IL MOBILE E LA BIOMETRIA

Uso del della Biometria per l'autenticazione

Autore: Aldo Pedico – Enterprise Security & Privacy Architect

Contatto: pedicoaldo@gmail.com

1. PREMESSA

Per la realizzazione di questo articolo, ho preso spunto dal manuale "Draft NIST IR 8334 Using Mobile Device Biometrics for Authenticating First Responders".

Molte organizzazioni di pubblica sicurezza (Public Security Organization - PSO) e private hanno adottato dispositivi mobili, come smartphone e tablet, per consentire l'accesso a informazioni sensibili.

I requisiti di autenticazione destinati a salvaguardare le informazioni, come l'immissione di una password complessa o il recupero di un token crittografico e la lettura di una password monouso, possono ostacolare l'accesso, ad esempio nel caso di utilizzi in ambito sanitario, qualsiasi ritardo, anche secondi, potrebbe creare molti rischi in una emergenza.

Le funzionalità biometriche sono diventate onnipresenti su smartphone e tablet commerciali, tra cui l'impronta digitale di Apple e la scansione del viso, l'impronta digitale di Samsung, la scansione del viso e dell'iride e molti altri.

L'utilizzo della biometria con i dispositivi mobili potrebbe potenzialmente aiutare a rendere l'autenticazione più rapida e semplice, ma ci sono ancora sfide da affrontare con la biometria dei dispositivi mobili in generale.

2. ANALISI DEL CONTESTO ATTUALE

DEFINIZIONE: *le linee guida sull'identità digitale del NIST definiscono la biometria come "**riconoscimento automatizzato di individui in base alle loro caratteristiche biologiche e comportamentali**".*

FATTORI DI AUTENTICAZIONE

È importante garantire che solo le persone autorizzate possano accedere alle informazioni sensibili.

L'autenticazione di un utente implica la verifica dell'evidenza di uno o più fattori di autenticazione, come descritto nella tabella seguente.

FATTORE DI AUTENTICAZIONE	DESCRIZIONE	ESEMPI
Something you know (***ciò che sai***)	*Informazione non pubblica condivisa tra un utente finale e un servizio digitale*	*- Password;* *- Personal Identification Number (PIN)*
Something you have (***ciò che possiedi***)	*Un supporto di memoria contenente una informazione riservata di proprietà esclusiva dell'utente*	*Token per la cifratura o crittografia*
Something you are (***ciò che sei***)	*Biometria*	*- Impronta digitale* *- Immagine del viso* *- Immagine dell'iride*

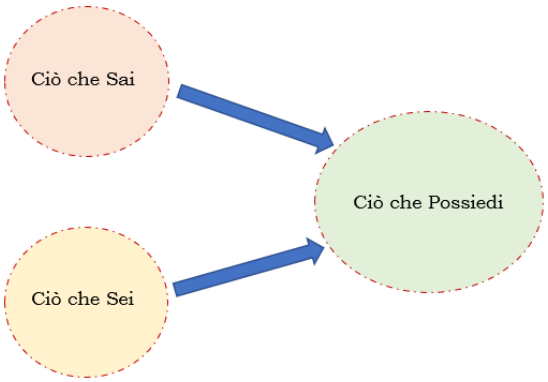
L'autenticazione che utilizza una combinazione di due o più tipi di fattori di autenticazione è definita **MULTI-FACTOR AUTHENTICATION (MFA)**. *Tale autenticazione per ovvi motivi è più forte rispetto all'autenticazione a un fattore.*

Un'opzione per l'MFA consiste nel richiedere all'utente finale di autenticarsi con "**ciò che possiedi**" *attivato da* "**ciò che sai**"*, in modo che il servizio abbia la prova del possesso del dispositivo fisico.*

Nel caso di un intervento sanitario, questo è spesso difficile per i primi soccorritori, che dovrebbero memorizzare i segreti e inserire rapidamente l'informazione durante un'emergenza per ottenere l'accesso a informazioni vitali.

Un'altra opzione per l'MFA è utilizzare "**ciò che sei**" *invece di* "**ciò che sai**" *per attivare* "**ciò che possiedi**".

