I trend della tecnologia biometrica - Sicurezza & User Experience

Di **Matthew Zajechowski**

USABILITYGEEK

16 Settembre 2013

Articolo originale:

Biometric Technology Trends – Security & User Experience

http://usabilitygeek.com/biometric-technology-trends-security-user-experience/

Foto di US Air Force

La scienza e le tecnologie biometriche comprendono tutto: dalla lettura delle impronte digitali (che è diventata una scienza già dal XIX secolo), al rilevamento dell'impronta del calore umano e della camminata, alla mappa delle vene, al DNA e, naturalmente, al riconoscimento facciale e alla scansione della retina o dell'iride.

Anche se la biometria, in un uno stadio più o meno embrionale, esiste da oltre 100 anni (pensiamo ad oltre un secolo di attività di identificazione delle impronte digitali, svolta dalla polizia), la tecnologia moderna ha portato la scienza a livelli completamente nuovi e l'ha ampliata includendo efficacemente tutte le caratteristiche fisiche citate sopra ed altre.

Strumenti analitici complessi come quelli per la decodifica genetica e sofisticati software basati su algoritmi che mettono insieme migliaia di piccole caratteristiche del corpo, hanno contribuito a rendere il campo della scienza biometrica moderna, più ampia e interessante di quanto non lo sia mai stata prima.

Ora che sappiamo che la tecnologia è lì pronta, la vera domanda è: come? Quanto sarà protettiva e quanto si rivelerà intrusiva, applicandola alla vita di tutti i giorni, negli anni a venire? In questo articolo analizzeremo le ultime tendenze della tecnologia biometrica con particolare attenzione all'impatto che queste avranno sulla sicurezza e sulla user experience dell'utente.

La sicurezza istituzionale

Oggi, si sta lentamente iniziando a inserire protocolli di sicurezza biometrici, nelle aree ad accesso ristretto, di molte strutture del governo e delle aziende; parliamo di enti governativi, grandi aziende o istituti di ricerca. Le tecnologie più comunemente utilizzate, includono la scansione dell'iride, l'identificazione facciale, le smart card con i dati biometrici del proprietario codificate nel chip e telecamere speciali in grado di leggere svariate caratteristiche del corpo.

Numerose società di sviluppo come la Homeland Security Corporation, Sense Technologies e Privaris, e molte altre, lavorano costantemente alla realizzazione di nuove soluzioni, che vengono poi adottate dalle istituzioni governative, i laboratori di ricerca tecnologica e gli uffici di grandi aziende.

In generale, il livello di utilizzo della biometria in questo tipo di ambienti è molto più diffuso di quanto non lo sia nella sfera pubblica e per una buona ragione: l'identificazione biometrica di solito rappresenta una sicurezza molto elevata, combinata con la comodità e la facilità d'uso; i dipendenti devono solo passare i loro occhi, o il viso, o le dita di fronte ad uno scanner, per essere identificati con certezza.

La sicurezza dall'elettronica di consumo

Quando si tratta di limitare l'accesso ai dispositivi elettronici di consumo, i sistemi biometrici sono ancora sorprendentemente assenti, considerato quanto sia facile e comoda la loro interfaccia uomo-macchina. Principalmente i sistemi che gestiscono dati digitali e i dispositivi elettronici che usiamo tutti, si affidano alla password o ad una chiave di accesso, come metodo per proteggere le nostre informazioni sensibili; nonostante il fatto che la maggior parte dei computer, portatili e smartphone tramite cui accediamo alle nostre informazioni digitali, siano dotati di fotocamere e potrebbero anche essere facilmente equipaggiati con altre tecnologie per la scansione biometrica.

Qualche progresso è stato fatto con i computer portatili che contengono sensori di scansione delle impronte digitali e telefoni cellulari con protocolli di lettura biometrica facciale, o dotati di scanner per le impronte digitali, ma l'uso di entrambi è ancora in grande misura poco diffuso. E la domanda diventa la seguente: perché mai?

In parte la risposta sta nell'inerzia dell'utilizzo della password; lo abbiamo fatto per così tanto tempo che è difficile adattarsi ad una nuova tecnologia, anche se è davvero molto più semplice da usare e più sicura di una stringa di caratteri che può essere manipolata, o indovinata da intrusi che vogliono penetrare nelle nostre macchine personali.

Un'altra possibile ragione per questo ritardo nell'adozione delle tecnologie biometriche, è il semplice fatto che applicare la biometria al mondo caotico in cui vivono i dispositivi dell'elettronica di consumo, che devono essere accessibili quotidianamente, in ogni genere di situazioni stressanti, la rende spesso inaffidabile. Mentre la digitazione di una password garantisce quasi sempre il funzionamento (fino a quando vi ricordate i caratteri da digitare), scorrere il dito su uno scanner dello smartphone con lo schermo umido, o il dito sporco, potrebbe produrre abbastanza insuccessi, da irritare l'utente.

Tuttavia, pare che questo tipo di problemi sia all'attenzione dei principali produttori di elettronica ed il recente acquisto da parte di Apple Computer, dell'azienda sviluppatrice di biometria, Authentec, per quasi 360 milioni dollari [http://www.patentlyapple.com/patently-apple/2013/07/apples-acquired-fingerprint-sensor-patent-from-authentec-comes-to-light.html], è un segno eloquente degli sviluppi futuri dell'iPhone e dei suoi cugini (e sappiamo tutti che se Apple decide di perseguire qualcosa di simile, l'altro principale concorrente del settore, Samsung, deve essere sulla stessa strada e non molto indietro).

