User Authentication

Autenticazione

Principi di autenticazione

- **Qualcosa che conosciamo** - Le password, PIN o risposte a domande predefinite fanno parte di questa categoria

- **Qualcosa di cui siamo in possesso** - Chiavi elettroniche, Smart card, chiavi fisiche, si chiamano token

- **Qualcosa che fa parte di noi** - Static biometrics authentication. Impronta digitale, retina, riconoscimento facciale

- **Qualcosa che facciamo** - Dynamic biometrics authentication. Riconoscimento vocale, riconoscimento della scrittura, ritmo di digitazione.

Autenticazione con password

Autenticazione con password

Password

Uno dei primi meccanismi di difesa sono proprio le password. Tutti i sistemi multiutente (che siano network-based, web-based o altri servizi) richiedono, oltre all'identificativo utente (User ID), una **password**.

Il sistema comparerà la password salvata (hash con salting) in precedenza con quella fornita dall'utente, la password serve a provare l'**identità di un utente**.

Autenticazione con password

User ID

- Determina se l'**utente è autorizzato** ad accedere ad un sistema
- Determina i privilegi accordati all'utente, il **ruolo** per cui è stato profilato (admin, user, viewer)
- Viene usato per assoggettare i privilegi, visualizzare le autorizzazioni in essere

Autenticazione con password

Vulnerabilità delle password

Autenticazione con password

Offline Dictionary Attack

- L’attaccante compara gli hash delle password rubate con gli hash delle password più comunemente utilizzate. Trovato il match l’attaccante può usare la combinazione UserID/ Password per bypassare i controlli

Autenticazione con password

Specific Account Attack

- L’attaccante prende di mira un target specifico e prova ad indovinare la password.
- Un meccanismo standard di difesa contro questo attacco è il lock dell’utente dopo vari tentativi di login sbagliati (tipicamente 3 o 5)

Autenticazione con password

Popular Password Attack

- È una variazione dell’attacco precedente, cambia il target che questa volta è un range di UserID.
- Gli utenti tendono a scegliere password semplici da ricordare
- Si può creare una lista di password da non usare (123456, password)

Autenticazione con password

Password guessing

- L’attaccante cerca di conoscere il target e le password policy del sistema così da poter indovinare la password con più facilità

- Policy di sicurezza più stringenti e ben strutturate sono una buona contromisura

Autenticazione con password

Workstation Hijacking

- L’attaccante aspetta fino a quando la workstation è lasciata incustodita con il login effettuato

Autenticazione con password

Exploiting user mistakes

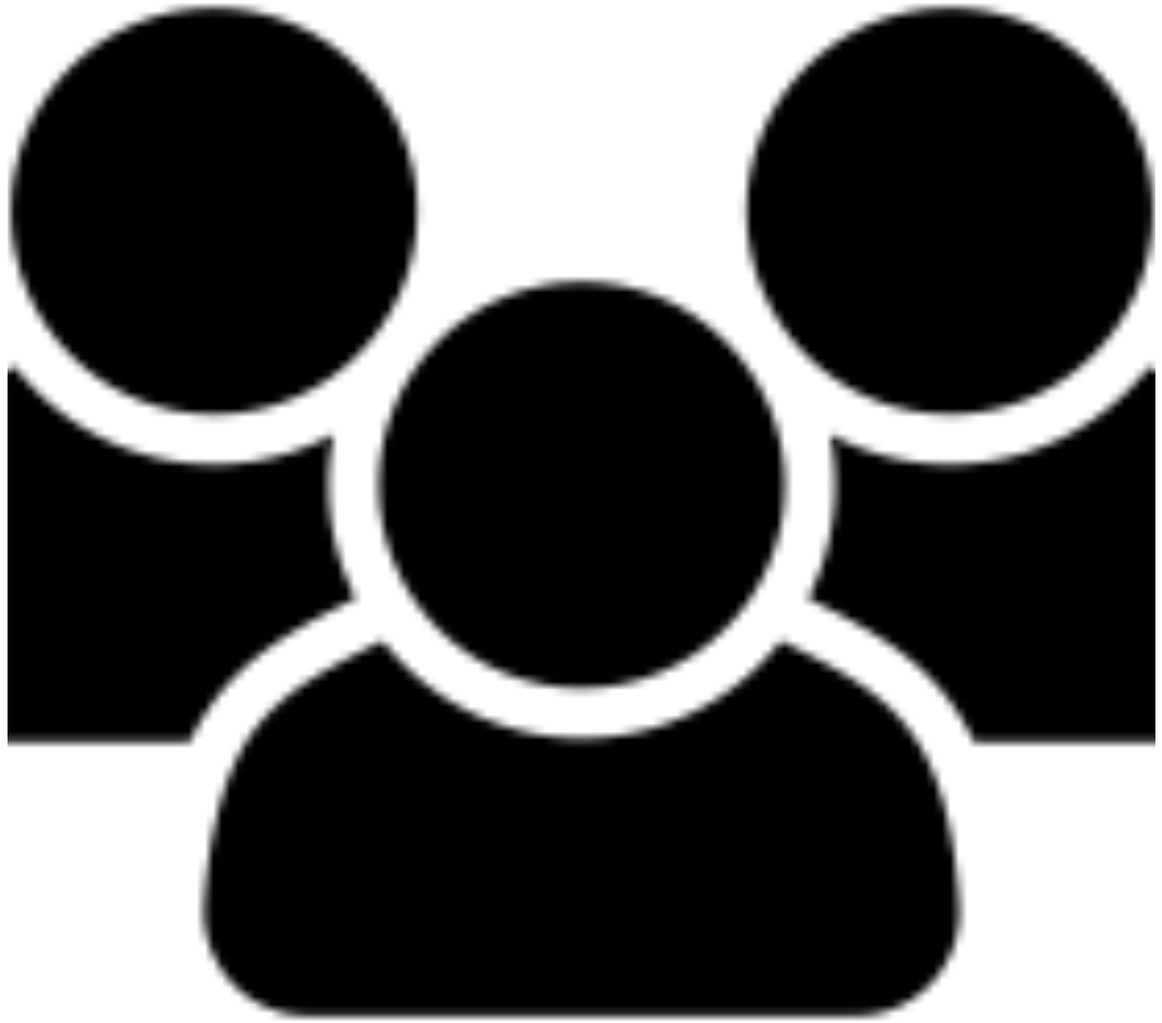
- Se il sistema assegna delle password generate casualmente, molto probabilmente l’utente l’appunterà da qualche parte perché difficile da ricordare