DIAGRAMMA FATTORI D'AUTENTICAZIONE



Ad esempio, nel caso di un intervento sanitario, un primo soccorritore potrebbe utilizzare un'impronta biometrica anziché un PIN o una password per attivare un dispositivo mobile contenente una chiave crittografica segreta ben protetta.

La biometria è stata utilizzata in un'ampia gamma di sistemi di autenticazione.

Sono utilizzati sia nel controllo dell'accesso logico (controllo dell'accesso a sistemi e applicazioni informatici) sia nel controllo dell'accesso fisico (controllo dell'accesso a edifici fisici, strutture e stanze), da soli o con altri fattori di autenticazione negli schemi MFA.

IL RUOLO DELLA BIOMETRIA

L'utilizzo della biometria per l'autenticazione è spesso frainteso.

Un malinteso comune è considerare la biometria un'azione di rilevamento segreta, in realtà la biometria di una persona può essere ottenuta online o scattando una foto di qualcuno con la fotocamera del telefono (ad es. immagini del viso) con o senza la sua conoscenza, sollevata da oggetti toccati da qualcuno (ad es. impronte digitali latenti) o catturata con immagini ad alta risoluzione (ad es. modelli dell'iride).

Una biometria può, tuttavia, essere utilizzata come parte dell'MFA in combinazione con uno specifico autenticatore fisico ("**ciò che possiedi**"*).*

Ad esempio, potrebbe trattarsi di un'impronta digitale utilizzata per accedere a una chiave crittografica segreta archiviata su un dispositivo mobile.

ABBINAMENTI BIOMETRICI E MODALITÀ DI VERIFICA

La figura successiva mostra i passaggi di un modello di corrispondenza biometrica semplificato per la verifica dell'identità di una persona.

Durante la registrazione, i dati biometrici di un nuovo utente vengono raccolti e archiviati per un uso futuro nella verifica dell'identità durante i tentativi di autenticazione.

La metà superiore della figura illustra i seguenti passaggi.

1. *Un campione biometrico viene raccolto catturando un'immagine (o qualche altra somiglianza) del tratto biometrico (noto anche come presentazione) dal nuovo utente.*
2. *Il campione biometrico viene elaborato in un set di caratteristiche contenente le caratteristiche utilizzate per caratterizzare la gamma di somiglianze e differenze tra i campioni.*
3. *Il set di funzionalità viene convertito, per mezzo di in una rappresentazione matematica, in una forma compatta denominata modello. Il modello di iscrizione (enrollment template) è un campione conforme ai requisiti di qualità del sistema biometrico.*

4. *Il modello di registrazione viene archiviato come riferimento per i confronti nelle richieste di identità future.*

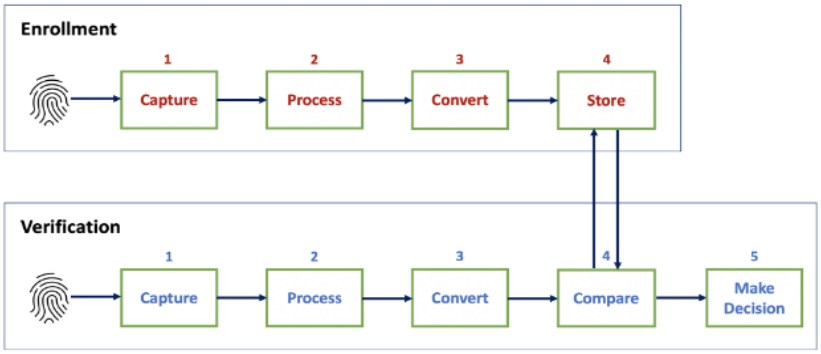


Figure 2: Simplified Biometric Matching Model

La metà inferiore della figura illustra i passaggi per verificare un'identità dichiarata:

1. *L'utente che rivendica l'identità dell'iscritto presenta un nuovo campione del biometrico precedentemente registrato (ad esempio, impronta digitale) per generare un campione di autenticazione (chiamato anche sonda/*probe*).*
2. *Il campione di autenticazione viene elaborato in un set di funzioni.*
3. *Il set di funzionalità viene convertito in un modello.*
4. *Il modello viene quindi confrontato con il modello di registrazione per l'identità rivendicata mediante un algoritmo di corrispondenza per generare un punteggio di somiglianza.*
5. *Il punteggio di somiglianza viene confrontato con un punteggio soglia per decidere se i due campioni provenissero dalla stessa persona e dallo stesso dito.*

Gli ultimi due passaggi, la generazione di un punteggio di somiglianza e il confronto con un punteggio di soglia, indicano ciò che rende la biometria significativamente diversa dagli altri tipi di fattori di autenticazione.

