

4. Autenticazione

Sicurezza dell'Informazione

Identificazione e Autenticazione

Identificazione: un'entità dichiara il proprio identificatore.

- **Esempi:** *"Sono Lorenzo", "Sono Michele"*

```
Ubuntu 12.04.3 LTS ubuntu64 tty1
ubuntu64 login: foobar
```

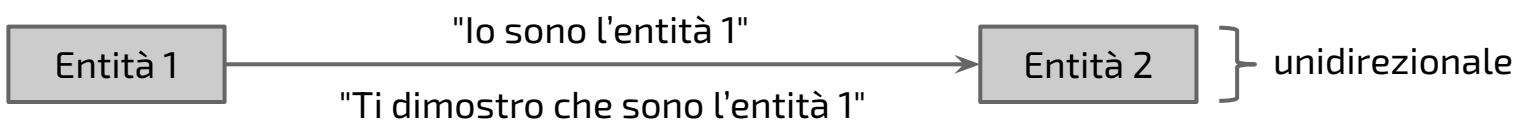
Autenticazione: l'entità fornisce una prova che verifica la sua identità..

- **Esempio:** *"Questa è la carta d'identità di Lorenzo"*

```
Ubuntu 12.04.3 LTS ubuntu64 tty1
ubuntu64 login: foobar
Password: 
```

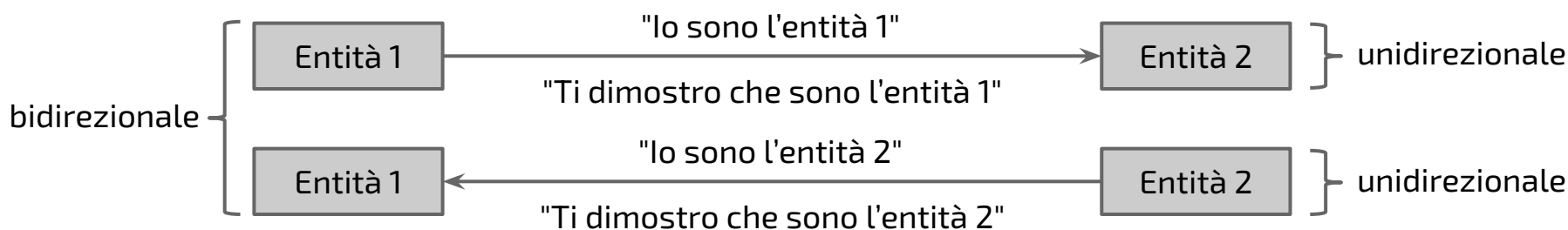
Autenticazione

Può essere *unidirezionale*.



Autenticazione

Può essere *unidirezionale* o *bidirezionale (mutuale)*.



Può avvenire tra qualsiasi entità:

- Da umano a umano
- Da umano a computer
- Da computer a computer

Costituisce la base per la successiva fase di autenticazione.



Tre fattori dell'autenticazione

Qualcosa che l'entità **sa** (to know).

1. Esempio: password, PIN, stretta di mano segreta.

Qualcosa che l'entità **possiede** (to have).

2. Esempio: chiave, smart card, token.

Qualcosa che l'entità **è** (to be).

3. Esempio: volto, voce, impronte digitali.

Umani:

Computer:

Tre fattori dell'autenticazione

Qualcosa che l'entità **sa** (to know).

1. Esempio: password, PIN, stretta di mano segreta.

Qualcosa che l'entità **possiede** (to have).

2. Esempio: chiave, smart card, token.

Qualcosa che l'entità **è** (to be).

3. Esempio: volto, voce, impronte digitali.

Umani: (3) usata più di (2) usata più di (1)

Computer:

Tre fattori dell'autenticazione

Qualcosa che l'entità **sa** (to know).

1. Esempio: password, PIN, stretta di mano segreta.

Qualcosa che l'entità **possiede** (to have).

2. Esempio: chiave, smart card, token.

Qualcosa che l'entità **è** (to be).

3. Esempio: volto, voce, impronte digitali.

Umani: (3) usata più di (2) usata più di (1)

Computer: (1) usata più di (2) usata più di (3)

Tre fattori dell'autenticazione

Qualcosa che l'entità **sa** (to know).

1. Esempio: password, PIN, stretta di mano segreta.

Qualcosa che l'entità **possiede** (to have).

2. Esempio: chiave, smart card, token.

Qualcosa che l'entità **è** (to be).

3. Esempio: volto, voce, impronte digitali.

Umani: (3) usata più di (2) usata più di (1)

Computer: (1) usata più di (2) usata più di (3)

L'autenticazione a fattori multipli (Multi-Factor Authentication) ne usa due o tre.

Il fattore sapere (To know)

Password e PIN

To know: password

L'utente deve dimostrare che *sa* qualcosa.

To know: password

L'utente deve dimostrare che *sa* qualcosa.

Vantaggi:

- Bassi costi.
- Facilità di implementazione.
- Basse barriere tecniche.

To know: password

L'utente deve dimostrare che *sa* qualcosa.

Vantaggi:

- Bassi costi.
- Facilità di implementazione.
- Basse barriere tecniche.

Svantaggi (minacce):

Le password possono essere:

- A. Rubate/Intercettate.
- B. Indovinate (Guessed).
- C. Enumerate (Cracked).
- D. Riutilizzate per altri siti.

To know: password

L'utente deve dimostrare che *sa* qualcosa.

Vantaggi:

- Bassi costi.
- Facilità di implementazione.
- Basse barriere tecniche.

Svantaggi (minacce):

Le password possono essere:

- A. Rubate/Intercettate.
- B. Indovinate (Guessed).
- C. Enumerate (Cracked).
- D. Riutilizzate per altri siti.

Contromisure:

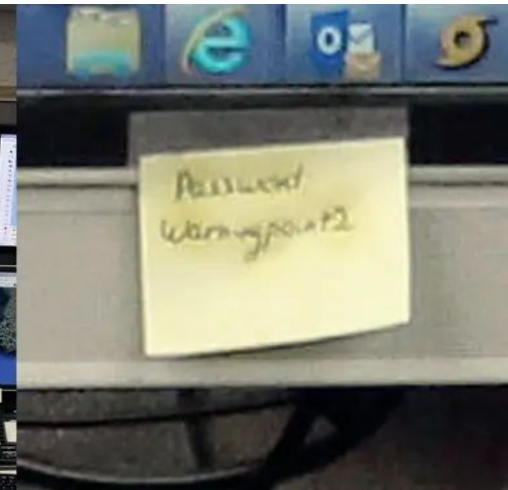
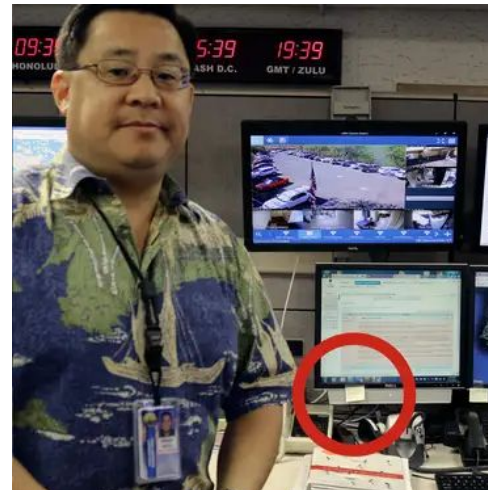
Fare in modo che la password sia:

- A. Cambiata frequentemente.
- B. Lunga.
- C. Complessa.
- D. Non legata all'utente.
- E. Non riutilizzata su diversi siti.

Costi indiretti sulla gestione delle password

Possiamo scegliere tutte le contromisure? Se no, perché?