Autenticazione con password

Exploiting multiple password use

- Un attacco alle password è molto più rischioso se la stessa password è condivisa su più Device di rete

- Per contromisura si possono applicare delle policy per impedire l’utilizzo delle stesse password su Device selezionati



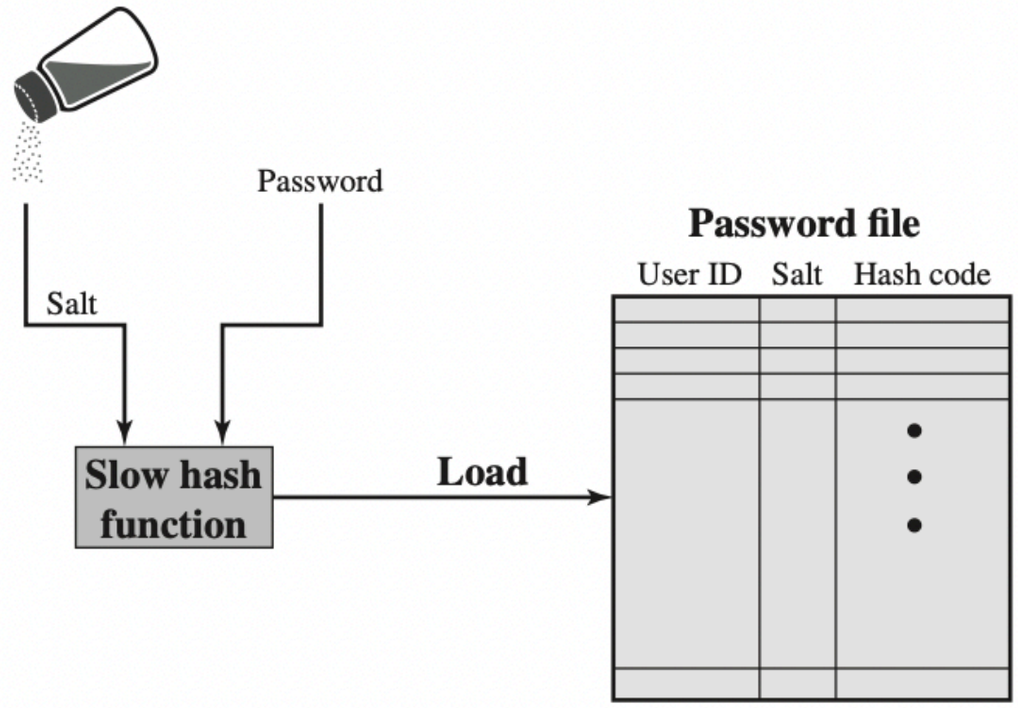
Autenticazione con password

Electronic monitoring

- Eavesdropping (origliare). Quando la password passa attraverso la rete può essere rubata da un attaccante

