

45134513134515313472346 1345 TFGHDF00VSAT3145134513245135
4582435234652346 341TEWRF623455ZHDF8 345
52345

EDTHSFDG0FGNSADGAF6AFSG

FDGBFGN

FGH0GBFTHF6HFGN

2345ERTERG00SFATTIGS0GLA

SCANNING...

57%

32452

54665

34523

23456

13452

32452345

5466572345

3452345

234562346

13452345

3452345

23452345236

3452345623465

234652345

2346524356

13457245431

4354565672

3425572345

34252346

23465234662345

2345234673245

23452345626123

34562342346

23452345

23542325623456

34252345234

Addio vecchie password:
il futuro della sicurezza
passa da noi. Ecco perché
useremo impronte, palmi,
occhi e anche il Dna come
chiave di accesso ai dati.

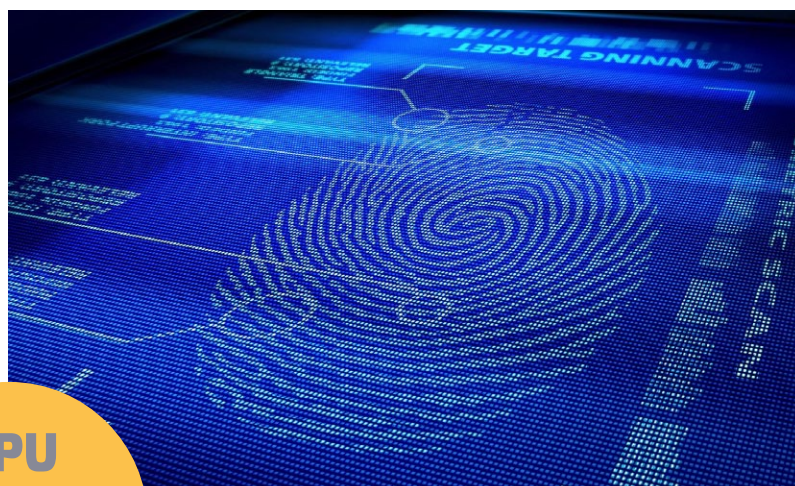
► Di Davide Piumetti

BIO ME TRIA

La sicurezza è uno di quei temi che, periodicamente, portano a grandi cambiamenti nell'informatica. Il bisogno di rendere sicure le informazioni più sensibili crea la necessità di sistemi di accesso sempre più difficili da eludere ma che, al tempo stesso, non siano eccessivamente complicati da utilizzare per gli utenti. In queste pagine vogliamo percorrere le prossime tappe che la necessità di sicurezza introdurrà in ambito informatico, ovvero l'autenticazione biometrica. Portare le credenziali di accesso a livello personale ci permetterà di utilizzare l'estrema varietà che la natura ci ha donato per prevenire accessi indesiderati da parte di malintenzionati.

È innegabile come al giorno d'oggi tutti noi dobbiamo confrontarci con l'utilizzo di sistemi elettronici che contengono dati o informazioni per noi molto sensibili: smartphone, tablet e computer sono esempi fisici sotto gli occhi di tutti, ma non possiamo non considerare anche i dati online come il conto corrente o i dati previdenziali, che contengono informazioni estremamente preziose. L'accesso a tali informazioni è di conseguenza molto appetibile ai malintenzionati, sempre pronti ad approfittare delle debolezze dei sistemi informatici per venire in possesso di dati sensibili da poter utilizzare per i propri scopi. Se fino agli albori dell'era informatica i crimini contro i dati personali erano riconducibili ai soli furti di proprietà, a oggi le cose sono estremamente più complicate.

I furti dei dati digitali possono infatti non essere immediatamente visibili (al contrario del furto di un'automobile), un cybercriminale può usare i dati di cui è venuto in possesso all'insaputa degli utenti e per molto tempo, causando a volte danni che vanno oltre il semplice valore economico. Sono innumerevoli i casi di furto di identità, casistica che porta un estraneo a impossessarsi di credenziali che forniscono una precisa identità, permettendo (tendenzialmente sul web) di spacciarsi per un'altra persona ed effettuare azioni per conto di essa con danni, anche a livello di immagine, a volte gravissimi. Per proteggere i dati "elettronici" da anni si fa utilizzo di sistemi di accesso adatti a identificare univocamente il proprietario, o



GPU

L'elevato parallelismo consente attacchi brute force con oltre 3 miliardi di tentativi al secondo

meglio, gli autorizzati ad accedervi. Il sistema più semplice e conosciuto è quello della parola chiave, la *password*.

Una parola, frase o numero segreto che blocca l'accesso ai dati, esattamente come la combinazione di una cassaforte. Esempi di password, o similari, sono di conseguenza la parola chiave per l'accesso al Pc, alla posta elettronica o, ampliando il discorso, anche il Pin del bancomat o il codice di accesso allo smartphone, così come le chiavi della porta di casa o dell'automobile.

Tutte queste chiavi di accesso presentano due caratteristiche opposte: devono essere facili da utilizzare per il proprietario ma difficilissime da replicare o da scovare per un malintenzionato. Questo è il fulcro di tutto quanto ruota attorno alla galassia della sicurezza: semplice se si è in possesso della chiave, complicato se non la si possiede o conosce.

OGGI: LA PASSWORD

Le misure impiegate oggi per limitare l'accesso a determinati sistemi da parte di malintenzionati si basano in grandissima parte su semplici parole chiave, a volte coadiuvate da un'autenticazione in due step (il primo tramite parola chiave e il secondo con un codice spedito su un dispositivo sotto il nostro controllo, lo smartphone o la mail per esempio).

