UNIVERSITÀ
DEGLI STUDI
DI PADOVA

DIPARTIMENTO
DI INGEGNERIA
DELL'INFORMAZIONE

DIPARTIMENTO DI INGEGNERIA DELL'INFORMAZIONE

CORSO DI LAUREA MAGISTRALE IN INGEGNERIA INFORMATICA

"Applicazione del protocollo PRISMA ad una rassegna sistematica sui sistemi di autenticazione per smartwatch"

Relatore: Prof. Migliardi Mauro

Laureando: Danieli Luca

ANNO ACCADEMICO 2024 – 2025

Data di laurea 4/12/2024

Ai miei genitori, per avermi sempre supportato.

Abstract

Gli smartwatch insieme agli activity tracker sono gli accessori di uso più comune nella categoria degli wearable. Tra i dispositivi indossabili risultano essere tra i più ricchi di funzionalità in quanto permettono di monitorare l'attività fisica e la salute, interagire con lo smartphone ed effettuare chiamate e pagamenti. Tali funzionalità rendono critica la protezione di questi dispositivi dagli accessi non autorizzati, per evitare che un'altra persona possa accedere alle informazioni personali o utilizzare funzionalità come quelle per i pagamenti a discapito del legittimo proprietario. Per proteggere il dispositivo vengono spesso utilizzati il PIN o il Pattern Lock che risultano però vulnerabili allo shoulder surfing, una strategia d'attacco che può essere perpetrata anche da avversari senza una formazione in ambito cyber security. L'utilizzo di una password è vulnerabile anche ad altri attacchi, tra cui il brute forcing e il guessing attack basato su dizionario, richiedendo all'utente di utilizzare password che siano al contempo memorabili e sufficientemente complesse da non poter essere indovinate. Al fine di analizzare lo stato dell'arte e individuare i possibili trend di ricerca riguardo l'autenticazione su smartwatch sono stati raccolti all'interno di una rassegna sistematica 14 studi. Nello stilare la rassegna ci si è attenuti alle linee guide riportate nel protocollo PRISMA 2020, protocollo originariamente pensato per la stesura di rassegne sistematiche in ambito medico. Nella rassegna sono stati inclusi gli studi reperibili tramite Google Scholar il cui testo integrale fosse liberamente accessibile senza necessità di registrazione ad alcun sito. Gli studi sono stati dapprima riportati e discussi singolarmente e successivamente confrontati dove ritenuto significativo. I sistemi più efficaci a prevenire lo shoulder surfing risultano essere quelli che fanno uso di un fattore biometrico per autenticarsi, per contro quelli per cui la behavioural biometric è visibile sono vulnerabili ad un altro tipo di attacco che non richiede una formazione tecnologica: il mimick attack. Per ovviare a questa limitazione è consigliabile utilizzare la sensor fusion aggiungendo ulteriori fattori che non siano visibili come le caratteristiche cardiache o la temperatura corporea. Data la capacità dei recenti smartwatch di rilevare l'attività fisica la soluzione ideale sarebbe un'autenticazione MFA adattiva, che faccia uso di un diverso insieme di caratteristiche biometriche sia in autenticazioni successive sia a seconda del contesto d'uso. In questo modo è possibile ottimizzare i modelli di machine learning utilizzati nei singoli contesti (quando l'utente è in stato sedentario e quando è fisicamente attivo) e rendere più difficoltoso lo spoofing di tutte le caratteristiche biometriche utilizzate per autenticarsi.

Sommario

Introduzione

Le rassegne ricoprono ruoli critici nel riportare lo stato dell'arte di un argomento, tra cui il fatto che terminologia, metodi e contenuti siano attuali. In esse possono essere identificati problemi, possono permettere di accertare teorie o riprodurre i risultati degli studi originari. Non da meno permettono di individuare possibili sviluppi futuri per un'ulteriore analisi. Per coloro che fanno uso della review è importante poter appurare la completezza, l'affidabilità e l'applicabilità di quanto rinvenuto. Nella trattazione ci si propone di riportare l'attuale stato dell'arte dei diversi sistemi di autenticazione per smartwatch proposti in letteratura facendo uso del protocollo PRISMA, protocollo utilizzato in ambito medico per la stesura di rassegna sistematiche. Nel seguire le linee guida proposte in PRISMA si cercherà di fornire una sintesi degli studi rinvenuti in letteratura garantendo un'elevata completezza informativa in modo da permettere al lettore di avere un'adeguata visione d'insieme e scegliere se limitarsi alla trattazione attuale o se approfondire con gli studi originari dove ritenuto necessario.

Introduzione alla suite PRISMA

Il Prefferred Reporting Items for Systematic reviews and Meta-Analyses (PRISMA) Statement [1] è stato pubblicato nel 2009 per poter scrivere rassegne in maniera sistematica ed esaustiva. Dal 2009 ad oggi vi sono stati numerosi cambiamenti nelle tecniche e nelle metodologie usate nello scrivere review, anche dal punto di vista tecnologico. Tramite l'uso del natural language processing, del machine learning e dell'intelligenza artificiale è possibile sintetizzare contenuti, individuare evidenze e altro che l'utilizzatore da solo avrebbe difficoltà ad estrapolare.

Per questi motivi si è reso necessario l'aggiornamento di PRISMA alla versione 2020.

Il protocollo PRISMA 2020 è composto da uno statement, da un development paper e dall'explanation and elaboration paper.

Lo Statement [1] è composto da una checklist di 27 elementi da includere all'interno di una rassegna per far sì che sia scritta in maniera sistematica e da un diagramma di flusso che descrive le fasi di identificazione, screening e inclusione degli studi.

Il Development Paper [2] riporta le motivazioni e gli step intrapresi per aggiornare la precedente versione del protocollo.

L'Explanation and Elaboration paper [3] descrive per ogni elemento della checklist perché è suggerito e dettaglia ulteriormente le raccomandazioni per il reporting dei singoli punti.

In quanto segue verrà dapprima introdotto il protocollo PRISMA 2020 e successivamente verranno seguite le 27 raccomandazione suggerite nello stesso per una review inerente ai sistemi per l'autenticazione su smartwatch.

PRISMA 2020 statement

La checklist PRISMA contiene sette sezioni e 27 elementi, alcuni dei quali contengono dei sotto elementi, ed è disponibile sottoforma di template personalizzabile [4]. Questo template suggerisce un ordine al quale attenersi nella scrittura; tuttavia, secondo quanto riportato dagli autori è preferibile inserire tutti i punti rispetto al seguire l'ordine suggerito. Il template contiene una colonna per tenere traccia di dove si è posizionato l'elemento, in modo da permettere di utilizzare un ordine diverso rispetto a quello suggerito e venire in contro alle necessità di chi scrive. In alternativa al template è disponibile un'applicazione web [5] sviluppata dagli stessi autori.

Le linee guida descritte in PRISMA 2020 sono pensate per gli studi che valutano un intervento in ambito sanitario ma la checklist PRISMA secondo quanto riportato dagli autori è applicabile ad altri ambiti anche non richiedenti un intervento in senso stretto. La checklist PRISMA è applicabile a diverse tipologie di rassegne sistematiche, quelle richiedenti una sintesi per un confronto tra due o più studi ma anche nel caso di sintesi di un unico studio. Le rassegne che combinano metodi misti, tra cui quelle sia qualitative sia quantitative, quelle nuove, aggiornate o quelle in continuo aggiornamento. Per i casi di "network meta-analyses, meta-analyses of individual participant data, systematic reviews of harms, systematic reviews of diagnostic test accuracy studies e scoping reviews" [3] è suggerito di affiancare il protocollo con l'apposita estensione di PRISMA.

PRISMA 2020 Explanation and Elaboration

In [3] viene descritto il PRISMA 2020 Explanation and Elaboration, documento che dettaglia per ogni elemento e sotto elemento quanto va riportato, una lista dei punti essenziali da trattare ed eventuali punti supplementari nella trattazione. Nel documento è suggerito di riportare i punti definiti essenziali nel corpo principale del testo in quanto funzionali a verificare l'affidabilità e applicabilità dei risultati o, dove possibile, permettere la riproducibilità degli stessi. I punti non essenziali servono invece come materiale supplementare volto a garantire una maggiore completezza e usabilità dell'informazione riportata. Entrambe le tipologie di elementi mirano a riportare la presenza di un metodo o risultato, a meno che l'assenza di questi ultimi possa

risultare rilevante ai fini del reporting. La scelta è a discrezione di chi scrive la rassegna. A seconda del contesto, ad esempio una rivista scientifica o altro, potrebbero essere infatti imposti dei limiti nel numero di parole utilizzate, di dimensione delle sezioni o altre limitazioni che vincolano chi scrive a riportare quanto necessario nel corpo principale della review e a fare riferimento ad altre fonti dove possibile. I punti appartenenti alla checklist, discussi nel PRISMA Explanation and Elaboration, verranno riportati e descritti in quanto segue.

1.Identificare il report come rassegna sistematica: L'inclusione nel titolo di "rassegna sistematica" facilità l'identificazione da parte del lettore e la corretta indicizzazione nei database. Utilizzare altra terminologia che non evidenzi la sistematicità non permetterebbe di distinguerla da una che non lo sia. È preferibile non utilizzare il termine metanalisi come sinonimo di rassegna sistematica in quanto la prima fa riferimento alle sole sintesi statistiche, che potrebbero essere anche svolte al di fuori di una rassegna sistematica.

2.Abstract: Un abstract dovrebbe contenere le informazioni chiave riguardo gli obiettivi o domande che la review affronta. I metodi, risultati e implicazioni delle scoperte dovrebbero aiutare il lettore a decidere se accedere all'intero report. L'abstract potrebbe essere la sola fonte a cui alcuni lettori potrebbero avere accesso per cui è importante che in esso vengano riportati i principali risultati inerenti alle domande e obiettivi prefissi. I termini usati nell'abstract verranno usati per indicizzare la review sistematica in database bibliografici, per questo si suggerisce di utilizzare parole chiave che descrivono accuratamente il contenuto.

3.Descrivere accuratamente i motivi che hanno portato alla stesura della review contestualizzandoli nell'attuale stato delle conoscenze: Descrivere il fondamento logico che ha portato alla stesura aiuta il lettore a capire perché è stata scritta la review e cosa aggiunge all'attuale stato dell'arte.

4.Esplicitare gli obiettivi o domande che la review affronta: Esplicitare in maniera concisa gli obiettivi o le domande affrontate nella review aiuta il lettore ad individuare lo scopo della stessa e valutare se i metodi usati sono coerenti con gli obiettivi.

5.Specificare i criteri di inclusione ed esclusione e come gli studi sono stati raggruppati: Specificare adeguatamente i criteri per cui si è deciso di includere o meno delle evidenze dovrebbe aiutare il lettore a capire lo scopo della review e accertarsi della qualità delle decisioni. Oltre alle review PICO vanno identificati e definiti l'intervento, i risultati e i gruppi di popolazione utilizzati nella sintesi.

6.Specificare tutti i database, registri, siti web, organizzazioni, liste di riferimento e altre fonti consultate per identificare gli studi specificando la data di ultima ricerca o consultazione: Gli autori dovrebbero riportare in maniera completa le varie fonti e le date di ultima consultazione indicando in questo modo il "cosa" e il "quando".

7.Presentare la strategia di ricerca completa per l'accesso alle fonti, comprensiva di filtri e limiti utilizzati: Riportare le query di ricerca utilizzate dovrebbe migliorare la trasparenza di una review sistematica, favorendone la replicabilità e l'aggiornamento. Presentare una sola strategia di ricerca ostacola il lettore nel valutare la globalità delle ricerche effettuate impedendo di individuare possibili errori e limitando la replicabilità delle ricerche su database diversi. Aggiungere una descrizione del processo di sviluppo della strategia di ricerca, ad esempio indicando come si è arrivati all'identificazione di parole chiave e sinonimi di queste, permette al lettore di individuare in che modo gli studi rilevanti rientrano nei criteri di inclusione.

8.Specificare i metodi utilizzati per decidere se uno studio è aderente ai criteri di inclusione, indicando quanti revisori hanno visionato ogni record e ogni report, se hanno lavorato in maniera autonoma ed eventuali tool utilizzati nel processo: La selezione degli studi avviene solitamente in più fasi, ad esempio, scremando gli studi sulla base del titolo e dell'abstract e successivamente sull'intero contenuto. Gli autori dovrebbero indicare nel dettaglio il processo decisionale per cui gli studi reperiti rientrano nei criteri di inclusione.

9.Specificare i metodi usati per raccogliere i dati dai report, indicando quanti revisori hanno raccolto i dati da ogni report, se hanno lavorato in modo autonomo, se vi sono state verifiche atte ad accertare i dati ed eventuali tool automatici usati: I metodi usati per la raccolta dei dati dai report permettono al lettore di verificare eventuali errori commessi durante il processo di raccolta.

10a. Elencare e definire tutti i risultati per i quali sono stati riportati i dati. Specificare se sono stati ricercati tutti i risultati compatibili con ciascun dominio di risultato in ciascuno studio (ad esempio, per tutte le misure, i punti temporali, le analisi) e, in caso negativo, i metodi utilizzati per decidere quali risultati raccogliere: Definire gli esiti in una review sistematica implica specificare il dominio di risultato (e.g. livello di dolore, qualità della vita etc.) e l'intervallo temporale di misurazione (e.g. meno di sei mesi fa). Ad esempio, uno studio potrebbe riportare risultati facendo uso di due scale per la misurazione del dolore e due intervalli temporali (e.g. quattro e otto settimane) compatibili con gli esiti definiti nella review come "meno di sei mesi". I revisori potrebbero voler riportare tutti i risultati compatibili con la definizione degli esiti presente nei singoli studi oppure selezionarne un sottoinsieme. Quando sono presenti molteplici risultati è importante definire il metodo utilizzato nel caso ne vengano selezionati solo alcuni, in quanto il lettore avrà così la possibilità di individuare potenziali bias nella selezione. I revisori durante il processo di inclusione degli studi potrebbero voler cambiare la definizione del dominio di risultato, ad esempio, definendo come "critico" nella review qualcosa che nello studio originario era indicato come "importante".

10b. Elencare e definire tutte le altre variabili per le quali sono stati riportati i dati (come caratteristiche dei partecipanti e dell'intervento, fonti di finanziamento). Descrivere eventuali ipotesi fatte su eventuali informazioni mancanti o poco chiare: Gli autori dovrebbero riportare i dati e le informazioni raccolte dagli studi così che il lettore possa capire le informazioni necessarie e per favorire la fase di raccolta dati in review simili. Tra le informazioni significative è possibile indicare il sesso, l'età e il numero dei partecipanti, se il campione utilizzato è randomico o meno, la nazione di provenienza e altre caratteristiche rilevanti.

11.Specificare i metodi usati per la valutazione del rischio di bias negli studi inclusi, compresi eventuali tool utilizzati, numero di revisori per ogni studio e se hanno lavorato in modo indipendente: Gli utilizzatori della review per poter interpretare le evidenze riportatevi devono poter valutare il rischio di bias negli studi contenuti in essa. Sono disponibili diversi tool atti alla valutazione del rischio di bias e riportarne le caratteristiche aiuta il lettore ad individuare possibili errori nella valutazione.

12. Specificare per ciascun risultato le misure degli effetti (come il rapporto di rischio, la differenza media) utilizzate nella sintesi o nella presentazione dei risultati: Per interpretare i risultati l'utente deve conoscere la misura degli effetti. La misura degli effetti si riferisce ad un costrutto statistico usato per il confronto tra risultati di due gruppi. La scelta della misura degli effetti ha ripercussioni sull'interpretazione di quanto scoperto e può influenzare i risultati della metanalisi. Gli autori potrebbero usare una misura degli effetti per riassumere i risultati e successivamente rielaborare la sintesi dei risultati usandone una differente. Inoltre, gli autori devono interpretare le stime degli effetti in relazione all'importanza dell'effetto per coloro che si baseranno sulla review per effettuare decisioni.

13a.Descrivere i processi utilizzati per decidere quali studi sono idonei per ciascuna sintesi (come la tabella delle caratteristiche dell'intervento dello studio e il confronto con i gruppi pianificati per ciascuna sintesi (punto n. 5)): Prima di effettuare una sintesi statistica va deciso quali studi sono idonei per la sintesi pianificata. Queste decisioni sono solitamente fatte sulla base di un giudizio soggettivo che potrebbe alterare il risultato della sintesi, ciononostante il processo e le informazioni a supporto di queste decisioni sono spesso assenti nella review. Riportarli è invece auspicabile in quanto fornisce una maggiore trasparenza nel raggruppare gli studi ai fini della sintesi. Un approccio strutturato può coinvolgere la tabulazione e codifica delle caratteristiche principali relative la popolazione, l'intervento e i risultati.

13b.Descrivere ciascun metodo richiesto per la preparazione dei dati ai fini della presentazione o della sintesi, ad esempio gestire la mancanza di sintesi sommarie o di conversione dei dati: Gli autori devono preparare i dati raccolti ai fini della presentazione o

della sintesi. Questo può richiedere una manipolazione algebrica per la conversione delle statistiche riportate, una trasformazione della stima degli effetti o assegnare per inferenza un valore a dei dati sommari.