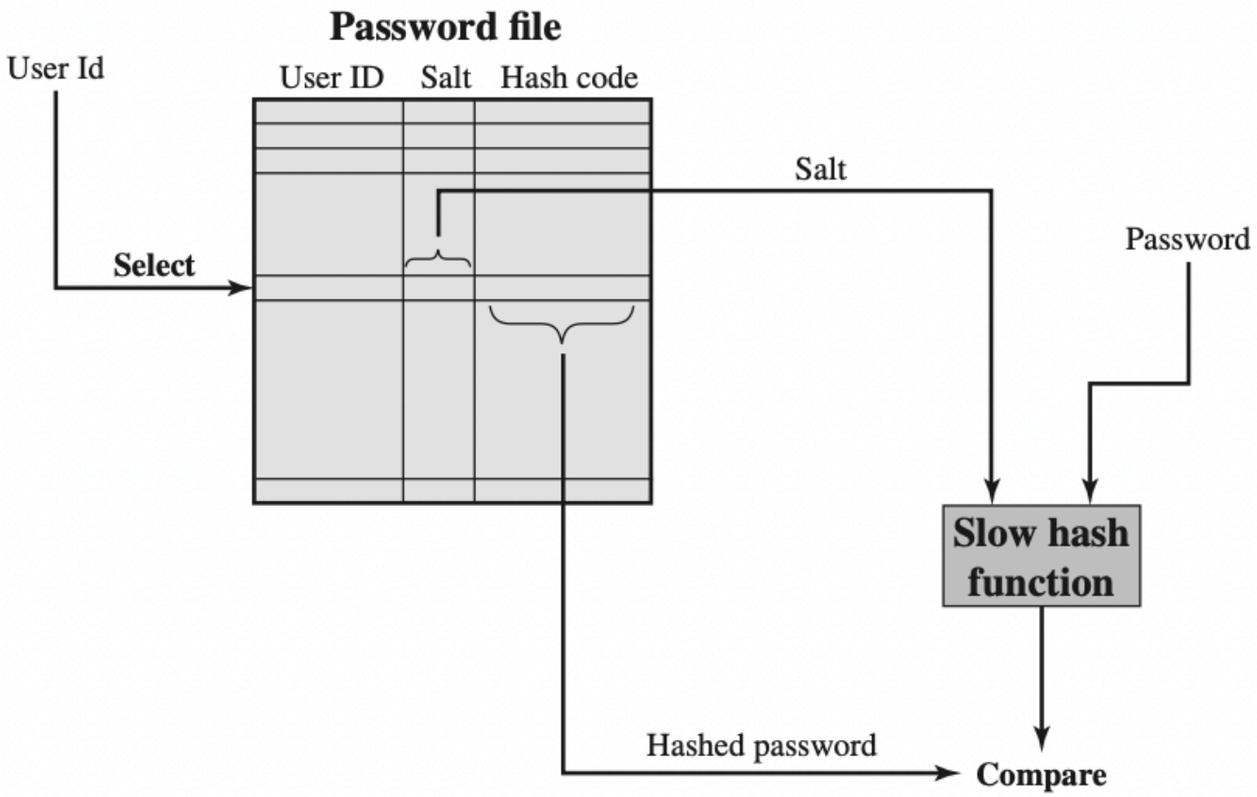
- La cifratura non risolve il problema perché è possibile decriptare il messaggio contenente la password

Autenticazione con password



(a) Loading a new password

Password salting



(b) Verifying a password

Autenticazione con password

Benefici del salting

- Previene che password uguali siano visibili “ad occhio” nel password file (o database)
- Aumenta la difficoltà in caso di Dictionary attack. Per un salt di b bit, il numero di password è aumentato di 2^b
- È molto improbabile che due hash siano uguali, pur usando la stessa password in due o più sistemi

Autenticazione con password

Password File Access Control

- Le hashed password sono contenute in un file accessibile solo da un utente privilegiato
- Le hashed password sono scritte in un file chiamato **shadow file**, per separarle dal file che contiene gli User ID

Autenticazione con password

Strategie di Password Selection

- Security Awareness agli utenti
- Password randomiche generate dal computer
- Check password reattivi - Il sistema esegue un proprio password cracker per identificare le password deboli presenti
- Check password proattivi - Nel momento in cui un utente sceglie una password, il sistema la controlla per verificarne la robustezza

Autenticazione Token-based

Autenticazione Token-based

Memory Card

Questo tipo di token può solo salvare dati, non elaborarli. Un esempio sono le vecchie carte bancarie, con la sola banda magnetica.