L'utilizzo di un sistema del genere permette di diffondere la parola chiave a più utenti autorizzati, facendo in modo che tutti possano usare la medesima per accedere (ma nulla vieta di utilizzarne una specifica per ogni persona). Essendo il sistema attualmente più diffuso è quello che, storicamente, ha avuto più studi sulla propria vulnerabilità e quello su quale si concentrano gli attacchi di tutti i malintenzionati. Scovare una parola chiave è infatti un procedimento che può avvenire in diversi modi; tralasciando quelli relativi

al farsi rivelare la password in maniera violenta possiamo citarne diversi. Il *phishing* per esempio sta prendendo sempre più piede e consiste nel farsi rivelare la password fingendosi un sito o un'istituzione attendibile (simulando una pagina web o reindirizzando la navigazione dell'utente su siti fraudolenti). Con password semplici, ovvero con un numero limitato di combinazioni possibili (vedi box a lato) uno dei sistemi più utilizzati è quello del cosiddetto attacco *brute force*, che consiste nel provare tutte le combinazioni possibili fino a trovare quella corretta.

Questo attacco, che sembra richiedere tempi lunghissimi se applicato in maniera semplice, ha delle evoluzioni che permettono di ridurre drasticamente le tempistiche. In ambito informatico si possono usare dei dizionari contenenti le password storicamente più utilizzate (no, la parola *password* non è proprio una buona idea come parola chiave d'accesso...) o, utilizzando algoritmi complessi, cercare di eliminare le combinazioni meno frequenti in modo da poter scovare una password in tempi più che decenti. Esempio concreto: una password per un sito web che può contenere caratteri minuscoli, maiuscoli e numeri e una lunghezza di 4 caratteri ha 14.776.336 combinazioni possibili. Un Pc in grado di provare 1.000 password al secondo impiega circa 4 ore per provare tutte le combinazioni. Resta inteso che il tempo necessario per scovare la

password può essere inferiore, visto che potrebbe essere trovata anche al primo tentativo...

Mediamente ipotizziamo che può essere trovata in 2 ore, la metà del tempo precedente. Se le cifre salgono a 6 il numero di combinazioni sale enormemente e raggiunge quota 56.800.235.584, che, con la potenza computazionale espressa in precedenza corrisponde a circa 22 mesi per testare tutte le password.

Con questi numeri le nostre password sembrano decisamente al sicuro, ma purtroppo l'enorme evoluzione tecnologica avvenuta nel mondo informatico ha portato a sistemi con una potenza enormemente superiore. Una moderna scheda grafica (quelle maggiormente malleabili per questi scopi visto il loro grande parallelismo) può effettuare un numero enorme di tentativi al secondo, anche oltre i 3 miliardi al secondo. Riportato ai valori precedenti possiamo verificare come il recupero di una password da 4 caratteri impiega anche meno di 1 secondo e una con 6 caratteri meno di 20 secondi...

Per evitare password così semplicemente ricavabili da qualche tempo i siti web, soprattutto quelli che trattano dati finanziari, hanno inserito l'obbligatorietà di password contenenti anche punteggiatura e caratteri speciali (!, %, &, e così via) e lunghezza di almeno 8 caratteri. Il numero di combinazioni in questo caso è nettamente superiore: 2,7



LE PASSWORD PIÙ DIFFUSE NEL 2014

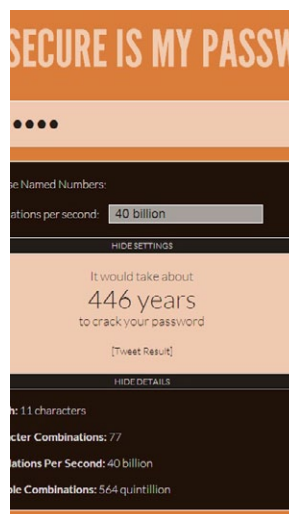


S spesso si crede che trovare una password sia difficile e tentativi "a casaccio" non portino ad alcun risultato. Peccato che poi, leggendo i rapporti periodici emersi online si può notare come, per accedere ad almeno il 50% dei sistemi, sia possibile usare una ridottissima lista di password. Le più comuni sono talmente scontate quanto diffuse, tanto che qualunque malintenzionato fa almeno un tentativo con queste. Nel 2013 la password più diffusa al mondo è stata "123456", seguita a ruota da "password". Al terzo posto, poco staccata "12345678", probabilmente usata dove sono richiesti almeno 8 caratteri. Altro grande classico sono le prime lettere in alto a sinistra della tastiera "qwerty", mentre si piazza al quinto posto la complicatissima "abc123". In ordine troviamo poi variazioni sul tema: "123456789", "111111", "1234567" e la prima che ha un senso diverso e compiuto: "iloveyou". Molto diffuse sono anche "admin" e "trustno1", direttamente dalla serie televisiva X-Files. La vostra è tra queste o simile? Bene, cambiatela.

QUANTO È SICURA LA MIA PASSWORD?

E sistono diversi siti web in grado di darvi un riscontro sulla sicurezza della vostra password attuale, basandosi sugli algoritmi brute force attualmente conosciuti, sui dizionari utilizzati dagli hacker e dalle potenze di calcolo proprie dei sistemi attuali. Per esempio la password "pcpro" può essere craccata in millesimi di secondo, aggiungendo dei numeri "pcpro2014" si passa a oltre 40 minuti, mentre con una lettera maiuscola "Pcpro2014" si arriva a 3 giorni. Una password davvero sicura contiene anche simboli. Per "PcPro2014!!" sono necessari oltre 400 anni.