13c.Descrivere ciascun metodo usato per tabulare o visualizzare graficamente i risultati dei singoli studi e della sintesi: La presentazione dei risultati degli studi in forma tabulare o grafica è importante per garantire una maggiore trasparenza e per facilitare l'individuazione di pattern nei dati. Lo scopo di tabulare i dati è spesso quello di fornire maggiore completezza e trasparenza dei risultati o per confrontare le caratteristiche degli studi. Utilizzare una struttura tabellare rispetto ad un'altra può essere funzionale a mettere in evidenza aspetti diversi e giustificare la struttura utilizzata e i dati contenutivi aiuta il lettore a capirne lo scopo nella presentazione.

13d.Descrivere ciascun metodo utilizzato per la sintesi dei risultati giustificando la scelta. Nel caso sia svolta una metanalisi, descrivere i modelli e i metodi usati per identificare la presenza ed estensione di eterogeneità statistica, indicando il pacchetto software utilizzato: Esistono diversi metodi per riassumere risultati, tra cui la metanalisi della stima degli effetti. La scelta del modello influenza la stima sommaria e il suo intervallo di confidenza ed è quindi importante che venga giustificato.

13e.Descrivere ciascun metodo usato per esplorare possibili cause di eterogeneità tra i risultati degli studi: In caso gli autori usino metodi per esplorare possibili cause di variabilità nei risultati tra gli studi dovrebbero anche fornire dettagli affinché il lettore possa appurare la validità degli stessi metodi e riprodurre i risultati riportati.

13f.Descrivere ciascuna analisi di sensibilità utilizzata per valutare la robustezza dei dati riassunti: Nel caso gli autori abbiano svolto delle analisi di sensibilità per valutare la robustezza dei dati sintetizzati dovrebbero anche fornire sufficiente dettaglio per garantire ai lettori di valutare l'appropriatezza dell'analisi e la possibilità di riprodurre i risultati ottenuti.

14.Descrivere ciascun metodo utilizzato per la valutazione del rischio di bias causato dalla mancanza di risultati nella sintesi: La validità di una sintesi può essere compromessa quando i risultati disponibili differiscono sistematicamente dai risultati mancanti. Esistono sia metodi statistici sia grafici per valutare se i dati osservati suggeriscono potenziali risultati mancanti e quanto robusta sia la sintesi rispetto ad assunzioni diverse sulla natura di risultati mancanti. Riportare il processo e i metodi seguiti per la valutazione del rischio di bias aiuta il lettore ad accertarne la validità ed individuare potenziali errori.

15.Descrivere ciascun metodo usato per valutare la certezza (o l'intervallo di confidenza) delle evidenze che supportano un risultato: Gli autori sono soliti usare un qualche criterio per decidere quanto certe siano le evidenze a supporto dei risultati principali. Tra questi criteri

vi sono la precisione della stima degli effetti, consistenza delle evidenze tra gli studi, limitazioni nel design degli studi e quanto direttamente gli studi affrontano la questione. Esistono tool e framework atti a fornire una valutazione sistematica ed esplicita per questi criteri, fornendo un approccio e della terminologia comuni per la valutazione della certezza. Riportare i fattori considerati e i criteri usati per investigarli aiuta il lettore a capire come è stata svolta la valutazione di certezza e descrivere il processo tramite il quale è avvenuta permette di individuare potenziali errori e facilitare la riproducibilità.

16a.Descrivere i risultati della ricerca e il processo di selezione, compresi i record estratti con la ricerca e il numero di studi inclusi nella review, idealmente usando un diagramma di flusso: Riportare i risultati delle ricerche e il processo di selezione, idealmente usando un diagramma di flusso, aiuta il lettore a capire il flusso per cui gli studi sono stati inclusi nella review. Questa informazione è utile per i futuri team che vorranno scrivere una rassegna sistematica, per la stima delle risorse richieste o per gli specialisti dell'informazione che valuteranno le ricerche. Specificare il numero di record estratti da un database aiuta a verificare la corretta riproduzione della ricerca.

16b.Citare gli studi che sembrano rientrare nei criteri di inclusione ma che sono stati esclusi, giustificando la scelta: Identificare gli studi esclusi permette al lettore di verificare la validità e l'applicabilità della review sistematica. Dovrebbe essere riportata quantomeno una lista degli studi che sembrano rientrare nei criteri di inclusione ma che sono stati esclusi e il motivo di tale esclusione. È anche utile riportare una lista degli studi potenzialmente rilevanti ma per cui non era disponibile il testo completo.

17.Citare ogni studio incluso e presentare le sue caratteristiche: Riportare i dettagli degli studi inclusi permette al lettore di capire le caratteristiche degli studi stessi. Tra le caratteristiche di interesse troviamo caratteristiche dei partecipanti, come i risultati sono stati accertati e fonti di finanziamento. Presentare le caratteristiche chiave degli studi in una tabella o figura facilita il confronto tra studi.

18.Presentare una valutazione del rischio di bias per ciascuno studio incluso: Il lettore per capire la validità dei risultati negli studi inclusi deve essere a conoscenza dei potenziali rischi di parzialità nei risultati. Riportare solo dati sommari non è sufficiente in quanto non indica quali studi siano soggetti a bias. Un approccio più informativo consiste nel riportare in una tabella o figura per ogni studio quali siano i bias in ciascuna componente/dominio/elemento valutato, così che il lettore possa capire quali fattori hanno portato alla valutazione del rischio di bias complessiva.

19.Per ciascun risultato presentare per ogni studio (a) statistiche sommarie per ciascun gruppo (dove appropriato) e (b) una stima degli effetti e la sua precisione (intervallo di

confidenza), idealmente usando una tabella o un grafico: Presentare i dati per ogni studio facilita la comprensione di questi ultimi e il riutilizzo dei dati per ulteriori analisi o per l'aggiornamento della review. La rappresentazione grafica dei dati facilita la comprensione mentre quella tabulare il riutilizzo. Raggruppare e riportare le statistiche sommarie dei gruppi permette di valutare la gravità del problema negli studi, che non è desumibile dai risultati del confronto fra gruppi (e.g. stima degli effetti).

20a.Per ogni sintesi riassumere brevemente le caratteristiche e il rischio di bias degli studi che vi contribuiscono: Molte review sistematiche includono le caratteristiche degli studi e il rischio di bias degli stessi in maniera discorsiva. Tuttavia, un approccio così generico non risulta utile quando gli studi sono variegati o molteplici. Fornire un breve riassunto delle caratteristiche e rischio di bias per ogni studio che contribuisce alla sintesi aiuterebbe il lettore a capire l'applicabilità e il rischio di bias dei risultati riassunti. Non da meno è più funzionale all'interpretazione dei risultati, permettendo al lettore di non dover far riferimento a più sezioni della review.

20b.Presentare i risultati di tutte le sintesi statistiche condotte. In caso sia stata svolta una metanalisi, presentare per ciascuna di esse una stima sommaria, la sua precisione (e.g. intervallo di confidenza) e una misura dell'eterogeneità statistica. Nel confrontare i gruppi indicare quello prediletto: Gli utilizzatori della review fanno affidamento su tutte le sintesi statistiche condotte così da avere evidenze complete e imparziali su cui basare le loro decisioni.

20c.Presentare i risultati delle indagini sulle possibili cause di eterogeneità statistica tra i risultati degli studi: Presentare i risultati delle indagini sulle possibili cause di eterogeneità statistica tra gli studi è importante per il lettore e per le ricerche future. Per il lettore capire i fattori che possono o meno spiegare la variabilità nella stima degli effetti garantisce una maggiore contezza nel prendere decisioni basate sulla review. Selettivamente riportare i risultati implica un'incompleta rappresentazione delle evidenze che può mal indirizzare coloro che fanno uso della review.

20d.Presentare i risultati di ogni analisi di sensitività condotta per la valutazione della robustezza dei risultati riassunti: Presentare i risultati di ogni analisi di sensitività condotta permette al lettore di valutare la robustezza dei risultati rispetto alle decisioni prese durante il processo di review. Riportare i risultati di ogni analisi di sensitività condotta è importante in quanto presentarne soltanto un sottoinsieme, sulla base della natura dei risultati, rischia di introdurre dei bias dovuti al reporting selettivo.

21.Presentare una valutazione del rischio di bias dovuta alla mancanza di risultati (derivante dal reporting dei bias) per ogni sintesi valutata: Presentare una valutazione del

rischio di bias dovuta alla mancanza di risultati permette al lettore di valutare possibili minacce all'affidabilità dei risultati riportati. Fornire evidenze a supporto della valutazione del rischio di bias permette al lettore di accertare la validità della valutazione.

22.Presentare una valutazione della certezza (o confidenza) nel corpo delle evidenze per ogni esito valutato: Una funzionalità importate dei sistemi usati per la valutazione della certezza (i.e. GRADE) è riportare esplicitamente sia il livello di certezza (o confidenza) delle evidenze sia della valutazione eseguita.

23a.Fornire un'interpretazione generale dei risultati nel contesto delle altre evidenze riportate: Discutere come i risultati riportati nella review si relazionano con le altre evidenze aiuta il lettore ad interpretare quanto rinvenuto. Ad esempio, gli autori potrebbero confrontare i risultati riportati con risultati rinvenuti in altre review sistematiche ed approfondire i casi di risultati discordanti. Similmente, gli autori potrebbero riassumere informazioni aggiuntive non approfondite nella review ma che possono risultare utili a coloro che ne faranno uso per prendere decisioni.

23b.Discutere eventuali limiti delle evidenze incluse nella review: Discutere la completezza, applicabilità e incertezza delle evidenze riportate nella review dovrebbe aiutare il lettore ad interpretare quanto rinvenuto in modo appropriato. Ad esempio, gli autori potrebbero riportare di aver trovato pochi studi o che questi sono stati svolti su un numero esiguo di partecipanti, avere dubbi inerenti al rischio di parzialità nei risultati o alla mancanza di questi ultimi oppure aver identificato studi che rispondono solo in modo parziale al quesito che la review si pone.

23c.Discutere le limitazioni del processo usato per la review: Discutere le limitazioni evitabili o meno nel processo usato per la review può aiutare il lettore ad accertare l'affidabilità di quanto rinvenuto nella review. Ad esempio, gli autori potrebbero riconoscere di avere attinto a soli studi in lingua inglese, ricercato solo un numero esiguo di database o che una sola persona ha revisionato i dati o i record. Potrebbero anche riconoscere di non aver potuto attingere a potenziali studi elegibili ai fini della review o di non aver svolto alcune analisi a causa della mancanza di dati.

23d.Discutere le implicazioni dei risultati per la pratica, policy o future ricerche: Ci sono diversi potenziali lettori di una review sistematica ciascuno dei quali vorrà sapere quali azioni intraprendere basandosi su quanto letto. Rispetto a dare raccomandazioni applicabili globalmente per la pratica o le policy gli autori dovrebbero discutere i fattori che possono risultare rilevanti per le diverse tipologie di pubblico. È raccomandato indirizzare la ricerca futura in maniera esplicita e suggerire i metodi che dovrebbero essere utilizzati.

24a.Fornire le informazioni di registrazione per la review, incluso il nome e numero di registro o indicare che la review non è registrata: Indicare dove la review sistematica è stata

registrata (e.g. PROSPERO, Open Science Framework) e il numero di registro o il DOI per la entry del registro facilita l'identificazione della review. Questo permette al lettore di confrontare cosa fosse specificato in precedenza rispetto a quanto è stato riportato così da capire se le deviazioni intraprese possano aver introdotto potenziali bias. Riportare le informazioni di registrazione facilità anche il collegamento con le pubblicazioni relative alla stessa review sistematica.

24b.Indicare dove è possibile accedere al protocollo della review o indicare che il protocollo non è stato preparato: Il protocollo della review potrebbe contenere informazioni riguardanti i metodi che non sono contenuti nella versione finale della review. Fornire un riferimento bibliografico, il DOI o un link al protocollo permette al lettore di reperirlo più facilmente. Confrontare i metodi specificati in precedenza nel protocollo con quanto è stato effettivamente fatto permette al lettore di individuare possibili bias introdotti nel deviare rispetto a quanto prefisso nel protocollo. Nel caso gli autori non abbiano preparato un protocollo per la review o non lo rendano accessibile andrebbe indicato in modo da evitare inutili ricerche al lettore.

24c.Descrivere e giustificare eventuali modifiche alle informazioni fornite in fase di registrazione o nel protocollo: Per una maggiore trasparenza le modifiche alle informazioni fornite in fase di registrazione o nel protocollo possono essere registrate in vari posti tra cui nel testo completo della review, in file supplementari oppure come modifiche del protocollo modificato o del record di registrazione.

25.Riportare le fonti di finanziamento e di supporto per la review, indicando quale ruolo hanno avuto i finanziatori e gli sponsor: Come per ogni ricerca, gli autori dovrebbero essere trasparenti nell'indicare le fonti di supporto ricevute per condurre la review. I finanziatori potrebbero stipendiare i ricercatori per condurre la review, fornire l'accesso a database commerciali che diversamente non sarebbero stati accessibili, contribuire a definire le domande alle quali risponde la review o stabilire i criteri di inclusione per gli studi oppure raccogliere e analizzare i dati o approvare la versione finale della review. Da questo coinvolgimento potrebbe derivare un bias nei risultati della review, in particolare se i finanziatori hanno interesse nell'ottenere particolari risultati.

26.Dichiarare possibili conflitti di interesse per gli autori della review: Gli autori potrebbero essere in relazione con organizzazioni o entità con un interesse nei risultati della review. Queste relazioni potrebbero minare l'integrità e credibilità della review sistematica. Le informazioni inerenti i rapporti e le attività degli autori, che il lettore può ritenere abbiano influenzato quanto riportato nella review, dovrebbero essere esplicitate nel formato richiesto dall'entità di

pubblicazione. Gli autori dovrebbero riportare come sono stati gestiti i possibili conflitti di interesse nei processi che hanno portato alla stesura della review.

27.Riportare quali dei seguenti sono disponibili pubblicamente e dove possono essere reperiti: template per la raccolta dati, dati estratti dagli studi inclusi, dati utilizzati per le analisi, codice analitico, altro materiale usato nella review: La condivisione dei dati, codice analitico e altro materiale permette il loro riutilizzo, la verifica di possibili errori, di tentare di riprodurre i risultati e di capire di più dell'analisi rispetto alla descrizione dei metodi. I dati, il codice analitico e altro materiale può essere caricato in uno degli svariati repository pubblici (e.g. Open Science Framework, Dryad, figshare). Il Systematic Review Data Repository (https://srdr.ahrq.gov/) è un altro esempio di piattaforma per la condivisione di materiale specifico per la community delle review sistematiche. I Findable, Accessible, Interoperable, Reusable (FAIR) data principle sono un'altra risorsa per la consultazione degli autori, in quanto forniscono delle linee guida per la condivisione di informazioni.

Introduzione all'autenticazione [6]

Cos'è l'autenticazione

L'autenticazione è un processo atto a verificare che l'entità che accede ad un sistema sia realmente chi dichiara di essere restituendo una risposta binaria che indica l'accessibilità o meno al sistema o alla risorsa. L'autenticazione opera in maniera interconnessa con il processo di autorizzazione che determina in che modo l'entità autenticata ha accesso al sistema o alle risorse del sistema.

Perché l'autenticazione è importante

Viviamo in un'epoca in cui la tecnologia informatica e la digitalizzazione dell'informazione e servizi ha coinvolto pressoché qualsiasi ambito: posta elettronica, e-commerce, food delivery, e-banking, sanità, social network, e-learning e molto altro sono ora accessibili da un dispositivo che sta nel palmo della mano. Per non parlare della vita lavorativa che in anni recenti ha visto un enorme cambiamento nelle metodologie di lavoro, che ora coinvolgono in maniera imprescindibile l'utilizzo di un computer o di altri dispositivi connessi ad una rete. In un contesto come questo il fatto che chi utilizza questi dispositivi o servizi sia effettivamente chi dice di essere e venga vincolato nell'accedere alle risorse in base alle autorizzazioni concesse diventa d'obbligo. Questo non solo da un punto di vista della sicurezza ma anche di protezione della privacy.