- Richiedono un reader particolare (ad es. lettore a banda magnetica)
- La perdita del token toglie all'utente la possibilità di accedere. L'attaccante deve solo indovinare il PIN
- L'utente accetta un tale sistema per prelevare in banca, ma non per accedere ad un computer

Autenticazione Token-based

Smart Card 1/2

- Includono un microprocessore (es. carte di credito moderne)
- Richiedono un'interfaccia utente (tastiera, display)
- Interfaccia elettronica: reader/writer per il token. **Contact** (token ad inserimento/interazione) oppure **contactless** (token wireless)
- Protocollo di autenticazione: **statico** quando l'autenticazione viene fatta sul token stesso, **dynamic password generator** se il token genera una password univoca periodicamente (es. ogni minuto), **challenge-response** se il token genera un stringa di numeri casuali in risposta alla "challenge" proposta dal server

Autenticazione Token-based

Smart Card 2/2

La categoria di smart token più importante è la smart card, simili alle carte di credito, hanno un microprocessore, memoria e porte di input/output.

Una smart card include 3 tipi di memoria: **ROM** (read-only memory) per salvare dati che non cambiano durante la vita della carta, **EEPROM** (electrically erasable programmare ROM) contiene i dati che possono variare, come i protocolli di comunicazione e **RAM** (random access memory) per i dati temporanei.

Autenticazione Token-based

Electronic Identity Card 1/2

Le eID (carte d'identità elettroniche) sono simili alle smart card, riescono a fornire una garanzia più forte sull'identità di una persona (ad es. salvando le impronte digitali).

Contiene le seguenti informazioni (stampate):

- **Dati personali**
- **Numero di documenti**
- **CAN** (Card Access Number): 6 cifre, usate come password
- **MRZ** (Machine Readable Zone): 3 linee di testo, leggibili da macchine e umani, può essere usata come password

Autenticazione Token-based

Electronic Identity Card 2/2

- **ePass**: È una funzione usata dai governi per salvare informazioni sulla persona, è simile alla funzione presente nei passaporti elettronici
- **eID**: Funzione generica per scopi governativi e applicativi, viene salvata l'identità
- **eSign**: Funzione opzionale, salva una chiave privata e un certificato che la verifica. Serve a firmare digitalmente

Autenticazione biometrica

Autenticazione biometrica

Caratteristiche fisiche utilizzate nell'autenticazione biometrica

- Caratteri facciali
- Impronte digitali
- Geometria della mano
- Retina
- Iride
- Firma
- Voce

Autenticazione biometrica

Caratteristiche fisiche utilizzate nell'autenticazione biometrica

- **Caratteri facciali** - Viene "fotografata" la faccia, un algoritmo calcola le distanze (ad es. occhio-occhio, occhi-naso, naso-bocca) e altre caratteristiche. Può essere utilizzata anche una fotocamera ad infrarossi per "vedere" il sistema vascolare della faccia

- **Impronte digitali** - Sono utilizzate specie dalle forze dell'ordine per identificare le persone. Le impronte contengono un insieme unico di righe e pattern, ciò consente di identificare una persona

- **Geometria della mano** - Viene calcolata la dimensione, distanze tra le dita, lunghezze delle dita, larghezza della mano

Autenticazione biometrica

Caratteristiche fisiche utilizzate nell'autenticazione biometrica

- **Retina** - Viene analizzato il pattern creato dalle vene sulla superficie della retina. Per salvare l'immagine della retina viene proiettato un fascio di luce infrarossa a bassa intensità