<https://howsecureismypassword.net/>



milioni di miliardi (più precisamente 2.724.905.250.390.625) ovvero circa 2 settimane di calcoli a piena potenza. Questi esempi sono semplicemente per mostrarvi come le password che vengono utilizzate ogni giorno sono intrinsecamente molto deboli e solo utilizzando almeno 10 o 12 caratteri è possibile avere meno preoccupazioni. Il punto è che, con le potenze di calcolo attuali, è necessario utilizzare password molto complesse per poter essere sicuri, esigenza che si scontra nettamente con la capacità di ricordare tali complessità, magari differenti per ogni sito web, dispositivo o elemento in nostro possesso, tendenzialmente impossibile per chiunque non possieda una memoria di ferro.

LA NATURA CI RENDE UNICI

L'evoluzione tecnologica ha di conseguenza portato a una sempre minor sicurezza delle password personali così come le conosciamo. La possibilità di ricavare velocemente parole anche complesse, contenenti numeri o caratteri speciali, ha indebolito notevolmente la sicurezza dei nostri dati digitali. A fare da contraltare a questa continua evoluzione è l'impossibilità a passare a parole chiave più complesse, con un maggior numero di combinazioni possibili. Memorizzare infatti un pin a 50 o 60 cifre è praticamente impossibile, anche se quello è il livello che oggi garantirebbe una sicurezza davvero inviolabile. Questo ostacolo insormontabile risulta però semplicemente aggirabile se ci basiamo su qualcosa che non ha inventato l'uomo, ma che la natura ci ha donato e che risulta al tempo stesso di immediato utilizzo e di

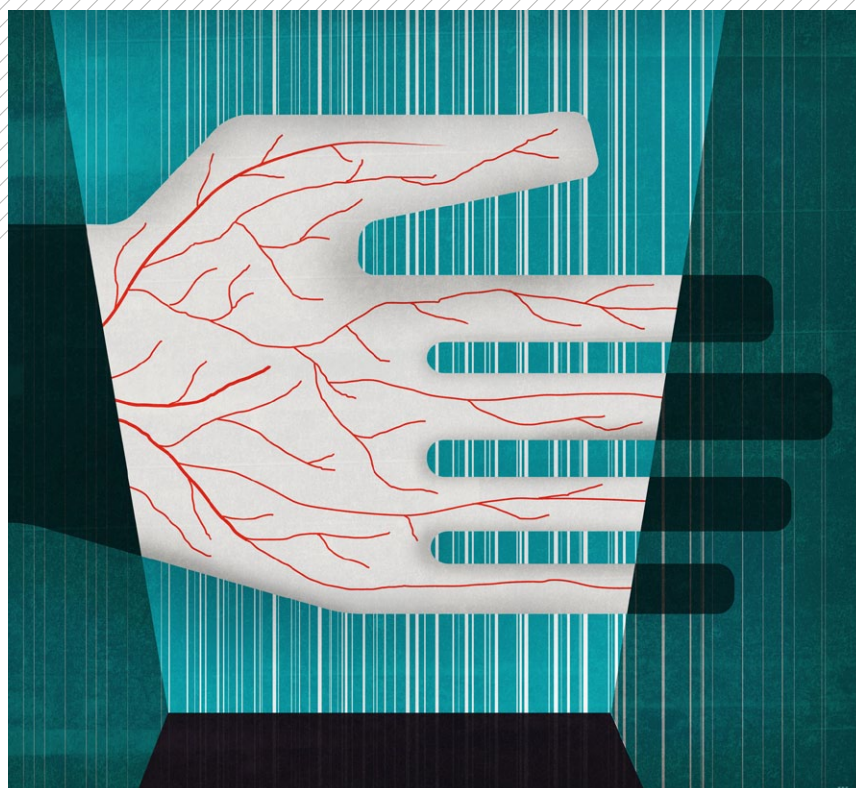
difficilissima contraffazione: noi stessi. Gli ultimi anni hanno infatti portato alla ribalta un nuovo settore tecnologico che racchiude in sé sia componenti digitali sia alcuni aspetti del corpo umano: la biometria.

Questa parola, che significa letteralmente *misura della vita* (da *bios* = vita e *metron* = misura) è la scienza che studia le dimensioni e le grandezze del corpo umano allo scopo di identificarne i valori di funzionamento in modo da poterli utilizzare in ambito tecnologico. Il succo è quello di utilizzare qualcosa di unico, non riproducibile e che non possiamo certo dimenticarci o appuntare su un biglietto che ci possa venire rubato, per autenticarci ad accedere ai nostri dati personali. Questa cosa è semplicemente il nostro corpo, o meglio, alcuni tratti personali che ci rendono unici e distinguibili

univocamente da chiunque altro.

I tratti biometrici identificano infatti univocamente un individuo e offrono una varietà tale da risultare al di fuori di ogni algoritmo di calcolo oggi conosciuto. Le microscopiche differenze tra ciascuno di noi, siano le impronte digitali, la disposizione dei vasi sanguigni o, addirittura, il Dna, hanno una varietà tale che solo la Natura poteva produrre. Le combinazioni possibili sono innumerevoli e vanificano ogni tentativo di forzatura tramite gli algoritmi brute force.

Nel seguito vediamo alcuni dei tratti biometrici che possono essere (o sono già) utilizzati per l'identificazione, partendo da quelli più conosciuti e anche diffusi, fino a quelli al limite della fantascienza.



