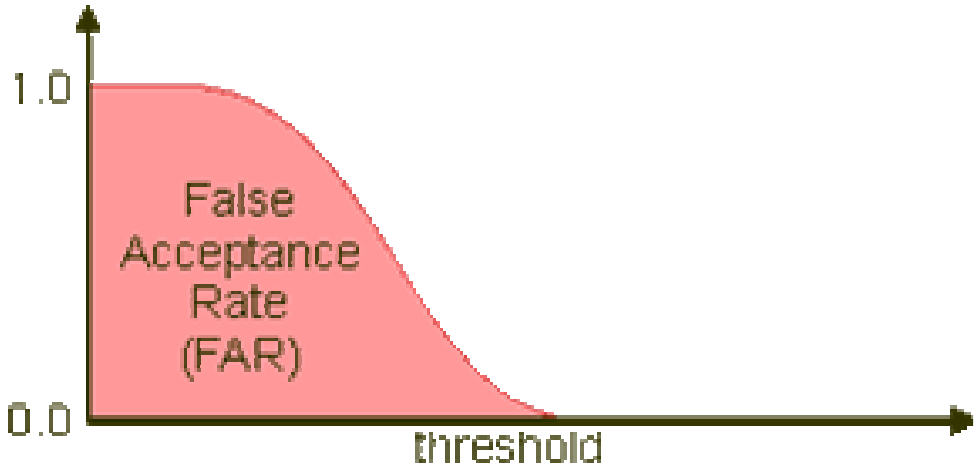
Il punto di equilibrio dove **FAR=FRR** è detto **EER** (**Equal Error Rate**)

Indici di accuratezza: FAR

FAR = False Acceptance Rate

percentuale di utenti non autorizzati che vengono erroneamente accettati = probabilità di accettare chi non è autorizzato



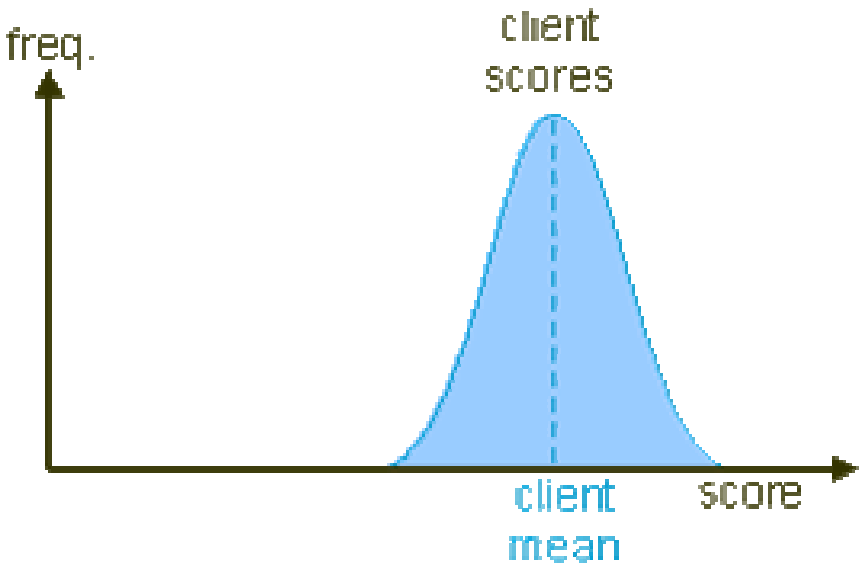


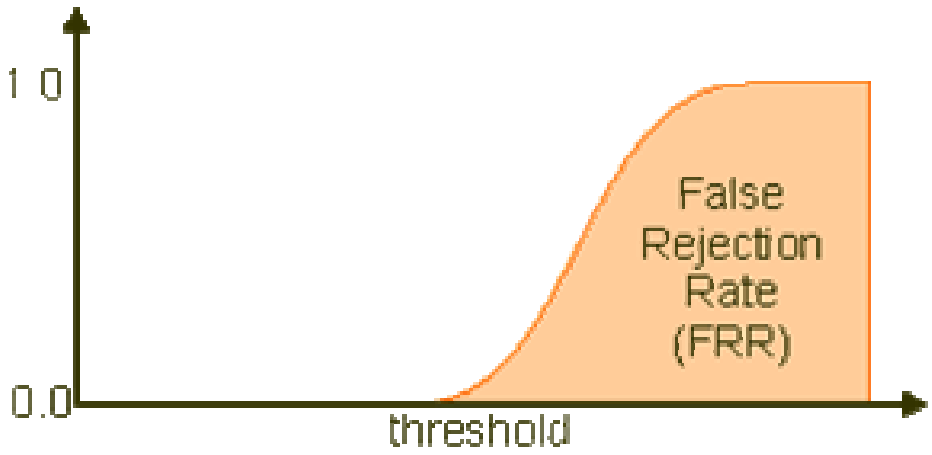
Immagini tratte dal sito http://www.bioid.com/sdk/docs/About_EER.htm