Tipologie di autenticazione

La scelta di un meccanismo di autenticazione è dettata da vari fattori quali i requisiti di sicurezza richiesti, i costi per l'implementazione e la facilità d'uso per l'utente. Possiamo suddividere questi metodi in quattro categorie che possono essere combinate fra loro per aumentare la robustezza complessiva:

- Cosa conosci: informazioni ricordate a memoria
- Cosa possiedi: un oggetto a disposizione dell'utente
- Cosa sei: le caratteristiche fisiologiche e comportamentali
- Dove sei: le informazioni relative alla posizione dell'utente

Cosa conosci

È il tipo di autenticazione più comune, richiede che l'informazione utilizzata per autenticarsi sia conosciuta solo dalla persona e che quest'ultima la mantenga segreta. Passwords, security codes, PINs, passphrases, etc. sono gli esempi più comuni. Talvolta può essere sotto forma di risposta a domande che solo l'utente dovrebbe conoscere. Il problema di questo tipo di autenticazione è che l'informazione identificativa può essere condivisa, permettendo così ad altre persone di impersonare l'utente o che quest'ultime tentino di impadronirsene facendo uso di strumenti più o meno avanzati che permettono di scoprirla. Non da meno richiede di ricordare una sequenza di caratteri che può essere facilmente dimenticata. Nella sezione seguente verranno discussi in dettaglio le tipologie di autenticazione che appartengono a questa categoria

Password

Una password consiste in una sequenza di caratteri atti a verificare l'identità dell'utente che vuole accedere alle risorse di un sistema informativo. Le password vengono usate quotidianamente per accedere a svariati servizi o sistemi, tra i quali applicazioni web, e-mail, database, account bancari, account istituzionali etc. Per evitare l'utilizzo di password facilmente indovinabili quali anniversari, date di nascita, nomi di animali etc., le organizzazioni stabiliscono delle policy che vincolino l'utente ad utilizzare svariate tipologie di caratteri diversi così da rendere più difficile il password guessing. Tra queste policy è frequentemente richiesto un numero minimo di caratteri, l'uso di caratteri maiuscoli e minuscoli, di numeri e di caratteri speciali. Oltre ai requisiti appena descritti esistono delle best practice per la creazione di password robuste tra cui:

1. Dovrebbe contenere almeno otto caratteri
2. Non dovrebbe contenere lo username, il nome reale o dell'istituzione per la quale è usata

3. Non dovrebbe contenere parole complete o prese da un dizionario
4. Deve essere sufficientemente diversa dalle password usate in precedenza
5. Contiene caratteri di ognuna delle seguenti categorie:
    a. Lettere maiuscole (e.g. A, B, C)
    b. Lettere minuscole (e.g. a, b, c)
    c. Numeri (e.g. 0-9)
    d. Caratteri speciali presenti nella tastiera e spazi (e.g. ~ ! @ # $ % ^ & * _ - + = {})

Per poter essere efficacemente usate durante l'autenticazione le password devono essere memorizzate in modo sicuro dall'applicazione, diversamente un attaccante potrebbe comprometterla rendendo vano lo scopo dell'autenticazione. Il National Institute of Standards and Technologies (NIST) fornisce delle linee guida per memorizzare le password alcuni dei quali vengono riportati di seguito:

1. Cifrare il file contenente le password. Questo può essere ottenuto dal sistema operativo, un'applicazione apposita o password management atti a proteggere la riservatezza delle password
2. Configurare il sistema operativo in modo da limitare l'accesso al file contenente le password, ad esempio permettendolo ad i soli amministratori di sistema
3. Memorizzare l'hash della password. Utilizzando una funzione di cifratura one-way il sistema operativo ha modo di verificare la corrispondenza della password senza memorizzarla in chiaro, evitando così che questa sia visibile anche a coloro che vi hanno accesso. Le funzioni di hash più comuni sono MD5, SHA-1 e SHA-256 e producono un output di lunghezza fissa in modo da non rilevare la lunghezza della password. Tuttavia, l'hash della password risulterà uguale anche se due utenti diversi utilizzano la stessa password

Per evitare che il riutilizzo della stessa password produca lo stesso hash viene aggiunto all'hash della password un numero casuale chiamato salt (sale). L'utilizzo di questa strategia produce diversi benefici:

- Previene la duplicazione dell'hash di password uguali nel file delle password o nel database
- Aumenta la difficoltà dei dictionary attack e guessing attack eseguiti offline
- Rende difficile individuare che l'utente utilizza la stessa password su sistemi diversi

Il processo di memorizzazione avviene come segue:

- Viene assegnato un numero casuale alla password selezionata dall'utente
- Viene eseguito l'hash della password dando in input alla funzione di hash sia la password sia il sale
- Viene memorizzata la tripletta username, sale, hash della password

In fase di verifica vengono eseguiti i seguenti step:

- Viene eseguito l'hash della password insieme al sale corrispondente all'utente dichiarato
- Viene confrontato l'hash della password con quello memorizzato nella tripletta e in caso affermativo viene permesso l'accesso

Di fatto l'uso del sale aggiunge un ulteriore livello di offuscamento della password non prevenendone però il cracking. Il cracking risulterà più difficile e duraturo da portare a termine in quanto l'attaccante dovrà individuare contemporaneamente la password e il sale assegnatogli.

L'utilizzo di una password più robusta previene la compromissione della stessa dove, in generale, la robustezza della password è determinata dalla lunghezza della password, dal numero di possibili caratteri (e.g. lettere maiuscole, minuscole, numeri e caratteri speciali) e dall'imprevedibilità della combinazione di questi ultimi. L'idea che sta alla base della difficoltà di indovinare una password in base alla lunghezza e al numero di possibili caratteri è che, se la nostra password è composta da caratteri appartenenti ad un insieme di 26 caratteri distinti (e.g. lettere minuscole) avremo 26 possibili scelte per il primo carattere, 26 per il secondo… e così via fino all'ennesimo. Per le regole della combinatoria ne deriva che avremo 26^N possibili combinazioni di password di N caratteri.

Data la quantità di servizi che fanno uso della password e la necessità dell'utente di ricordarle e al contempo costruirne di difficilmente prevedibili, sono state introdotte delle tecnologie che permettono di limitare il numero di password che l'utente necessità di ricordare a memoria. Una di queste sono i password manager, uno strumento atto a memorizzare in un solo posto le password dell'utente mantenendole protette e al contempo facilmente accessibili, facendo uso di una sola master password per accedervi. Ne esistono di svariati tipi, tra cui versioni desktop, portable o web-based e costituiscono una valida alternativa al ricordare le password a memoria seppur rappresentando un single point of faillure in caso di compromissione. Il Single Sign-On (SSO) è un altro meccanismo che permette all'utente di autenticarsi utilizzando una sola coppia di credenziali per accedere a più servizi o risorse del sistema per i quali ha i permessi. L'uso del SSO fa spesso uso del Lightweight Directory Access Protocol (LDAP), dove il database LDAP è mantenuto su più server differenti. In generale applicazioni e servizi diversi fanno uso

di meccanismi diversi per supportare l'SSO ed è quindi fondamentale che il sistema esegua preventivamente un processing e memorizzazione interni delle credenziali richieste dai diversi meccanismi di autenticazione. I vantaggi dell'uso del SSO sono i seguenti:

- Applicazione uniforme delle policy aziendali su diversi sistemi
- Riduce la numerosità di reset della password da parte dell'helpdesk
- Riduce l'affaticamento dell'utente nel reintrodurre le credenziali per accedere a diverse risorse aziendali
- Riduce i tempi di reinserimento password e gli errori nel rieseguire l'autenticazione più volte

PIN Passwords

Solitamente i PIN sono utilizzati per accedere a dispositivi fisici come gli ATM, sono di breve lunghezza e fanno uso del solo tastierino numerico per l'inserimento (e.g. 0-9). Data la scarsa variabilità di combinazioni sono particolarmente vulnerabili ai guessing attack, rendendo fondamentale l'utilizzo di numeri non ripetuti, sequenziali o, in generale, con un particolare significato, ordine o simmetria. I sistemi basati su PIN hanno dei problemi comuni:

- Vulnerabilità al guessing attack e al brute forcing attack data la scarsa variabilità di combinazioni
- Vulnerabile allo shoulder surfing, un avversario che osservando l'inserimento del PIN diventa a sua volta detentore del segreto e può quindi autenticarsi
- Difficoltà nel ricordare un PIN sufficientemente randomico

Domande di sicurezza

Le domande di sicurezza (algorithm password) vengono richieste durante il processo di autenticazione e forniscono un ulteriore livello di sicurezza per verificare le credenziali utente, facendo uso di risposte che solitamente riguardano informazioni personali o lavorative. Diversi siti web le utilizzano per il reset/recupero della password e per verificare l'identità dell'utente in fase di sign-in o telefonicamente. Dal momento che queste domande sono spesso standard e contenenti informazioni quali la data di nascita o la scuola frequentata, potrebbero essere reperite online da persone diverse dal legittimo interessato, rivelate inconsciamente durante una conversazione o estorte tramite social engineering. L'utente si trova quindi di fronte a due possibilità di scelta: scegliere risposte corrette, facili da ricordare ma facilmente reperibili online oppure utilizzare risposte false e quindi più difficili da reperire online ma anche da ricordare. Un'alternativa a queste due opzioni è utilizzare risposte vaghe tipo "verdognolo"

come colore preferito, trovando così un compromesso tra le due scelte menzionate. È quindi importante saper trovare la giusta combinazione di domande di sicurezza, possibilmente seguendo questi criteri:

1. Sicura: non può essere indovinata facilmente o recuperata sul web
2. Stabile: la risposta deve rimanere invariata
3. Memorabile: facilmente ricordabile
4. Semplice: la risposta dovrebbe essere facile e consistente
5. Molteplice: può avere più risposte possibili

Cosa possiedi

In questa categoria rientrano tessere sanitarie, carte d'identità, carte magnetiche e smart card (e.g. dotate di chip). Questi oggetti devono essere tenuti al sicuro da furti o smarrimento, richiedono la verifica da parte di una persona o di una macchina e la loro sostituzione comporta dei costi. Il loro utilizzo come standard ha delle implicazioni in quanto il livello di sicurezza che forniscono dipende dal personale addetto alla verifica e non da meno avendo formati standard sono suscettibili alla falsificazione, alterazione e duplicazione.

Carta d'identità

La carta d'identità contiene una moltitudine di informazioni ed è utilizzata da diverse organizzazioni come scuole, aziende e governi per identificare la persona. Il tempo necessario alla verifica cambia a seconda dei requisiti di sicurezza e quindi alle informazioni che vengono verificate. Ad esempio, in un bar sarà sufficiente verificare che la foto corrisponda alla persona che la presenta e che l'età sia adeguata in caso vengano ordinati alcolici. Diversamente in un aeroporto la verifica dell'identità richiederà molto più tempo per effettuare tutte le verifiche del caso. Le moderne carte d'identità elettroniche permettono la lettura tramite dispositivi ottici che automatizzano e abbreviano i tempi di verifica.

Carte magnetiche e smart card

Sono comunemente utilizzate con sistemi automatizzati e differiscono dalle carte d'identità cartacee in quanto l'ispezione manuale non richiede necessariamente l'autenticazione della persona. Sono utili a ridurre i tempi di verifica dell'identità in quanto solitamente richiedono solo pochi secondi per l'identificazione, rispetto al tempo richiesto per la verifica manuale. Per contro una verifica manuale potrebbe individuare caratteristiche per cui i sistemi automatizzati non sono programmati.

Carte magnetiche

Le carte magnetiche sono tessere di carta o plastica dotate di una fascia magnetica che può essere letta e sovrascritta da un apposito lettore. La banda magnetica è suddivisa in tre settori numerati in modo sequenziale da quello più vicino al bordo superiore a quello più lontano e vengono utilizzati per applicazioni diverse. La "track" 1 è usata solitamente per le transazioni che coinvolgono l'accesso ad un database. Può contenere fino a 79 caratteri alfanumerici, tra cui identificativo dell'account, nome, cognome e data di scadenza. La seconda traccia è utilizzata per automatizzare le transazioni finanziarie e può contenere fino a 40 caratteri alfanumerici, tra cui l'identificativo dell'account e la data di scadenza. L'identificativo dell'account contiene l'issuing industry, l'issuer e l'identificativo dell'utente. In questa track è possibile memorizzare un offset o un PIN fino a cinque caratteri. Quando la carta viene inserita nel lettore i dati relativi al titolare vengono inviati ad un sistema centralizzato ai fini di verifica. La terza track è utilizzata per transazioni finanziarie e può contenere fino a 107 caratteri alfanumerici, tra cui identificativo dell'account e dati relativi all'utente e la sicurezza quali: codice nazionale, codice della valuta, ammontare consentito per ogni ciclo e codici per la verifica crittografica. Questa traccia è utilizzata in applicazioni in cui i dati memorizzati sono sovrascritti ad ogni transazione ed è l'unica a poterlo essere, può inoltre contenere una versione cifrata del PIN per evitare di contattare un sistema centralizzato per la verifica dell'identità del detentore della carta.

Smart card

La smart card è simile alla carta magnetica ma è dotata di un chip che le aggiunge capacità computazionale e una maggiore memoria. È alimentata da una fonte energetica che può consistere in una batteria integrata, in un accoppiamento induttivo che permette sia ai dati sia all'energia di essere scambiati attraverso l'aria (o una superficie non metallica) oppure tramite dei contatti metallici posti sulla superficie del chip che permettono di scambiare energia quando la carta è inserita nell'unità di lettura/scrittura. La memoria di cui è dotata una smart card può essere di tipo Read Only Memory (ROM), Random Access Memory (RAM), Electrically Programmable Read Only Memory (EPROM) e Electrically Erasable Programmable Read Only Memory (EEPROM). Una smart card deve inoltre essere in grado di comunicare con l'esterno tramite dei processi di input/output cosa che può avvenire in diversi modi, ad esempio nelle carte a contatto sono presenti dei terminali metallici tramite i quali avviene il trasferimento mentre nelle carte contactless la comunicazione avviene tramite un processo chiamato modulazione di frequenza o frequency shift keying. Il microprocessore presente nelle smart

card si occupa invece della manipolazione ed interpretazione dei dati utilizzando l'insieme di istruzioni memorizzate nel chip stesso. Una smart card può fornire diversi livelli di sicurezza, ad esempio può contenere una versione cifrata di una caratteristica biometrica del titolare per la verifica dell'identità. La smart card risulta più sicura rispetto alle carte magnetica in quanto con quest'ultima il PIN viene generato algoritmicamente a partire dall'identificativo del titolare dal sistema mentre nella smart card la potenza computazionale di cui è dotata permette di gestire internamente le operazioni di cifratura/decifratura e di generazione del PIN senza fornire l'identificativo utente. In questo modo risulta più difficile la duplicazione della carta o l'appropriazione della chiave tramite uno skimmer che legge il contenuto della carta e ne permette la replica. La possibilità di utilizzo di una caratteristica biometrica in sostituzione del PIN fornisce inoltre un ulteriore livello di sicurezza per quelle applicazioni che lo richiedono, applicazioni che possono coesistere all'interno della stessa carta.

Security dongle

I security dongle, comunemente chiamate chiavette di sicurezza, sono dei dispositivi utilizzati per l'autenticazione elettronica. Possono agire da ricevitori di codici randomici, generare codici randomici, contenere passphrase cifrate o una combinazione di questi. Dal momento che sono progettati per funzionare con sistemi specifici risultano difficili da duplicare e al contempo facili da usare.

I ricevitori di codici randomici ricevono da un server una one-time password (OTP) in fase di autenticazione, il ricevitore corretto (il dongle dell'utente) risponderà con lo stesso codice e se anche le credenziali sono corrette viene permesso l'accesso.

Nei generatori di codici randomici una one-time password (OTP) viene generata quando viene richiesta l'autenticazione dal sistema e se anche le credenziali corrispondono viene concesso l'accesso.

I token storage hanno una memoria interna cifrata per la memorizzazione delle passphrase. Quando il dongle riceve un segnale dal sistema viene decifrata la passphrase che verrà utilizzata come livello aggiuntivo di sicurezza per la verifica dell'identità.

Cosa sei

Questo tipo di autenticazione fa uso di caratteristiche fisiologiche o comportamentali che sono uniche per la persona, difficilmente condivisibili e per cui è difficile il ripudio. Dal momento che queste caratteristiche fanno parte della persona non possono andare perdute o rubate e risultano più difficili da falsificare. Le caratteristiche biometriche utilizzate più di frequente per

l'identificazione sono la firma, il riconoscimento del volto, la scansione dell'impronta digitale, dell'iride e il riconoscimento delle dinamiche di digitazione. Essendo difficili da compromettere risultano ideali in contesti in cui il grado di sicurezza richiesto è elevato. Il processo di autenticazione è automatizzato e il confronto tra il sample fornito e quello memorizzato nel sistema avviene comunemente tramite l'uso di uno scanner che rileva in real time le caratteristiche identificative. Rispetto ad altre tipologie di autenticazione l'utilizzo di scanner per il riconoscimento richiede hardware costoso e che spesso quando disponibile in prodotti commerciali ha caratteristiche e un'affidabilità limitata. Il processo di autenticazione biometrica richiede tre step:

- Devono essere raccolti i dati biometrici tramite l'uso di un sensore
- I dati raccolti vengono convertiti in una loro rappresentazione digitale chiamata template
- Viene confrontato l'input con il template memorizzato nel sistema e se c'è una corrispondenza viene garantita l'autenticazione

Diversamente da altre autenticazioni la corrispondenza tra input e rappresentazione memorizzata nel sistema avviene per somiglianza, dove quest'ultima è determinata da una soglia che permette di gestire le inaccuratezze che possono verificarsi in fase di input del segnale. L'autenticazione biometrica in fase di verifica calcola uno score che dovrà ricadere in un intervallo di confidenza per cui l'input e il template memorizzato risultano sufficientemente simili. Se questa soglia non è configurata in modo adeguato, ad esempio permettendo un'ampia differenza tra l'input e il template memorizzato, sarà maggiore la frequenza di falsi positivi ovvero che il sistema conceda l'accesso a persone non autorizzate. Al contrario se questo intervallo di confidenza è ridotto sarà maggiore la frequenza di falsi negativi e che l'utente venga quindi rifiutato nonostante abbia accesso al sistema.