ASPETTI LEGALI

L'uso di dati personali come le misure biometriche per l'accesso ad altri dati è un argomento che, dal punto di vista legislativo, ha sollevato ben più di una critica. Nel 2005 il Garante per la privacy (l'Autorità garante per la protezione dei dati personali) ha espresso il proprio parere in relazione all'utilizzo di dati biometrici in ambito lavorativo. In particolare l'Autorità si è espressa indicando due aspetti legali riguardanti la possibilità di utilizzare tali dati biometrici per controllare gli spostamenti del personale a fini di controllo e retributivo. In particolare il Garante ha indicato la necessità di informare a priori i dipendenti circa la modalità di recupero e seguente gestione di tali dati, garantendo la possibilità di registrare la presenza sul luogo di lavoro con metodi alternativi rifiutando il conferimento all'azienda di dati biometrici.



IMPRONTE E PALMO

Il più semplice sistema di riconoscimento biometrico, conosciuto praticamente da chiunque, è l'impronta digitale. Largamente utilizzato da anni, permette di identificare univocamente una persona partendo dall'impronta lasciata dai dermatoglifi dell'ultima falange delle dita della mano.

Un dermatoglifo è il profilo risultante dall'alternanza di creste e valli presenti sull'epidermide superficiale di mani e piedi, con dimensioni nell'ordine dei micrometri. L'altezza di questi solchi è variabile da individuo a individuo e compresa indicativamente tra 100 e 300 micrometri, il periodo tra due creste è invece grande circa 500 micrometri. Dal punto di vista organico queste variazioni sono dovute alla costituzione della pelle, composta da tessuto, epidermide e derma. Gli ultimi due strati sono l'epidermide (più esterna) e il derma, che offre supporto e connessioni con il resto del corpo. Tali connessioni, dette papille dermiche, hanno spessori e dimensioni unici, sostenendo di più gli strati superficiali in alcuni punti e meno in altri. Ogni individuo, gemelli omozigoti inclusi, ha impronte digitali uniche, immutabili e individuali, caratteristiche che le rendono perfette come strumento di identificazione e accesso a dati e sistemi. Vista la loro costituzione biologica le impronte digitali sono infatti immutabili, anche tagli o abrasioni non comportano (dopo

la loro guarigione) a modifiche nel disegno delle impronte.

Chirurgicamente inoltre è impossibile modificare le impronte in maniera da essere identiche a quelle di qualcun altro, è possibile un'abrasione profonda, con danni permanenti, ma in questo caso i danni si riflettono anche a livello funzionale sul tessuto sottostante. A livello biometrico le impronte digitali rappresentano dunque una fotografia unica appartenente a un singolo individuo. Gli strumenti per leggerne lo stato e garantire o negare l'accesso a dati o sistemi sono in commercio da anni, sono integrati in diversi sistemi e ormai di uso comune.

Uno scanner di impronte digitali agisce come un normale scanner per documenti, solo in scala molto più piccola. La prima configurazione avviene leggendo più volte l'impronta in modo da memorizzare alcuni tratti caratteristici nel database cifrato all'interno. La lettura per l'accesso avviene nel medesimo modo, e se il sistema riconosce l'impronta come identica (entro certi limiti) all'originale, approva l'accesso a dati o sistemi.

In commercio esistono sensori integrati nei dispositivi o separati e utilizzabili per scopi diversi. Su molti notebook è da anni presente un piccolo lettore a fessura



Ingrandimento del dito della mano. Si notano le creste e le valli che compongono le impronte digitali. Ciascuna di esse è unica, sia nella forma sia nelle dimensioni.

sul quale far scorrere il dito. In questi casi il lettore è fermo e il trascinamento del dito permette di effettuare una scansione completa da comparare con l'originale. Molto spesso è utilizzato il dito indice, sia per la sua maggior comodità e rapidità d'uso sia per motivi pratici: esso è infatti il dito con l'impronta

maggiormente chiara per via della sua normale conformazione quasi piana. In questo tipo di dispositivi è comunque possibile utilizzare qualunque dito, senza distinzioni. Altri sistemi di lettura delle impronte digitali hanno ampiezza maggiore

ed è sufficiente appoggiare il dito, senza scorrere, per un riconoscimento completo. L'evoluzione tecnologica e la conseguente riduzione delle dimensioni di questi sistemi, ha permesso la loro integrazione anche negli smartphone più in voga, come l'iPhone 5s o il Galaxy S5, permettendo (con risultati alterni) di rendere sicuri i propri dispositivi in maniera definitiva.

Sul mercato, per poche decine di euro, si possono trovare lettori Usb esterni di impronte digitali: con un dispositivo di questo tipo è possibile rendere sicuro il proprio desktop o notebook imponendo l'inserimento di una password biometrica per l'accesso (tutti i più diffusi sistemi operativi la supportano ormai nativamente). L'importante è avere una password di backup (lunga e complessa) da utilizzare in caso di fallimento del riconoscimento biometrico o di guasto hardware del dispositivo. Le impronte digitali consentono dunque una sicurezza d'accesso davvero notevole con una praticità e un'efficacia che le normali password non possono raggiungere. In realtà esiste la possibilità di duplicare le impronte di una persona (leggendole da

Password

È importante avere una password (complessa) di backup, nel caso il sistema biometrico si guastasse



Anche gli **smartphone più evoluti** iniziano a integrare lettori biometrici. Il più semplice, quello di impronte digitali, è presente da tempo sull'iPhone 5S, sostituendo il pin e permettendo un accesso sicuro ai dati.

Un **sistema di controllo degli accessi** con identificazione delle impronte. Questo sensore legge l'impronta del richiedente e ne certifica l'identità.



un'impronta lasciata su una qualunque superficie) e replicando la struttura su un supporto di silicone. Questo approccio permette di superare i lettori biometrici più semplici e rappresenta uno dei pochi punti deboli di questo approccio.