Conclusioni riguardo all'elettronica di consumo: Se un importante produttore cominciasse ad abilitare opzioni biometriche efficaci e costantemente affidabili nei suoi dispositivi, la gente comincerebbe sicuramente ad utilizzare la tecnologia su larga scala.

E' semplicemente naturale che lo facciano, perché strisciare velocemente il dito sullo schermo o guardare nella fotocamera del telefono, tablet o laptop, per un momento, è un'interfaccia di sicurezza chiaramente molto più comoda, rispetto al digitare password lunghe e complesse, o magari utilizzare sistemi basati su due diversi fattori di riconoscimento. Sapere che nessun altro può manipolare o copiare il vostro volto,

dito, o occhio, come possono fare con la password, è un vantaggio aggiuntivo per l'utente.

La sicurezza pubblica

Infine arriviamo alla sicurezza pubblica generale. E' una arena in cui i dati biometrici diventeranno quasi certamente un fattore di grande importanza, in particolare nel settore dei viaggi e dei trasporti pubblici.

Che si tratti di aeroporti, valichi di frontiera o di punti di ingresso al trasporto pubblico, l'uso di una biometria efficace è un modo molto più veloce, più passivo e molto più efficiente, per identificare rapidamente un gran numero di persone senza bisogno di fermarle, o di far loro presentare le credenziali, per sottoporle ad un lungo esame.

Un esempio eccellente è il programma NEXUS [http://www.cbp.gov/xp/cgov/travel/trusted_traveler/nexus_prog/], gestito congiuntamente dalle agenzie per la sicurezza delle frontiere degli Stati Uniti e del Canada: i viaggiatori che si iscrivono al programma, vengono sottoposti ad un controllo accurato dei loro precedenti relativi a questioni di sicurezza, vengono date loro delle password speciali, che contengono le loro informazioni biometriche facciali e le impronte digitali, codificate e dopo possono spostarsi tra i due paesi molto più velocemente dei viaggiatori normali. La popolarità di questo sistema fra i chi viaggia per affari non può essere sottovalutata ed è molto probabile che vedremo programmi simili a questo, spuntare in altre regioni di frontiera di grande passaggio di tutto il mondo.

Le tendenze delle tecnologiche biometriche e l'esperienza utente

Abbiamo già discusso di come sia difficile equilibrio tra la sicurezza e l'esperienza utente nella vita reale. Infatti, le ultime tendenze della tecnologia biometrica indicano che i due fattori più importanti nella percezione dell'utente delle procedure biometriche, sono la user experience e l'accettazione di quella tecnologia da parte dell'utente. C'è da dire che le tecnologie biometriche solo adesso (e da poco), sono sufficientemente evolute, da poter essere considerate praticamente utilizzabili. Così come è stato per la tecnologia digitale, per la maggior parte della sua storia, la biometria è stata caratterizzata da numerosi problemi di usabilità. Naturalmente, le password ancora oggi condividono alcuni di questi problemi, ma almeno si collocano nel contesto di una tecnologia ben nota, non intrusiva e universalmente riconosciuta, rendendo le persone più tolleranti dei loro capricci.

Nell'usabilità, deve essere considerato anche il fattore tempo e qui è dove i sistemi biometrici più comunemente utilizzati, sono ancora perdenti, rispetto alla digitazione di un codice PIN memorizzato o di una password. Questo fatto ovviamente è destinato a cambiare nel corso del tempo, grazie all'evoluzione dei software di scansione, ma per adesso risulta ancora un elemento fastidioso a molte persone che devono sottoporsi regolarmente alle identificazioni biometriche.

Quando i problemi di usabilità delle biometrie commerciali ad ampia diffusione, saranno completamente risolti, sui nostri dispositivi di uso quotidiano, il prossimo ostacolo sarà quello della sua accettazione sociale e individuale (come gli studi hanno dimostrato [http://faculty.washington.edu/aragon/pubs/UsabilityETBiometrics-ICB13.pdf]).

Una cosa è comunque evidente: se una tecnologia per la sicurezza biometrica funziona senza intoppi, la sua facilità di utilizzo viene percepita da molte persone come molto elevata, dal momento che non è più necessario memorizzare stringhe di caratteri e che basta mostrare una caratteristica del proprio corpo ad un dispositivo di scansione ed è fatto. Tuttavia, nonostante questo, molte persone sembrano ancora

preferire il numero di accesso PIN, o la password, alla vecchia maniera, per pura abitudine. Questa resistenza sarà inevitabile, anche se la tecnologia biometrica verrà generalmente percepita come più sicura di questi vecchi metodi!

La prove sembrano dimostrare che, con un utilizzo sufficientemente ripetuto, di una tecnologia di lettura biometrica, che richiede un atto breve e soprattutto senza intoppi, molti utenti si adattano e oltretutto finiscono per preferirla, perché percepiscono questi sistemi, se non altro, come più sicuri rispetto alle loro attuali password e codici di accesso.

Matthew Zajechowski

Matthew Zajechowski scrive sui trend delle tecnologie biometriche e di altri argomenti correlati alla sicurezza e l'autenticazione, per Authentify [http://www.authentify.com/]. Contattate Matthew su Google+ [https://plus.google.com/118161543754778855946/posts].

Traduzione di **Marco Dini**

Questo articolo si trova qui:
www.ideawebitalia.it/usabilita-web/5974/