

Human Authentication

Thierry Sans

Intuitive definition

What is human authentication?

➡ “Determining the identity of a person”

Why would I need to authenticate you?

➡ “To be sure that you are the person that you claim to be”

Identification vs Authentication

Identification

- ➔ Assigning a set of data to a person or an organization (subject)

Authentication

- ➔ Making a safe link between a subject and one or several of identities

Authentication Factors

Something that you know

- ✓ Password, PIN number, secret key, secret handshake, secret questions ...

Something that you have

- ✓ IDs, badges, physical key ...

Something that you are or do (biometrics)

- ✓ Fingerprint, voice recognition, face recognition ...

Something that you know



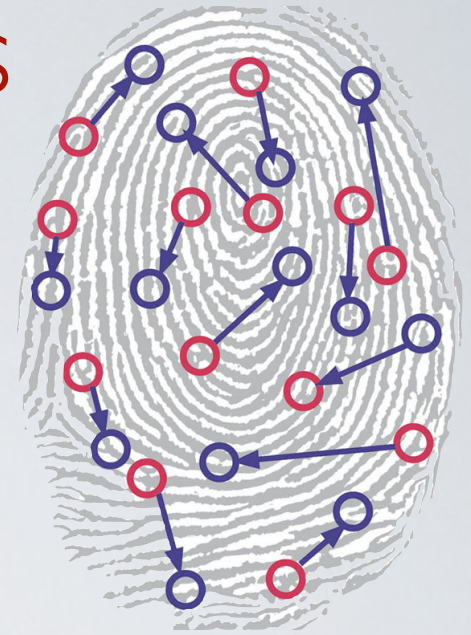
- ✓ **Good as long as** you remember the secret and nobody can uncover or guess this secret
- ⦿ **Gets compromised as soon as** someone else knows this secret and is able to use it

Something that you have



- ✓ **Good as long as** you do not lose or damage the token and there is only one instance for a “given token”
- ⦿ **Gets compromised as soon as** someone can duplicate or fake the token

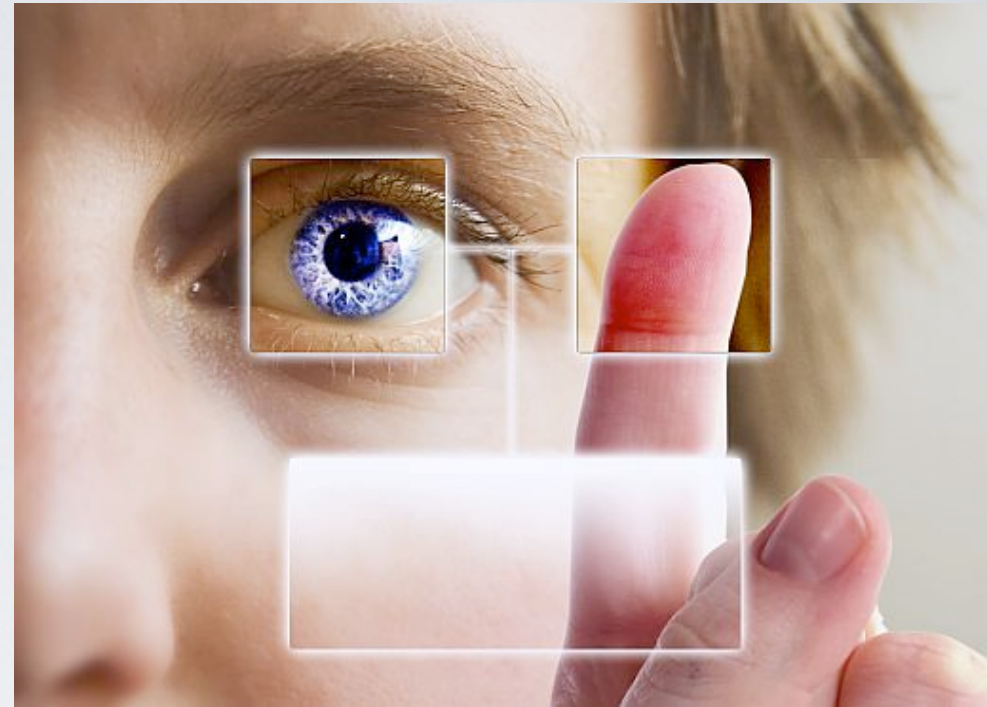
Something that you are or do - Biometrics



“An authenticator takes a measure of your physical characteristics and compare it with an existing measure of what you are suppose to be”

- ✓ The robustness depends on the precision of this measure and the similarity criteria (often not strict equality)
- But how to recover from an attack where the physical characteristics are compromised?