LETTURA DELLA MANO

Non serve allontanarsi molto dalle dita per trovare un'altra caratteristica biometrica che rende ogni individuo unico e indistinguibile: la mano e la sua struttura. Due sono gli elementi che la rendono utilizzabile per il riconoscimento, la sua impronta e la sua struttura interna. L'impronta rappresenta l'estensione all'intera superficie della mano di quanto espresso in precedenza, con le stesse considerazioni sull'utilizzo e sul sistema di accesso. Questo approccio, ipotizzato ma nella pratica utilizzato molto di rado, è stato ormai soppiantato da un miglior (e più sicuro) modo di leggere le informazioni biometriche della mano.

Se le impronte digitali possono essere duplicate utilizzando processi di lettura e stampa su materiali flessibili (ma entriamo nel campo dello spionaggio), non si può dire la stessa cosa per la struttura vascolare. Ognuno di noi ha infatti all'interno di ogni mano un reticolo fittissimo di vene, arterie e capillari che costituiscono

una ragnatela unica per ogni individuo. Essendo interna alla mano essa non risulta modificabile o alterabile e rappresenta un ottimo elemento da utilizzare in termini di sicurezza e accessi biometrici. Questi percorsi, che prendono il nome di *matrice vascolare*, sono unici e forniscono una caratteristica biometrica non visibile a tutti, ampia e stabile nel tempo, immutabile anche da fattori fisici e ambientali esterni, come cicatrici, ferite o semplici mani sporche. Il rilevamento di questa matrice 3D di vene e arterie viene effettuata tramite una luce infrarossa proiettata sul palmo e una lettura di quanto riflesso. La prima lettura consiste nel mapping completo della struttura tridimensionale, salvata poi (ovviamente in maniera sicura) sui dispositivi che operano il riconoscimento.

Successivamente avvicinando la mano, anche tenendola a distanza di circa 5 cm dal lettore, una luce infrarossa effettuerà la scansione e il software si occuperà di valutare a quale profilo salvato si riferisce la mano in questione. I sistemi di accesso più recenti impiegano circa 20 secondi per il setup iniziale, mentre per la scansione di accesso è sufficiente poco più di un secondo, decisamente meno rispetto a quanto necessario per digitare una password o strisciare un'impronta digitale. I punti di forza di una soluzione di questo

tipo sono innegabili: non essendo invasivo e non richiedendo un contatto diretto con il sensore offre garanzie anche dal punto di vista igienico, al contrario dei sistemi a impronta digitale.

L'utilizzo è semplice e immediato, con nessuno o pochissimo training per il personale e una precisione molto buona rispetto ad altri sistemi. A differenza di punti che toccheremo più avanti anche la privacy ne guadagna in quanto a essere schedata è la sola rappresentazione matematica della matrice vascolare, non l'immagine vera e propria. I contro sono ridotti e si possono limitare a un prezzo superiore a quello di un lettore di impronte e la necessità di una buona potenza computazionale qualora gli autorizzati all'accesso fossero un numero considerevole, in quanto la comparazione tra matrice esposta e quella salvata impiega non poche risorse.

In commercio troviamo diverse soluzioni di questo tipo. Una tra le più apprezzate è la *Palm Secure* di Fujitsu, di cui potete vedere il funzionamento qui sotto. Questa soluzione è tra le prime in grado di rendere possibile il riconoscimento biometrico anche su comuni Pc, tramite alcuni device in grado di utilizzare la semplice connessione Usb e software compatibile con la maggior parte dei sistemi operativi.

PALM SECURE: LA LETTURA DELLA MANO

Ecco come è possibile leggere la matrice vascolare della mano e usarla come chiave di riconoscimento univoca.



Il palmo della mano deve essere posizionato da 3 a 8 cm dal sensore.



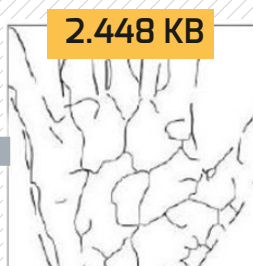
Per la lettura il sensore emette una luce infrarossa sul palmo.



Solo l'ossigeno presente nel sangue assorbe la luce.



La matrice viene salvata e identifica univocamente una persona.



Il software crea una mappa digitale, la codifica e la cifra.



In questo modo è possibile ricavare un'immagine dei vasi sanguigni.

OCCHI: RETINA E IRIDE



IMPRONTA RETINICA

Oggetto di moltissimi film di fantascienza uno dei più studiati sistemi di autenticazione biometrica è l'*impronta della retina*. Simile nel concetto alla matrice vascolare della mano il concetto si applica però alla profondità dell'occhio, nascondendo ancora di più le informazioni personali dai malintenzionati.

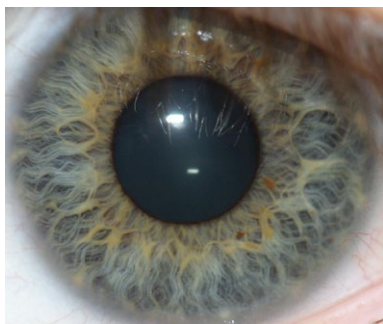
L'occhio umano infatti è composto da vari elementi; la retina è un tessuto composto da cellule neurali localizzata sul fondo dell'occhio e presenta una complessa struttura di capillari necessari per l'ossigenazione di tutti i suoi elementi. Tale struttura, proprio come nella mano, è unica e irripetibile e non cambia mai durante la vita (a meno di gravi patologie oculari). La sua posizione la rende inoltre difficilmente accessibile, tanto da risultare nascosta in ogni frangente se non quando necessaria per l'autenticazione.