*I fattori di autenticazione "***ciò che sai***" e "***ciò che possiedi***" utilizzano confronti deterministici per verificare l'identità.*

In altre parole, quando un utente fornisce una password per l'autenticazione, tale password deve corrispondere esattamente alla password memorizzata con cui viene confrontata.

Quando una chiave crittografica viene utilizzata in un protocollo di autenticazione, la chiave deve essere esattamente la chiave necessaria.

> *I passaggi nella figura possono essere utilizzati anche per identificare una persona sconosciuta. Il modello da verificare può essere confrontato con tutti i modelli di iscrizione, non solo con uno. Tuttavia, è importante notare che le immagini utilizzate per la verifica possano funzionare diversamente se utilizzate a scopo di identificazione.*

Quando la biometria è utilizzata nell'autenticazione, una misurazione corrente di una caratteristica o di un tratto è confrontata con misurazioni memorizzate. Le misurazioni nuove e memorizzate non sono esattamente le stesse, quindi il confronto delle misurazioni determina una valutazione della probabilità che siano misurazioni della stessa persona.

Un'autenticazione che utilizza la biometria è probabilistica, non deterministica.

COMPONENTI DI UN SISTEMA BIOMETRICO

In questa parte, accenno brevemente alla composizione di un modello di corrispondenza biometrico.

Il modello di corrispondenza biometrica è implementato da un sistema biometrico.

Un tipico sistema biometrico ha diversi componenti di base, inclusi i seguenti.

- ✓ *Un* **SENSOR** *raccoglie un campione; esempi includono lettori di impronte digitali e fotocamere. I sensori vengono utilizzati sia per la registrazione che per la verifica.*
- ✓ *Un* **EXTRACTOR** *converte il campione in un modello.*
- ✓ *Un* **DATABASE** *di* **REFERENCE** *memorizza i modelli di iscrizione.*
- ✓ *Un* **COMPARATOR** *genera un punteggio confrontando i modelli da verificare con i riferimenti memorizzati.*
- ✓ *Un* **MATCHER** *genera un risultato di corrispondenza controllando il punteggio di somiglianza con il punteggio di soglia.*

Questi componenti non sono necessariamente tutti in un unico posto.

Alcuni sistemi biometrici per dispositivi mobili hanno tutti i componenti all'interno dei dispositivi mobili stessi, mentre altri sistemi biometrici hanno alcuni componenti all'interno dei dispositivi mobili ed altri su server remoti.

Ad esempio, il **COMPARATOR** *potrebbe trovarsi all'interno di un dispositivo mobile, consentendo il confronto locale.*

Oppure potrebbe essere su un server remoto, in modo che i dati biometrici acquisiti dal dispositivo mobile locale possano essere trasferiti a quel server per il confronto con i riferimenti archiviati.

SBLOCCO DI UN SISTEMA MOBILE (SCREEN UNLOCKING)

Il caso d'uso principale per le funzionalità biometriche fornite dai produttori di dispositivi mobili è consentire all'utente di sbloccare lo schermo senza inserire un PIN o una password. Questa funzionalità è completamente locale per il dispositivo mobile.

I modelli biometrici dell'utente sono archiviati sul dispositivo mobile e in genere non possono essere esportati.

La registrazione e la verifica avvengono localmente sul dispositivo e possono verificarsi quando il dispositivo è offline.

Lo sblocco dello schermo non autentica intrinsecamente l'utente su alcun sistema o applicazione remota, né fornisce alcuna affermazione dell'identità dell'utente oltre al fatto che la biometria presentata corrisponda a un modello precedentemente registrato su quel dispositivo specifico.

Una volta sbloccato, tuttavia, il dispositivo può concedere all'utente l'accesso a sistemi e applicazioni remoti tramite credenziali memorizzate o sessioni e token attivi.

Lo sblocco dello schermo è un importante controllo di sicurezza, ma le Linee guida sull'identità digitale rilevano che lo sblocco di un dispositivo tramite corrispondenza biometrica non può essere considerato un fattore di autenticazione.

