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, passphrase, secret key, secret handshake, secret questions ...

Something that you have

- ✓ IDs, badges, physical key, mobile phone ...

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"

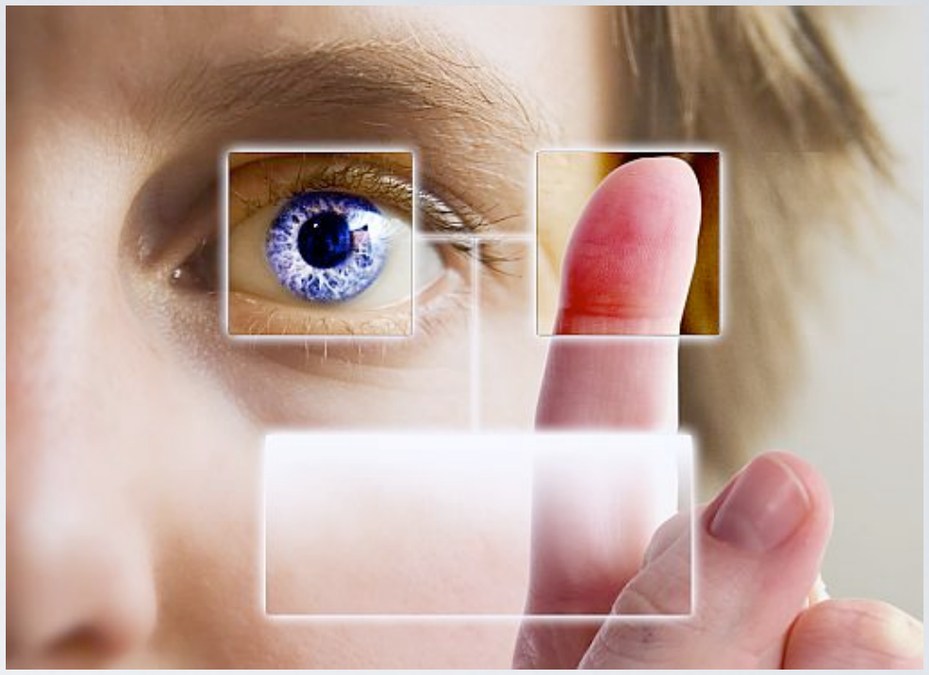
- ◉ **Gets compromised as soon as** someone can duplicate or fake the token

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	

Choosing the authentication mechanism

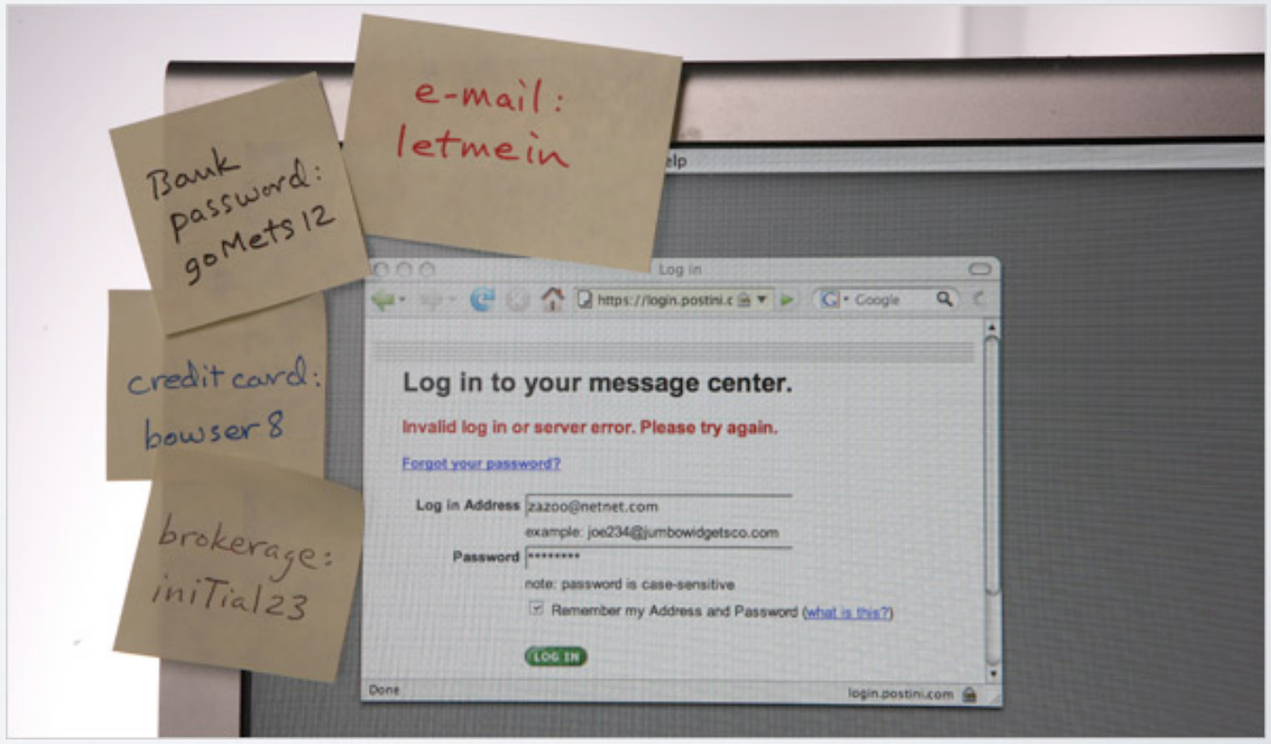
➡ Driven by the risk analysis and the costs
How hard is it to?