Lo strumento necessario per l'identificazione prende il nome di scanner retinico e rappresenta un'apparecchiatura derivata da quella utilizzata in ambito medico per la diagnosi delle malattie. Il funzionamento è semplice: partendo dal presupposto che i vasi sanguigni assorbono la luce infrarossa in maniera leggermente diversa dal tessuto che li circonda è possibile, immettendo una

piccola quantità di luce di questo tipo nell'occhio e misurandone l'immagine riflessa. In particolare i vasi sanguigni assorbono maggiormente la luce rispetto al tessuto neurale in cui sono immersi e nell'immagine risultante risultano più scuri. L'immagine risultante, che potete vedere in queste pagine, rappresenta una mappa accurata dell'occhio di una persona (e ogni occhio è differente) e viene analizzata e convertita in un pattern numerico, che viene salvato alla stregua di una password e usato come sistema identificativo.

In maniera simile ai vasi della mano un sistema di riconoscimento di questo tipo è molto sicuro sia dal punto di vista dell'utilizzo sia da quello igienico. Per uno scan retinico non è infatti necessario toccare alcun oggetto, ma basta avvicinare il viso a un lettore apposito. Altri vantaggi sono la scarsissima presenza di falsi positivi, la più bassa tra i sistemi biometrici attualmente in essere e una quasi inesistente casistica di falsi negativi. La velocità di elaborazione è inoltre molto buona in quanto i vasi, come numero, sono minori rispetto a quelli della mano. Di contro c'è che un peggioramento della vista in termini di astigmatismo provoca una variazione della messa a fuoco dei vasi e l'immagine risultante potrebbe essere diversa e falsare i risultati. La comodità non è inoltre tra i punti di forza e i costi sono superiori alla maggior parte degli altri sistemi.

Una curiosità: gli "occhi rossi" che appaiono in molte fotografie sono proprio il risultato della riflessione della luce del flash sul fondo della retina che appare di questo colore per via di una proteina fotosensibile presente nei bastoncelli, il cui colore viene riflesso all'esterno. Nei cani e nei gatti, non essendoci questa proteina ma altre, gli occhi nelle fotografie con flash possono risultare gialli o blu.



L'iride umana, vista da vicino, nasconde una complessità inimmaginabile. Tramite formule matematiche la forma delle strutture interne viene elaborata e convertita in una password di grande complessità, unica per ciascun iride.

SCANSIONE DELL'IRIDE

L'occhio umano ha una complessità tale da permettere però un utilizzo duplice per quanto riguarda il riconoscimento biometrico. Oltre allo scanner retinico,



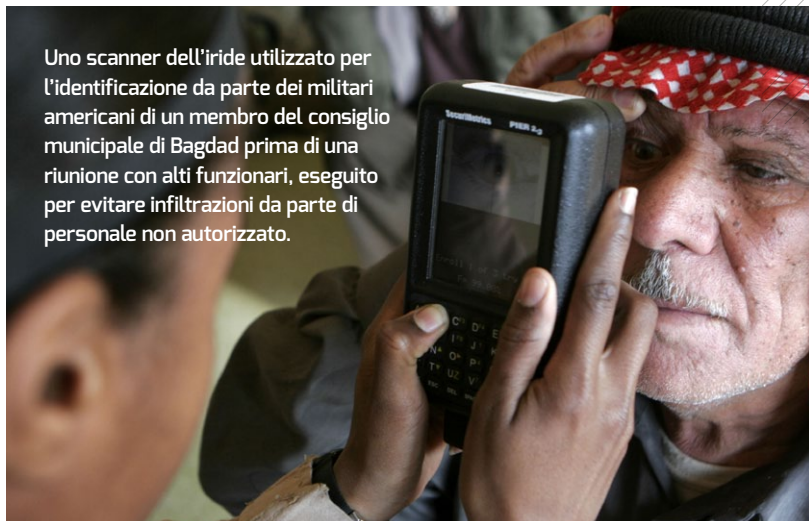
Due scansioni della retina umana. Si può notare il disco ottico, la macchia chiara nella quale convergono tutti i vasi sanguigni e il corpo luteo, la sagoma scura vicina al centro del disco.

in grado di identificare la struttura unica dei capillari sul fondo della retina, c'è un'altra caratteristica che ci rende unici e che è possibile utilizzare.

A differenza di capillari, sangue o impronte, siamo finalmente di fronte a qualcosa che guardiamo ogni giorno, spesso con ammirazione e un pizzico di invidia in base alle situazioni: parliamo dell'iride. L'iride è una membrana posta nella parte anteriore del bulbo oculare che svolge la funzione di diaframma e regola la quantità di luce che penetra all'interno dell'occhio e raggiunge la retina. Si trova dietro la cornea ed è attraversata completamente dalla pupilla. È la parte colorata dell'occhio, quella che ci colpisce di più nello sguardo degli altri e che più caratterizza il viso di una persona. Biologicamente l'iride è un tessuto composto da tre strati, il più profondo, detto epitelio, dona una pigmentazione fondamentale, solitamente di colore

VOCE

Uno scanner dell'iride utilizzato per l'identificazione da parte dei militari americani di un membro del consiglio municipale di Bagdad prima di una riunione con alti funzionari, eseguito per evitare infiltrazioni da parte di personale non autorizzato.



blu, che subisce una serie di rifrazioni nell'emergere della luce e assume nelle persone dagli occhi chiari un colore che varia dal grigio all'azzurro al blu. La parte superficiale include invece una parte di melanina e, in base alla quantità presente, modifica il colore dell'iride da verde a marrone scuro.