Indici di accuratezza: FRR

FRR = False Rejection Rate

percentuale di utenti autorizzati che vengono erroneamente respinti = probabilità di non riconoscere chi è autorizzato





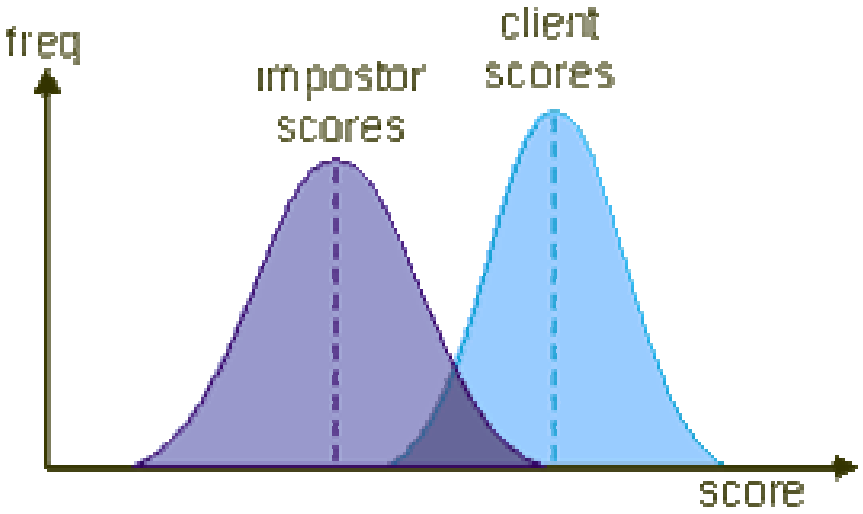
Immagini tratte dal sito http://www.bioid.com/sdk/docs/About_EER.htm

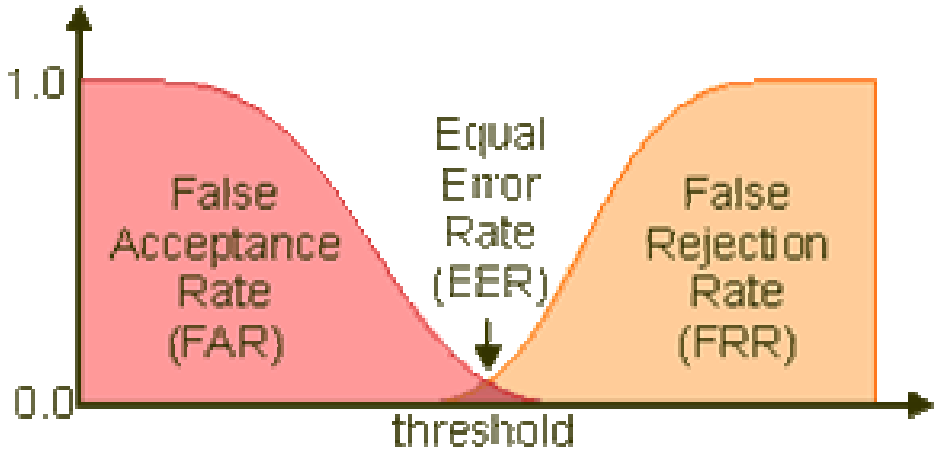
Indici di accuratezza: EER

Il punto di equilibrio dove **FAR=FRR** è detto **EER (Equal Error Rate**)

L'EER può essere usato come indice di prestazione:

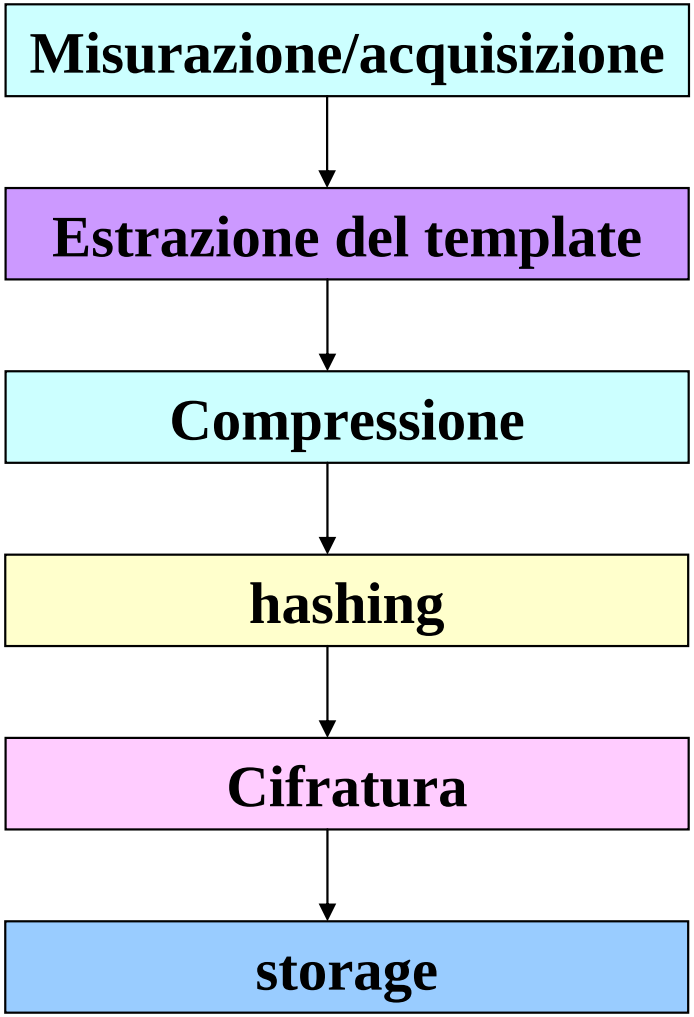
Tanto più è piccol l'EER, tanto migliore è la prestazione del sistema (teoricamente)