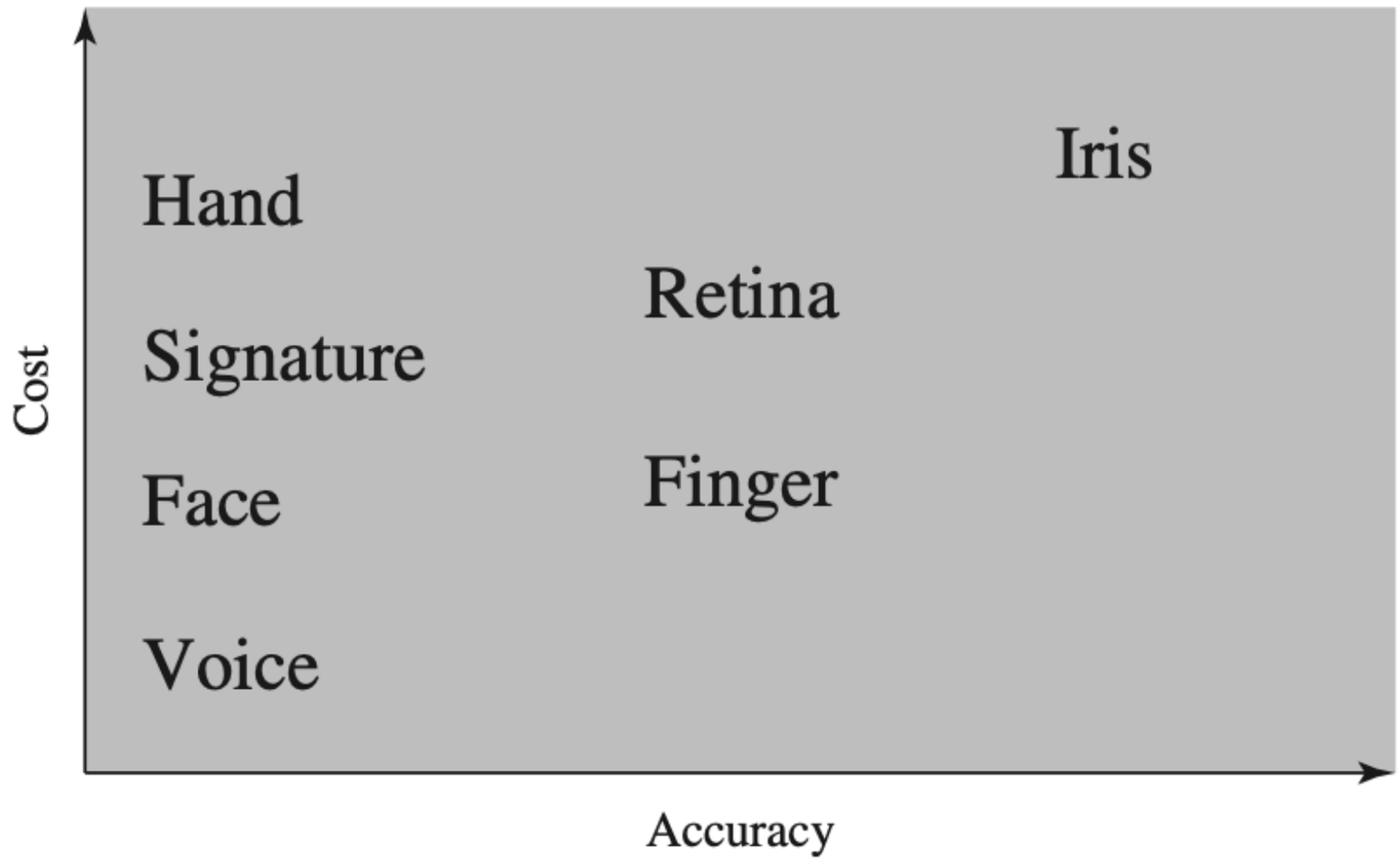
- **Iride** - La struttura dell'iride è considerata univoca, pertanto viene utilizzato da alcuni sistemi di autenticazione

- **Firma** - Ogni persona ha un diverso stile di scrittura, salvando molti sample di firma autografa e inserendoli in un algoritmo, è possibile identificare la stessa persona la prossima volta che firmerà

- **Voce** - La voce è un altro elemento univoco, viene registrata da un microfono per calcolare intensità, velocità di dizione e altre particolarità (ad es. R moscia)