L'autenticazione biometrica è suddivisa in due tipologie di attributi: comportamentali e fisiologici. I primi comprendono il riconoscimento della camminata, dei pattern di digitazione su una tastiera e il riconoscimento vocale mentre i secondi comprendono il riconoscimento facciale, lo scan dell'impronta digitale e della retina.

Le performance di un sistema biometrico sono misurate in termini di errori di decisione: false positive rate e false negative rate.

Quando un sistema autentica per errore una persona non autorizzata viene detto false positive ed è considerato l'errore di sicurezza più grave. Il false positive rate (FPR), anche conosciuto come false acceptance rate (FAR) o false match rate (FMR) misura quindi la facilità con cui il

sistema permette l'accesso ad un utente non autorizzato. Può essere espresso con la seguente formula:

$$FPR = \frac{Number\ of\ false\ sucessful\ attempts\ made\ in\ authenticating\ users}{Total\ number\ of\ attempts\ made\ in\ authenticating\ users}$$

Il false negative rate si verifica quando all'utente autorizzato non viene permesso di autenticarsi nel sistema. È conosciuto anche come false rejection rate (FRR) o false non-match rate (FNMR) e misura la probabilità che l'input dell'utente non abbia un match con i template memorizzati nel database. Può essere espresso con la seguente formula:

$$FNR = \frac{Number\ of\ false\ reject\ made\ in\ authenticating\ genuine\ users}{Total\ number\ of\ attempts\ made\ in\ authenticating\ users}$$

L'equal error rate (EER), chiamato anche crossover rate, è il valore per cui data una threshold di somiglianza il FPR e il FNR risultano identici. In generale minore è l'EER e maggiore sarà l'accuratezza del sistema. I parametri FPR e FNR possono essere modellati a seconda dei requisiti del sistema: possiamo quindi azzerare il FNR, garantendo che un utente non autorizzato non acceda mai al sistema, a discapito del FPR oppure viceversa garantendo che l'utente corretto non venga mai rifiutato.
L'accuratezza (ACC) è la probabilità che l'utente sia correttamente identificato e viene calcolata con la seguente formula:

$$ACC = \frac{TPR\ +\ TNR}{TPR\ +\ TNR\ +\ FNR\ +\ FPR}$$

Dove TPR è il true positive rate ed è la misura complementare del FNR mentre il TNR è il true negative rate ed è la misura complementare del FPR.
La precisione (PR) è la probabilità che un utente accettato dal sistema sia effettivamente un utente legittimo ed è calcolata tramite la seguente formula:

$$PR = \frac{TPR}{\mathrm{TPR}\ +\ \mathrm{FPR}}$$

Behavioral Attributes

Sono attributi che riguardano le caratteristiche comportamentali della persona e in quanto tali variabili nel tempo e a seconda delle condizioni.

La gait recognition riconosce la persona sulla base di come cammina. Può essere svolta tramite l'ausilio di una registrazione video, misurando la traiettoria delle giunture e l'angolo creato dalle gambe oppure tramite sensori di movimento come l'accelerometro e il giroscopio presenti negli smartphone, che registrano la ciclicità che caratterizza l'andatura della persona.

La Keystroke recognition utilizza i pattern di digitazione su una tastiera per identificare l'utente. Può essere svolta calcolando le tempistiche di spostamento fra i tasti, la forza impressa sui tasti e la durata per cui gli stessi vengono tenuti premuti

La voice recognition autentica la persona sulla base del suo modo di parlare (e.g. intonazione, velocità etc.) misurando le onde sonore emesse mentre l'utente parla. Può essere suddivisa in due categorie: text-dependent e text-independent. La prima utilizza lo stesso testo nella fase di enrollment e di verifica mentre la seconda è in grado di autenticare l'utente anche utilizzando un testo diverso da quello sottoposto in fase di enrollment.

Physiological Attributes

Sono caratteristiche fisiche della persona e non possono essere alterate facilmente. In quanto più consistenti nel tempo rispetto a quelle comportamentali risultano essere più affidabili di queste ultime.

Il riconoscimento facciale misura la distanza tra gli occhi, lo spessore del naso, la distanza tra gli zigomi e altre caratteristiche uniche del volto per autenticare l'utente. Tra le difficoltà nell'effettuare un corretto riconoscimento facciale tramite telecamera vi sono le condizioni di luce e l'angolo d'inquadratura, ciò nonostante, viene utilizzato in contesti ad elevato livello di sicurezza come nelle ambasciate e nelle agenzie governative

Il riconoscimento dell'impronta digitale misura le creste e gli avvallamenti che si formano sulla superficie del polpastrello. Durante la scansione viene catturata un'immagine digitale del dito e individuati dei punti unici che caratterizzano l'impronta.

La scansione della retina opera proiettando una luce nella parte posteriore dell'occhio, luce che viene assorbita diversamente dai capillari rispetto al tessuto circostante. La distribuzione dei capillari nella retina è unica da persona a persona e similmente all'impronta digitale è caratterizzata da punti unici, la distanza tra questi e, in generale, la distribuzione dei capillari permette di identificare l'utente. Rispetto al riconoscimento dell'iride richiede fotocamere più sofisticate ed è più suscettibile all'errore in quanto il minimo movimento dell'occhio può causare il rifiuto da parte del sistema di autenticazione.

Dove sei

Questo tipo di autenticazione sfrutta la posizione dell'utente per identificarlo facendo uso di strumenti come il global positioning system (GPS), l'indirizzo IP o la cella telefonica a cui è collegato. Viene spesso utilizzato in concomitanza con altri strumenti di autenticazione come fattore secondario, atto a verificare che la persona sia autorizzata all'accesso dalla posizione in cui si trova. Può essere anche utilizzato per verificare che posizione e orario di accesso siano coerenti con altri accessi, ad esempio se a distanza di pochi minuti l'utente si autentica da posti che non è realistico che abbia raggiunto in quel lasso temporale. Le location-based authentication (LBA) richiedono una location signature (LS) costituita dalla posizione e da un timestamp. Questi ultimi vengono generati da un location signature sensor (LSS) che una volta generata la signature la inoltrano per autenticare l'utente. Questo tipo di autenticazione può essere utilizzato in caso di furto del dispositivo che funge da sensore, per individuare un accesso da una località insolita ed eventualmente bloccare o effettuare ulteriori verifiche. Un altro dei vantaggi di questa tipologia è che può essere utilizzata in modo continuativo generando ininterrottamente signature e inoltrandole insieme ai dati, così da interrompere l'accesso nel caso di hijack della connessione.

Attacchi ai sistemi di autenticazione [1]

Nell'Attack Model considerato si assume che un'attaccante non possa bypassare il meccanismo di autenticazione e sia quindi costretto ad autenticarsi con successo.

Brutal-force and Guessing Attacks

Il brute forcing consiste nel tentare ripetutamente di autenticarsi utilizzando svariate combinazioni dell'informazione identificativa dell'utente (e.g. password). Questo metodo è spesso esoso di risorse computazionali e richiede tempo per essere efficace. Per contro il guessing attack può essere più o meno efficace a seconda che l'informazione identificativa dell'utente sia facilmente prevedibile (e.g. disponibile su un dizionario).

Observation Attacks

Le knowledge-based authentication e le biometrics-based authentication sono spesso vulnerabili a questo tipo di attacco, basato sull'osservazione del processo di autenticazione e conseguente furto dell'informazione identificativa. Può essere portato a termine utilizzando tecnologie atte alla cattura di immagini e video o semplicemente spiando l'inserimento (e.g. shoulder surfing di una password).

Impersonation Attacks

L'impersonation attack mira ad assumere l'identità dell'utente presentando la stessa informazione identificativa o una simile. Solitamente richiede che venga portato a termine un observation attack per impadronirsi dell'informazione utilizzata durante l'attacco e comprende il replay attack, l'imitation attack e il synthesis attack. Il replay attack riutilizza l'informazione identificativa dell'utente legittimo (e.g. password o foto dell'utente). L'imitation attack è solitamente utilizzato per le behavorial biometric e consiste nell'imitare la caratteristica. Il synthesis attack è un tipo avanzato di attacco che consiste nel replicare l'informazione identificativa dell'utente da informazioni parziali della stessa (e.g. l'intero viso da una foto di profilo).

Side-channel Attacks

Il side-channel attack mira a inferire l'informazione identificativa sfruttando l'information leakage non strettamente legato all'informazione identificativa che può avvenire durante il processo di autenticazione. Il side-channel attack è stato sfruttato in origine per ridurre la robustezza dei sistemi crittografici, facendo uso non tanto dell'input quanto delle informazioni legate ad esso quali timinig e consumo energetico. Data la varietà di sensori disponibili sui dispositivi mobili un avversario potrebbe sfruttarli per derivare l'informazione identificativa e passare l'autenticazione (e.g. la posizione cliccata date le vibrazioni prodotte durante l'inserimento della password su un touchscreen). Il side-channel attack potrebbe essere sfruttato da un malware che ha accesso ad un sensore per raccogliere informazioni relative all'informazione identificativa, garantendo una maggiore probabilità di successo rispetto al brute force o al guessing attack.

Authentication Model Attacks via Adversarial Examples

In anni recenti è stato sviluppato un nuovo tipo di attacco che mira ad attaccare l'authentication model rispetto al rubare l'informazione identificativa. Questo attacco consiste nel generare un advesarial example che non è l'informazione identificativa dell'utente ma può essere riconosciuta dal sistema come tale. Un esempio può essere il modificare la foto di un utente che non è quello legittimo ma che viene riconsociuta dal face ID come se lo fosse o analogamente riprodurre un audio che non contiene la voce dell'utente ma permette ugualmente di passare l'autenticazione. L'idea è falsificare le caratteristiche dell'input di cui fa uso l'authentication model (e.g. Mel Frequency Cepstral Coefficents o MFCC). Questo attacco non emula l'input dell'utente ma ne utilizza uno diverso con le stesse caratteristiche.

Tipologie di attacco per tipologia di autenticazione

È possibile suddividere le tipologie di autenticazione disponibili su dispositivi mobili in quattro categorie basandosi sulle authentication metrics (e.g. knowledge factor, biometric factor, ownership factor): knowledge-based authentication, physiological biometrics-based authentication, behavioral biometrics-based authentication e two/multi-factor authentication.

Knowledge-based Authentication

La Knowledge-based Authentication utilizza un segreto disponibile solo all'utente e al sistema su cui si autentica. Questo segreto può essere testuale (e.g. password) o grafico (e.g. pattern lock). È il sistema di uso più comune per la sua semplicità d'uso ma è vulnerabile al furto e alla knowledge leakage. Il metodo più semplice per compromettere questa autenticazione è usando lo shoulder surfing ma in letteratura sono disponibili svariate tipologie di attacco che fanno uso delle impronte lasciate sullo schermo e altre che fanno uso di side channel disponibili sul dispositivo. Tra queste ultime: è possibile individuare il movimento della mano tramite informazioni relative al timing di inserimento, tramite l'uso dei sensori di movimento e tramite la cattura dei segnali wireless emessi. Per questi motivi questo metodo di autenticazione non risulta più sufficientemente sicuro per la verifica dell'identità dell'utente.

Attacchi

Visual-based attack: un attaccante può osservare o registrare l'utente durante l'inserimento della password, questo è anche possibile registrando il contenuto dello schermo durante lo swipe o digitazione della password. Tecniche più avanzate sono riportate in letteratura. È infatti possibile individuare la password data la registrazione con una videocamera dei movimenti effettuati dal dispositivo, che a seconda del punto di pressione sullo schermo si sposterà in maniera diversa. Similmente è possibile catturare i movimenti del dito sul touchscreen e basandosi sulla geometria dei movimenti del dito e ridurre il numero di possibili gesti effettuati durante lo sblocco tramite pattern lock. Lo smudge attack fa invece uso delle tracce oleose lasciate dalle dita sullo schermo.

Timing Information-based attacks: le system timing information si sono rivelate una fonte per estrapolare la password sia facendo uso del tempo che intercorre tra la digitazione di un tasto e l'altra sia facendo uso del numero di interrupt che produce il touchscreen di un sistema Android durante la digitazione del lock pattern.

Privacy Leakage via Embedded Sensors on Mobile Devices: i sensori di movimento (e.g. giroscopio e accelerometro) forniscono anche più informazioni riguardo i pattern di input rispetto alle timing information. L'intuizione è che le vibrazioni propagate lungo il dispositivo e catturate da questi due sensori siano distinte per pattern di inserimento differenti. Questi sensori possono anche essere usati in concomitanza col sensore di luce ambientale. Quest'ultimo rilevando diversi cambi di luminosità durante il movimento del dispositivo si è rivelato fornire ulteriore informazione aggiuntiva per inferire l'input dell'utente.

Radio Signal-based Attacks: Le Channel State Information (CSI) estratte dal segnale WiFi ricevuto dal dispositivo sono utilizzabili per inferire l'input utente. Questo è dovuto a come la

mano copre il dispositivo e al movimento della stessa, che unite causano degli effetti multi-path unici utilizzabili in condizioni ideali per poter estrarre la password.

Wearable-based Attack: Smartwatch e fitness band permettono una maggiore granularità nel catturare i movimenti della mano durante le knowledge-based authentication permettendo una maggiore accuratezza dei rilevamenti. Tramite l'accelerometro e il microfono è possibile calcolare lo spostamento del polso durante la digitazione su un POS o su una tastiera inferendo così l'input digitato. È stato inoltre dimostrato che tramite la combinazione dei rilevamenti di accelerometro, giroscopio e magnetometro è possibile individuare gli spostamenti della mano con una precisione millimetrica. Questo ha permesso di individuare la passcode di pagamento indipendentemente dalla mano utilizzata per indossare lo smartwatch e per tenere lo smartphone.

Physiological Biometrics-based Authentication

Le Physiological Biometrics-based Authentication sono disponibili su svariati dispositivi in aggiunta alle knoledge-based. Queste risultano più comode rispetto alle seconde in quanto non richiedono di memorizzare un segreto e risultano più sicure perché lo stesso è più difficile da rubare. Questi vantaggi derivano dallo sfruttare caratteristiche biometriche uniche della persona (e.g. impronta digitale, geometria del viso) e che risultano sempre disponibili alla stessa. Tuttavia, i sensori utilizzati per lo scan di queste caratteristiche sono costosi e non sempre disponibili sui dispositivi e sebbene sia possibile utilizzare sensori non dedicati a tal fine i risultati non garantiscono un adeguato livello di sicurezza. L'unicità e l'invariabilità di queste caratteristiche le rende particolarmente vulnerabili in caso di furto e dal momento che si è dimostrato possibile falsificarle (e.g. impronta digitale, geometria del viso) l'utente risulta spesso restio ad utilizzarle.

Attacchi

Le physiological biometrics-based authentication sono più difficili da forzare tramite attacchi brute force o tramite il guessing attack rispetto alle knowledge-based e in letteratura sono stati rilevati relativamente pochi metodi per far uso dei side-channel attack. Tuttavia, sono risultate vulnerabili all'observation attack. Un attaccante potrebbe infatti far uso delle tracce oleose lasciate inconsciamente su varie superfici per riprodurre l'impronta digitale o il palmo della mano. L'utilizzo di dita fatte di plastilina e silicone è infatti risultato efficace nel passare l'autenticazione degli scanner di impronte digitali commerciali, tra i quali quelli ottici, ad ultrasuoni e quelli che fanno uso di un sensore capacitivo. Questo è stato ottenuto sfruttando il False Positive Rate (FPR) che caratterizza i sistemi biometrici. Sebbene l'impronta digitale

corretta producesse un matching score più elevato, quello dell'impronta digitale fasulla si è rivelato sufficientemente simile ai sample utilizzati in fase di enrollment da riuscire passare l'autenticazione. Similmente le caratteristiche visive dell'utente quali viso, occhi, orecchie e geometria della mano sono difficili da mantenere segrete data la varietà di foto e video disponibili sui social media. È stato infatti dimostrato che i sistemi che fanno uso di queste caratteristiche risultano facilmente compromettibili tramite l'uso di foto e video riprodotte su carta o sullo schermo di un dispositivo. Tecniche più avanzate fanno uso di stampanti 3D per riprodurre il viso o la geometria della mano dell'utente legittimo o ancora stampando l'iride dello stesso su una lente a contatto. Non sono state invece rinvenute in letteratura tecniche che siano in grado di compromettere i sistemi che fanno uso dell'EEG e dell'ECG come informazione identificativa.