- A false alert warning of an inbound missile was broadcast in Hawaii on Saturday.
- Since then, people have discovered that a photo taken in Hawaii's Emergency Management Agency for a news article in July includes a sticky note with a password.
- Hawaii says the alert was sent was because "an employee pushed the wrong button," not because of a hack, but the photo has sparked criticism about the agency's level of security.



Costi indiretti sulla gestione delle password

Possiamo scegliere tutte le contromisure? Se no, perché?



Costi indiretti sulla gestione delle password

Possiamo scegliere tutte le contromisure? Se no, perché?



Costi indiretti sulla gestione delle password

Possiamo scegliere tutte le contromisure? Se no, perché?

Gli umani non sono macchine:

- Non sono in grado di tenere segreti.
- Non sono in grado di ricordarsi password complesse

Come scegliamo le contromisure adatte?



To know: password

L'utente deve dimostrare che *sa* qualcosa.

Vantaggi:

- Bassi costi.
- Facilità di implementazione.
- Basse barriere tecniche.

Svantaggi (minacce):

Le password possono essere:

- A. Rubate/Intercettate.
- B. Indovinate (Guessed).
- C. Enumerate (Cracked).
- D. Riutilizzate per altri siti.

Contromisure:

Fare in modo che la password sia:

- A. Cambiata frequentemente.
- B. Lunga.
- C. Complessa.
- D. Non legata all'utente.
- E. Non riutilizzata su diversi siti.

Stimiamo la contromisura più adatta al tipo di attacco

Linee guida alle contromisure

Categorie: importante, può aiutare, irrilevante.

Contro il furto/intercettazione:

- A. Cambiata frequentemente.
- B. Lunga.
- C. Complessa.
- D. Non legata all'utente.
- E. Non riutilizzata su diversi siti.

Linee guida alle contromisure

Categorie: importante, può aiutare, irrilevante.

Contro il furto/intercettazione:

- A. Cambiata frequentemente.
- B. Lunga.
- C. Complessa.
- D. Non legata all'utente.
- E. Non riutilizzata su diversi siti.

Linee guida alle contromisure

Categorie: importante, può aiutare, irrilevante.

Contro il furto/intercettazione:

- A. Cambiata frequentemente.
- B. Lunga.
- C. Complessa.
- D. Non legata all'utente.
- E. Non riutilizzata su diversi siti.

Contro i tentativi (guessing):

- A. Cambiata frequentemente.
- B. Lunga.
- C. Complessa.
- D. Non legata all'utente.
- E. Non riutilizzata su diversi siti.

Linee guida alle contromisure

Categorie: importante, può aiutare, irrilevante.

Contro il furto/intercettazione:

- A. Cambiata frequentemente.
- B. Lunga.
- C. Complessa.
- D. Non legata all'utente.
- E. Non riutilizzata su diversi siti.

Contro i tentativi (guessing):

- A. Cambiata frequentemente.
- B. Lunga.
- C. Complessa.
- D. Non legata all'utente.
- E. Non riutilizzata su diversi siti.

Linee guida alle contromisure

Categorie: importante, può aiutare, irrilevante.

Contro il furto/intercettazione:

- A. Cambiata frequentemente.
- B. Lunga.
- C. Complessa.
- D. Non legata all'utente.
- E. Non riutilizzata su diversi siti.

Contro i tentativi (guessing):

- A. Cambiata frequentemente.
- B. Lunga.
- C. Complessa.
- D. Non legata all'utente.
- E. Non riutilizzata su diversi siti.

Contro l'enumerazione:

- A. Cambiata frequentemente.
- B. Lunga.
- C. Complessa.
- D. Non legata all'utente.
- E. Non riutilizzata su diversi siti.

Linee guida alle contromisure

Categorie: importante, può aiutare, irrilevante.

Contro il furto/intercettazione:

- A. Cambiata frequentemente.
- B. Lunga.
- C. Complessa.
- D. Non legata all'utente.
- E. Non riutilizzata su diversi siti.

Contro i tentativi (guessing):

- A. Cambiata frequentemente.
- B. Lunga.
- C. Complessa.
- D. Non legata all'utente.
- E. Non riutilizzata su diversi siti.

Contro l'enumerazione:

- A. Cambiata frequentemente.
- B. Lunga.
- C. Complessa.
- D. Non legata all'utente.
- E. Non riutilizzata su diversi siti.

Linee guida alle contromisure

Categorie: importante, può aiutare, irrilevante.

Contro il furto/intercettazione:

- A. Cambiata frequentemente.
- B. Lunga.
- C. Complessa.
- D. Non legata all'utente.
- E. Non riutilizzata su diversi siti.

Contro i tentativi (guessing):

- A. Cambiata frequentemente.
- B. Lunga.
- C. Complessa.
- D. Non legata all'utente.
- E. Non riutilizzata su diversi siti.

Contro l'enumerazione:

- A. Cambiata frequentemente.
- B. Lunga.
- C. Complessa.
- D. Non legata all'utente.
- E. Non riutilizzata su diversi siti.

Contro il riutilizzo in altri siti:

- A. Cambiata frequentemente.
- B. Lunga.
- C. Complessa.
- D. Non legata all'utente.
- E. Non riutilizzata su diversi siti.

Linee guida alle contromisure

Categorie: importante, può aiutare, irrilevante.

Contro il furto/intercettazione:

- A. Cambiata frequentemente.
- B. Lunga.
- C. Complessa.
- D. Non legata all'utente.
- E. Non riutilizzata su diversi siti.

Contro i tentativi (guessing):

- A. Cambiata frequentemente.
- B. Lunga.
- C. Complessa.
- D. Non legata all'utente.
- E. Non riutilizzata su diversi siti.

Contro l'enumerazione:

- A. Cambiata frequentemente.
- B. Lunga.
- C. Complessa.
- D. Non legata all'utente.
- E. Non riutilizzata su diversi siti.

Contro il riutilizzo in altri siti:

- A. Cambiata frequentemente.
- B. Lunga.
- C. Complessa.
- D. Non legata all'utente.
- E. Non riutilizzata su diversi siti.

Contestualizzazione della minaccia

- La minaccia è anche da contestualizzare nel **threat model**. Esempi:
 - Hanno rubato uno zip protetto da password.
 - Il fidanzato/la fidanzata vogliono farsi gli affari vostri sui social.
 - Una organizzazione criminale prova a entrare in account bancari/aziendali.
- Qual è la minaccia più concreta in questi casi?
- Come potete immaginare è diversa.

Contestualizzazione della minaccia

- La minaccia è anche da contestualizzare nel **threat model**. Esempi:
 - **Hanno rubato uno zip protetto da password.**
 - Il fidanzato/la fidanzata pubblica i tuoi affari vostri sui social.
 - Una organizzazione criminale ha accesso ai tuoi account bancari/aziendali.
- Qual è la minaccia più comune?
- Come potete immaginare...

Contro l'enumerazione:

- A. Cambiata frequentemente.
- B. Lunga.
- C. Complessa.
- D. Non legata all'utente.
- E. Non riutilizzata su diversi siti.

Contestualizzazione d

- La minaccia è anche da co
threat model. Esempi:
 - Hanno rubato uno zip protetto da password.
 - **Il fidanzato/la fidanzata vogliono farsi gli affari vostri sui social.**
 - Una organizzazione criminale prova a entrare

Contro il riutilizzo in altri siti:

- A. Cambiata frequentemente.
- B. Lunga.
- C. Complessa.
- D. Non legata all'utente.
- E. Non riutilizzata su diversi siti.

Contro il furto/intercettazione:

- A. Cambiata frequentemente.
- B. Lunga.
- C. Complessa.
- D. Non legata all'utente.
- E. Non riutilizzata su diversi siti.

Contro i tentativi (guessing):

- A. Cambiata frequentemente.
- B. Lunga.
- C. Complessa.
- D. Non legata all'utente.
- E. Non riutilizzata su diversi siti.

