PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 3 - numero 446 di mercoledì 21 novembre 2001

Biometria: luci ed ombre

Una riflessione sulla sicurezza dei sistemi di riconoscimento basati sulla tecnologia biometrica.

L'emergenza terrorismo ha reso pressante la ricerca di adeguate misure di sicurezza.
L'attenzione si e' rivolta in particolare nei confronti dei sistemi di individuazione basati sulla biometria cioe' sul riconoscimento di caratteristiche della persona non modificabili (ad esempio: impronte digitali, iride...).

Le tecniche biometriche funzionano secondo il principio per cui le informazioni sono trasformate in un 'modello' matematico che serve per il confronto con un insieme di dati precedentemente memorizzati.

Tuttavia l'entusiasmo e la fiducia nei confronti di questa tecnologia sono talvolta eccessivi, come mostra un'analisi presentata dal giornale tedesco "Die Zeit", e ripresa nella newsletter del Garante italiano per la privacy.
L'articolo apparso nei giorni scorsi, illustrando i risultati di due ricerche, mette in luce pregi e limiti della biometria.

La prima ricerca e' stata condotta nell'aprile del 2000 dall'Ufficio federale tedesco per la sicurezza delle tecnologie informatiche con l'obiettivo di verificare la violabilità di alcuni sistemi biometrici disponibili in commercio.

Sebbene falsificare le informazioni biometriche sia molto difficile, anche se teoricamente possibile, l'analisi ha dimostrato che alcuni sistemi biometrici non sono a prova di hacker.
Infatti si sono dimostrati vulnerabili a due tipi di attacchi, precisamente gli "attacchi-replay" e mediante la manipolazione dei valori di soglia.

Negli "attacchi replay" l'hacker, introducendosi nel sistema informatico, ruba una copia dell'immagine digitalizzata e se ne serve in diversi modi .
Negli attacchi mediante la manipolazione del " valore di soglia" viene invece modificato il valore di tolleranza, proprio di ciascun sistema, fra i dati registrati e il modello matematico elaborato sulla base della rilevazione effettuata dall'apparecchio.
Un valore di tolleranza e' necessario in quanto i valori rilevarti possono essere influenzati da alcuni fattori, quali ad esempio temperatura e pressione.

Un hacker potrebbe tentare di manipolare questa soglia di tolleranza, aumentandola in modo da facilitare l'accettazione da parte del sistema dei dati biometrici registrati.

La seconda ricerca, realizzata da un gruppo di studiosi dell'IBM, ha individuato otto possibili modalità per attaccare un sistema biometrico.
Ad esempio introducendo nel sistema informatico un codice capace modificare il risultato finale della procedura biometria, in modo tale che anche se l'inserimento e l'analisi dei dati sono effettuati in modo corretto, il risultato generato dal sistema è sbagliato.

Requisito fondamentale per garantire la sicurezza dei dati biometrici e' la possibilita' di criptarli.
Per rendere inefficaci eventuali attacchi, alcuni sistemi dispositivi utilizzati per la rilevazione delle informazioni biometriche si identifichino rispetto al sistema informatico attraverso un codice numerico, altri utilizzano filigrane digitali per garantirsi contro la falsificazione di stringhe di dati.

Un altro importante interrogativo e' stato inoltre sollevato: cosa accade nel caso i dati biometrici siano "rubati" nel corso di un attacco messo a punto da pirati informatici?
Una password si puo' sempre cambiare...non cosi' le caratteristiche sulle quali sono effettuate le rilevazioni biometriche.