Behavioral Biometrics-based Authentication

Le Behavioral Biometrics-based Authentication sfruttano abitudini o altre caratteristiche uniche comportamentali (e.g. voce, camminata). Il vantaggio di queste caratteristiche è che fanno uso di informazioni meno private e utilizzano sensori già disponibili sulla maggior parte dei dispositivi. Non da meno la raccolta di queste informazioni risulta trasparente all'utente e permette un'autenticazione continua, senza la necessità di interazione dell'utente anche in quei casi in cui è richiesto un periodo di autenticazione e protezione più duraturo. Tuttavia, i sensori disponibili soffrono spesso di una bassa frequenza di campionamento e bassa fedeltà, da questo ne deriva un elevato numero di falsi negativi. Inoltre, questo tipo di autenticazione risulta vulnerabile agli attacchi che sfruttano l'imitazione del comportamento.

Attacchi

Per compromettere una behavioral biometrics-based authentication è necessario inserire in input il corretto pattern comportamentale. Un avversario potrebbe quindi utilizzare il proprio comportamento tentando un random o guessing attack e sperare in un successo. Potrebbe invece aumentare le proprie chance di riuscita osservando l'inserimento del pattern (observation attack) e imitando l'inserimento (imitation attack). Tecniche più avanzate disponibili in letteratura hanno dimostrato che il random attack ha probabilità pressoché nulla di successo mentre l'imitation attack ha un basso successo, questo perché le caretteristiche comportamentali sono difficili da imitare. Inoltre, quando l'autenticazione comprende l'uso di più sensori (e.g. touchscreen e accelerometro) si è dimostrata più robusta alla compromissione tramite observation attack. Questo perché all'avversario risulta più difficile riprodurre tutte le caratteristiche rilevate dai sensori durante l'inserimento del pattern comportamentale. Le

autenticazioni che fanno uso della voce sono quelle risultate più vulnerabili a causa della natura non riservata del canale di cui fanno uso. Un avversario può portare a compimento diversi tipologie di attacco, tra cui replay attacck, synthesis attack, imitation attack e random attack. Il replay attack può infatti essere ottenuto semplicemente registrando la voce e riproducendola in prossimità del microfono. Similmente un avversario può studiare il modo di parlare dell'utente quotidiano e impersonare o sintetizzare il suono della voce dell'utente in modo da passare l'autenticazione. In anni recenti sono state sviluppate tecniche più avanzate che sebbene non siano ancora state testate su sistemi di autenticazione sono risultate promettenti per il futuro. L'Hidden voice commands e il dolphin attack possono essere usati anche quando l'utente è in prossimità del dispositivo e senza che se ne renda conto. L' Hidden voice command attack consiste nel generare un suono che non sia comprensibile agli umani ma che venga riconosciuto dai sistemi che fanno uso dei controlli vocali. Esso consiste nel generare un suono percepito dall'orecchio umano come rumore e che imiti le caratteristiche acustiche dei comandi vocali riconosciuti dal sistema, suono che può essere nascosto anche all'interno di una traccia musicale. Similmente il dolphin attack modula il suono della voce registrata a frequenze non udibili e lo riproduce su degli speaker ad ultrasuoni. Data la non linearità del microfono la riproduzione degli ultrasuoni viene riconosciuta dal sistema.

Two/multi-factor Authentication

La Two/multi-factor Authentication combina due o più fattori per fornire un'autenticazione più sicura rispetto all'uso di un singolo fattore. Questo può avvenire sia combinando diverse authentication metrics (e.g. password e impronta digitale) sia utilizzandone una singola ma usando due diversi fattori (e.g. voce e impronta digitale). Se da un lato è più difficile per un avversario compromettere più fattori dall'altro richiedere all'utente di inserire più fattori consecutivamente può risultare in un'autenticazione meno user-friendly. Un esempio potrebbe essere quello di inserire il face ID, l'impronta digitale e una password per sbloccare il telefono. Per contro utilizzare il MAC address del dispositivo usato dall'utente combinato con una password fornisce una two-factor authentication più robusta rispetto all'uso dei singoli fattori e non risulta meno conveniente per l'utente. Tuttavia, anche in questo caso un malintenzionato potrebbe modificare il proprio MAC address ed essersi impossessato della password. Questo implica che non è sufficiente combinare diversi fattori tra loro ma che è necessario che tra di essi vi sia un'integrazione per aumentare a tutti gli effetti il livello di sicurezza fornito. Un esempio è la cattura delle physiological e behavioral biometric mentre l'utente firma sullo schermo dello smartphone. La pressione e la velocità di firma possono essere combinate con la

calligrafia dell'utente rendendo più difficile per l'avversario la compromissione di tutte queste caratteristiche contemporaneamente. L'utilizzo della sensor fusion sembrerebbe quindi essere una alternativa promettente alla combinazione di più fattori consecutivi.

Usabilità e vulnerabilità

Rispetto all'utilizzo di un singolo fattore, la multi-factor authentication risulta essere sempre più sicura in quanto all'avversario è richiesto di compromettere più fattori per portare a termine l'attacco. Tuttavia, sebbene implementare un'autenticazione multi-fattore a cascata aumenta la difficoltà dell'avversario nel compromettere il sistema per contro richiede all'utente uno sforzo ulteriore, non rimuovendo le vulnerabilità presenti nei singoli step. In letteratura viene infatti riportato che l'utilizzo di più fattori consecutivi non aumenta solo la difficoltà dell'attaccante per comprometterla ma anche quella dell'utente nell'inserire tutti i fattori correttamente. In alternativa, l'utilizzo di un secondo fattore ownership-based non richiede all'utente uno sforzo maggiore ma può essere perso, rubato o falsificato nel caso ad esempio del MAC address. Inoltre, la presenza di un dispositivo mobile utilizzato come ownership factor è stata dimostrata essere vulnerabile all'acoustic attack. È stato sufficiente generare un suono quale una suoneria sul dispositivo mobile e riprodurre lo stesso suono sul dispositivo nel quale ci si vuole autenticare per simulare la coesistenza dei due dispositivi nello stesso luogo.

Sistemi di autenticazione per smartwatch

In questa sezione verranno riportati i sistemi di autenticazione per smartwatch proposti in letteratura il cui testo integrale fosse reperibile su Google Scholar. Si è scelto di suddividere gli studi raccolti in due gruppi sulla base della tipologia di informazione usata ai fini dell'autenticazione: qualcosa che l'utente conosce e qualcosa che l'utente fornisce sulla base di ciò che fa/è. Nel primo caso i risultati sono stati inclusi senza ulteriori screening mentre nel secondo si è scelto di includere i soli report che riportassero una misura dell'efficacia del meccanismo di autenticazione in termini di false acceptance rate (FAR), false match rate (FMR), equal error rate (EER), accuracy (ACC) e precisione (PR) o loro sinonimi o misure complementari. La misura di questi effetti è stata uniformata nella trattazione utilizzando gli indicatori di false positive rate (FPR) analogo al FAR, false negative rate (FNR) analogo al FMR, l'equal error rate (EER), accuracy (ACC) e precisione (PR). Nel reperire i risultati delle ricerche si è fatto uso delle seguenti parole chiave o di una loro combinazione: authentication, continuous, smartwatch, system, mechanism, wearable.

Sistemi basati su qualcosa che l'utente conosce/possiede

I metodi più utilizzati per autenticarsi su uno smartwatch sono l'uso di un PIN o di un pattern su una griglia. Questi due meccanismi sono vulnerabili allo shoulder surfing: un avversario che osservando l'inserimento è in grado di riprodurlo impersonando l'utente.

In [8] Guerar et al. propongono 2gesture PIN, un meccanismo che permette l'inserimento del PIN in due gesti tramite la corona laterale presente negli smartwatch. L'interfaccia grafica è composta da due ruote concentriche. La ruota esterna contiene le cifre ordinate tra 0 e 9 mentre in quella interna le cifre sono disposte in maniera casuale e variano a ogni sessione e step. Per autenticarsi, l'utente utilizza la corona laterale dello smartwatch per far ruotare la corona interna finché la prima cifra del PIN contenuta nella ruota interna e la seconda cifra contenuta nella ruota esterna non coincidono e confermando premendo la corona laterale. La stessa procedura viene eseguita per la terza e la quarta cifra. Questo sistema risulta essere efficace nel contrastare lo shoulder surfing e il video recording attack basati su singole osservazioni, senza l'uso di

hardware addizionale e risolvendo i possibili problemi di digitazione che affliggono l'inserimento del PIN classico. Il sistema è però vulnerabile nel caso di osservazioni multiple. Osservando la digitazione più volte è possibile individuare quali coppie di cifre vengono sempre associate nei due step, in quanto la disposizione delle cifre sebbene variabile preserverà sempre le coppie corrette.

In [9] gli autori propongono di rendere l'inserimento della password più resistente allo shoulder surfing saltando l'inserimento di alcuni dei suoi caratteri. Il sistema in fase di inserimento rimuove dai 2 ai 4 caratteri casuali dalla password riducendo al contempo il numero di caratteri necessari a comprometterla.

ESPIT [10] sostituisce le cifre del PIN con dei pattern acustici trasmessi tramite gli auricolari. Il sistema, ogni volta che l'utente deve inserire una cifra, produce una lista di oggetti a cui sono associati dei suoni in maniera casuale. Per autenticarsi è quindi richiesto di individuare l'oggetto a cui è associato il suono corretto e trascinare l'elemento per confermare. Questa procedura viene quindi iterata per ogni elemento che corrisponde ad una delle cifre del classico PIN.

SpinPad [11] è composto da un'app la cui interfaccia grafica è composta da due ruote concentriche e due pulsanti. La ruota più interna contiene i caratteri alfabetici dalla A alla J mentre quella esterna i numeri tra 0 e 9. Ogni volta che l'utente deve inserire una cifra del PIN il sistema comunicherà tramite l'uso degli auricolari una lettera casuale a cui far corrispondere la cifra contenuta nella ruota più esterna. Successivamente la ruota interna comincerà a girare e l'utente dovrà attendere che la lettera di riferimento sia adiacente alla cifra del PIN per confermare l'inserimento. L'utente può utilizzare il tasto CD per invertire il senso di rotazione oppure il tasto PK per confermare l'inserimento del carattere.

IPIN [12] fa uso di una tecnica chiamata "immagini ibride" per illudere l'avversario. Il sistema sfrutta un algoritmo che crea due tastiere sovrapposte e che si avvale del fatto che l'utente e un malintenzionato osservano la tastiera da due distanze e angolazioni diverse. La soglia di separazione tra queste due distanze è dettata dall'algoritmo di visibilità usato. Dai due punti di vista entrambi vedranno una tastiera ma con un ordine delle cifre differente.

Sistemi basati su qualcosa che l'utente è/fa

In [13] Cheung et al. fanno uso di tre caratteristiche per autenticare l'utente: il battito cardiaco, il pattern di camminata e il respiro. La funzione di autenticazione primaria utilizza il battito cardiaco, rilevato col fotopletismografo. Se questo garantisce una confidenza accettabile sulla legittimità dell'utente allora l'utente viene autenticato. In caso contrario viene verificato se l'utente sta camminando o meno. In caso affermativo il sistema utilizza il pattern di camminata insieme a quelli cardiaci e se questi garantiscono una confidenza accettabile l'utente viene autenticato. Se i pattern di movimento non sono disponibili o non è garantita una confidenza accettabile, vengono combinati i pattern respiratori rispettivamente con quelli del battito cardiaco o con quelli del battito cardiaco e i pattern di movimento. Se ancora non è possibile autenticare l'utente con una confidenza accettabile verrà utilizzata l'autenticazione già disponibile sul dispositivo. Il sistema tramite l'uso della sensor fusion e l'utilizzo in cascata di diverse combinazioni di sensori cerca di ovviare alle possibili inaffidabilità nei rilevamenti che le singole tipologie di autenticazione presentano. I rilevamenti effettuati tramite il fotopletismografo sono infatti affetti da artefatti dovuti al movimento del polso, come non rilevamenti o falsi rilevamenti del battito cardiaco dovuti alla deformazione della pelle o dinamiche del flusso sanguigno [14]. I pattern di camminata potrebbero invece subire variazioni a seconda dell'abbigliamento indossato mentre i pattern respiratori potrebbero essere influenzati dalla condizione fisica, dall'umore, dalle condizioni di salute e dal rumore di sottofondo dovuto all'ambiente circostante. L'analisi è stata svolta su tre dataset, tra cui: uno è stato popolato con i rilevamenti del battito cardiaco raccolti ad una frequenza di un campione per minuto su tre persone tramite un Fitbit Charge HR; il WISDM [15] in cui sono stati raccolti i dati lungo i tre assi dall'accelerometro e dal giroscopio, ad una frequenza di un campione ogni 50 ms, tramite un LG G Watch e infine un dataset audio, l'ESC-50 [16] dove la frequenza di campionamento è di 22.05 Hz e la durata del campione è di 5 secondi. Data la differenza nella frequenza di campionamento nei dati relativi al battito cardiaco e ai pattern di movimento, i dati sono stati segmentati in finestre di dieci sample ai fini di uniformarli mentre i campioni audio respiratori sono stati segmentati in modo da avere un singolo pattern respiratorio per campione audio. Per simulare le possibili variazioni del respiro i campioni audio sono stati alterati con 15 cambi di intonazione tra $-\frac{7}{2}$ e $\frac{7}{2}$ con incrementi di $\frac{1}{2}$ ed 8 cambi di velocità compresi tra 0.25x e 2x ad incrementi di 0.25x. Per la selezione delle feature più rilevanti è stato fatto uso del pacchetto Sci-kit learn ed applicate le tecniche: Correlation approach, Select from a Model e Select K Best. Per evitare l'overfitting sono stati utilizzati un numero di istanze dieci volte superiore al numero di feature utilizzate mentre i modelli sono stati allenati utilizzando la

strategia leave-one-out, dove un'istanza viene utilizzata per il testing e le restanti per il training di tre classificatori: k-Nearest Neighbor (k-NN), Random Forest (RF) e Support Vector Machine (SVM). Gli autori hanno scelto di ottimizzare la scelta dei classificatori in base alla coppia (o tripla) di parametri biometrici utilizzati per il riconoscimento, sviluppando così un sistema modulare che fa uso del classificatore più performante per ogni modulo. Il miglior modello per il battito cardiaco è risultato l'SVM facendo uso di un kernel polinomiale e parametri d=2 e C=1, dove ACC=61% (18%), FPR=70% (20%) e FNR=8% (16%). Utilizzando sia i pattern di movimento sia il battito cardiaco è risultato più performante il modello RF con numero di estimatori n=500, dove ACC=84% (9%), FPR=26% (10%) e FNR=5% (3%). Per il battito cardiaco e i pattern respiratori i migliori risultati sono stati ottenuti usando il k-NN con parametri k=6 e la Minkowski distance per la misura della prossimità, dove ACC=91% (4%), FPR=17% (4%) e FNR=0% (0%). La fusione dei tre sensori è risultata invece più performante usando un modello k-NN con i parametri k=2 e la Minkowski distance. I risultati ottenuti sono ACC=93% (6%), FPR=14% (7%) e FNR=0% (0%), dove tra parentesi è indicato l'intervallo di confidenza.

In [17] Vhaduri e Poellabauer usano il battito cardiaco, le calorie bruciate, i pattern di camminata e il metabolic equivalent of task (MET) per mantenere autenticato l'utente sia durante i periodi di attività sia durante quelli sedentari. Il MET è un'unità di misura che stima la quantità di energia utilizzata dall'organismo durante un'attività [18]. Il dataset utilizzato per allenare il sistema è il NetHealth Study Dataset [19], raccolto su 400 individui che hanno indossato un Fitbit Charge HR. Questo dataset raccoglie i dati del battito cardiaco ad una frequenza di un minuto, battito cardiaco medio, calorie bruciate, MET, livello e intensità dell'attività fisica, conteggio dei passi, e monitoraggio del sonno. Questi dati possono essere suddivisi in tre categorie: behavorial (e.g. contapassi e attività fisica), physiological (e.g. battito cardiaco) e hybrid (e.g. calorie bruciate e MET), dove i dati relativi a queste ultime sono derivati dalle prime due. Ai fini di allenare un modello di tipo Quadratic Support Vector Machine (q-svm), classificatore rivelatosi ottimale in uno studio precedente, sono stati segmentati i dati di battito cardiaco, calorie bruciate, MET e conteggio passi in finestre di cinque minuti non sovrapposte. Il dataset è stato quindi costituito in modo che fossero presenti dieci finestre temporali per ogni feature in modo da evitare l'overfitting ed è stato fatto uso del 75% dei campioni per il training e del 25% per il testing. Per selezionare le feature più rilevanti è stato usato il Two-sample Kolmogorov-Smirnov (KS-test) con null hypothesis H_0: "i due dataset hanno la stessa distribuzione". Successivamente è stato applicato il Coefficient of Variation (COV)-approach sulle feature ottenute dal KS-test, dove le feature che variano maggiormente

ovvero quelle con un COV più elevato tra i soggetti hanno maggiore probabilità di distinguere gli utenti e risultano quindi essere più rilevanti ai fini della classificazione. L'autenticazione dell'utente è stata fatta separatamente per i periodi di attività e per quelli sedentari, si è quindi ricercato quali fossero i parametri ottimali per i diversi approcci di selezione delle feature e successivamente per ognuno di questi ultimi sono state confrontate le diverse combinazioni di parametri biometrici per trovare la migliore. I risultati ottenuti mostrano che durante i periodi sedentari la migliore combinazione di parametri biometrici comprende tutti e quattro quelli considerati; tuttavia, i risultati sono simili usando le altre combinazioni di parametri ad eccezione del conteggio dei passi usato come unico fattore di riconoscimento. Nei periodi di attività è risultato invece ottimale fare uso del MET e delle calorie bruciato per autenticare l'utente. Il sistema ha riportato un'ACC del 92% e un FPR del 2% quando l'utilizzatore è in stato sedentario. Quando invece l'utente è fisicamente attivo l'accuratezza del sistema è dell'88% mentre il FPR è dell'1%.