In genere non è possibile per il verificatore ottenere alcuna informazione su come o se il dispositivo è stato sbloccato.

> **ATTENZIONE!** *le Linee guida sull'identità digitale rilevano che lo sblocco di un dispositivo tramite corrispondenza biometrica non può essere considerato un fattore di autenticazione.*

VERIFICA BIOMETRICA LOCALE E REMOTA

Le Linee guida sull'identità digitale consigliano che i soli dati biometrici non forniscono una garanzia sufficiente dell'identità dell'utente e devono essere combinati con un fattore **"ciò che possiedi"** *nell'MFA.*

Le Digital Identity Guidelines descrivono diversi tipi di MFA che potrebbero incorporare dati biometrici, inclusi dispositivi OTP (One Time Password) e dispositivi crittografici in forme hardware e software.

Questi autenticatori in genere richiedono la verifica dell'utente con un segreto biometrico (o un segreto memorizzato) per attivare l'autenticatore.

Una volta attivato, l'autenticatore svolge la sua funzione crittografica (ad esempio, genera una password monouso o firma crittograficamente una richiesta di autenticazione).

Quando la biometria è utilizzata per attivare un autenticatore a più fattori in questo modo, la convalida biometrica è locale (sul dispositivo dell'utente o su un autenticatore hardware stesso).

Il servizio remoto o l'applicazione a cui l'utente si sta autenticando non ha un'interazione diretta con il biometrico, ma poiché è noto che l'autenticatore richieda l'attivazione biometrica, il processo di autenticazione crittografica garantisce che l'autenticazione a più fattori sia stata eseguita.

In alternativa alla verifica locale, la misurazione biometrica può essere inviata (tipicamente in forma astratta) a un server remoto per la verifica.

La verifica lato server elimina la necessità per gli utenti di registrare i propri dati biometrici su ciascun dispositivo mobile, ma richiede l'aggregazione di tutti i modelli biometrici degli utenti in un database lato server per la verifica, aumentando il rischio di una compromissione di massa dei modelli biometrici.

Per questo motivo, le linee guida sull'identità digitale affermano che la verifica locale della biometria è "preferita" e raccomanda controlli di sicurezza aggiuntivi per la verifica remota.

I meccanismi biometrici integrati nei dispositivi mobili commerciali come Face ID di Apple sono in genere di progettazione proprietaria, supportano solo la verifica locale e includono controlli per impedire l'estrazione di dati biometrici dal dispositivo. Di conseguenza, non possono essere utilizzati in uno schema di verifica biometrica a distanza.

Gli sviluppatori di app mobili possono ancora utilizzare le fotocamere dei dispositivi mobili e altri sensori (ma non i sensori di impronte digitali integrati, a causa dei suddetti controlli) per implementare la biometria che potrebbe supportare la verifica lato server.

ATTENZIONE: *Le linee guida identità digitale consigliano che la biometria debba essere combinata con un fattore "***ciò che possiedi***" in MFA.*

BIOMETRIA E PRIVACY

I dati biometrici sono intrinsecamente personali e alcuni tipi di dati biometrici possono essere abusati per identificare e tracciare le persone.

Alcuni dati biometrici, come le immagini facciali, possono essere acquisiti a distanza senza la cooperazione o la conoscenza del soggetto.

Identificatori come nomi utente o indirizzi e-mail possono essere modificati se sono esposti a individui non autorizzati, ma i dati biometrici sono legati alle caratteristiche innate del soggetto e in genere non possono essere modificati.

I dati biometrici costituiscono Informazioni di Identificazione Personale (PII), che comportano l'obbligo di proteggerli dall'accesso o dalla divulgazione non autorizzati (Comma 2 dell'articolo 32 del Reg. (UE) 2016/679).

La compromissione dei dati biometrici registrati richiede in genere l'ottenimento del dispositivo fisico e l'annullamento dei meccanismi di sicurezza del software e del firmware.

3. RISCHI

Quando viene utilizzata la verifica remota, i modelli biometrici sono generalmente archiviati in un database centrale e l'immagine biometrica (o una rappresentazione astratta da essa derivata) è inviata in rete.