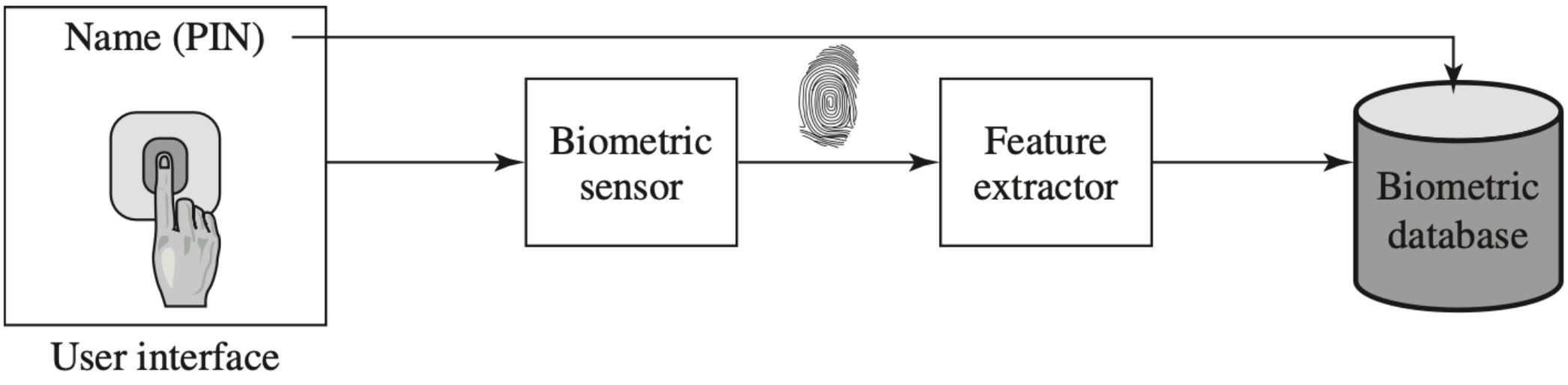
Autenticazione biometrica

Costo e accuratezza dei sistemi di autenticazione biometrica



Autenticazione biometrica

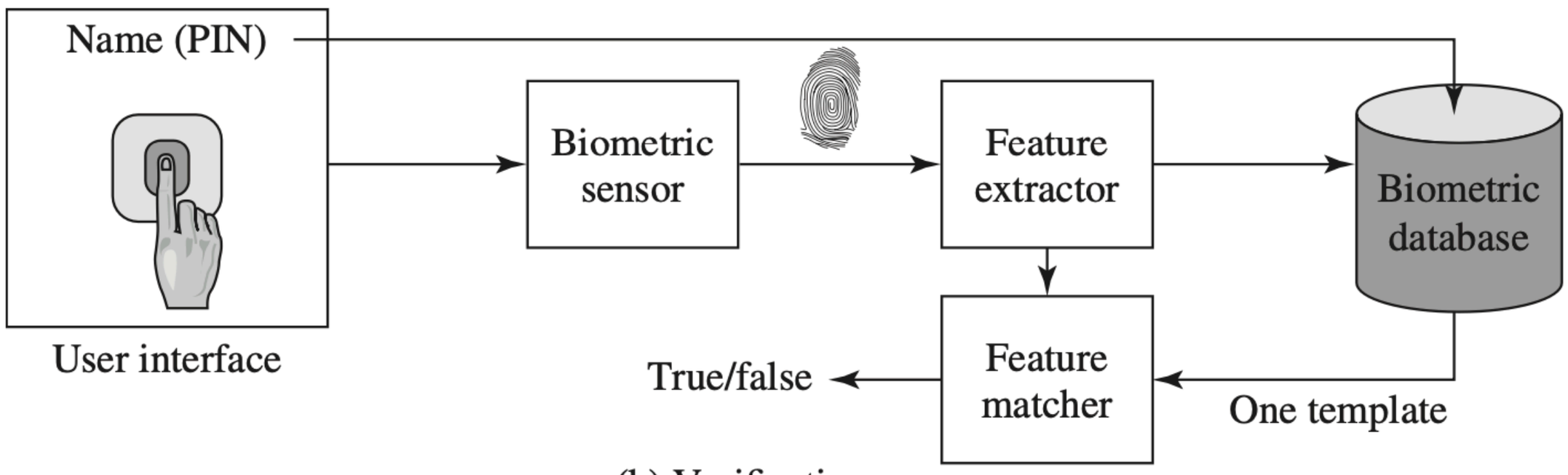
Registrazione ad un sistema di autenticazione biometrica



(a) Enrollment

Autenticazione biometrica

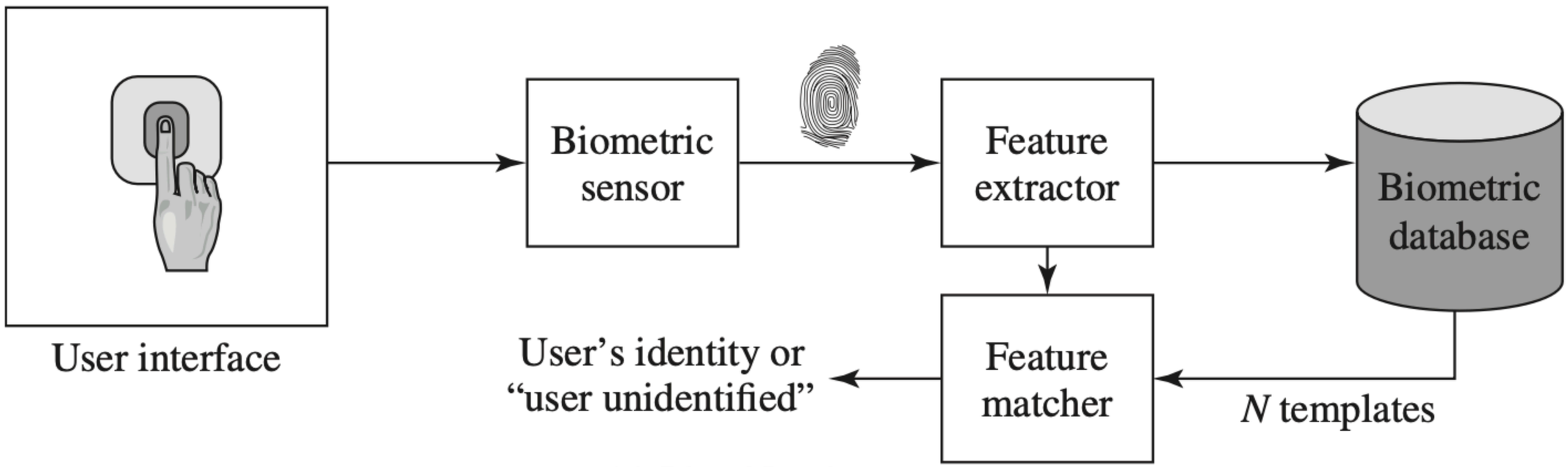
Verifica di identità tramite autenticazione biometrica