Immagini tratte dal sito http://www.bioid.com/sdk/docs/About_EER.htm

Schema di massima



Può essere locale, remoto, o su device portabile

Vulnerabilità dei sistemi biometrici (1)

A livello di dispositivo:

spoof attack = Resistenza allo spoofing (finte impronte, registrazioni vocali, ecc)

replay attack = Resistenza agli attacchi volti alla replicazione delle caratteristiche biometriche acquisite

communication attack = Resistenza all'intercettazione in transito delle grandezze acquisite

Vulnerabilità dei sistemi biometrici (2)

A livello di sistema:

Database attack = attacco che si basa sulle debolezze del db in cui vengono conservati i template

Reverse engineering = attacco volto a individuare i punti deboli dei vari algoritmi con cui sono processate le grandezze

Alteration attack = si basa su falle nella gestione dei permessi del sistema, che può consentire di alterare i template biometrici

Software attack = sfruttamento delle vulnerabilità dei driver che interfacciano il dispositivo biometrico

La posizione UE sui sistemi biometrici

L'1 agosto 2003 a Brussels i Garanti Europei durante una riunione con presidenza italiana hanno approvato un documento di lavoro relativo ai sistemi biometrici e la privacy:

.....L'impiego di sistemi biometrici non è lecito se non è proporzionato agli scopi che si vogliono raggiungere**, in particolare nei casi in cui si propone di creare archivi centralizzati. Tali informazioni sono particolarmente delicate e il loro uso, se da un lato può contribuire a salvaguardare la privacy riducendo il ricorso ad altri dati personali quali nome, indirizzo o domicilio, dall'altro può comportare **rischi legati all'utilizzazione indebita o indiscriminata di informazioni desunte da tracce fisiche (come le impronte digitali) che una persona può lasciare anche senza rendersene conto.....

Biometria e rischi per la privacy

Nell'ultima relazione del Garante della Privacy (28 aprile 2004), un intero capitolo è dedicato ai dispositivi biometrici. In particolare:

..."Lo ripetiamo: il corpo in sè sta diventando una password."...

*..." Il **principio di necessità** impone di accertare se la finalità perseguita non possa essere realizzata utilizzando dati che non coinvolgano il corpo. Il **principio di proporzionalità** esige una considerazione rigorosa della legittimità di raccolte generalizzate rispetto a raccolte mirate, di una conservazione centralizzata o decentrata dei dati raccolti. Il **principio di dignità** fa emergere la necessità di rispettare l'autonomia delle persone di fronte a particolari raccolte di dati (quelle riguardanti la salute, in primo luogo)."....*

Bibliografia

Bibliografia

- http://www.privacy.gov.au/news/speeches/sp10_03.pdf
- http://www.bioid.com/sdk/docs/About_EER.htm
- http://www.extremetech.com/article2/0,1558,13919,00.asp
- http://www.dia.unisa.it/~ads/corso-security/www/CORSO-9900/biometria/sommario.htm
- http://www.biometrics.org
- http://www.bioapi.org/BIOAPI1.1.pdf

E molti altri siti e documenti liberamente reperibili in rete utilizzando motori di ricerca.

Progetto Winston Smith

per maggiori informazioni: **marcoc@dada.it**

mail list su Freenet in italiano

http://lists.firenze.linux.it/mailman/listinfo/freenet-list

Sito ufficiale Freenet

http://www.freenetproject.org/

Il progetto Winston Smith

freenet:SSK@Dgg5lJQu-WO905TrlZ0LjQHXDdIPAgM/pws/13//

Grazie per l'attenzione :)

Yvette Agostini
yvette@yvetteagostini.it http://yvetteagostini.it

oppure:

vodka
vodka@s0ftpj.org http://www.s0ftpj.org