In [20] gli autori utilizzano la combinazione dell'ECG e la pressione arteriosa del sangue (ABP) per autenticare l'utente. Il sistema è stato testato sia su utenti che soffrono di patologie cardiache sia su soggetti sani sotto questo aspetto e la scelta di utilizzare sia l'ECG sia l'ABP è giustificata dal fatto che il solo ECG è caratterizzato da forme e proprietà temporali che potrebbero non presentarsi nel caso di utenti che sono in particolari condizioni di salute. Il dataset utilizzato è costituito da 36 utenti, sia in stato di salute sia con patologie cardiache, appartenenti al MIT PhysioBank Fantasia e al MGH database [21]. Il primo contiene istanze di persone sane mentre il secondo contiene principalmente istanze di persone con patologie cardiache. I segnali sono stati segmentati in modo che ogni finestra temporale contenesse almeno un intervallo RR, ovvero l'intervallo che intercorre tra due battiti cardiaci consecutivi. Il dataset è stato utilizzato per allenare un classificatore di tipo Extremely Randomized Tree. Il sistema è caratterizzato da due parametri principali che sono il tempo di allenamento Δ, ovvero la quantità di dati usata per il training, e la lunghezza dell'intervallo utile in fase di autenticazione ω. Il secondo parametro è stato ottimizzato tenendo fisso Δ=10 minuti e ottenendo i risultati migliori in termini di accuracy per ω=3 secondi, dove ACC=97,24%, FPR=3,6 e FNR=1,91 e EER=2,97. Fissato ω=3 secondi sono stati testati i valori per Δ tra 5 e 20 minuti ad intervalli di 5 minuti, dove i risultati per i valori tra 10 e 20 minuti sono simili seppur i migliori sono risultati quelli con Δ=20 minuti, dove l'ACC=97,33%, FPR=3,49% e FNR=1,86% e EER=3,04%. Riducendo la fase di enrollment a Δ=5 minuti le performance sono tuttavia di poco inferiori ACC=96,94%, FPR=4,16% e FNR=1,96% e EER=3,38%. Il sistema è stato quindi testato con dei campioni appartenenti ad utenti diversi rispetto a quelli per cui il modello è stato allenato (utenti

illegittimi) e con campioni appartenenti ad utenti per cui il sistema è stato allenato ma che non fossero già stati utilizzati per il training. I campioni sono stati presi in un intervallo temporale di 15 minuti, suddivisi in intervalli di tre secondi, e idealmente dovrebbero risultare tutti accettati (in caso di utente legittimo) o respinti (in caso di utente illegittimo). Il sistema ha riportato un ACC=97,43%, EER=2,39%, FPR=1,2% e un FNR=3,94%.

Handwriting Watcher [22] è un meccanismo atto a verificare l'identità dell'autore di uno scritto. Per la valutazione del sistema sono stati svolti tre esperimenti svolti in due sessioni in giorni diversi: il primo richiede che tutti i partecipanti trascrivano lo stesso testo; nel secondo ad ogni partecipante viene assegnata randomicamente una pagina diversa da trascrivere; nel terzo è richiesto che ogni utente risponda a delle domande univocamente assegnate ma alle quali ha già avuto accesso in precedenza e potuto prendere nota di quanto rispondere. Il primo esperimento ha coinvolto 20 partecipanti mentre il secondo e terzo 21, i quali erano studenti di cui per l'80% maschi. Ai fini della classificazione è stato scelto di utilizzare i dati raccolti dal giroscopio e l'accelerazione lineare, quest'ultima è stata preferita all'accelerazione (che include la gravità) al fine di isolare la dinamica di movimento del polso. I dati sono stati segmentati in finestre di 30 secondi con un overlap del 50% e sono state estratte 182 feature normalizzate tramite lo Scikit-learn StandardScaler, ridotte successivamente alle 60 più significative applicando il RelifF feature ranking. Sono stati testati diversi classificatori dei quali sono stati riportati i due più performanti. Il primo è il SVM con kernel lineare, C=0,03 ed un balanced class weight, dove C e altri hyper-parameters sono stati ottimizzati tramite Grid-search. Il secondo classificatore è il Multilayer Perceptron (MLP) con 60 neuroni nel primo layer e 30 nel secondo mentre per il numero di utenti illegittimi contenuti nel dataset è stato scelto un rapporto di 10 a 1 rispetto a quelli legittimi, dove questi parametri sono stati scelti dopo una fase iniziale di testing per valutare quali fossero ottimali. Il classificatore MLP è risultato più performante nel primo esperimento dove ha ottenuto un EER medio di 8,40% mentre il modello SVM nel secondo e terzo esperimento ha ottenuto un EER medio rispettivamente di 11,30% e 16,54%, risultati che però sembrano essere stati influenzati da un numero esiguo di utenti con EER elevato. Il 70% degli utenti coinvolti ha infatti un EER inferiore al 10% ed un EER medio del 5%, il restante 30% contribuisce invece ad un incremento dell'EER medio del 2-4% nei primi due esperimenti e del 5% nel terzo. La lunghezza dei campioni di dati segmentati è un fattore che in fase di testing ha mostrato impattare le performance del sistema. Aumentando la finestra temporale da 30 a 70 secondi ha comportato una riduzione dell'EER medio da 9% a 7% per il primo esperimento e una riduzione dell'EER medio nel terzo esperimento a poco più del 13%.

BT-Authen [23] è un meccanismo di autenticazione che fa uso della temperatura corporea e della risposta galvanica della pelle (GSR) per mantenere l'utente autenticato. La GSR è la misura delle variazioni continue nelle caratteristiche della pelle a seguito della sudorazione del corpo umano. Il dataset è stato popolato facendo uso di un Microsoft Band 2 indossato da 30 partecipanti per almeno quattro ore al giorno durante le quali è stato chiesto agli utenti di mantenersi attivi per almeno una. Sono quindi stati svolti tre esperimenti di cui il primo esperimento ha coinvolto quattro ore di raccolta dati di cui il 60% è stata usata per il training e il 40% per il testing, nel secondo sono stati usati i dati raccolti nel primo giorno per il training e quelli del secondo per il testing mentre il terzo esperimento fa uso dei dati raccolti nei primi due giorni per il training e quelli del terzo per il testing. Per l'estrazione delle feature è stata usata la tecnica delle Wavelet Transform, nello specifico è stato scelto di usare i Wavelet coefficient e la Wavelet packet extraction, l'output è stato quindi normalizzato e dato in input a un classificatore Feedforward Neural Network (FNN). Gli autori riportano un EER del 1,46% nel primo esperimento e del 2,18% e 3,4% rispettivamente per il secondo e terzo esperimento. Presi singolarmente i partecipanti al primo e secondo esperimento hanno riportato per lo più un EER inferiore al 5% mentre nel terzo giorno alcuni dei partecipanti hanno riportato un EER superiore al 10%. Nel primo esperimento il 50% dei partecipanti ha riportato un EER inferiore all'1% mentre per il secondo e terzo rispettivamente il 46,6% e il 43,3%, Alcuni utenti hanno inoltre riportato una performance invertita rispetto alla maggioranza, ovvero hanno ottenuto il miglior EER nel terzo esperimento e il peggiore nel primo. Non da meno, le performance riportate nel secondo e terzo esperimento sono risultate significativamente peggiorate dalla presenza di pochi soggetti che presentavano un'EER molto elevato incrementando lo stesso dell'1,57% nei risultati del terzo esperimento e costituendo il 17,4% dell'EER totale nel secondo esperimento. Il sistema con l'utilizzo di un algoritmo che seleziona la migliore performance nei tre giorni è stato ulteriormente migliorato riducendo l'EER dal 3,4% allo 0,54%.

In [24] è stato sviluppato un meccanismo di autenticazione continua che fa uso del battito cardiaco ai fini dell'autenticazione. La raccolta dati è avvenuta facendo uso di un Samsung Gear S, Samsung Gear S2 e un Empatica E4, dove nei primi due dispositivi la frequenza di campionamento del battito cardiaco è di 100 Hz e nell'ultimo di 64 Hz. Il preprocessing e la rimozione degli artefatti sono stati fatti tramite MATLAB, dove è stato caricato il CSV contenente i valori campionati e questi sono stati segmentati in finestre di 120 secondi. La rimozione degli artefatti è avvenuta considerando come tali i campioni che superavano di oltre

il 20% la media degli ultimi tre battiti cardiaci e dopo la rimozione di questi sono state applicato l'algoritmo cubic spline interpolation per ripristinare i dati mancanti. Sono stati quindi allenati cinque classificatori: k-Nearest Neighbor (k-NN), Random Forest (RF), Multi-Layer Perceptron (MLP), Logistic Regression (LR) e N NaiveBayes. Per k-NN è stato scelto di usare N=3, RF fa uso di 100 alberi mentre per MLP sono stati usati hidden layer 1 e hidden unit 5. Il dataset è stato raccolto su 28 partecipanti sani di cui 16 uomini e 12 donne di età compresa tra i 25 e i 35 anni ed è stato testato sia suddividendolo in 90% per il training e 10% per il testing sia in 70% per il training e il restante per il testing. Il battito cardiaco dei partecipanti è stato raccolto per un totale di 110 minuti durante i quali sono state poste ai partecipanti le stesse situazioni in modo da emulare la variabilità cardiaca nell'arco di una giornata seppur rimanendo in un ambiente di controllo. Il sistema è stato testato tenendo traccia della quantità di dati percentuale che non sono stati interpolati misurando così la qualità dei dati utilizzata, fattore che insieme al modello di smartwatch e il classificatore utilizzato ha influito sulla misura dell'EER. Utilizzando il 90% del dataset per il training la migliore performance è stata ottenuta sul Samsung Gear S facendo uso di un classificatore LR e ottenendo EER=3,53% e qualità dei dati 87,33% mentre mediando sui tre dispositivi il miglior classificatore è risultato essere RF con EER=10,08% e qualità dei dati 77,30%. Utilizzando invece il 70% dei dati per il training il Samsung Gear S è rimasto il dispositivo più performante in termini di EER, che si attesta sul 3,18% con una qualità dei dati del 87,33%. Mediando sui tre dispositivi RF è risultato di poco il miglior classificatore rispetto k-NN riportando un EER del 15,17% contro il 15,21% con k-NN. Dato l'uso di tecniche per la correzione delle anomalie nei rilevamenti del battito, questo meccanismo di autenticazione è stato ulteriormente testato per verificare l'impatto che queste correzioni hanno sull'efficacia del sistema. Il sistema che ne è derivato ha ottenuto i migliori risultati in termini di EER sul Samsung Gear S, dove EER=3,796% mentre l'Empatica E4 e Samsung Gear S2 hanno riportato rispettivamente un EER=6,77% e del 13,66% quando la qualità dei dati è bassa. Fissando invece una soglia di qualità del 95% Samsung Gear S ha riportato un EER=2,67%, L'Empatica E4 EER=4,4% e Samsung Gear S2 EER=18,557%.

Cola et al. [25] hanno sviluppato un sistema che fa uso dei dati raccolti dall'accelerometro durante la camminata per autenticare l'utente. Il sistema rileva l'atto di camminare raccogliendo i dati grezzi dell'accelerometro e costruendo un "gait segment" ogni otto passi compiuti. Secondo quanto riportato dagli autori questo metodo risulta essere ragionevolmente leggero per il monitoraggio real-time su piccoli dispositivi indossati a livello del polso o in tasca. L'algoritmo di detection della camminata è stato dotato di un filtro basato sull'autocorrelazione per la rilevazione di irregolarità tra due cicli di camminata consecutivi, dove un ciclo di

camminata è costituito da due passi consecutivi. Così facendo gli autori mirano a ridurre la rilevazione di falsi positivi nell'individuazione di un gait segment. Il risultato del preprocessing e della feaures extraction è definito come gait instance e costituisce l'input di un classificatore di tipo k-Nearest Neighbor, con distanza euclidea come misura della prossimità. Il classificatore è utilizzato per assegnare un anomaly score ad ogni gait instance, score che verrà confrontato con una soglia di accettazione per identificare se l'utente è legittimo o meno. La fase sperimentale si è svolta facendo uso di uno Shimmer 3 che montava un microcontroller TI MSP430 e un accelerometro ST Micro LSM303DLHC, accelerometro simile a quelli utilizzati negli smartwatch commerciali e con una frequenza di campionamento di 50 Hz. Negli esperimenti sono stati coinvolti 15 volontari di cui quattro donne e undici uomini di età 28,2 ± 2,5 anni, altezza 174,2 ± 9,6 cm e peso 68,7 ± 14,9 kg, Ogni partecipante indossava due Shimmer 3 di cui uno nella tasca laterale dei pantaloni e uno al polso. Ai partecipanti è stato chiesto di percorrere un corridoio due volte con un'andatura qualsiasi, due con andatura rapida e due tenendo una mano in tasca durante il passo mentre al termine degli esperimenti è stato chiesto agli utenti di effettuare movimenti casuali col polso in modo da testare la fake gait detection. La selezione delle feature è stata fatta facendo uso del metodo Correlation-based Feature Subset Selection e la Greedy Hill Climbing Search, dove per il dispositivo indossato in tasca sono state utilizzate come feature l'acceleration magnitude **m**, la vertical acceleration **v** e l'horizontal acceleration **h** mentre per il dispositivo indossato al polso sono state utilizzate le stesse feature in un primo esperimento e l'accelerazione basata sulle coordinate locali del dispositivo (**x**, **y**, **z**) ed **m** in un secondo esperimento. Per la valutazione delle performance del sistema è stata usata la tecnica leave-one-instance-out cross validation in cui, dopo aver selezionato l'utente legittimo, il FNR è stato ricavato testando le istanze corrispondenti su un classificatore allenato sulle rimanenti istanze mentre il FPR è stato ricavato usando queste ultime come input per lo stesso classificatore. Il FNR e il FPR finali sono infine stati ricavati mediando sulle diverse iterazioni della cross-validation. L'algoritmo di detection dei gait segment è risultato ragionevolmente efficace riportando in media una differenza di due gait segment tra il dispositivo indossato al polso e quello in tasca. In quest'ultimo un gait segment veniva rilevato in media ogni 4,9 secondi mentre nel primo ogni 5,5 secondi. Inoltre, sono stati rilevati correttamente dall'algoritmo di anomaly detection tutti i fake gait segment prodotti volontariamente dai partecipanti. Facendo uso delle coordinate locali al dispositivo l'EER è risultato del 2,9% mentre facendo uso del secondo set di feature l'EER è risultato 2,5% quando il dispositivo era indossato in tasca e del 8,0% quando indossato al polso. I risultati sono risultati più promettenti nei test effettuati facendo uso dell'autocorrelation-based filtering dove l'EER è stato ridotto del 3,7% quando il dispositivo era tenuto in tasca mentre è stato ridotto del 7,8%

quando il dispositivo era indossato al polso ed è stato fatto uso delle coordinate locali al dispositivo come feature.