(b) Verification

Autenticazione biometrica

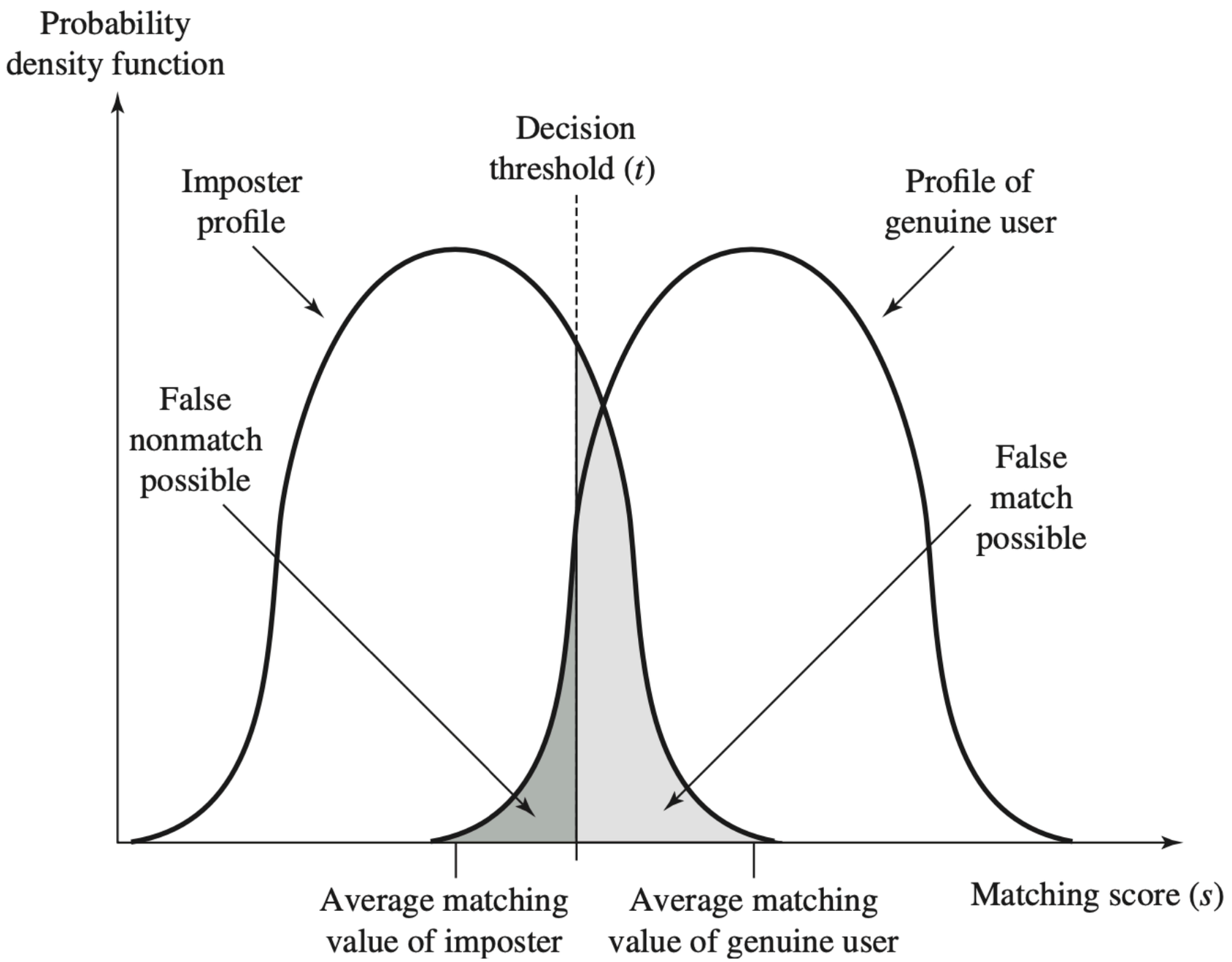
Identificazione con sistema di autenticazione biometrica



(c) Identification

Autenticazione biometrica

Sovrapposizione impostore/utente



Autenticazione remota

Autenticazione remota

Password protocol 1/3

L’autenticazione con password per sistemi remoti avviene tramite protocolli **challenge-response**.

Le implementazioni moderne sono più complesse di quelle spiegate di seguito, tuttavia ne ripercorrono il funzionamento logico.