Contestualizzazione della minaccia

Contro l'enumerazione:

- A. Cambiata frequentemente.
- B. Lunga.
- C. Complessa.
- D. Non legata all'utente.
- E. Non riutilizzata su diversi siti.

Contro il riutilizzo in altri siti:

- A. Cambiata frequentemente.
- B. Lunga.
- C. Complessa.
- D. Non legata all'utente.
- E. Non riutilizzata su diversi siti.

- **Una organizzazione criminale prova a entrare in account bancari/aziendali.**
- Qual è la minaccia più concreta in questi casi?
- Come potete immaginare è diversa.

Contestualizzazione della minaccia

Contro l'enumerazione:

- A. Cambiata frequentemente.
- B. Lunga.
- C. Complessa.
- D. Non legata all'utente.
- E. Non riutilizzata su diversi siti.

Contro il riutilizzo in altri siti:

- A. Cambiata frequentemente.
- B. Lunga.
- C. Complessa.
- D. Non legata all'utente.
- E. Non riutilizzata su diversi siti.

- **Una organizzazione criminale prova a entrare in account bancari/aziendali.**
- Qual è la minaccia più concreta in questi casi?
- Come potete immaginare è diversa.

Molte realtà mettono un limite di tentativi.

Complessità delle password

Educazione degli utenti

Gli utenti sono spesso considerati “l’anello debole” della sicurezza. Per questo è importante formarli e guidarli nell’uso corretto delle password.

- Applicare processi che impongono l’uso di password robuste.
- Stabilire (o rivedere criticamente) politiche di scadenza e cambio della password.



Complessità delle password

- must h4v3 4 r1ch, ch4r4ct3r, s3t!
- mUsT hAvE a MiXeD cAsE
- muuuuust beeeeeee loooooong enoooogh

Utilizzare indicatori di forza della password (**password meters**) per trovare un buon equilibrio tra *sicurezza* e *facilità d’uso*.



Password meters

.....|



Password must:

- ☒ Have at least one letter
- ☐ **Have at least one capital letter**
- ☐ **Have at least one number**
- ☒ Not contain more than 3 consecutive identical characters
- ☒ Not be the same as the account name
- ☒ Be at least 8 characters

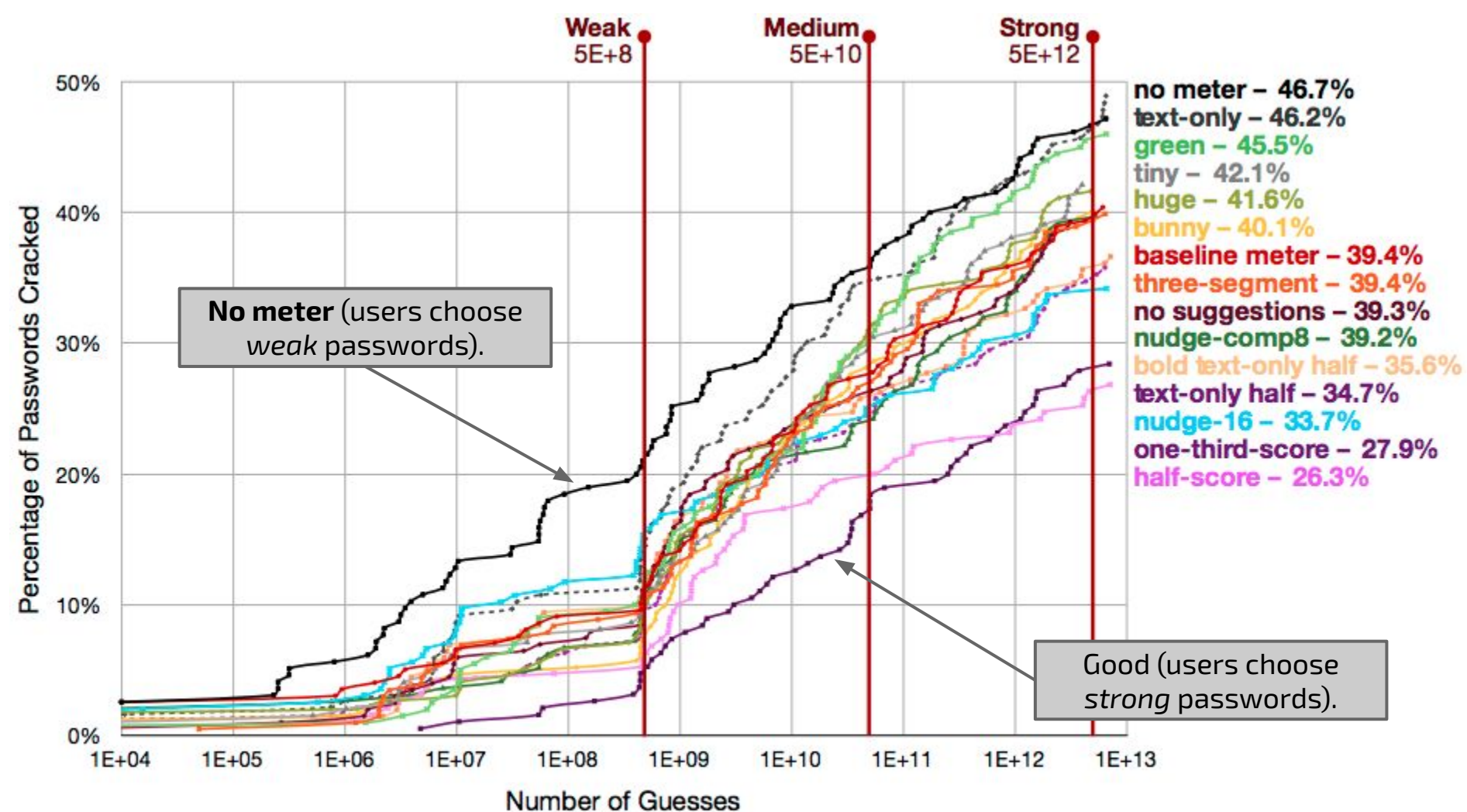


Figure 3: This graph contrasts the percentage of passwords that were cracked in each condition. The x-axis, which is logarithmically scaled, indicates the number of guesses made by an adversary, as described in Section 2.4. The y-axis indicates the percentage of passwords in that condition cracked by that particular guess number.

B. Ur, P.G. Kelley, S. Komanduri, J. Lee, M. Maass, M. Mazurek, T. Passaro, R. Shay, T. Vidas, L. Bauer, N. Christin, and L.F. Cranor. [How does your password measure up? The effect of strength meters on password creation.](#) USENIX Security 2012.

Enter a Password, and click Analyze

.....

Analyze

Hide Examples

Show Options

Weak Passwords that pass typical policies:

qwerQWER1234!@#\$ - l1cracked - cracked7& -

Strong Passwords that fail typical policies:

udnkzdejhdowjpo - seattleautojesterarbol

[passfault](#)

This password needs more strength

Time To Crack:

less than 1 day

Total Passwords in Pattern:

8 Billion

HORIZONTAL
English

25%

of total strength

HORIZONTAL
English

25%

of total strength

HORIZONTAL
English

25%

of total strength

HORIZONTAL
English

25%

of total strength

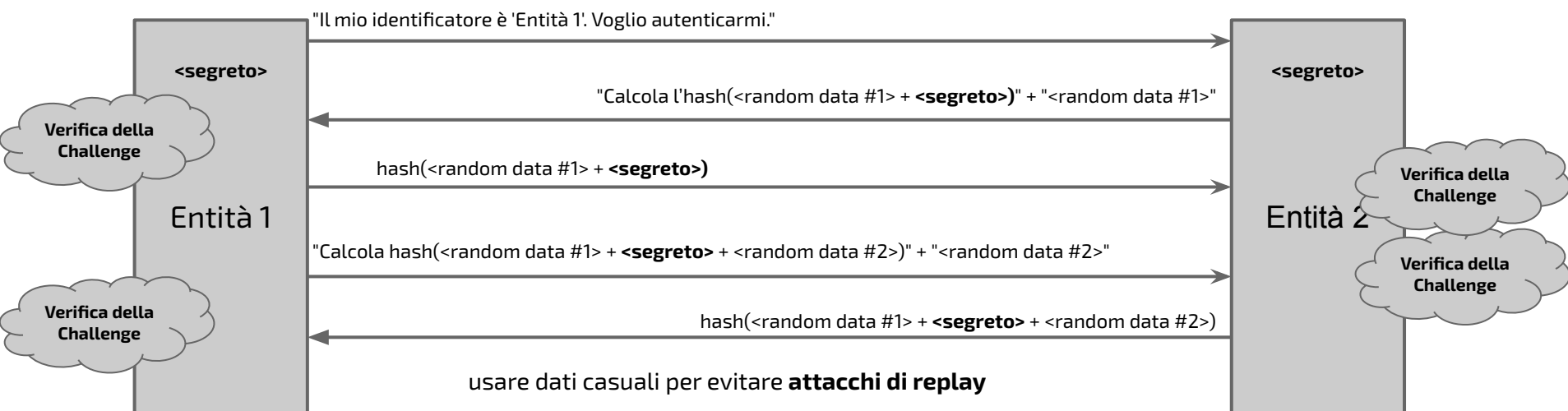
"Scambio" sicuro di password

L'autenticazione riguarda la condivisione di un segreto.

Come minimizzare il rischio che i segreti vengano rubati?

- usare, se possibile, l'autenticazione reciproca.
- usare uno schema di **challenge-response** o una **prova a conoscenza zero (Zero Knowledge Proof)**.

Esempio di un semplice schema di challenge e response



Archiviazione Sicura delle Password

L'autenticazione riguarda anche la *conservazione* di un segreto.

Il sistema operativo memorizza un file contenente nomi utente e password.

Un attaccante potrebbe tentare di compromettere la riservatezza o l'integrità di questo file delle password.

Come ridurre il rischio che i segreti vengano rubati?

- **Protezione crittografica**
 - non memorizzare mai le password in chiaro: usa hashing + salting per mitigare gli attacchi a dizionario (bruteforce).
- **Politiche di controllo degli accessi**: limita i privilegi di lettura e scrittura.

!;--have i been pwned?

Check if your email address is in a data breach

Using Have I Been Pwned is subject to [the terms of use](#)

876

pwned websites

14,947,323,864

pwned accounts










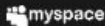
115,799

pastes











229,165,825

paste accounts

Largest breaches

	772,904,991 Collection #1 accounts
	763,117,241 Verifications.io accounts
	711,477,622 Onliner Spambot accounts
	622,161,052 Data Enrichment Exposure From PDL Customer accounts
	593,427,119 Exploit.In accounts
	509,458,528 Facebook accounts
	457,962,538 Anti Public Combo List accounts
	393,430,309 River City Media Spam List accounts
	361,468,099 Combolist Posted to Telegram accounts
	359,420,698 MySpace accounts

Recently added breaches

	672,546 Lexipol accounts
	220,503 Color Dating accounts
	33,294 Flat Earth Sun, Moon and Zodiac App accounts
	518,643 Spyzie accounts
	556,557 Orange Romania accounts
	284,132,969 ALIEN TXTBASE Stealer Logs accounts
	875,999 Spyic accounts
	1,798,059 Cocospy accounts
	11,052,071 Storenvvy accounts
	136,461 Doxbin (TOoDA) accounts

Il fattore avere (To have)

Token, smart card e smart phones

Il fattore To have

L'utente deve dimostrare che *ha* qualcosa.

Il fattore To have

L'utente deve dimostrare che *ha* qualcosa.

Vantaggi:

- Fattore umano (meno probabilità di consegnare una chiave).
- Costo relativamente basso.
- Buon livello di sicurezza.

Il fattore To have

L'utente deve dimostrare che *ha* qualcosa.

Vantaggi:

- Fattore umano (meno probabilità di consegnare una chiave).
- Costo relativamente basso.
- Buon livello di sicurezza.

Svantaggi:

1. Potenzialmente difficile da implementare.
2. Può essere perso o rubato.

Il fattore To have

L'utente deve dimostrare che *ha* qualcosa.

Vantaggi:

- Fattore umano (meno probabilità di consegnare una chiave).
- Costo relativamente basso.
- Buon livello di sicurezza.

Svantaggi:

1. Potenzialmente difficile da implementare.
2. Può essere perso o rubato.

Contromisure:

1. Nessuna
2. Usare in coppia con un altro fattore.

Esempi di tecnologie classiche

Generatori di password monouso (One-Time Password):

- *Chiave segreta* + *contatore* sincronizzato con l'host.
- **Client**: calcola **hash**(contatore, chiave).
- **Server**: verifica **hash**(contatore, chiave).
- Si controlla che il contatore sia quello atteso.
- Il contatore cambia ogni 30–60 secondi.

Esempi di applicazione: online banking, console di amministrazione (ad es. Amazon AWS).



Smart card (anche con lettore integrato in chiavette USB):

- CPU + RAM non volatile con una *chiave privata*.
- La smart card si autentica presso l'host tramite un protocollo **challenge-response**.
 - Utilizza la *chiave privata* per firmare la challenge.
- La *chiave privata* non lascia mai il dispositivo.
- Dovrebbe essere almeno in parte resistente a manomissioni (tamper-proof).

Esempi di applicazione: carte di credito (+ PIN).



Liste di OTP statiche (alternativa più economica)



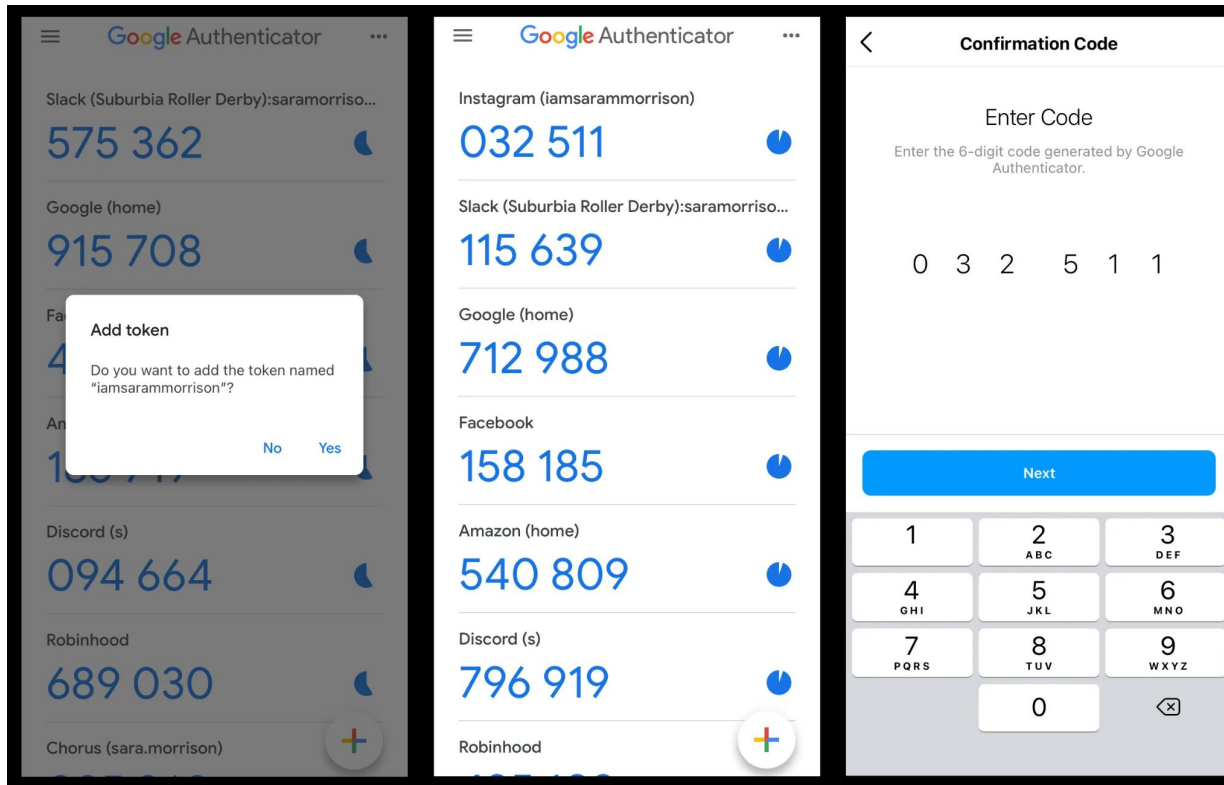
► Esempio di codice personale



Esempio di codice personale

- Condivise tra client e host.
- L'host sceglie una challenge: numeri casuali (ad es. "seconda cifra della cella 14").
- Il client invia la risposta (preferibilmente su un canale cifrato).
- L'host non dovrebbe conservare la lista in chiaro (ad es. usando hash).