Ciò introduce il rischio di intercettazione dei dati biometrici in transito; inoltre, se il database di verifica è compromesso, ciò potrebbe consentire la compromissione di massa dei dati biometrici di tutti gli individui iscritti al sistema.

ERRORI

Ogni componente in un sistema biometrico introduce una probabilità di errore per l'intero sistema:

1. **ERRORE DI ACQUISIZIONE (FAILURE OF CAPTURE - FTC)** *si verifica quando un sensore non riesce a rilevare correttamente un campione a causa di alcune limitazioni (ad esempio, cattive condizioni di illuminazione).*
2. **ERRORE DI ESTRAZIONE (FAILURE OF EXTRACT - FTX)** *si verifica quando la qualità del campione non è sufficientemente buona per generare un modello valido.*
3. **MANCATA REGISTRAZIONE (FAILURE TO ENROLL - FTE)** *si verifica quando un modello non soddisfa i criteri di registrazione (ad esempio, il modello non è un identificatore di riferimento distinguibile in modo univoco).*
4. **FALSA CORRISPONDENZA (FALSE MATCH - FM)** *si verificano quando il matcher decide erroneamente che un modello appena raccolto corrisponde al riferimento memorizzato e gli errori di falsa corrispondenza* **(FALSE NON MATCH - FNM)** *si verificano quando decide erroneamente che un modello appena raccolto non corrisponde al riferimento memorizzato.*

La combinazione di questi errori definisce l'accuratezza complessiva del sistema biometrico.

METRICHE

Varie metriche sono utilizzate per descrivere l'accuratezza dei sistemi biometrici:

1. **FALSE ACCEPT RATE (FAR)** *è la frequenza della falsa corrispondenza. Ciò si verifica quando il campione di un individuo viene confrontato con il riferimento di un altro individuo e il punteggio di confronto supera la soglia, quindi viene effettuata una corrispondenza errata.*
2. **TASSO DI FALSO RIFIUTO (FALSE REJECT RATE - FRR)** *è la frequenza dei falsi non corrispondenti (frequenza dei falsi negativi – nota di Aldo Pedico). Ciò si verifica quando il campione di un individuo viene confrontato con il riferimento dello stesso individuo e il punteggio di confronto è inferiore alla soglia, quindi erroneamente non viene effettuata una corrispondenza.*
3. **SPOOF ACCEPT RATE (SAR)** *è la frequenza con cui un sistema biometrico accetta un campione noto precedentemente registrato (ad esempio, una fotografia o una registrazione della voce di qualcuno) per il confronto invece di un campione effettivo. SAR non è un termine standard del settore, ma viene utilizzato nella documentazione di Google.*

Sfortunatamente, l'applicazione di queste metriche per confrontare le capacità biometriche dei dispositivi mobili non è generalmente fattibile in questo momento. I produttori non rilasciano dati sulle prestazioni per nessuno dei componenti dei loro sistemi biometrici.

Il software utilizzato nel sistema biometrico è proprietario, quindi la valutazione indipendente di componenti come il matcher non è possibile.

Tuttavia, i produttori forniscono alcune informazioni sulle prestazioni complessive dei loro sistemi biometrici.

ATTENZIONE! *a volte viene utilizzato il termine False Match Rate (FMR) al posto di FAR, ma questi termini hanno in realtà significati leggermente diversi e non dovrebbero essere scambiati. L'FMR include tutti i campioni, indipendentemente dai problemi di qualità dell'immagine, mentre il FAR include solo i campioni che possono essere elaborati correttamente in modelli. La stessa distinzione vale per il tasso di falsa corrispondenza (FNMR) e l'FRR*

4. IL FUTURO DELLA BIOMETRIA

La biometria è un'area di ricerca e sviluppo attivi, con capacità nuove e migliorate che appaiono regolarmente.

MISURAZIONI TRIDIMENSIONALI

I sensori di impronte digitali di oggi funzionano catturando una misurazione bidimensionale di un'impronta digitale.

Questi sensori sono soggetti a diverse sfide, come le dita bagnate che interferiscono con la cattura.

Alcuni fornitori commerciali hanno sviluppato sensori a ultrasuoni che catturano misurazioni tridimensionali di un'impronta digitale. Ciò include le misurazioni delle creste e delle valli delle impronte digitali, fornendo dati aggiuntivi che potrebbero potenzialmente creare un modello altamente accurato.