Dal punto di vista biometrico l'iride è una struttura che appare estremamente variegata. L'origine biologica di tale variazioni deriva dalle fibre muscolari che compongono lo strato centrale, e che donano a ciascuno di noi due occhi unici al mondo. Questo sistema di riconoscimento si basa di conseguenza sul medesimo principio degli altri ma, a differenza dello scanner retinico, non risulta così invasivo e costoso.

Dal punto di vista pratico questo sistema si basa sull'acquisizione di un'immagine a lunghezza d'onda visibile e nel vicino infrarosso (tra 700 e 900nm). Questa doppia scansione (effettuata comunque in un unico momento dagli scanner in circolazione), permette di visualizzare differenti pattern dell'iride: con luce visibile si eccita infatti la melanina presente e si illuminano pattern ben definiti, mentre con luce nel vicino infrarosso vengono analizzati percorsi più profondi. La combinazione di queste due immagini viene gestita tramite un software che ne crea una rappresentazione matematica univoca, che viene memorizzata come parola chiave.

Il principio operativo è pubblico e consiste nell'identificare fino a 200 punti all'interno dei disegni iridei, valutare i punti di inizio e fine di iride e pupilla e tracciare tramite alcuni algoritmi dei punti di identificazione nell'occhio. Successivamente queste informazioni vengono tradotte in serie di numeri complessi che identificano ampiezza

e fase delle strutture matematiche trovate e, successivamente, trasformate in un numero binario (solitamente a 2048 bit) che rappresenta il disegno specifico dell'iride.

L'identificazione di un soggetto avviene tramite la scansione dell'iride e la comparazione del risultato ottenuto con quanto salvato in precedenza. Ovviamente, viste le piccole distanze in gioco e la complessità matematica degli algoritmi, non ci si aspetta di arrivare a due risultati identici, ma perlomeno molto, molto simili.

L'identificazione è certa quando la distanza tra i due valori è al di sotto di una ben determinata soglia.

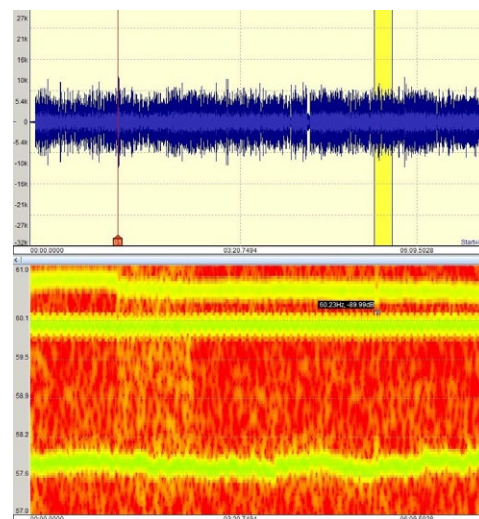
I vantaggi di questo metodo di identificazione sono diversi e hanno portato a considerare questo metodo come uno tra i più sicuri, ricevendo le maggiori attenzioni dagli sviluppatori. L'iride è infatti un organo interno, protetto dall'esterno e dalla maggior parte dei danni accidentali (a differenza delle impronte digitali ad esempio). Come altri sistemi di riconoscimento non è necessario un contatto diretto con lo scanner; anzi i moderni sistemi permettono di fotografare un volto e rilevarne l'iride anche a diversi metri di distanza, permettendo il riconoscimento preventivo anche prima del necessario. Questo è forse eccessivo, motivo per cui la legislazione in materia si sta muovendo sempre più velocemente.

In commercio ci sono decine e decine di soluzioni adatte allo scopo, la maggior parte delle quali utilizzate a fini di riconoscimento in ambito frontaliero o in siti produttivi ad accesso ristretto. L'utilizzo di sistemi di riconoscimento di questo tipo permette, ed è tra i pochi a poterlo fare, di ottenere un riconoscimento anche con guanti e occhiali protettivi.

Dopo vasi sanguigni, impronte o pattern oculari possiamo concentrarci su un altro aspetto personale che ci caratterizza e distingue da ogni altro: la voce. L'accesso a riconoscimento vocale è una branca della biometria che deriva dal pattern unico prodotto dalle nostre corde vocali mentre parliamo.

Da distinguere innanzitutto tra "riconoscimento vocale" in cui si riconosce *cosa* viene detto e "identificazione vocale" dove si identifica *chi* parla. La voce, che non è nient'altro che una combinazione di onde sonore variabili a seconda dell'assetto della bocca, di laringe, faringe e corde vocali, è infatti unica e inimitabile per ciascun individuo. Essendo una caratteristica prodotta da tante variabili, sia fisiologiche come la forma e le dimensioni di gola e bocca sia appresa come il tono di voce e lo stile di parlata.

Questo sistema biometrico si basa come gli altri su due fasi distinte, una prima registrazione e identificazione del soggetto e il successivo utilizzo come identificazione. La prima fase prevede la registrazione di frasi predefinite, in modo che il sistema possa estrarre matematicamente alcuni parametri chiave univoci per ciascun



La voce umana può essere scomposta nelle sue armoniche fondamentali, che caratterizzano ciascuno di noi. Anche una registrazione, per quanto perfetta, produrrà la nostra voce partendo da elementi meccanici e non dalle parti molli del corpo, che donano un tono unico alla voce.

individuo. Vengono evidenziati il timbro di voce, la cadenza e i picchi di determinati vocalizzi e sillabe, il tutto utilizzando alcuni algoritmi matematici molto diffusi come la stima di frequenza, la trasformata di Fourier e nelle implementazioni più avanzate anche algoritmi relativi alle reti neurali in modo da rendere ancora più preciso il riconoscimento di un pattern base specifico per la voce.