Tecnologie moderne: Time-based OTP (TOTP)



Software che implementa la stessa funzionalità dei generatori di password:

- Differenza chiave:
 - I generatori di password sono sistemi chiusi ed incorporati.
 - Le app per la generazione delle password funzionano su piattaforme hw/sw generiche.
- Cosa succede se il dispositivo è infettato da un'app malevola?: Dmitrienko et al., [When More Becomes Less: On the \(In\)Security of Mobile Two-Factor Authentication](#), FC 2014

SIM SWAPPING – A MOBILE PHONE SCAM

SIM swapping occurs when a fraudster, using social engineering techniques, takes control over your mobile phone SIM card using your stolen personal data.



HOW DOES IT WORK?

A fraudster obtains the victim's personal data through e.g. data breaches, phishing, social media searches, malicious apps, online shopping, malware, etc.



With this information, the fraudster dupes the mobile phone operator into porting the victim's mobile number to a SIM in his possession



The fraudster can now receive incoming calls and text messages, including access to the victim's online banking



The victim will notice the mobile phone lost service, and eventually will discover they cannot login to their bank account



Tecnologie moderne: chiavi Sicure

- **Plug & Touch:** la chiave viene inserita in una porta USB e premuta quando richiesto.
- Da usare in combinazione con un altro fattore (2FA).
- **Genera un codice Sicuro:** Il dispositivo invia una password monouso (OTP) oppure una chiave crittografica per l'autenticazione.
- Un'evoluzione delle precedenti più moderna (basta solo inserirla).



Il fattore essere (To be)

Autenticazione biometrica

Il fattore To be

L'utente deve dimostrare che ha *specifiche caratteristiche*.

Il fattore To be

L'utente deve dimostrare che ha *specifiche caratteristiche*.

Vantaggi:

- Alto livello di sicurezza e robustezza.
- Non richiede hardware aggiuntivo da portare con sé.

Il fattore To be

L'utente deve dimostrare che ha *specifiche caratteristiche*.

Vantaggi:

- Alto livello di sicurezza e robustezza.
- Non richiede hardware aggiuntivo da portare con sé.

Svantaggi:

1. Estremamente difficile da implementare.
2. Corrispondenza probabilistica.
3. Misurazione invasiva.
4. Clonazione possibile.
5. le caratteristiche biometriche potrebbero cambiare nel tempo.
6. Problemi di privacy.
7. utenti con disabilità (non sempre possono usarlo)

Il fattore To be

L'utente deve dimostrare che ha *specifiche caratteristiche*.

Vantaggi:

- Alto livello di sicurezza e robustezza.
- Non richiede hardware aggiuntivo da portare con sé.

Svantaggi:

1. Estremamente difficile da implementare.
2. Corrispondenza probabilistica.
3. Misurazione invasiva.
4. [Clonazione](#) possibile.
5. le caratteristiche biometriche potrebbero cambiare nel tempo.
6. Problemi di privacy.
7. utenti con disabilità (non sempre possono usarlo)

Contromisure:

1. Nessuna.
2. Nessuna.
3. Nessuna.
4. Nessuna.
5. Misurare spesso (aggiornare).
6. Mettere in sicurezza il processo.
7. Serve un metodo alternativo (più debole?)

Esempi di tecnologie

Estrazione delle caratteristiche (ovvero feature) di:

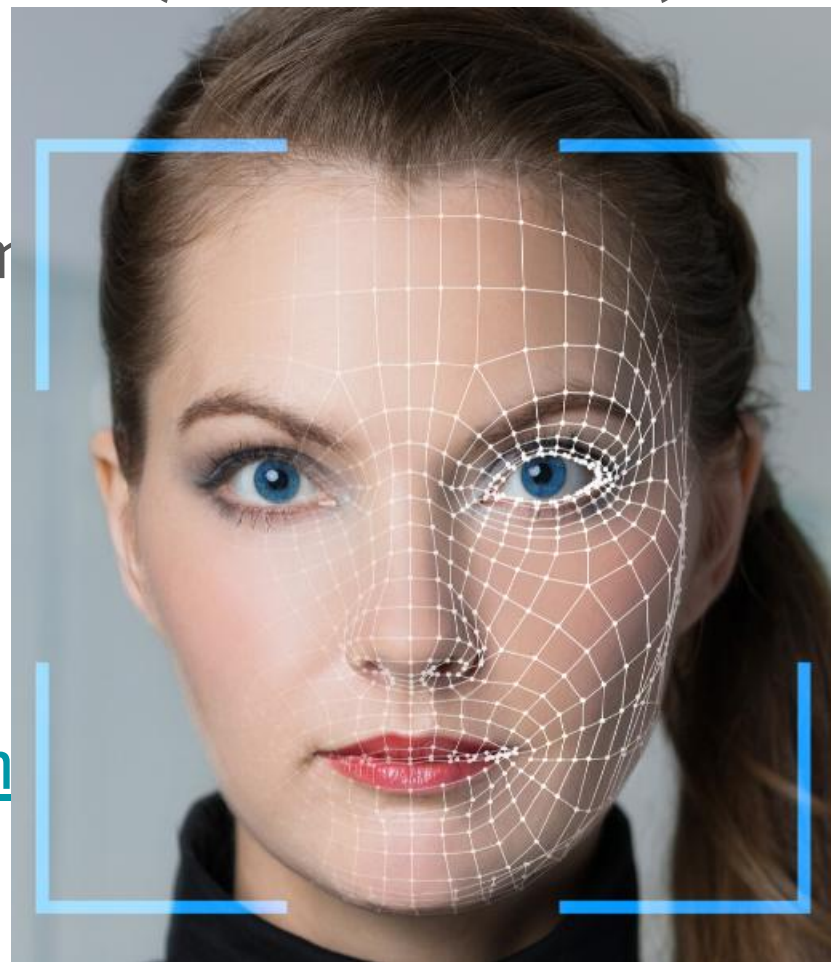
- **Impronte digitali.**
- Geometria del viso.
- Geometria della mano.
- Scansione della retina.
- Scansione dell'iride.
- Analisi della voce.
- DNA.
- Dinamica di digitazione.
- Modo di impugnatura.