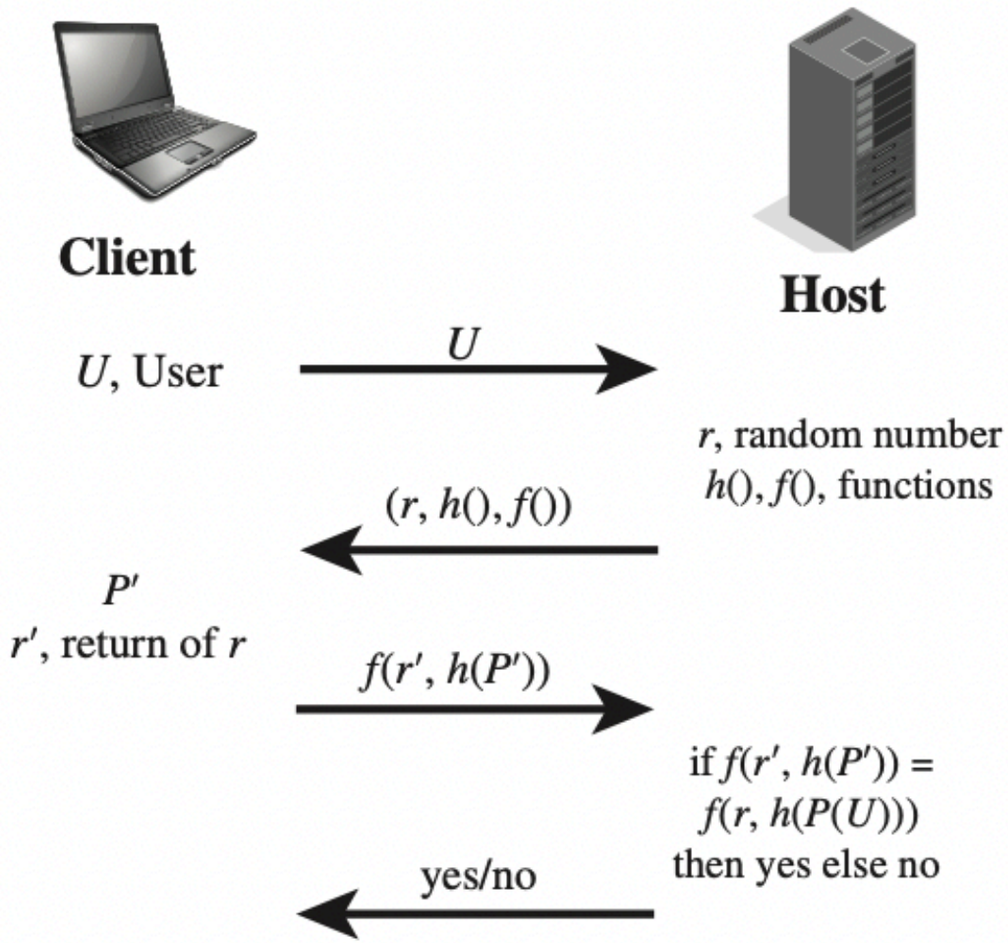
Autenticazione remota

Password protocol 2/3

1. L’utente invia la propria identità all’host
2. L’host genera un numero casuale “r” chiamato **nonce** (Number once) e lo invia all’utente. L’host definisce anche due funzioni “h” e “f” e le comunica all’utente
3. L’utente invia “f(r’, h(P’))” dove “r’ = r” e “P’” è la password dell’utente. La funzione “h” è una funzione di hashing
4. L’host confronta quanto ricevuto dall’utente con il risultato della funzione “f”, eseguita con i dati in proprio possesso. Se il risultato è uguale, l’utente è autenticato. (Vedi figura successiva)

Autenticazione remota

Password protocol 3/3



(a) Protocol for a password

Problemi di sicurezza nell’autenticazione

Problemi di sicurezza nell'autenticazione

Table 3.5 Some Potential Attacks, Susceptible Authenticators, and Typical Defenses

Attacks	Authenticators	Examples	Typical Defenses
Client attack	Password	Guessing, exhaustive search	Large entropy; limited attempts
	Token	Exhaustive search	Large entropy; limited attempts; theft of object requires presence
	Biometric	False match	Large entropy; limited attempts
Host attack	Password	Plaintext theft, dictionary/exhaustive search	Hashing; large entropy; protection of password database
	Token	Passcode theft	Same as password; 1-time passcode
	Biometric	Template theft	Capture device authentication; challenge response
Eavesdropping, theft, and copying	Password	"Shoulder surfing"	User diligence to keep secret; administrator diligence to quickly revoke compromised passwords; multifactor authentication
	Token	Theft, counterfeiting hardware	Multifactor authentication; tamper resistant/evident token
	Biometric	Copying (spoofing) biometric	Copy detection at capture device and capture device authentication
Replay	Password	Replay stolen password response	Challenge-response protocol
	Token	Replay stolen passcode response	Challenge-response protocol; 1-time passcode
	Biometric	Replay stolen biometric template response	Copy detection at capture device and capture device authentication via challenge-response protocol
Trojan horse	Password, token, biometric	Installation of rogue client or capture device	Authentication of client or capture device within trusted security perimeter
Denial of service	Password, token, biometric	Lockout by multiple failed authentications	Multifactor with token