Something that you are




- ✓ **Good as long as** you act or look like the same and nobody cannot be “good enough” in doing what you do or “pretend” to look like you
- ⦿ **Gets compromised as soon as** someone can “nearly” act like your “nearly” look like you (depending on the authenticator)

Multi-factor authentication



	Something that you		
	know	have	are
ID card		X	X
Credit Card	X	X	
Biometric Passport		X	X X
Two-factor authentication	X	X	


Example of two-factor authentication

[Get Started](#)


[Home](#) [Features](#) [Help](#)

Stronger security for your Google Account

With 2-Step Verification, you'll protect your account with both your password and your phone



[Why you need it](#) **How it works** [How it protects you](#)



Signing in to your account will work a little differently

- 1 Enter your password**
Whenever you sign in to Google, you'll enter your password as usual.
- 2 Enter a verification code**
Then, you'll be asked for a code that will be sent to your phone via text, voice call, or our mobile app.

<https://twofactorauth.org/>

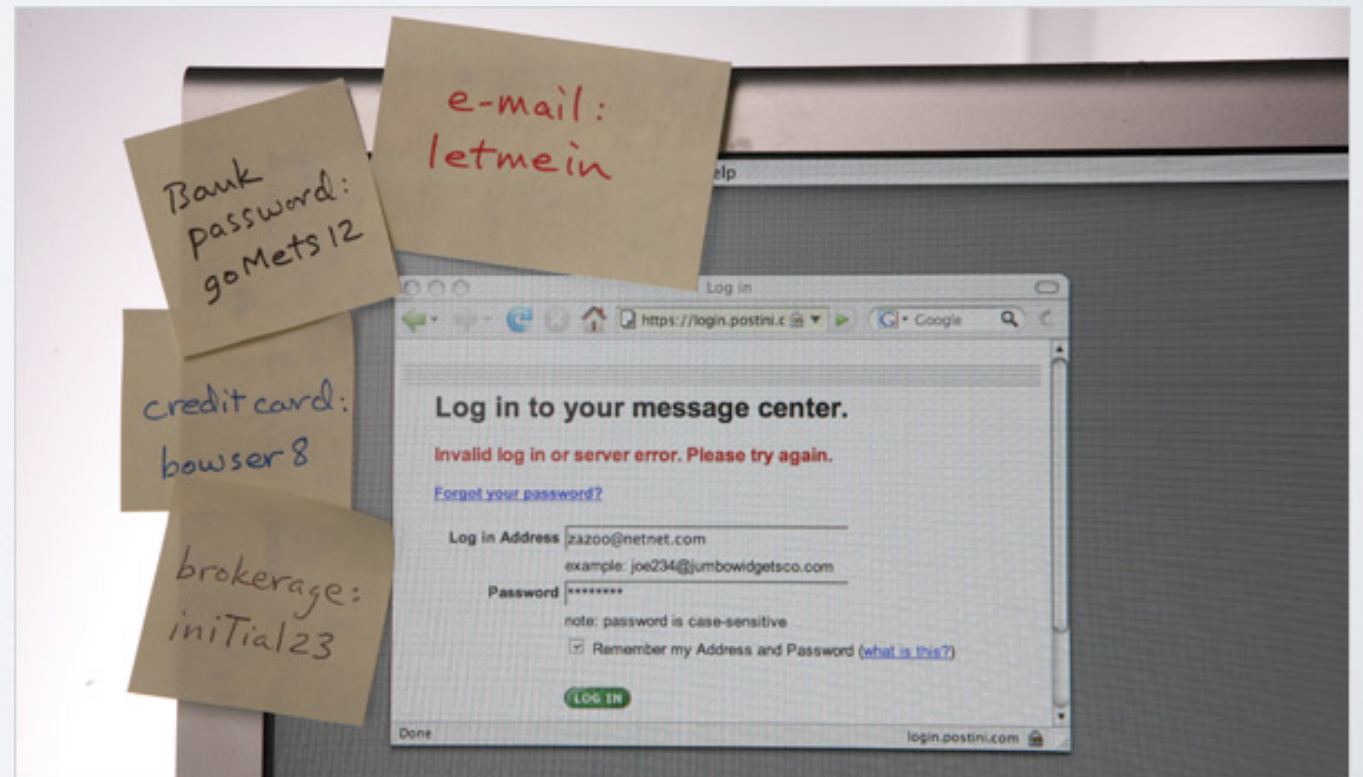
Choosing the authentication mechanism

- ➔ Driven by the risk analysis and the costs
How hard is it to?
 - Make you reveal your secret password
 - Duplicate a credit card
 - Fake your fingerprints
- ◎ There is no perfect authentication



Something else to consider - usability

- How restrictive is the use of several authentication mechanisms?
- How the users will use handle and appropriate the authentication process?



To go further

- Can the authentication process be delegated to a third party?
 - Can we use the same identity over different information systems?
- ➔ Identity management systems

Passwords

Managing Passwords

- How many passwords do you have?
- What password for what kind of application?
- How often do you change your password?
- How do you remember your password?
- How strong is your password?

Using passwords

- Where are passwords stored?
- How are they stored?
- How are they compared with an input?
- How are they transmitted on the network?

Hacking passwords

- How would you steal someone's password?
- How would you crack someone's password?

Cracking a password from the login box

How to crack a password on challenge/response?

- Guessing attack (default and common passwords)
- Brute force attack
- Dictionary attack

What are the counter-measures?

- Timing
- Limit number of tries

Tool :THC Hydra



How passwords are stored

- **In clear** (really bad)
- **Hashed** (bad)
- **Salted Hash** (better and easy to manage)
- **Encrypted** (best but complex to manage)

Unsalted passwords



