PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 19 - numero 4115 di lunedì 06 novembre 2017

Riconoscimento biometrico: non è tutto oro quello che luccica!

Il riconoscimento biometrico delle impronte digitali, ha ormai conquistato una posizione di assoluta preminenza nel mondo del controllo degli accessi. Un recente studio mette in evidenza i significativi problemi della tecnologia adottata.

Pubblicità
<#? QUI-PUBBLICITA-MIM-[BIA0001] ?#>

Oggi la gran parte dei moderni smartphone offre al possessore la possibilità di farsi riconoscere dall'apparato, utilizzando l'impronta digitale. Credo che non valga più la pena di ricordare ai lettori quanto sia comoda questa tecnica di controllo dell'accesso al contenuto dell'apparato, per la estrema semplicità d'uso e per l'elevato livello di sicurezza.

Tuttavia è bene avere una idea chiara su come funzionano queste tecniche di riconoscimento, perché in realtà non è tutto oro quello che luccica.

Uno studio di specialisti di un'università americana ha messo in evidenza come la tecnologia adottata dalla grande maggioranza dei produttori di smartphone disponga di limitazioni intrinseche, che possono rendere assai meno affidabile il riconoscimento dell'impronta digitale.

Siamo tutti d'accordo che non esistono due persone che abbiano la stessa impronta digitale, ma questa affermazione va accompagnata dalla affermazione che il controllo deve essere effettuato fra due intere impronte digitali e non su due piccole parti.

In realtà, la stragrande maggioranza dei dispositivi biometrici non cattura e non analizza l'intera impronta digitale, ma solo alcune parti. Le ragioni sono dovute, ad esempio, alla opportunità di ridurre il carico di lavoro informatico e la quantità di memoria destinata ad archiviare i punti chiave dell'impronta digitale.

La stessa polizia scientifica dichiara che due impronte sono uguali quando vengono trovati almeno 17 punti di concordanza, opportunamente distribuiti sull'intera impronta digitale. Non viene effettuato un confronto analitico, millimetro quadro per millimetro quadro, dell'intera impronta digitale con quella sotto controllo. Quando si trovano 17 punti, identificati con specifiche coordinate, che presentano identità, le due impronte si ritengono identiche. Si può sempre proseguire l'esame, per maggior certezza, effettuando un confronto fra l'intera impronta digitale di riferimento è quella da esaminare, ma quest'operazione non viene effettuata spesso.

Vediamo ora come funzionano i sistemi di controllo accesso che vengono installati sugli smartphone.

Il proprietario dell'apparato appoggia la sua impronta digitale sullo schermo e una piccolissima parte di questa impronta, tipicamente dell'ordine di sei per sei millimetri o poco più, viene catturata e memorizzata. Con questa tecnica lo spazio di memoria necessario e il tempo necessario per l'elaborazione vengono ridotti in maniera drammatica. Quando il proprietario appoggia nuovamente il dito, viene catturata una analoga superficie e viene effettuato un confronto. A questo punto, se il confronto ha esito positivo, l'apparato dichiara che chi ha presentato l'impronta digitale è abilitato ad operare.

Appare evidente il fatto che, se è ben vero che non esistono due impronte digitali uguali, nessuno ha mai affermato che non possano esistere delle aree della impronta digitale che siano uguali tra più persone. Questa rappresenta la debolezza della tecnica di riconoscimento adottata.

Per questa ragione i ricercatori dell'università di New York hanno ipotizzato che vi potrebbero essere sufficienti similarità tra le impronte parziali di differenti persone, da poter creare una sorta di impronta maestra. I ricercatori, partendo da questo assunto, hanno cominciato a vedere se era possibile individuare una impronta maestra, che potesse consentire l'accesso agli apparati, aggirando il vincolo del riconoscimento del proprietario.

Lo studio ha messo in evidenza che alcune caratteristiche della distribuzione dei solchi e delle creste dell'impronta digitale umana hanno elementi di similarità tali da sollevare significativi dubbi sulla effettiva sicurezza.

Ad esempio, utilizzando un software commerciale di verifica delle impronte digitali, gli studiosi sono riusciti, analizzando la bellezza di 8200 impronte digitali parziali, a trovare circa 90 impronte maestre, che corrispondevano, almeno per il quattro percento, ad altri impronte digitali del campione esaminato.

Non può sorprendere il fatto che vi sia una ben maggiore probabilità di un accoppiamento ritenuto corretto tra una impronta digitale parziale ed una completa, ed ecco dove nasce la debolezza specifica dell'architettura utilizzata.

Avendo creato questa impronta digitale maestra, la squadra ha dimostrato che è riuscita ad effettuare degli accoppiamenti positivi tra il 25 ed il 65 per cento degli utenti, in funzione di quante impronte parziali venivano archiviate sul dispositivo. È bene infatti ricordare che molti utenti registrano più impronte digitali sullo stesso dispositivo e questo fatto porta ad un accrescimento del livello di vulnerabilità.

Il fatto poi che i produttori di sensori di impronte digitali costruiscano dispositivi sempre più piccoli, fa sì che la risoluzione del sensore, se non viene accresciuta in modo significativo, possa costituire un limite assai preoccupante alla qualità e validità del riconoscimento.

I lettori, appassionati di tecniche di riconoscimento basate su impronte digitali, sono adesso avvertiti!

Adalberto Biasiotti

 Questo articolo è pubblicato sotto una Licenza Creative Commons.

---

www.puntosicuro.it