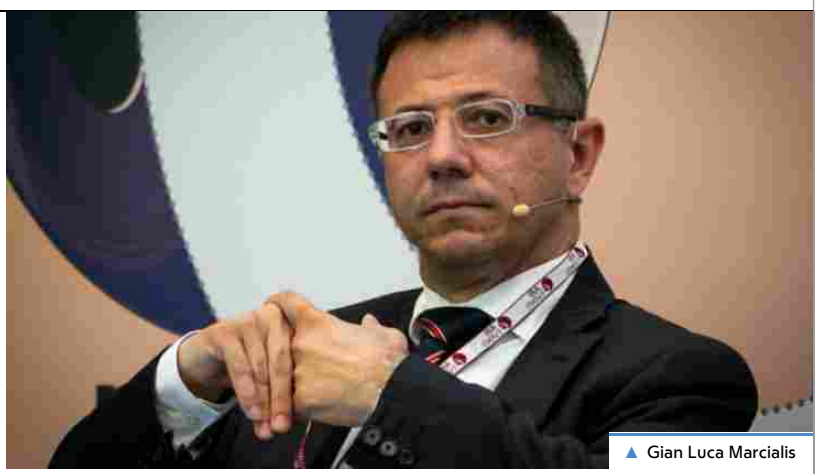
Ultim'ora 17.29 **Covid, 8.824 nuovi casi nelle ultime 24 ore con 158mila tamponi e 377 morti**

Addio password arriva il riconoscimento biometrico, ma i cyber ladri si stanno attrezzando



Gian Luca Marcialis

di Rosaria Amato

Intervista a Gian Luca Marcialis, docente di Tecnologie biometriche e sicurezza comportamentale all'Università di Cagliari e coordinatore del gruppo di studiosi che sta affinando i metodi per sventare i tentativi di contrattazione delle nuove barriere di sicurezza

18 GENNAIO 2021 3 MINUTI DI LETTURA

ROMA - L'accelerazione dei pagamenti digitali ci rende sempre più dipendenti dalle password. Ma tra pochi anni potrebbe non essere così: a breve potrebbero essere sostituite, o affiancate, dalle impronte digitali, o dal riconoscimento facciale o attraverso altre caratteristiche personali note come "biometriche". E se i cyber criminali sono già pronti, e hanno già affinato metodi per replicare gli aspetti più caratteristici di una persona, anche i ricercatori che lavorano su queste tecnologie hanno messo a punto contromisure efficaci, anche grazie all'intelligenza artificiale. "La biometrica non è replicabile così facilmente, ed è nel complesso più sicura di una password", dice Gian Luca Marcialis, docente di Tecnologie biometriche e sicurezza comportamentale all'Università di Cagliari.

Come si possono riprodurre le impronte digitali di una persona?

"Abbiamo iniziato a occuparcene nel 2006; il problema era già noto nel 2002, anche se la riproduzione di impronte digitali veniva considerato un evento raro ed improbabile, e tutto sommato ancora si usavano pochissimo, mentre oggi le abbiamo negli smartphone. La replica può essere fatta in modo abbastanza verosimile, per esempio attraverso una fotografia con il proprio smartphone, oppure usando una polvere magnetica che va a identificare l'esaltazione lasciata sulle superfici dal nostro dito. Oppure si può utilizzare un falso dell'impronta digitale impossessandosi della "traccia" lasciata da qualche parte, per esempio su una tazzina di caffè. Negli anni il mio gruppo ha sviluppato una considerevole esperienza nella riproduzione delle impronte attraverso materiali come siliconi e gelatine, e ne cerchiamo sempre nuovi e più efficaci. Questa abilità ci ha consentito e ci consente di riprodurre algoritmi "consapevoli" del problema, grazie all'analisi delle immagini ottenute da smartphone o da altro sensore (v. carta d'identità elettronica). Attraverso questa via stiamo quindi mettendo a punto le contromisure, di certo necessarie man mano che l'uso dell'impronta coinvolgerà applicazioni sempre più rilevanti sul fronte economico e personale".

Quindi dobbiamo preoccuparci che le nostre impronte possano essere rubate proprio come i nostri codici di accesso?

"I tratti biometrici non sono replicabili così facilmente, e risultano comunque più "affidabili" di una password che può essere dimenticata. Essi sono ormai un futuro che non possiamo più evitare; per esempio, mi sento di dire che la tecnologia dell'impronta in sé è molto matura, e insieme al riconoscimento dell'iride è anche quella più sicura. La via per renderla sempre più sicura è quella di individuare, grazie all'intelligenza artificiale, le caratteristiche che distinguono un'impronta autentica da una sua possibile replica, ed utilizzare poi algoritmi di riconoscimento personale efficaci anche in rapporto al loro utilizzo nei dispositivi mobili come i cellulari. Infatti, se sono capace di replicare esattamente un'impronta, posso anche trovare delle caratteristiche che mi permettono di distinguere il falso. Grazie alle tecniche di memorizzazione ed "apprendimento" basate sull'intelligenze artificiale, posso individuare tuttavia sia le caratteristiche "univoche", sia quelle le distinguono da un eventuale falso. I sistemi biometrici basati sull'intelligenza artificiale sono potenzialmente in grado di filtrare queste caratteristiche e bloccare un tentativo di accesso fraudolento. E' un po' come implementare, attraverso la macchina, la rappresentazione "interiore" che noi abbiamo dei nostri amici: non ricordiamo ogni singolo dettaglio fisico di loro, ma quelle

Milano, bolletta a 37 euro contro i 20 euro di Palermo

I capi junior delle griffe a noleggio su Clootee

caratteristiche che ce li rendono unici e non confondibili con "impostori"".

Utilizzate lo stesso metodo anche per scoprire le false identificazioni facciali?

"Attraverso l'uso degli algoritmi è possibile anche capire in un video se il volto di una persona è stato giustapposto, e identificare il volto contraffatto. Sono i cosiddetti "deep-fake" di cui tanto si parla. A livello di ricerca, si lavora affinché gli attuali software di intelligenza artificiale permettano anche di identificare un volto anche se parzialmente coperto, per esempio, dalla mascherina usata per proteggerci durante la pandemia, e si stanno ottenendo già risultati promettenti".

E la voce? Anche la voce può essere contraffatta

"La voce rientra nelle biometrie comportamentali, opposte a quelle fisiologiche: in questo caso il riconoscimento è legato al nostro comportamento. Per esempio l'andatura non deriva solo dal fatto che abbiamo due gambe, ognuno di noi ha un suo stile. Anche la voce è un altro tratto comportamentale: io posso urlare, parlare veloce, o lento, avere il tratto vocale alterato da stato di salute, ma ci sono delle invarianti, cioè delle caratteristiche misurabili che non variano con l'umore o con lo stato d'animo e che permettono il riconoscimento delle persone".

Tra quanto l'uso della biometrica potrebbe diventare quotidiano?

"Non posso fare con certezza una proiezione, ma posso dirle tranquillamente che se dovessimo solo fare riferimento al livello di tecnologia raggiunto, è molto probabile che nell'arco di 10 anni il mondo cambi da questo punto di vista. Già due anni fa al Salone dei Pagamenti dell'Abi è stata presentata la carta di credito con il sensore integrato. Un'altra via potrebbe essere quella dei pagamenti con il cellulare, già diffusissimi in Cina: ci sono grandi passi in avanti anche da noi in questa direzione da parte di importanti "player" nel settore".