Esempi di tecnologie

Estrazione delle caratteristiche (ovvero feature) di:

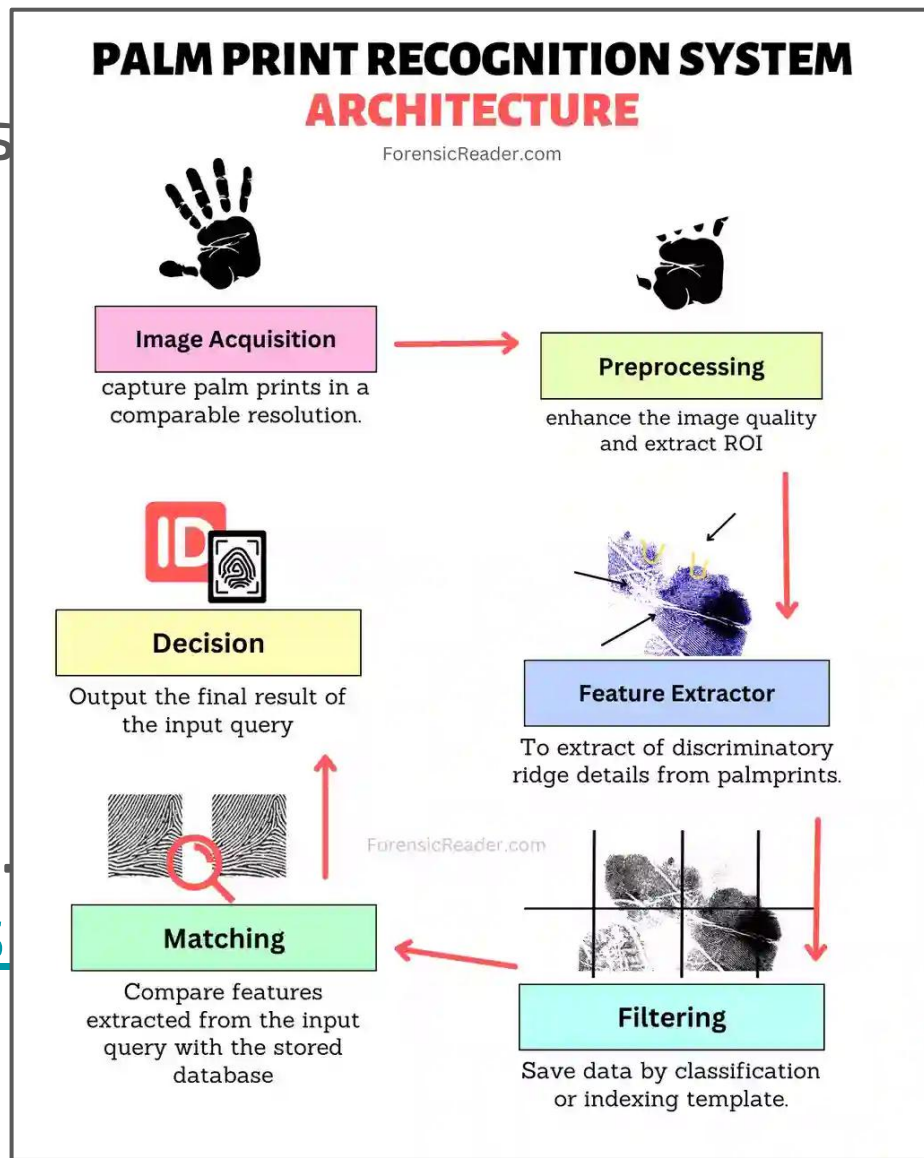
- Impronte digitali.
- **Geometria del viso.**
- Geometria della mano (impronta)
- Scansione della retina.
- Scansione dell'iride.
- Analisi della voce.
- DNA.
- Dinamica di digitazione.
- Modo di impugnare lo sm



Esempi di tecnologie

Estrazione delle caratteris

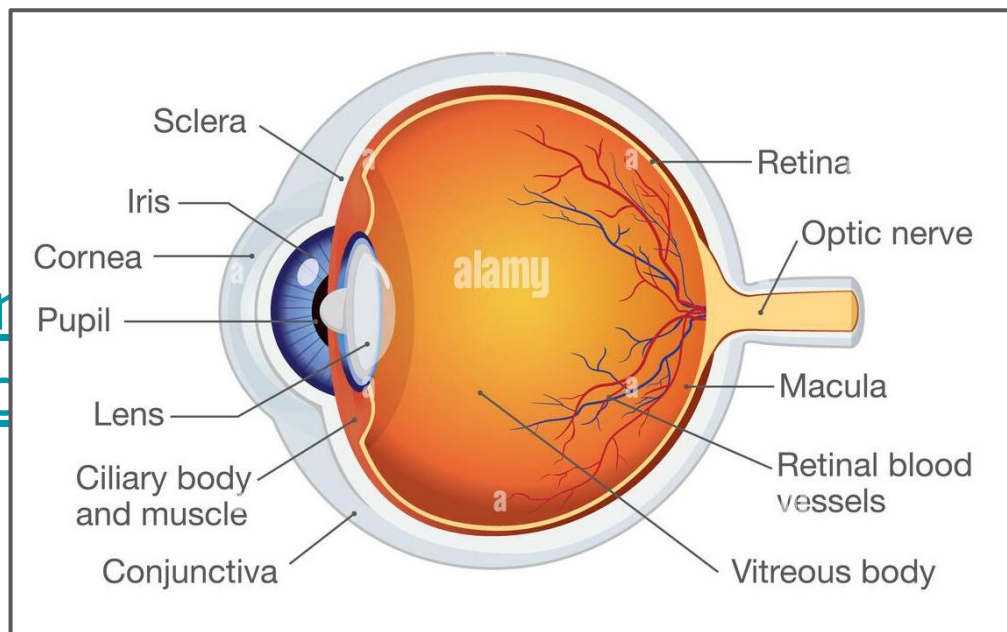
- Impronte digitali.
- Geometria del viso.
- **Geometria della mano**
- Scansione della retina.
- Scansione dell'iride.
- Analisi della voce.
- DNA.
- Dinamica di digitazione.
- Modo di impugnare lo s



Esempi di tecnologie

Estrazione delle caratteristiche (ovvero feature) di:

- Impronte digitali.
- Geometria del viso.
- Geometria della mano (impronta del palmo).
- **Scansione della retina.**
- Scansione dell'iride.
- Analisi della voce.
- DNA.
- Dinamica di digitazione
- Modo di impugnare lo



Esempi di tecnologie

Estrazione delle caratteristiche (ovvero feature) di:

- Impronte digitali.
- Geometria del viso.
- Geometria della mano (impronta del palmo).
- Scansione della retina.
- **Scansione dell'iride.**
- Analisi della voce.
- DNA.
- Dinamica di digitazione.
- Modo di impugnare lo sma



Esempi di tecnologie

Estrazione delle caratteristiche (ovvero feature) di:

- Impronte digitali.
- Geometria del viso.
- Geometria della mano (impronta del palmo).
- Scansione della retina.
- Scansione dell'iride.
- Analisi della voce.
- DNA.
- Dinamica di digitazione.
- Modo di impugnare lo smartphone.

Esempio: impronte digitali

- Viene acquisito un campione di riferimento dell'impronta digitale dell'utente tramite un lettore di impronte.
- Dal campione vengono estratte le caratteristiche (feature) principali.
 - Le minuzie dell'impronta includono: punti terminali delle creste, punti di biforcazione, nucleo (core), delta, anse (loops), vortici (whorls), ecc.
 - Per una maggiore accuratezza, si registrano le caratteristiche di più dita e da diverse posizioni.
- I vettori di caratteristiche vengono archiviati in un database sicuro.
- Quando l'utente effettua l'accesso, viene acquisita una nuova lettura dell'impronta digitale; le caratteristiche estratte vengono confrontate (in base alla similarità) con quelle di riferimento. L'utente viene accettato se il grado di corrispondenza supera una soglia predefinita.

Problema principale: falsi positivi e falsi negativi.