- 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 been delegate to a third party?
- Can we use the same identity over different information system?

➡ 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

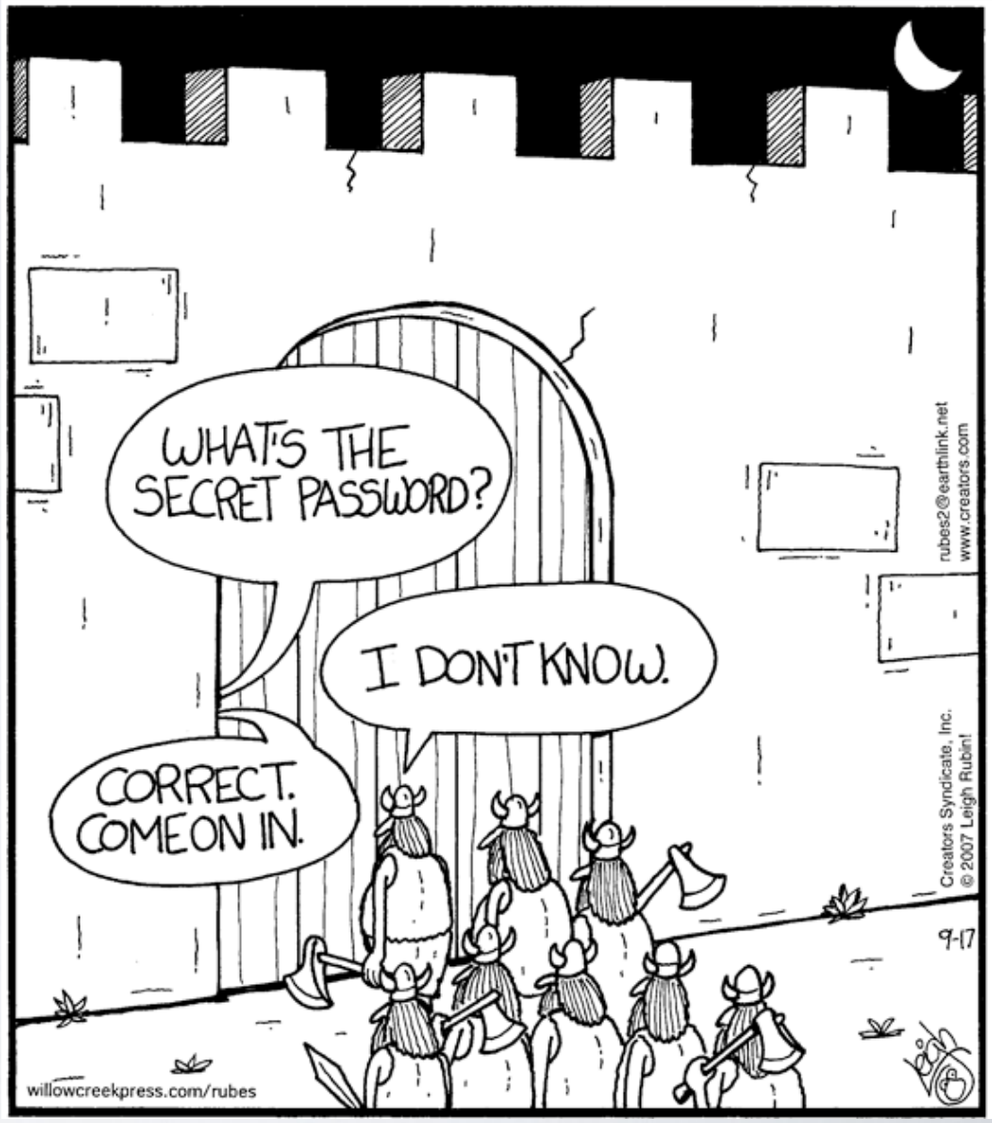
How to crack a password on challenge/response?