Inoltre, questa tecnologia può essere in grado di misurare con precisione le impronte digitali in condizioni avverse come umidità o contaminazione.

Sebbene non sia attualmente implementato, potrebbe essere possibile leggere le impronte digitali attraverso rivestimenti come i guanti in lattice.

Sono in fase di sviluppo sensori in grado di fornire misurazioni tridimensionali delle caratteristiche del viso con la promessa di misurazioni più accurate.

SENSORI INDOSSABILI

Gli smartwatch contengono già sensori in grado di misurare l'andatura e la frequenza cardiaca e i più recenti hanno sensori in grado di catturare i ritmi cardiaci e i livelli di saturazione di ossigeno. Questi sensori hanno lo scopo di fornire dati di monitoraggio della salute per aiutare a rilevare problemi medici.

Tuttavia, sono dati biometrici che possono essere utili per altri scopi. Ad esempio, supponiamo che un dispositivo indossabile utilizzi il riconoscimento delle impronte digitali per autenticare una persona.

Quando una persona viene autenticata tramite un'impronta digitale, l'indossabile potrebbe associare l'identità a una misurazione dell'elettrocardiogramma.

Attraverso il monitoraggio continuo dell'elettrocardiogramma, l'indossabile potrebbe autenticare continuamente chi lo indossa.

La combinazione dell'elettrocardiogramma e della scansione delle impronte digitali potrebbe fornire una forma di PAD, rendendo più difficile per un utente malintenzionato utilizzare un'impronta digitale fabbricata o altri dati biometrici senza falsificare anche l'autenticazione indossabile.

*Oltre ai tipi di sensori aggiuntivi, i dispositivi indossabili collegati a un dispositivo mobile tramite Bluetooth o Near Field Communication (NFC) offrono la possibilità di aggiungere un fattore "***ciò che possiedi***" al processo di autenticazione senza creare l'onere di trasportare un altro dispositivo, questi offrono anche potenziali vantaggi funzionali.*

QUALITÀ BIOMETRICA COMPORTAMENTALE /AUTENTICAZIONE CONTINUA

I sistemi biometrici possono distinguere i soggetti in base a caratteristiche fisiche (o biologiche) e comportamentali.

Alcune delle modalità fisiche includono viso, impronte digitali, iride, schema vascolare/venoso, geometria della mano e retina.

Le modalità comportamentali includono voce, firma, scrittura a mano, battitura e dinamica dell'andatura.

Molte tecnologie biometriche comportamentali incorporano strategie di apprendimento automatico (Machine Learning - ML) che utilizzano un periodo di formazione iniziale per creare un profilo modello dell'utente registrato.

Una volta stabilito, il profilo può essere costantemente confrontato con gli input del sensore per produrre una probabilità che il comportamento attualmente osservato corrisponda al profilo stabilito.

*Poiché la biometria comportamentale generalmente implica la raccolta di informazioni per un periodo di tempo, è più comunemente utilizzata come parte di una strategia di "***autenticazione continua***" per valutare la fiducia durante una sessione piuttosto che come metodo di autenticazione iniziale all'inizio di una sessione.*

Questo approccio si basa sul presupposto che le misurazioni effettuate durante la fase di apprendimento siano affidabili (cioè che non includano misurazioni di individui diversi).

*Alcuni dati biometrici comportamentali possono essere soggetti a "***deriva***" ("***drift***"), in cui il comportamento dell'utente registrato cambia nel tempo o cambiamenti drammatici improvvisi come gli effetti di un infortunio o di un intervento chirurgico sull'andatura di un utente.*

La biometria comportamentale in genere coinvolge algoritmi proprietari per l'interpretazione dei dati dei sensori, la creazione di profili e il confronto continuo, rendendo difficile misurarne l'efficacia in modo standard e uniforme.

Il NIST è impegnato nella ricerca sia di base sia applicata sull'intelligenza artificiale (AI) e ML e può fornire risorse ai PSO e privati interessati a saperne di più sulle capacità, le applicazioni e i rischi delle tecnologie AI.

Dal punto di vista dell'implementazione, la biometria fisica può essere classificata più come una scienza che come un'arte.

D'altra parte, la biometria comportamentale può essere vista più come arte che come scienza.