TapMeIn [26] autentica l'utente sulla base del ritmo con cui picchietta le dita sullo schermo dello smartwatch. L'idea è che l'utente inserisca una password melodica caratterizzata da un certo numero di tocchi. Ogni tocco è caratterizzato dalla pressione del dito sullo schermo, ampiezza del tocco, durata per cui lo schermo viene toccato e durata per cui il dito rimane sollevato. Il fatto che vengano prese in considerazione sia caratteristiche fisiologiche sia comportamentali permette così identificare in maniera diversa due utenti che usino la stessa sequenza di tocchi. Data la mancanza di campioni di utenti non legittimi in fase di enrollment del sistema gli autori hanno scelto di sintetizzare dei campioni negativi costruendo dapprima le distribuzioni di ogni caratteristica che contraddistingue una tap password e successivamente selezionando un valore casuale per ogni caratteristica che ricada nella corrispondente distribuzione e iterando per l'intera durata della tap password scelta dall'utente. Ai fini del riconoscimento dell'utente sono stati utilizzati i classificatori Support Vector Machine (SVM) e Random Forests (RF) dove i parametri per questi classificatori sono stati scelti facendo uso di una Grid Search e selezionando quelli che davano una migliore performance in termini di accuracy. La fase sperimentale è stata svolta su un Samsung Gear Live e richiedeva che l'utente testasse il sistema in due possibili condizioni: seduto e in movimento. Sono quindi stati coinvolti 41 partecipanti di cui 13 donne di età compresa tra i 18 e i 57 anni dei quali 10 ricoprivano il ruolo dell'attaccante. In una fase iniziale ai partecipanti è stato permesso di familiarizzare con TapMeIn finchè non riuscissero a loggarsi cinque volte per ogni scenario (seduti e in movimento). Successivamente si è svolta la fase di enrollment in cui è stato chiesto agli utenti di inserire per tre volte la stessa tap password testata in precedenza e di autenticarsi per dieci volte mentre erano seduti e altre dieci mentre camminavano. Per emulare lo shoulder surfing attack l'inserimento della password è stato registrato con una videocamera posta al di sopra della spalla e in modo che lo schermo non fosse nascosto dalla mano durante la digitazione. Gli attaccanti similmente agli altri partecipanti sono stati introdotti a TapMeIn e hanno avuto occasione di testarlo in prima persona, dopodiché sono stati posti di fronte a uno smartwatch e un monitor con 21 pollici in cui è stato riprodotto il video con audio attivo ed una risoluzione di 1080p. Sono quindi stati sperimentati tre tipologie di attacco di cui la prima consisteva nella visione del filmato e tre possibili tentativi di sblocco dello smartwatch. Nella seconda è stata data la possibilità di visionare una seconda volta il video e tre ulteriori tentativi per lo sblocco. Nella terza l'attaccante aveva la possibilità di riprodurre il video quante volte voleva e aveva un totale di nove tentativi per sbloccare lo smartwatch. Nella costituzione del

dataset 31 utenti hanno fornito 13 sample (tre in fase di enrollment e 10 login) mentre l'utente è seduto e similmente è stato fatto per i 10 ulteriori sample prodotti mentre l'utente cammina, per un totale di 713 sample. In modo analogo i dieci attaccanti hanno fornito ciascuno tre sample per ogni tipologia di attacco su ogni utente legittimo per un totale di 2790 sample. Per ogni utente si è scelto quindi di prendere casualmente gli n sample necessari nella fase di enrollment ed aggiungerli al training set insieme a 5n sample negativi generati dalle distribuzioni dei vari parametri usati. I campioni rimanenti degli utenti legittimi e quelli corrispondenti agli attacchi verso gli stessi sono stati usati per il testing dei classificatori. Onde evitare randomicità nella produzione dei sample negativi questa procedura è stata reiterata per 30 volte e i risultati sono stati mediati su tutte e 30 le iterazioni. Per ottenere le performance finali del sistema è stata fatta la media dei risultati ottenuti su tutti gli utenti. Il tuning dei classificatori è stato quindi effettuato tramite Grid Search e facendo uso dei parametri con le migliori performance. Per verificare l'impatto che il numero di sample fornito in fase di enrollment aveva sulle performance del sistema è stato fatto un tuning del parametro riscontrando in tutti i casi che i migliori risultati si ottenevano facendo uso del classificatore SVM e per n>=5. Dal momento che il numero di sample da fornire in fase di autenticazione aveva impatto sulla durata della fase di enrollment iniziale è stato quindi scelto n=5. Per selezionare le feature utilizzate dai classificatori è stato fatto un feature ranking allenando un classificatore Random Forest per ogni utente in modo che restituisse un punteggio inerente all'importanza della feature. Questa procedura è stata poi iterata 30 volte per ogni utente con n=5 sample casuali e al termine sono state estratte le 20 feature più rilevanti basandosi sulla frequenza e l'importance score ottenuto. I primi risultati riportano un FNR del 5,3% e del 9,1% rispettivamente quando l'utente è seduto e mentre cammina. Il random guessing attack ha riportato un EER del 1,3% mentre il video recording attack ha riporta un EER del 2,3% con una sola visione, del 3,5% con due visioni e del 4,1% quando il video poteva essere riprodotto una quantità di volte a discrezione dell'attaccante.

DeepAuth [27] sfrutta i dati raccolti da accelerometro e giroscopio durante l'inserimento del Pattern Lock per garantire un'autenticazione più robusta. Il sistema è composto da tre moduli, tra cui il participatory motion sensing module che raccoglie i dati estratti dall'accelerometro e dal giroscopio durante l'inserimento della password per trasferirli nel cloud e costituire il dataset che insieme all'ID associato all'utente va ad alimentare il deep representation learning module, utilizzato per estrarre le feature che meglio contraddistinguono l'utente in fase di inserimento. Il learned feature extractor è infine usato dall'in-situ authentication module risiedente nello smartwatch per autenticare l'utente durante la digitazione della password. Per

assicurarsi che i dati vengano raccolti dal solo legittimo proprietario questo meccanismo inizializza la raccolta dati solo quando lo smartwatch è accoppiato con lo smartphone. Un classificatore Support Vector Machine (SVM) è utilizzato per il riconoscimento delle variazioni rilevate dall'accelerometro durante l'inserimento della password, dopodiché vengono campionati sia i rilevamenti dell'accelerometro sia quelli del giroscopio. I dati prelevati insieme all'user ID sono quindi caricati sul cloud. Il sistema si propone di essere agnostico dalla password e per questo non necessità di conoscere la password digitata ma i soli campioni generati dai sensori e l'ID utente, questi dati andranno poi ad alimentare una deep Recurrent Neural Network (RNN) risiedente nel cloud capace di produrre una funzione f in grado di autenticare solo l'utente legittimo a prescindere dalla password utilizzata e al contempo in grado di saper distinguere due utenti che utilizzano la stessa password. Per fare ciò nei training data vanno a confluire tutti i dati raccolti per l'utente a prescindere dalla password utilizzata così da poter prelevare i pattern più comuni che contraddistinguono l'inserimento della password da parte dell'utente. Nel concreto dato un certo numero di sample e di utenti a cui appartengono è stato fatto uso di una combinazione di una softmax loss e di una centre loss per il training della RNN. L'hyper-parameter λ utilizzato come trade-off tra softmax e centre loss è stato ottenuto tramite cross validation. La funzione learned feature extractor f è caricata sullo smartwatch dove DeepAuth costruisce un behavourial model localmente codificando le caratteristiche uniche riscontrate nei movimenti del dispositivo durante l'inserimento della password. Le caratteristiche estratte sono quindi elaborate tramite un Multivariate Normal Model (MVN) e sono confrontate con il behavioural model in modo da calcolarne la distanza e in caso superino una soglia di accettazione l'utente viene accettato. Per adattarsi alle risorse limitate degli smartwatch, nei quali una modello di RNN potrebbe essere esoso in termini di memoria e computazionali è stato assunto dagli autori che l'inizio e la fine dell'input digitato nella password non siano correlati, così da spezzare in due sub-RNN il task di elaborazione dell'input suddividendolo a metà e potendo così occupare meno memoria e poter parallelizzare l'elaborazione. Per raccogliere il dataset sono stati dapprima intervistati 112 volontari anonimi e sono stati selezionati i 64 Android Pattern Lock (APL) più frequenti. Successivamente sono stati coinvolti 155 partecipanti di cui il 38% donne, con età compresa tra 20 e 35 anni e ad ognuno di essi sono stati assegnati casualmente 6 APL e di inserirli indossando lo smartwatch al polso sinistro per diverse volte distribuite su diversi giorni. Sono stati così raccolti 27145 sample ognuno dei quali contiene i segmenti di movimento e l'identificativo utente. Il dataset è stato quindi separato in due modi, usando l'80% di esso per il training e il restante per il testing e viceversa, dove il rapporto tra utenti legittimi e impostori è dello 0,4. Tutti gli hyper-parameter compresa la soglia del modello MVN sono stati determinati tramite 5-fold cross

validation. Il sistema è stato infine testato su tre modelli di smartwatch, tra cui il Sony SW3, il Samsung Gear Live e il Moto 360 Sports. ottenendo un'accuratezza del 97% e una precisione del 90% nel caso migliore.

Rischio di parzialità e strategia di ricerca e selezione dei risultati

In quanto riportato nella review si è fatto principalmente uso del motore di ricerca Google/Google Scholar e utilizzando i termini di ricerca e loro combinazione: Smartwatch, Authentication, Continuous, Sensor, Password, Passwordless, Wearable. Gli studi esclusi dalla review sono quelli non reperiti facendo uso dei suddetti metodi, risultati non disponibili tramite i suddetti metodi senza registrazione a specifici siti web o senza previa richiesta di accesso. Dove non esplicitamente specificato si è assunto che le misurazioni prive del simbolo percentuale fossero intese su una scala compresa tra 0 e 1. Non vi è inoltre certezza sui metodi e risultati ottenuti nei singoli studi in quanto non sono stati riprodotti.

Discussione

TapMeIn [26] unisce la conoscenza di un fattore noto all'utente (la tap password) alle caratteristiche fisiologiche e comportamentali dell'utente durante la digitazione. L'uso di caratteristiche derivate dalla dimensione e conformazione del dito e dalla pressione e velocità con cui l'utente digita la tap password rendono questo meccanismo più robusto e più resistente allo shoulder surfing rispetto alla classica password. Gli autori riportano che un random guessing attack risulta efficace nel 1,3% dei casi mentre il video recording attack, quando l'attaccante può visionare l'inserimento indefinitamente, ha successo nel 4,1% dei casi. Il sistema sebbene aggiunga dei fattori aggiuntivi che rendono più difficoltoso per l'avversario impersonare l'utente, per contro non elimina la necessità dell'utente di ricordare il segreto autenticativo. Questo potrebbe portare l'utente comune a ricadere negli stessi schemi tipici dell'uso della password ovvero l'uso di pattern melodici comuni o di breve lunghezza al fine di garantire un più facile accesso al dispositivo.

DeepAuth [27] permette di autenticare l'utente tramite i soli dati raccolti da accelerometro e giroscopio durante l'inserimento del Pattern Lock. Il sistema, nonostante la necessità di inserimento del Pattern Lock, è in grado di riconoscere l'utente a prescindere da quale sia quest'ultimo ed è stato testato facendo uso dei 64 Pattern Lock più comuni raccolti durante un sondaggio iniziale. Ai partecipanti è stato successivamente chiesto di inserire i sei Pattern Lock

assegnati a ciascuno diverse volte nell'arco di diversi giorni. Il sistema proposto garantisce un'ACC=97% e una PR=90%, risultati presumibilmente dovuti al fatto che raccogliendo in unica fase i campioni per il training e testing il Pattern Lock utilizzato per il riconoscimento coincideva con uno di quelli con cui il modello è stato allenato.

Quanto proposto in [25] è un sistema leggero che permette il monitoraggio real time della camminata e capace di individuare i falsi rilevamenti dell'accelerometro dovuti a movimenti accidentali del polso. Questo meccanismo facendo uso dell'accelerazione basata sulle coordinate locali al dispositivo ha riportato un EER del 2,9%, risultato in linea con i meccanismi più performanti riscontrati in letteratura. Questa autenticazione risulta efficace durante i periodi di attività dell'utente ma nei periodi sedentari richiede l'uso di altri tipi di autenticazione o che dal termine dell'attività l'utente venga mantenuto autenticato per un certo periodo di tempo. Il sistema potrebbe risultare meno efficace al variare dell'abbigliamento, della pavimentazione o delle condizioni fisiche rendendo più difficoltosa l'autenticazione per l'utente legittimo. Inoltre, la caratteristica biometrica utilizzata è visibile da un osservatore esterno che potrebbe tentare di impersonare l'utente legittimo anche se dai risultati riportati la probabilità di successo è esigua.

Il fotopletismografo, sensore utilizzato per la rilevazione continua del battito cardiaco, presenta degli artefatti costituiti da falsi rilevamenti del battito cardiaco o da mancati rilevamenti dello stesso. In [24] gli autori hanno cercato di ridurre il rumore filtrando i battiti che si discostavano di oltre il 20% dalla media degli ultimi tre battiti cardiaci e interpolando i dati grezzi mancanti. Su due smartwatch su tre è stato riscontrato un deterioramento della performance all'aumentare del rumore nei rilevamenti riportando un EER del 3,796% quando era presente più rumore e un EER del 2,67% quando oltre il 95% dei dati grezzi non hanno richiesto correzioni. I dati sono stati raccolti per 110 minuti durante i quali i partecipanti sono stati sottoposti a diverse condizioni di stress e di sforzo cosa che dato l'EER contenuto ha mostrato buoni risultati sia quando l'utente è in stato sedentario sia quando svolge attività fisica o è sottoposto a situazioni di stress. Questo sistema risulta trasparente all'utente al quale non è richiesta alcuna interazione per autenticarsi e permette la re-autenticazione continua finchè il dispositivo è indossato. Risulta inoltre efficace contro gli attacchi atti all'imitazione del comportamento, costringendo un potenziale attaccante a ricorrere al guessing attack.

Handwriting Watcher [22] non è un meccanismo pensato tanto per l'autenticazione quanto più per identificare l'autore di uno scritto. Tuttavia, un simile meccanismo potrebbe essere adattabile ai fini dell'autenticazione, permettendo di riconoscere l'utente dai soli dati raccolti dall'accelerometro e dal giroscopio quando scrive quindi senza la necessità di memorizzare una password. Il sistema permette di riconoscere l'utente in maniera meno efficace rispetto agli altri

sistemi rilevati in letteratura, ottenendo un EER dell'8,4% quando tutti i partecipanti trascrivono lo stesso testo, dell'11,3% quando i partecipanti trascrivono pagine diverse e del 16,54% quando viene risposto a domande diverse ma conosciute a priori dagli utenti. Sebbene il sistema permetta di riconoscere l'utente tramite il solo uso dell'accelerometro e del giroscopio durante la scrittura, il random guessing attack risulterebbe più facile da portare a termine non escludendo la possibilità di tentare di imitare l'utente dopo averlo osservato. Per contro l'uso di un segreto conosciuto dall'utente permette di ridurre l'efficacia di un mimicking attack e del random guessing attack aggiungendo un secondo fattore conosciuto all'utente.

Il sistema proposto in [20] permette ad utenti che soffrono di patologie cardiache di autenticarsi facendo uso dell'ECG e della pressione arteriosa del sangue (ABP) come parametri identificativi. Gli autori hanno fatto uso dei dataset MIT PhysioBank Fantasia e MGH preventivamente disponibili per allenare e testare i modelli utilizzati, ottenendo un ACC=96,94%, un FPR=4,16%, un FNR=1,96% e un EER=3,38%. I buoni risultati ottenuti sono presumibilmente dovuti al fatto che i dati contenuti in questi due dataset non sono stati raccolti utilizzando smartwatch commerciali che tuttavia sono in grado di raccogliere questi dati sebbene non in maniera continuativa. Grazie all'uso congiunto di ECG e ABP il sistema è risultato efficace sia in pazienti sani sia in pazienti affetti da patologie cardiache cosa che, sebbene non garantisca l'efficacia al variare dell'attività fisica risulta promettente. Questo meccanismo, oltre a richiedere solo tre secondi di rilevamenti per autenticarsi garantisce i risultati sopracitati con una fase di enrollment di cinque minuti. Il sistema risulta inoltre essere efficace contro gli attacchi orientati all'imitazione del comportamento costringendo un attaccante ad affidarsi al random attack, cosa resa ulteriormente difficile dal fatto che i parametri biometrici utilizzati sono difficilmente controllabili dall'attaccante.

L'uso della temperatura corporea e della risposta galvanica della pelle (GSR) ai fini dell'autenticazione continua riportato in [23] ha riportato margini di errore in linea con i sistemi più performanti riscontrati in letteratura. L'EER ottenuto è dell'1,46% quando il modello è stato allenato e testato sui dati raccolti durante la stessa giornata, del 2,18% quando i dati raccolti nel primo giorno sono stati usati per il training e quelli del secondo per il testing e del 3,4% quando i dati per il training sono stati raccolti nei primi due giorni e quelli del terzo per il testing. Ai partecipanti è stato chiesto di indossare il dispositivo per almeno quattro ore al giorno di cui almeno una in cui si mantenevano attivi, in modo da garantire l'efficacia del sistema anche al variare delle condizioni ambientali e psicofisiche. Il sistema costringe inoltre un avversario ad utilizzare il guessing attack in quando le caratteristiche biometriche utilizzate non sono visibili né facilmente alterabili.