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

What are the counter-measures?

- Timing
- Limit number of tries

Tool : THC Hydra

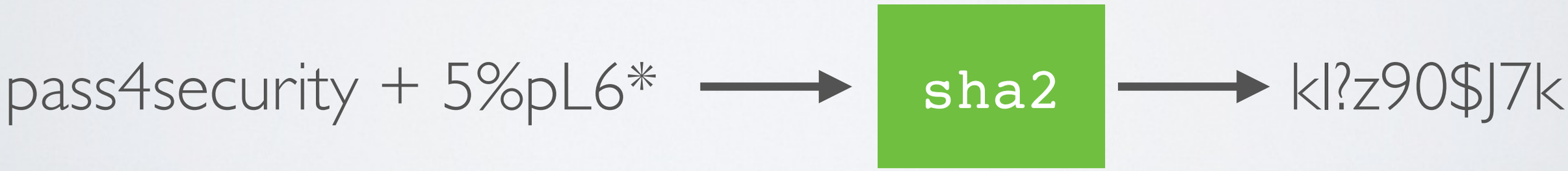


How passwords are stored

- **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, …)

Tools : John the Ripper, HashCat

Password Strength

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	57 minutes	2 hours	4 hours
6	Instantly	46 minutes	2 days	6 days	2 weeks
7	Instantly	20 hours	4 months	1 year	2 years
8	Instantly	3 weeks	15 years	62 years	164 years
9	2 hours	2 years	791 years	3k years	11k years
10	1 day	40 years	41k years	238k years	803k years
11	1 weeks	1k years	2m years	14m years	56m years
12	3 months	27k years	111m years	917m years	3bn years
13	3 years	705k years	5bn years	56bn years	275bn years
14	28 years	18m years	300bn years	3tn years	19tn years
15	284 years	477m years	15tn years	218tn years	1qd years
16	2k years	12bn years	812tn years	13qd years	94qd years
17	28k years	322bn years	42qd years	840qd years	6qn years
18	284k years	8tn years	2qn years	52qn years	463qn years

Time it takes a hacker to brute force your password in 2025

Hardware: 12 x RTX 5090
Password hash: bcrypt (10)

Hive Systems

Read more and download at
hivesystems.com/password

Check for yourself

How strong is your password?

https://www.security.org/how-secure-is-my-password/

Has your password been leaked?

https://haveibeenpwned.com/

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 PD

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.

CNET | News
Reviews | News | Download | CNET TV | How To | Deals

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 or mobile app code (something you own)

Newest Trends

Two-factor authentication

➡ Use a mobile phone or email to provide a one-time password

There are two standards

- HOTP (HMAC-based one-time password)
- TOTP (Time-based one-time password)

YubiKeys

Hardware device (USB and/or Bluetooth) to provide authentication

- Support one-time pad (HOTP or TOTP)
- Support digital signature (OpenPGP and PKCS#11)
- Compatible with WebAuthn

WebAuthn

The beginning of the end of the password

May 03, 2023

1 min read

For the first time, we've begun rolling out passkeys, the easiest and most secure way to sign in to apps and websites and a major step toward a "passwordless future."

C **Christiaan Brand**
Group Product Manager

S **Sriram Karra**
Senior Product Manager

Share

➡ Also called FIDO standard or **Passkeys**

Authentication based on

- Mobile phone's biometric features for user's authentication
- Trust-platform module (TPM) for managing public keys and signing credentials