Salted password



Getting someone's password

How to get a password in clear?

- Social engineering - Phishing
- Data mining (emails, logs)
- Keyloggers (keystroke logging)

How to get an encrypted or hashed password?

- Know where it is stored

Cracking an encrypted or hashed password

How to crack a password knowing its stored form?

- Guessing attack (default and common passwords)
- Brute force attack
- Dictionary attack
- Rainbow tables

What are the counter-measures?

- Protect it well at the OS or application level
- Store it somewhere else (portable device, kerberos, ...)

Tool : John the Ripper

Password Strength

How strong is your password?

<http://howsecureismypassword.net/>

How long does it take to crack a password?

<http://www.lockdown.co.uk/?pg=combi>

68

comments



11.3K



2.3K



3.6K



402

More +

CNET > News > Security & Privacy

Millions of LinkedIn passwords reportedly leaked online

A hacker says he's posted 6.5 million LinkedIn passwords on the Web -- hot on the heels of security researchers' warnings about privacy issues with LinkedIn's iOS app.



by Lance Whitney | June 6, 2012 6:31 AM PDT

Follow

Update 1:08 p.m. PT: [LinkedIn confirms that passwords were "compromised."](#)

LinkedIn users could be facing yet another security problem.

A user in a Russian forum says that he has hacked and [uploaded almost 6.5 million LinkedIn passwords](#), according to The Verge. Though his claim has yet to be confirmed, Twitter users are already reporting that they've [found their hashed LinkedIn passwords on the list](#), security expert Per Thorsheim said.

38

comments



865



265



72



78

More +

CNET > News > Security & Privacy

Hackers post 450K credentials pilfered from Yahoo

Credentials posted in plain text appear to have originated from the Web company's Yahoo Voices platform. The hackers say they intended the data dump as a "wake-up call."



by Steven Musil | July 11, 2012 11:06 PM PDT

Follow

Yahoo has been the victim of a security breach that yielded hundreds of thousands of login credentials stored in plain text.

The hacked data, posted to the hacker site D33D Company, contained more than 453,000 login credentials and appears to have originated from the Web pioneer's network. The hackers, who said they used a union-based SQL injection technique to penetrate the Yahoo subdomain, intended the data dump to be a "wake-up call."



Stronger password (used for e-banking for instance)

Visual Pad (weak)

One time password (stronger)

- Calculator
- Password sheet

Two-factor authentication (better)

- Password (something you know)
- SMS code (something you own)