Nel sistema in [13] il solo uso del fotopletismografo è risultato poco performante rispetto quanto ottenuto in [24], infatti nonostante il sensore permetta di ottenere relativamente pochi falsi negativi (8%) per contro i falsi positivi risultano molto elevati (70%), cosa che in sistema di autenticazione biometrica non è accettabile in quanto non vogliamo che un impostore riesca ad accedere facilmente. Con l'uso di due sensori le performance risultano migliorate, riportando un FPR del 26% e un FNR del 5% quando si utilizzano i pattern cardiaci insieme a quelli di camminata ed un FPR del 17% e FNR dello 0% quando invece i pattern cardiaci sono utilizzati insieme al respiro. I risultati migliori sono stati ottenuti utilizzando i tre sensori in simultanea (FPR del 14% e FNR dello 0%) che risultano notevolmente più elevati rispetto a quelli degli altri sistemi in analisi. Questo sistema risulta robusto quanto la più debole delle autenticazioni implementate. Dato l'elevato numero di falsi positivi nell'autenticazione primaria il rischio è che ad un avversario non sia richiesto di introdurre ulteriori fattori biometrici. Questo sistema anche supposto che l'avversario non raggiunga la soglia di confidenza necessaria per poter accedere utilizzando meno di tre sensori avrebbe successo in media ogni sei tentativi di accesso tramite il random guessing attack.. I buoni risultati ottenuti in termini di FNR potrebbero essere inoltre più limitati a causa dell'abbigliamento, dal rumore di fondo o dalle condizioni di salute. Infine, i risultati lievemente migliori nell'utilizzo dei pattern respiratori sono presumibilmente dovuti al fatto che il modello è stato allenato con diverse tonalità e velocità di respirazione, cosa non scontata durante una fase di enrollment in quanto difficilmente l'utente può fornire una variabilità simile di campioni respiratori.

I risultati ottenuti in [17] risultano essere promettenti per mantenere l'utente autenticato sia nei periodi sedentari sia in quelli di attività fisica. L'uso del battito cardiaco, delle calorie bruciate, del conta passi e del MET ha infatti riportato un FPR di solo 2% e un'ACC del 92% quando l'utente è in stato sedentario mentre un FPR dell'1% e un'ACC del 88% quando l'utente è fisicamente attivo. Anche in questo caso l'uso di caratteristiche biometriche non imitabili (ad eccezione del conta passi) rende il meccanismo robusto contro gli attacchi che non richiedono una formazione tecnologica per essere portati a termine, costringendo un impostore qualsiasi a ricorrere al random attack. Il sistema è stato allenato e testato su un dataset che garantisce un'adeguata variabilità di stati fisici ma richiederebbe presumibilmente una duratura fase di enrollment, sebbene trasparente all'utente. L'utilizzo dI fattori hybrid quali calorie bruciate e MET, essendo derivati dai rilevamenti degli altri sensori utilizzati, non aggiunge parametri biometrici indipendenti che rendano meno difficoltoso portare a termine un attacco basato sul solo battito cardiaco e conteggio dei passi.

Conclusione

In letteratura sono state proposte varie soluzioni per ovviare alla vulnerabilità della password allo shoulder surfing e la necessità di memorizzarne una che sia al contempo difficile da indovinare e memorabile. Gli approcci utilizzati si dividono in due categorie: One Time Authentication, quando l'utente si autentica interagendo con il dispositivo e rimane autenticato per un certo lasso di tempo come in [26] e [27], e la continuous authentication ovvero quando l'utente viene ripetutamente autenticato fintanto che è disponibile il segnale che funge da fattore autenticativo come in [17], [23], [24] e [25]. Entrambe queste tipologie, oltre a dover garantire un basso FPR ai fini dell'inacessibilità del sistema ad un attaccante, devono anche garantire un basso FNR e tempo necessario all'autenticazione, in quanto diversamente risulterebbe più difficile accedere per l'utente legittimo. Nell'autenticazione continua questi vincoli diventano più stringenti in quanto il tempo richiesto per l'autenticazione deve essere necessariamente inferiore alla frequenza con cui avviene l'autenticazione. Rispetto alla One Time Authentication uno dei vantaggi dell'autenticazione continua risiede proprio nella continua verifica dell'identità di chi indossa il dispositivo, permettendo di prevenire l'accesso allo stesso in caso di furto. L'usabilità dell'autenticazione continua può essere più o meno limitata dal fattore biometrico utilizzato, ad esempio in [25] si permette all'utente di rimanere autenticato mentre cammina, facendo uso di altre tipologie di autenticazione quando l'utente è in stato sedentario. Per contro soluzioni che fanno uso del battito cardiaco [13], [17], [24], temperatura corporea e GSR [23] o calorie bruciate e MET [17] permettono di mantenere l'utente autenticato sia quando è in stato sedentario sia quando svolge attività fisica. Questi stessi attributi biometrici presentano l'ulteriore vantaggio di risultare trasparenti non solo all'utente ma anche ad un osservatore esterno. In questo modo viene impedito da un lato il portare a termine un mimicking attack, possibile in sistemi come Handwriting Wacher [22] e quelli che autenticano l'utente mentre cammina come in [25], e dall'altro costringendo un attaccante senza una formazione tecnologica ad affidarsi al guessing attack, cosa resa ulteriormente ostica data la difficoltà nel controllare i suddetti attributi biometrici. Per contro l'uso delle sole caratteristiche biometriche quali il battito cardiaco [24] e temperatura corporea e GSR [23], sebbene siano sempre disponibili, fa sorgere il problema della variabilità delle stesse nel tempo. Conseguentemente richiedono una fase di enrollment che, per quanto trasparente all'utente, può risultare significativamente lunga per poter risultare efficace al variare dell'intensità dell'attività fisica o potrebbe richiedere l'aggiornamento del template al variare di quest'ultima nel tempo. Similmente a quanto fatto in [13] è possibile ovviare alle limitazioni che l'uso statico degli stessi fattori biometrici impone facendo uso della Adaptive Multifactor Authentication (A-MFA) [6]. Quest'ultima

contestualizza l'autenticazione facendo uso di un diverso insieme di fattori biometrici a seconda delle condizioni di rumore o della loro disponibilità. In questo modo è possibile sviluppare un sistema modulare che faccia uso di un insieme di attributi biometrici ottimizzato in base al contesto e dove idealmente ogni contesto fa uso di diversi insiemi di caratteristiche per la re-autenticazione. Quest'ultima caratteristica rende più robusta l'autenticazione in caso di spoofing dei parametri biometrici visto e considerato che un sistema che implementa l'A-MFA risulta robusto quanto la più debole delle autenticazioni che lo compongono. In fase di autenticazione rispetto all'uso di un singolo attributo biometrico (unimodale) come in [24] e [25] è quindi preferibile utilizzare più fattori (multimodale o sensor fusion) per garantire una maggiore discriminazione tra gli utenti (unicità) e rendere più difficoltoso lo spoofing di più caratteristiche biometriche, come ad esempio in [17], [13], [20], [22] e [23]. Nel combinare diverse caratteristiche biometriche è possibile agire durante l'estrazione delle feature, durante il calcolo del matching score o durante la decisione se autenticare o meno. La prima è quella più utilizzata in letteratura e consiste nel mettere insieme le feature estratte dai diversi sensori e costituire il nuovo set di caratteristiche biometriche. La seconda calcola separatamente il matching score per ognuno degli attributi biometrici e combina i diversi score in uno su cui verrà fatta la decisione se autenticare o meno. Nella terza viene presa una decisione in base al matching score per ognuno dei parametri biometrici e successivamente viene presa una decisione in base ai risultati ottenuti dalla maggioranza. Combinare i matching score delle caratteristiche biometriche risulta essere la soluzione più flessibile in quanto rende possibile applicare pesi differenti ai sensori così da rendere meno influenti quelli più rumorosi [6].

Smartwatch e fitness tracker data la larga diffusione che hanno avuto negli ultimi anni, la praticità di essere sempre indossati e le crescenti capacità computazionali, durata della batteria e dotazione di sensori risultano essere i dispositivi ideali per il monitoraggio continuo della salute, del sonno e dell'attività fisica. Allo stato dell'arte questi dispositivi sono già in grado di riconoscere alcune attività come il sonno, la corsa, la camminata e lo stato sedentario. Da queste premesse risulta naturale credere che per mantenere l'utente autenticato garantendo un alto livello di sicurezza sia necessaria un'autenticazione continua specifica in base all'attività svolta. In questo modo, e facendo uso di un diverso insieme di parametri biometrici per ogni attività, si ha modo di ottimizzare le singole autenticazioni utilizzate in modo da garantire il massimo livello di sicurezza per ogni contesto. L'uso di più sensori per le singole autenticazioni garantisce una maggiore distinguibilità dei pattern rilevati in utenti diversi e rende il meccanismo più resistente allo spoofing delle singole caratteristiche biometriche. Comprendere tra queste ultime un fattore non visibile ad occhio nudo rende inefficaci i tentativi di imitazione del comportamento. In fine calcolare il matching score per ogni caratteristica biometrica e

combinarli dando pesi diversi in base alla rumorosità o accuratezza del sensore in un determinato contesto permette di ovviare alle limitazioni hardware seppur non privandosi di un ulteriore fattore autenticativo. È in questa direzione che ci si prospetta vadano i futuri trend in fatto di autenticazione su smartwatch.

Bibliografia

[1] Page MJ, McKenzie JE, Bossuyt PM, et al. The PRISMA 2020 statement: an updated guideline for reporting systematic reviews.BMJ2021;372:n71. doi:10.1136/bmj.n71 – Last access 12/09/2024

[2] Page MJ, McKenzie JE, Bossuyt PM, et al. Updating guidance for reporting systematic reviews: development of the PRISMA 2020 statement. J Clin Epidemiol2021;S0895-4356(21)00040-8. doi:10.1016/j.jclinepi.2021.02.003. pmid:33577987 – Last access 12/09/2024

[3] BMJ 2021; 372 doi: https://doi.org/10.1136/bmj.n160 – Last access 12/09/2024

[4] http://prisma-statement.org/PRISMAStatement/Checklist – Last access 12/09/2024

[5] https://prisma.shinyapps.io/checklist/ – Last access 12/09/2024

[6] Dasgupta, Dipankar & Roy, Arunava & Nag, Abhijit. (2017). Advances in User Authentication. 10.1007/978-3-319-58808-7. https://www.researchgate.net/profile/Dipankar-Dasgupta/publication/334559194_Advances_in_User_Authentication/links/5d314b3aa6fdcc2462ebb09e/Advances-in-User-Authentication.pdf – Last access 12/09/2024

[7] Chen Wang, Yan Wang, Yingying Chen, Hongbo Liu, Jian Liu, User Authentication on mobile devices: Approaches, threats and trends, Computer Networks, Volume 170, 2020, 107118, ISSN 1389-1286, https://doi.org/10.1016/j.comnet.2020.107118. – Last access 12/09/2024

[8] M. Guerar, L. Verderame, M. Migliardi and A. Merlo, "2GesturePIN: Securing PIN-Based Authentication on Smartwatches," *2019 IEEE 28th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE)*, Napoli, Italy, 2019, pp. 327-333, doi: 10.1109/WETICE.2019.00074. - https://www.meriemguerar.net/papers/pdf/2gesture-pin-2019.pdf – Last access 12/09/2024

[9] Lai, Jianwei & Arko, Ernest. (2021). A Shoulder-Surfing Resistant Scheme Embedded in Traditional Passwords. 10.24251/HICSS.2021.860. https://scholarspace.manoa.hawaii.edu/bitstream/10125/71481/1/0698.pdf – Last access 12/09/2024

[10] Il-Soo Jeon, Myung-Sik Kim Contemporary Engineering Sciences, Vol. 10, 2017, no. 5, 203-210 "An enhanced simple PIN input technique resisting shoulder surfing and smudge attacks" doi: 10.12988/ces.2017.612194 https://pdfs.semanticscholar.org/817b/e8381707f8cd469429aaacddc8b08b00599a.pdf – Last access 12/09/2024

[11] Srinivasan, Rajarajan & Kalita, Rahul & Gayatri, Tara & Priyadarsini, PLK. (2018). SpinPad: A Secured PIN Number Based User authentication Scheme. 53-59. 10.1109/ICRTAC.2018.8679257. https://www.researchgate.net/profile/Rajarajan-Srinivasan/publication/332224690_SpinPad_A_Secured_PIN_Number_Based_User_authentication_Scheme/links/5cbef6bba6fdcc1d49a89d3d/SpinPad-A-Secured-PIN-Number-Based-User-authentication-Scheme.pdf – Last access 12/09/2024

[12] Divyapriya, K & Prabhu, P. (2018). Image Based Authentication Using Illusion Pin for Shoulder Surfing Attack. International Journal of Pure and Applied Mathematics. 119. 10.20894/IJCOA.101.007.001.009. https://www.researchgate.net/publication/324273320_Image_Based_Authentication_Using_Illusion_Pin_for_Shoulder_Surfing_Attack – Last access 12/09/2024

[13] W. Cheung and S. Vhaduri, "Continuous Authentication of Wearable Device Users from Heart Rate, Gait, and Breathing Data," 2020 8th IEEE RAS/EMBS International Conference for Biomedical Robotics and Biomechatronics (BioRob), New York, NY, USA, 2020, pp. 587-592, doi: 10.1109/BioRob49111.2020.9224356. https://arxiv.org/pdf/2008.10779.pdf – Last access 12/09/2024

[14] Investigating sources of inaccuracy in wearable optical heartrate sensors - https://www.nature.com/articles/s41746-020-0226-6 – Last access 12/09/2024

[15] Wisdm: Wireless sensor data mining," Accessed: November 2019. https://bit.ly/37fwI7j – Last access 12/09/2024

[16] "Esc-50: Dataset for environmental sound classification," https://bit.ly/2uT9Ddc – Last access 12/09/2024

[17] Vhaduri, Sudip & Poellabauer, Christian. (2018). Biometric-Based Wearable User Authentication During Sedentary and Non-sedentary Periods. – Last access 12/09/2024

[18] https://www.medicalfacts.it/2019/09/10/met-ecco-come-si-misura-lintensita-dellattivita-fisica/ – Last access 12/09/2024

[19] https://sites.nd.edu/nethealth/ – Last access 12/09/2024

[20] *Cai, H., & Venkatasubramanian, K.K. (2016). Fusion of Electrocardiogram and Arterial Blood Pressure Signals for Authentication in Wearable Medical Systems.* http://web.cs.wpi.edu/~kven/papers/CPS-Sec.pdf – Last access 12/09/2024

[21] A. L. Goldberger, L. A. N. Amaral, L. Glass, J. M. Hausdorff, P. C. Ivanov, R. G. Mark, J. E. Mietus, G. B. Moody, C.-K. Peng, and H. E. Stanley, "Physiobank, physiotoolkit, and physionet: Components of a new research resource for complex physiologic signals," Circulation, vol. 101, no. 23, pp. e215–e220, 2000. – Last access 12/09/2024

[22] Griswold-Steiner, Isaac & Matovu, Richard & Serwadda, Abdul. (2017). Handwriting Watcher: A Mechanism for Smartwatch-Driven Handwriting Authentication. 10.1109/BTAS.2017.8272701. https://www.researchgate.net/profile/Isaac-Griswold-Steiner/publication/319448466_Handwriting_Watcher_A_Mechanism_for_Smartwatch-Driven_Handwriting_Authentication/links/59aab6a4aca272f8a154cab7/Handwriting-Watcher-A-Mechanism-for-Smartwatch-Driven-Handwriting-Authentication.pdf – Last access 12/09/2024

[23] Enamamu, Timibloudi & Clarke, Nathan & Haskell-Dowland, Paul & Li, Fudong. (2017). Smart watch based body-temperature authentication. 1-7. 10.1109/ICCNI.2017.8123790. https://www.researchgate.net/profile/Timibloudi-Enamamu/publication/321406743_Smart_watch_based_body-temperature_authentication/links/5c227318299bf12be399ffa7/Smart-watch-based-body-temperature-authentication.pdf – Last access 12/09/2024

[24] D. Ekiz, Y. S. Can, Y. C. Dardagan and C. Ersoy, "Can a Smartband be Used for Continuous Implicit Authentication in Real Life," in IEEE Access, vol. 8, pp. 59402-59411, 2020, doi: 10.1109/ACCESS.2020.2982852. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9044709 – Last access 12/09/2024

[25] Guglielmo Cola, Marco Avvenuti, Fabio Musso, and Alessio Vecchio. 2016. Gait-based authentication using a wrist-worn device. In Proceedings of the 13th International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services (MOBIQUITOUS 2016). Association for Computing Machinery, New York, NY, USA, 208–217. https://doi.org/10.1145/2994374.2994393 http://vecchio.iet.unipi.it/vecchio/files/2010/02/article-2.pdf – Last access 12/09/2024

[26] Nguyen, Toan & Memon, Nasir. (2018). Tap-based User Authentication for Smartwatches. Computers & Security. 78. 10.1016/j.cose.2018.07.001. https://arxiv.org/pdf/1807.00482.pdf – Last access 12/09/2024

[27] Chris Xiaoxuan Lu, Bowen Du, Peijun Zhao, Hongkai Wen, Yiran Shen, Andrew Markham, and Niki Trigoni. 2018. Deepauth: in-situ authentication for smartwatches via deeply learned behavioural biometrics. In Proceedings of the 2018 ACM International Symposium on Wearable Computers (ISWC '18). Association for Computing Machinery, New York, NY, USA, 204–207. https://doi.org/10.1145/3267242.3267252 https://ora.ox.ac.uk/objects/uuid:439b6b0f-0455-4ae3-b943-5aa0d42e9754/download_file?safe_filename=LuetalAAM2019.pdf&file_format=application%2Fpdf&type_of_work=Conference+item – Last access 12/09/2024