Autenticazione biometrica a livello consumer



<http://cryptome.org/fake-prints.htm>

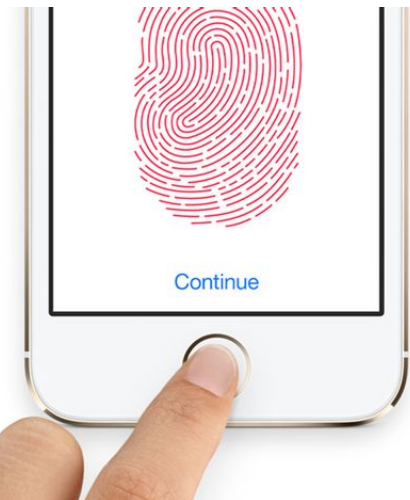
Manufacturer	Model	Technology	Date	Difficulty
Identix	TS-520	Optical	Nov. 1990	First attempt
Fingermatrix	Chekone	Optical	Mar. 1994	Second attempt
Dermalog	DemalogKey	Optical	Feb.1996	First attempt
STMicroelectronics	TouchChip	Solid state	Mar. 1999	First attempt
Veridicon	FPS110	Solid state	Sept.1999	First attempt
Identicator	DFR200	Optical	Oct. 1999	First attempt

20 september 2013 **RELEASED**

21 september 2013 **CRACKED**

Examples:

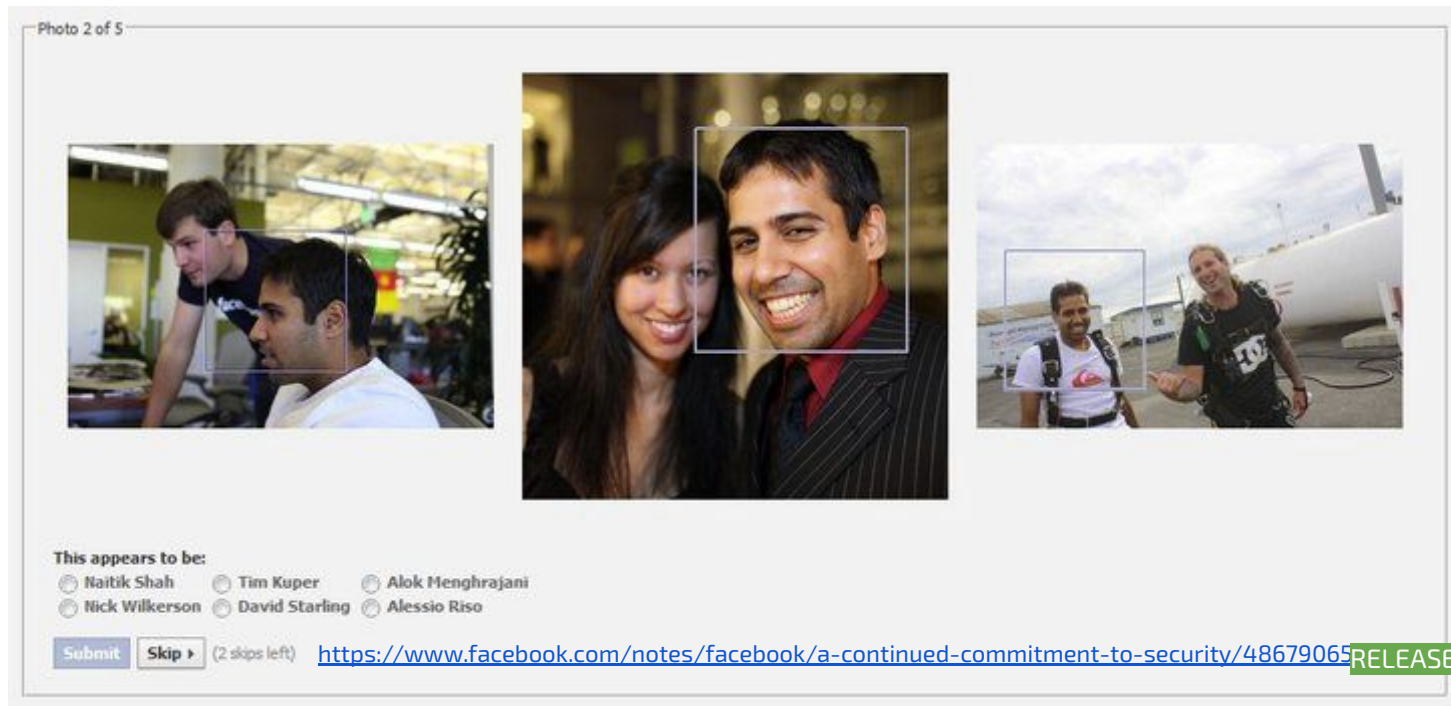
- <http://www.ccc.de/en/updates/2013/ccc-breaks-apple-touchid> (short) - <https://www.heise.de/multimediateil/iPhone-5s-Touch-ID-hack-in-detail-1965628.html> (long)
- <https://www.ccc.de/en/updates/2017/iriden>
- <https://i.blackhat.com/USA-19/Wednesday/us-19-Chen-Biometric-Authentication-Under-Threat-Liveness-Detection-Hacking.pdf>
- https://www.youtube.com/watch?v=ZwCNG9KFdXs&ab_channel=Forbes



**Nuovi e sperimentali modi
di autenticarsi**

Il fattore sociale: Chi conosci

Occorre dimostrare che si *conosce* qualcuno.



RELEASED

Papers

- H. Kim, J. Tang, and R. Anderson. [Social authentication: harder than it looks](#). In Proceedings of the 2012 Financial Cryptography and Data Security conference.
- J. Polakis, M. Lancini, G. Kontaxis, F. Maggi, S. Ioannidis, A. Keromytis, S. Zanero, [All Your Face Are Belong to Us: Breaking Facebook's Social Authentication](#). In Proceedings of 2012 Annual Computer Security Applications Conference.

CRACKED

Single Sign-On (SSO)

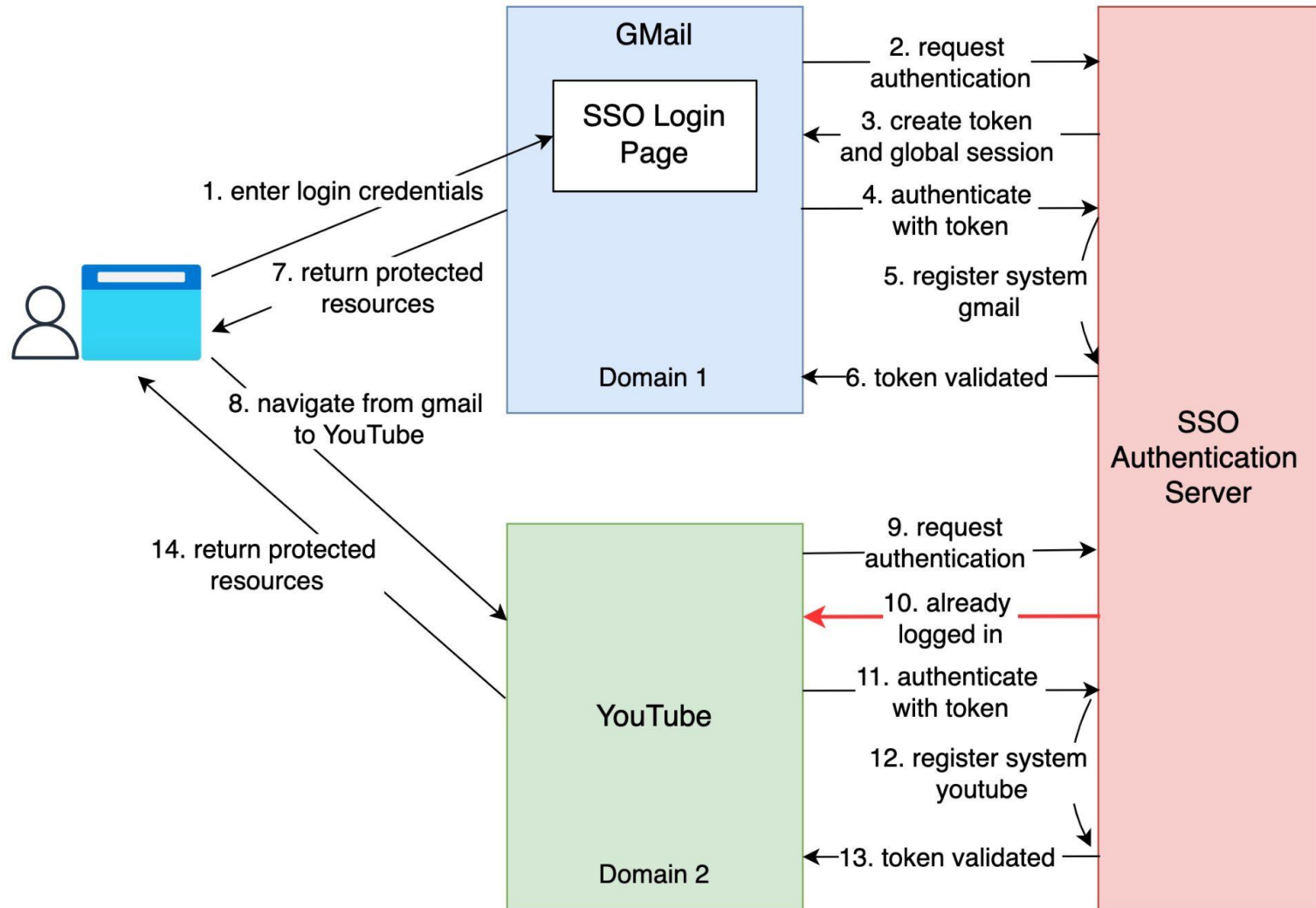
Problema: gestire e ricordare più password è complesso.