Questa particolare tecnica viene utilizzata in termini di riconoscimento in due scenari distinti e molto diversi tra loro. Il primo è come ulteriore fattore di autenticazione nella conferma dell'identità: una volta inseriti username e password che identificano univocamente una persona (oppure una qualunque altra forma di accesso biometrico) la voce viene registrata e confrontata direttamente con quella del proprietario delle credenziali d'accesso.

Il secondo scenario è relativo all'identificazione di un preciso individuo tramite la voce. Alcuni esperimenti effettuati hanno mostrato come già oggi bastino 30 secondi di registrazione telefonica (senza dunque frasi predefinite) per poter ricercare su un database il proprietario e identificarlo univocamente.

Questo è uno scenario in grado di promuovere diversi dubbi sulla liceità dell'utilizzo del riconoscimento biometrico, ma in alcuni casi diverse società stanno lavorando per una sua messa in atto. Alcune ipotesi d'uso sono relative agli assistenti vocali che sono già presenti su smartphone evoluti come l'iPhone (dalla generazione 4s) o i terminali Android con Google Now. Tramite identificazione della persona che chiede un'informazione sarà possibile restituire risultati ancora più accurati in base alle sue specifiche esigenze, migliorando l'esperienza d'uso e raffinando ulteriormente i risultati offerti.

A oggi i sistemi di identificazione vocale non sono alla portata di tutti, sia dal punto di vista delle problematiche relative alla potenza di calcolo sia per il proliferare di numerose soluzioni alternative di più semplice utilizzo. Invece, nell'ottica aziendale, le cose si stanno muovendo e i primi sistemi completi basati su questa tecnologia sono già attivi o in sperimentazione in molti ambiti.

IL FUTURO? ANCHE IL DNA

Tutti i metodi descritti in precedenza si basano su caratteristiche uniche di ogni individuo. In futuro potremo però essere identificati da quella che più di ogni altra ci contraddistingue: il Dna. L'acido desossiribonucleico è infatti la mappa completa di come è costruito il nostro corpo ed è di certo la cosa più unica che ciascuno di noi possiede. In pratica racchiude al suo interno tutte le informazioni biometriche di cui abbiamo parlato nelle pagine precedenti e anche molte di più. In più, a differenza degli altri elementi biometrici di accesso, si trova replicato in maniera identica in ogni cellula del nostro corpo e non localizzato in un singolo punto o elemento. Il Dna è composto da una doppia elica costituita da uno scheletro composto da un gruppo fosfato, uno zucchero e quattro basi azotate (*Adenina, Guanina, Citosina, Timina*) che si accoppiano due a due. Per questo è assimilabile a un codice quaternario che risulta unico per ciascun individuo. La sequenza del Dna può di conseguenza essere utilizzata come accesso biometrico, anche se la tecnologia attuale non ne permette un'adozione su larga scala. Analizzare il Dna non è infatti un'operazione da poco conto, ma richiede macchinari complessi e tempo da dedicare all'analisi e alla raccolta dei dati. Il risultato, a scopi di identificazione biometrica, non è nient'altro che una sequenza lineare delle basi azotate che lo compongono, del tipo "AGCTAGGCTA....." e assimilabile a un codice o a una password di complessità inimmaginabile. Attualmente l'analisi del Dna richiede un macchinario dedicato e i tempi per la lettura sono molto elevati, anche se negli ultimi anni si è passati da un periodo temporale di anni per decifrare la struttura alle poche ore necessarie oggi. Certamente i tempi necessari per garantire un riconoscimento e un accesso sono nettamente inferiori, ma è possibile ipotizzare che l'evoluzione tecnologica porterà, nei prossimi anni, a raggiungere tempi molto più stretti. Come abbiamo visto esistono dunque diverse tipologie di riconoscimento biometrico, dalle più semplici e già utilizzate ad altre che risultano essere quasi fantascientifiche. Tutti questi sistemi hanno o avranno un grande impatto sulla nostra vita in quanto, nei prossimi anni, molte informazioni o accessi saranno protetti con sistemi di questo tipo. Pensate solo per un momento alla comodità di non dover mai più digitare o ricordare una password, non aver più bisogno delle chiavi di casa o dell'automobile, con sistemi che si attivano (magari in maniera diversa) solo per le persone autorizzate. Se oggi può capitare di dimenticarsi i propri documenti o una parola chiave è decisamente meno probabile scordarsi i propri dati biometrici: occhi, mani e voce li portiamo infatti sempre con noi. Questa visione del futuro può sembrare lontana dal realizzarsi ma, a differenza di molte altre tecnologie promesse e mai pronte, questa potrebbe avere un percorso evolutivo differente. La motivazione è semplice, tramite queste tecnologie le grandi aziende potranno, in maniera simile a quanto avviene attualmente con i cookie sui siti web, tracciare le abitudini dei consumatori e rendere ancora più incisive e personalizzate le campagne pubblicitarie. Non dobbiamo però temere troppo questa deriva orwelliana, il controllo di questi dati è soggetto a leggi ferree e (nonostante le rivelazioni emerse negli ultimi mesi relative alle politiche della NSA statunitense) utilizzate principalmente per garantire la sicurezza dei cittadini. Sarebbe auspicabile, in ottica di un sempre maggior controllo dei controllori, avere un organismo normativo di alto livello in grado di vigilare sull'utilizzo nazionale di dati tanto sensibili.

LA STRUTTURA DEL DNA

La struttura del Dna può essere vista come una lunghissima password sequenziale che contraddistingue ognuno di noi.

