Authentication

COMP620

Who are you?

- **Authentication** is the process of verifying that the user or system is who they claim to be.
- A system may be acting on behalf of a given principal.
- Authentication differs from **authorization** which is the process of verifying that an authenticated subject has the authority to perform a given action.

Means of Authentication

- What you know
- What you have
- Where you are
- What you are
- What you can do

Enter userid and password

- Most systems use simple authentication
- The first step is called identification. You announce who you are.
- The second step is called authentication. You prove that you are who you claim to be.

Problems with Passwords

- Authentication by password is widely accepted and not too difficult to implement.
- Managing password security can be quite expensive; obtaining a valid password is a common way of gaining unauthorised access to a computer system.
- Typical issues that need to be addressed:
  - how to get the password to the user,
  - forgotten passwords,
  - password guessing,
  - password spoofing,
  - compromise of the password file.

Authenticating a Remote User

- Do not give the password to the caller but call back an authorized phone number from your files
- Call back someone else, e.g. the caller's manager or local security officer
- Send passwords that are valid only for a single log-in request so that the user has to change immediately to a password not known by the sender
- Send mail by courier with personal delivery

Resetting Passwords

- When setting up a new user account some delay in getting the password may be tolerated.
- If you have forgotten your password but are in the middle of an important task you need instant help.
- The procedures for resetting a password are the same as mentioned previously, but now instant reaction is desirable.
  - In global organisations a hot desk has to be available round the clock.
- Password support can become a major cost factor
- Proper security training has to be given to personnel at the hot desk.

Guessing Passwords

- **Exhaustive search** (brute force): Try all possible combinations of valid symbols up to a certain length.
- **Dictionary attack** tries all passwords from an on-line dictionary.
- You cannot prevent an attacker from accidentally guessing a valid password, but you can try to reduce the probability of a password compromise.

Strong Passwords

- Password length: to slow down exhaustive search, prescribe a minimal password length
- Password format: mix upper and lower case symbols and include numerical and other non-alphabetical symbols in your password
- Long complex passwords are hard to remember
- A password can be composed of a sentence you can remember

Avoiding Brute Force Attacks

- Delay response to an incorrect password
- Lock out after *X* tries
  - Provides an opportunity for Denial of Service
- Store the passwords in encrypted form
- Do not allow access to the password file

Replay Threats

- Someone may be able to copy the data you send to a server to log in.
- Even if they cannot decrypt the data, they might be able to send it to the server themselves to log in.
- This can be prevented by using different encryption keys for each login session or by using secure authentication protocols.

11

Secure Authentication

- If the server and the client share an encryption key

Client	**Server**
Send ID & nounce1	
	Send encrypted nounce1& nounce2
Send encrypted nounce2	
	Send OK

Augmenting password logins

- Some sites display a personalized phrase when you are asked to enter your password
- If you do not see the correct phrase, you should not enter your password.
- The sites IP address can be used as part of the user authentication

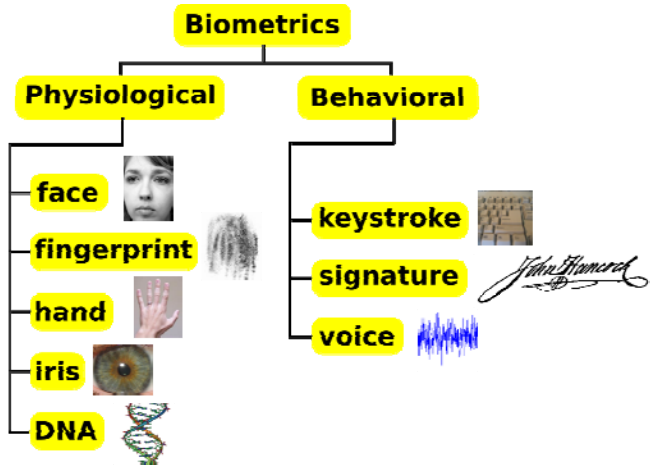
What You Have

- Users can be required to have a device to identify them
  - ID card
  - smartcard
  - USB with security file
- Should be used in conjunction with other authentication methods

Where You Are

- Some operating systems grant access only if you log on from a certain terminal.
  - Typically the IP address of the computer is used
- Global Positioning System (GPS) might be used to established the precise geographical location of a user during authentication

What You Are - Biometrics



What You Can Do

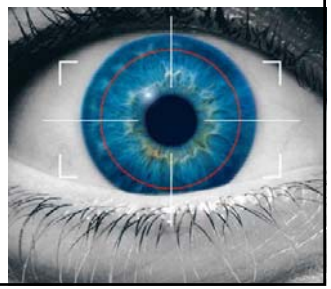
- People perform mechanical tasks in a way that is both repeatable and specific to the individual.
- Users could sign on a special pad that measures attributes like writing speed and writing pressure.
- On a keyboard, typing speed and key strokes intervals can be used to authenticate individual users.

Fingerprints

- Fingerprint readers are simple and inexpensive
- For most people they have high reliability
- Not every person has usable fingerprints

Iris Matching

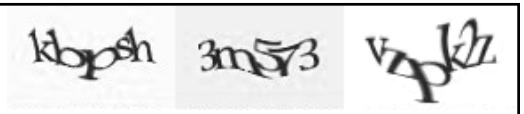
- Every person's iris is said to be unique
- You have to get a close image
- Better for authentication than recognition



Revoking Biometrics

- You can easily change your password if someone learns what it is.
- How do you change your fingerprint (or other biometric) if someone gets a copy?
- What if the biometric is unavailable?

Captcha



- "**C**ompletely **A**utomated **P**ublic **T**uring test to tell **C**omputers and **H**umans **A**part."
- A type of challenge-response test used to ensure that the response is not generated by a computer
- Sometimes described as a reverse Turing test
- The purpose is to keep automated systems from accessing systems designed for humans

Captcha Requirements

- Current software is unable to solve accurately
- Most humans can solve
- Does not rely on the type of CAPTCHA being new to the attacker.

Captcha Accessibility

- People with visual impairment may not be able to read a captcha
- Alternatives need to be available
  - Audio captchas have been used
  - "Common sense" questions such as "what color is the sky on a clear day?"
  - Image-recognition CAPTCHAs
  - Difficult to automatically generate

Captcha Circumvention

- Optical character recognition
- Human solvers
  - Human hacker is asked to solve captchas when a program cannot
  - Enticed users to solve captchas on a high traffic website owned by an attacker
- Circumvention of captchas may violate the anti-circumvention clause of the Digital Millennium Copyright Act