- Gli utenti riutilizzano le password su più siti.
- Le politiche sulle password sono diverse (1 carattere speciale, 1 carattere maiuscolo, ...)

Soluzione: 1 identità, 1–2 fattori di autenticazione, 1 host fidato.

- Si elegge un host di fiducia (Google, Facebook, LinkedIn).
- Gli utenti si autenticano (sign on) presso l'host fidato.
- Gli altri host chiedono all'host fidato se l'utente è autenticato.

How does SSO Work?



Single Sign On: challenges

Punto unico di *fiducia*: il server di fiducia.

- Se viene compromesso, tutti i siti sono compromessi.
- Lo schema di reset delle password deve essere a prova di proiettile.
- La email è l'elemento di fiducia.

Kontaxis G. et al., [SAuth: Protecting User Accounts from Password Database Leaks](#). In Proceedings of the 20th ACM Conference on Computer and Communications Security (CCS), 2013.

Difficile da fare bene per gli sviluppatori.

- Il flusso è complesso da implementare.
- Esistono librerie, ma possono contenere bug.

<http://homakov.blogspot.it/2014/02/how-i-hacked-github-again.html>

Password managers

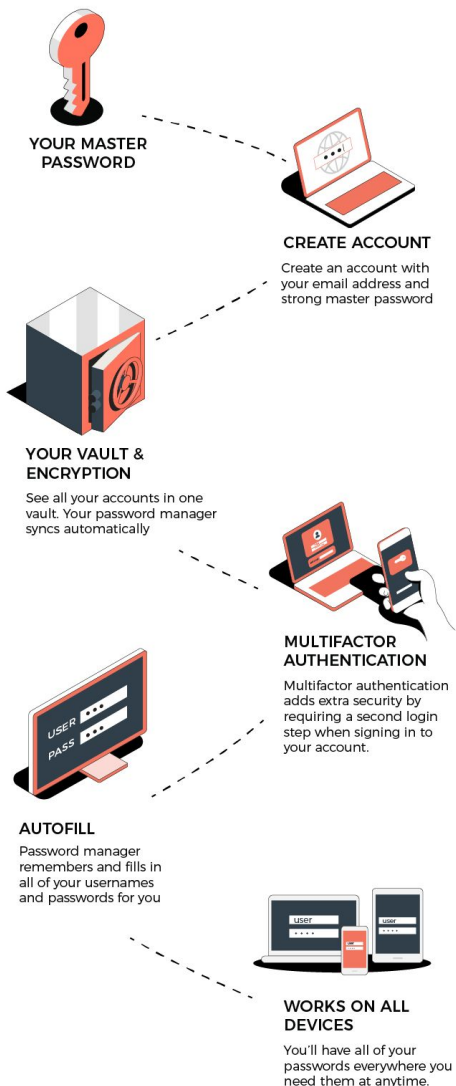
Problema: gestire e ricordare più password è complesso.

- Gli utenti riutilizzano le password su più siti.
- Le politiche sulle password sono diverse (1 carattere speciale, 1 carattere maiuscolo, ...)

Soluzione: 1 identità, 1–2 fattori di autenticazione, 1 password manager.

- Si elegge un password manager di fiducia (Google, Apple, Android).
- Gli utenti si autenticano (sign on) sul password manager fidato.
- Si genera una nuova password per ogni sito.

HOW DOES A **PASSWORD MANAGER** WORK



Password managers

Pro

- Non c'è bisogno di ricordarsi tutte le password.
- Permette di avere password complesse.
- Usabilità
 - Compilazione automatica
 - Sincronizzazione
 - Dispositivi multipli

Contro

- Singolo punto di fiducia che può essere preso di mira.
- Larga superficie di attacco:
 - I password managers sono software.
 - Le estensioni del browser possono essere malevoli.
 - Facilmente accessibile.

- <https://stuartschechter.medium.com/before-you-use-a-password-manager-9f5949ccf168>

Gangwal, A., Singh, S., & Srivastava, A. (2023, April). AutoSpill: Credential Leakage from Mobile Password Managers. In *Proceedings of the Thirteenth ACM Conference on Data and Application Security and Privacy* (pp. 39-47).

Il fattore To Know e l'interesse nel diritto penale

Accesso abusivo

- Il fattore “to know” è un **atto della mente**: rappresenta la volontà di riservare l'accesso a pochi.
- In diritto penale è la linea di confine tra:
 - **Accesso abusivo** (art. 615-ter c.p.) → superamento di una barriera cognitiva.
 - **Assenza di reato** se l'accesso è libero o non protetto.
- Per la Cassazione (es. n. 41210/2017): anche una semplice password manifesta la volontà di escludere i non autorizzati.
- Quindi: la misura “conoscitiva” dà valore penale alla protezione del sistema.

Diritto al silenzio

- **Principio generale:** *nemo tenetur se detegere* → nessuno può essere costretto ad autoincriminarsi.
- **Conseguenza:** non si può obbligare un imputato a rivelare ciò che sa (password, PIN).
- **Giurisprudenza italiana:**
 - Cass. pen., Sez. V, 10 marzo 2016, n. 10630 → rifiuto di rivelare password non sanzionabile.
 - Cass. pen., Sez. VI, 20 gennaio 2021, n. 11105 → diritto al silenzio si estende ai codici di accesso.
- **Idea chiave:** Password e PIN sono estensioni della mente: rientrano nella sfera cognitiva tutelata dai diritti di difesa.
- **Diverso invece per:**
 - “Qualcosa che ho” → oggetto fisico, consegnabile.
 - “Qualcosa che sono” → dato fisico, rilevabile.

Conclusioni

- **Identificazione, autenticazione e autorizzazione** sono tre concetti distinti, ma tra loro interdipendenti.
- Esistono **tre tipi di fattori di autenticazione**, che dovrebbero essere usati in combinazione.
- Le password stanno mostrando sempre più i loro limiti.
- Incolpare l'utente per aver scelto una password debole è una semplificazione eccessiva: la **responsabilità ricade anche su chi progetta i sistemi** di autenticazione, che dovrebbe fornire strumenti e alternative più sicure.
- I nuovi schemi di autenticazione sono **promettenti**, ma devono essere utilizzati con **cautela**.