La biometria comportamentale è generalmente utilizzata insieme agli autenticatori convenzionali e ha il potenziale per aumentare la sicurezza fornendo segnali di rischio aggiuntivi.

Se un dispositivo mobile sbloccato viene rubato da un utente autorizzato, ad esempio, la biometria comportamentale potrebbe rilevarlo e bloccare lo schermo o richiedere in altro modo la riautenticazione con PIN o password convenzionali.

UNIONE DEI DATI BIOMETRICI

*Ai fini di questo documento, "**Unione Biometrica**" si riferisce a questo ampio concetto di unione in cui la biometria fisica, la biometria comportamentale e altri dati contestuali o segnali di rischio possono essere considerati in un calcolo complessivo della fiducia.*

Gli attuali sistemi biometrici dei dispositivi mobili utilizzano in genere un'unica modalità biometrica.

Questi sistemi possono guastarsi quando cambia l'ambiente in cui sono utilizzati.

Ad esempio, negli ultimi anni, i produttori di smartphone di fascia alta sono passati dai lettori di impronte digitali al riconoscimento facciale per le funzionalità di sblocco del dispositivo.

Il riconoscimento facciale può essere più facile da usare in alcune circostanze e non richiede l'hardware aggiuntivo di un lettore di impronte digitali.

Ha funzionato bene fino a quando la pandemia di COVID-19 ha portato gli utenti a indossare maschere che impediscono il riconoscimento facciale.

La sfida per l'unione di tipi di dati biometrici è imparare quali tratti fondere, quando fondere i tratti e come fondere i tratti per ottenere i migliori risultati complessivi. L'unione può avvenire all'interno o attraverso uno qualsiasi dei componenti di un sistema biometrico.

Le misurazioni biometriche possono anche essere unite con segnali resi disponibili da altri sensori su un dispositivo client, inclusi dati biometrici comportamentali e altri dati contestuali come la posizione.

I dispositivi mobili in genere includono una vasta gamma di sensori, comprese le fotocamere rivolte all'utente; radio cellulari, Bluetooth e Wi-Fi; Ricevitori GPS (Global Positioning System); e accelerometri.

Le modalità biometriche fisiche e comportamentali come il volto, la voce, l'andatura e le dinamiche delle interazioni del dispositivo (incluso l'angolo con cui l'utente tiene il dispositivo) possono essere misurate utilizzando una combinazione di input del sensore.

Oltre alla biometria, è possibile misurare e analizzare gli attributi contestuali.

Gli attributi contestuali potrebbero includere dispositivi connessi (inclusi dispositivi indossabili e altri dispositivi Bluetooth), reti disponibili e connesse (ad es. Wi-Fi) e posizione GPS.

*Qualsiasi combinazione di questi attributi biometrici e contestuali può essere misurata, analizzata e utilizzata per creare e aggiornare continuamente un "**punteggio di affidabilità**" composito che indica la sicurezza che il dispositivo è utilizzato dall'utente autorizzato.*

COMPENSAZIONE DELLE DISPARITÀ

Come con la biometria comportamentale, questa valutazione continua della fiducia sfrutta spesso il machine learning e la valutazione rispetto a un modello addestrato di comportamenti e input previsti.

In una revisione del 2019 dei documenti di ricerca disponibili sulla Unione Biometrica, il NIST ha concluso che tale biometria aveva potenziali vantaggi, tra cui la **COMPENSAZIONE DELLE DISPARITÀ** *in termini di universalità, unicità e permanenza di diverse modalità biometriche e rendendo più difficili gli attacchi di presentazione.*

Sebbene sia difficile determinarne la precisione e l'efficacia, l'unione biometrica presenta potenziali vantaggi se utilizzata insieme agli autenticatori convenzionali, il punteggio di affidabilità composito generato dall'unione biometrica potrebbe essere utilizzato per ridurre i requisiti di autenticazione per le risorse meno sensibili, ad esempio consentendo l'accesso senza richiedere MFA quando un punteggio di affidabilità è alto.

Come con la biometria comportamentale, un punteggio di affidabilità composito potrebbe essere utilizzato per richiedere un'autenticazione aggiuntiva o graduale quando il punteggio è inferiore a una certa soglia o attivare un blocco del dispositivo mobile e richiedere una riautenticazione completa.