PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 4 - numero 559 di martedì 21 maggio 2002

Sistemi biometrici poco affidabili?

Un ricercatore giapponese afferma di poter gabbare con la gelatina i rilevatori di impronte digitali. Realta' o fantasia? Ecco cosa ne pensa un esperto di sicurezza...

Su un noto quotidiano di informatica è stata recentemente data notizia di una ricerca condotta da Tsutomu Matsumoto, ricercatore dell'università giapponese Yokohama National, sull'affidabilità dei sistemi di identificazione basati sul riconoscimento delle impronte digitali.

Il ricercatore sostiene che è possibile ingannare questi sistemi creando una impronta "clonata" grazie alla gelatina.
Dopo aver modellato una forma, in plastica, del proprio dito ed averla coperta di gelatina, Tsutomu Matsumoto sarebbe riuscito 4 volte su 5 a gabbare i sistemi di autenticazione basati sul riconoscimento delle impronte digitali.

Ma il ricercatore è andato oltre...
Afferma infatti che le impronte rilevate su un oggetto, ad esempio su un bicchiere, dopo essere state rielaborate, possono essere trasferite sulla gelatina ed utilizzate per aggirare i sistemi di riconoscimento delle impronte digitali.
Gli esperimenti sono stati condotti su 11 diversi tipi di sistemi.

Ciò significa che i sistemi biometrici non sono affidabili? Lo abbiamo chiesto a Nicola Bartesaghi, esperto nella progettazione di sistemi di sicurezza.
Ecco la sua opinione:

"Un esperto in sicurezza tende a creare una netta distinzione tra le tecnologie biometriche esistenti in commercio:
1) dispositivi da abbinare al controllo dei PC, dei Server di rete, di terminali mobili quali cellulari, palmari, ecc...
2) prodotti dedicati per il controllo degli accessi a varchi pedonali

Gli apparati del primo tipo hanno un costo di pochi dollari e presentano una possibilità di elusione abbastanza nota, soprattutto i prodotti di tipo ottico.
Tali apparati sono impiegati per proteggere i dati contenuti nella memoria del PC al posto di una password; ma il loro utilizzo non è adatto per applicazioni di altissima sicurezza.
Le ragioni di impiego di un prodotto possono dipendere dal prezzo: basso prezzo corrisponde ad una maggiore penetrazione nel mercato e quindi un maggiore numero di vendite di pezzi (parlando con logiche di Marketing).
La diffusione su larga scala di questi prodotti è legata soprattutto all'aumento della velocità di calcolo dei microprocessori e alla estrema miniaturizzazione dei sensori e abbattimento dei costi di produzione.

Lo studio di Tsutomu Matsumoto ha riguardato i sistemi del primo tipo e sarebbe interessante conoscere nello specifico i prodotti presi in esame.
L'analisi sui metodi di elusione di questi sistemi è stata affrontata seguendo una teoria per niente nuova.
Lo studio di Tsutomu Matsumoto si é concentrato infatti sui lettori di impronte digitali e la tecnica di elusione utilizzata é stata quella della duplicazione, con strumenti e materie oggi facilmente disponibili, della stessa impronta.

Diverso il discorso per gli apparati del secondo tipo, quelli progettati e sviluppati per essere impiegati negli insediamenti ad alto rischio come dei sistemi di controllo accessi ai varchi, sistemi che hanno un costo e dei contenuti in termini tecnologici decisamente più elevati.

Se un lettore biometrico per PC costa pochi dollari, un lettore biometrico impiegato in installazioni di alta sicurezza ne costa qualche migliaio.

Questa differenza di prezzo é legata ai contenuti in termini di funzionalità e prestazioni di questo secondo genere di tecnologia. Vi é infatti un maggiore numero di controlli da parte del lettore: analisi impronta, misura della temperatura corporea, misura conducibilità della pelle, opacità dei tessuti, ecc....

Nelle applicazioni che richiedono grande sicurezza, l'acquisizione di una impronta da parte di un lettore biometrico é associata spesso anche ad una immagine ripresa da una telecamera che documenta sottoforma di immagine, la persona che compie l'azione di riconoscimento.
Tutto questo produce un livello di sicurezza maggiore, ma anche un limite di impiego, legato soprattutto al costo di queste tecnologie.

Nei varchi cosiddetti ad alto rischio viene spesso impiegata una doppia tecnologia con procedure di controllo legate alle logiche booleane di "AND". Ad esempio oltre al lettore dell'impronta digitale viene installato un lettore di badge.
Tutti e due i sistemi, biometrico + badge, devono infatti riconoscere l'individuo e l'oggetto in suo possesso prima di autorizzare l'accesso.
Possedere un dito finto in gelatina o in gomma non servirebbe comunque a nulla senza il possesso fisico anche della tessera/badge.

E' giusto infine ricordare quelli che sono i reali limiti delle tecnologie biometriche che circoscrivono le possibilità di impiego di tali sistemi:
-un lettore biometrico può causare inconventienti e disagi fisici durante l'uso; es. una persona che indossa dei guanti deve togliere gli stessi se deve farsi riconoscere dal lettore, lo stesso dicasi per il controllo della retina che necessita da parte dell'utente di togliersi gli occhiali prima della lettura, ecc...
-un lettore biometrico può richiedere un tempo per il risconoscimento maggiore rispetto alla tecnologia tradizionale (es. singolo badge); questo rende non idonea la tecnologia per il controllo di varchi ove vi é un flusso elevato di persone.

La qualità di un sistema biometrico viene poi misurato confrontando i seguenti valori:
-percentuale di "falsa accettazione": per la quale un individuo non autorizzato viene erroneamente riconosciuto;
-percentuale di "falso rigetto": per la quale un individuo autorizzato in realtà non viene accettato dal sistema.
Più sono bassi i valori percentuali e più un prodotto é buono.
Per la scelta della soluzione più adatta alla propria esigenza, il consiglio é sempre quello di rivolgersi ad un esperto di una azienda di sicurezza che possa valutare nello specifico le reali problematiche ed i rischi connessi con l'attività lavorativa."

---

www.puntosicuro.it