Authentication

COMP620 Information Privacy and Security

*"The whole notion of passwords is based on an oxymoron. The idea is to have a random string that is easy to remember. Unfortunately, if it's easy to remember, it's something nonrandom like 'Susan' And if it's random, like 'r7U2*Qnp,' then it's not easy to remember."*

Bruce Schneier

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

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 easy 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

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.

Popular Passwords

- The most popular passwords account for about 10% of all passwords used with 123456 representing about 3% of all passwords
- The top 10 all numerical PINs represent about 50% of all PINs used

1. 123456
2. Password
3. 12345678
4. qwerty
5. 12345
6. 123456789
7. letmein
8. 1234567
9. football
10. iloveyou

Initial Password Issues

- If you have access to a system, but did not create the userid yourself, there is the problem of getting the initial password to the user
- Some systems try to create an initial password with information that only you and the organization are expected to know
- Security of sending the password to the user depends on the security of the communications media

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.

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

Protecting the Password File

- The operating system maintains a file with user names and passwords
- An attacker could try to compromise the confidentiality or integrity of this password file
- Separate security relevant data from data that should be openly available.
  - In Unix, **`/etc/passwd`** contains both types of data

Storing the Password

- Instead of storing the password, many systems store the result of a one way function or hash of the password, such as SHA-1
- When a user enters a password, it is hashed and compared with the stored hash value
- If someone gets access to the password file, they still do not know the passwords

Improving Password Strength

- Don’t keep initial default passwords
- Make brute force difficult
  - Use long passwords
  - Use a large character set
  - Do not use words that may be in a dictionary
- Inform users of how many unsuccessful logins have been attempted since they last logged in

If an attacker has a list of passwords, they can determine the password from a list of hashed passwords.

A. True
B. False
C. All of the above
D. None of the above

Password Stealing on Public Computers

- An attacker runs a program that displays a fake login screen identical to the regular one
- A user comes to the computer and enters their userid and password to the fake login program
- The login program prints a fake bad password error
- The login program terminates and logs out presenting the user with the correct login screen

Password as an Encryption Key

- Assume a client and a server share a password
- Define a simple series of messages that can be sent between the client and the server to authenticate the client
- Consider using the password as a encryption key

- Work with 2 -3 students

Possible Solution

- Assume Alice wants to authenticate herself to Bob
- Both share a symmetric key

Alice → Bob: Alice, nonce

Bob → Alice: $\{nonce\}_{KeyAlice}$

Alice → Bob: $\{f(nonce)\}_{KeyAlice}$

Means of Authentication

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

Multifactor Authentication

- To be more secure, many systems require two or more types of authentication from the different categories
- Frequently users must have something and also enter a password

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

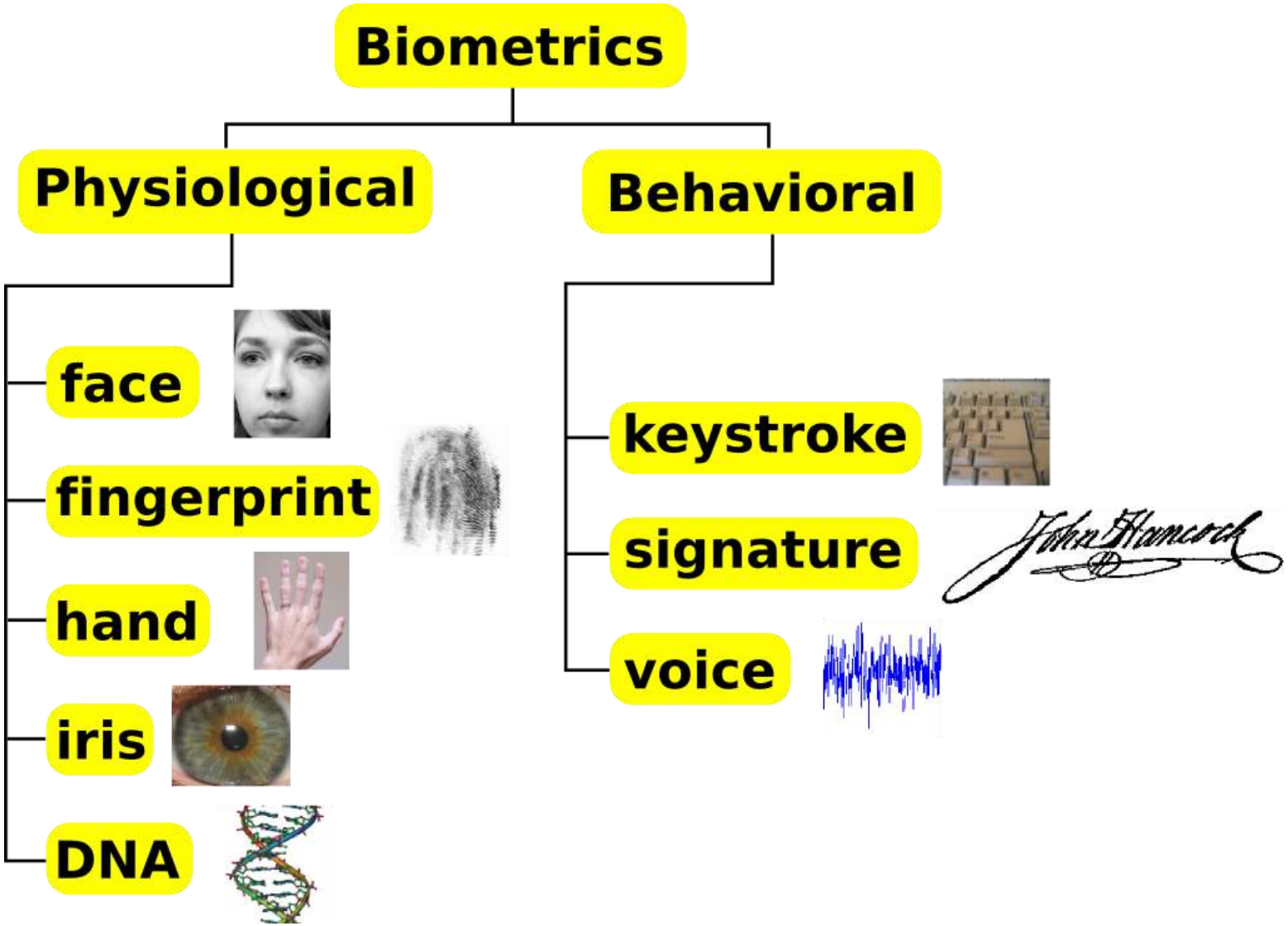
Where You Are

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

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

What You Are - Biometrics



Fingerprints

- Fingerprint readers are simple and inexpensive
- For most people they have high reliability
- Not every person has usable fingerprints
- Microsoft recently added the Fingerprint Logon Manager to Windows 10

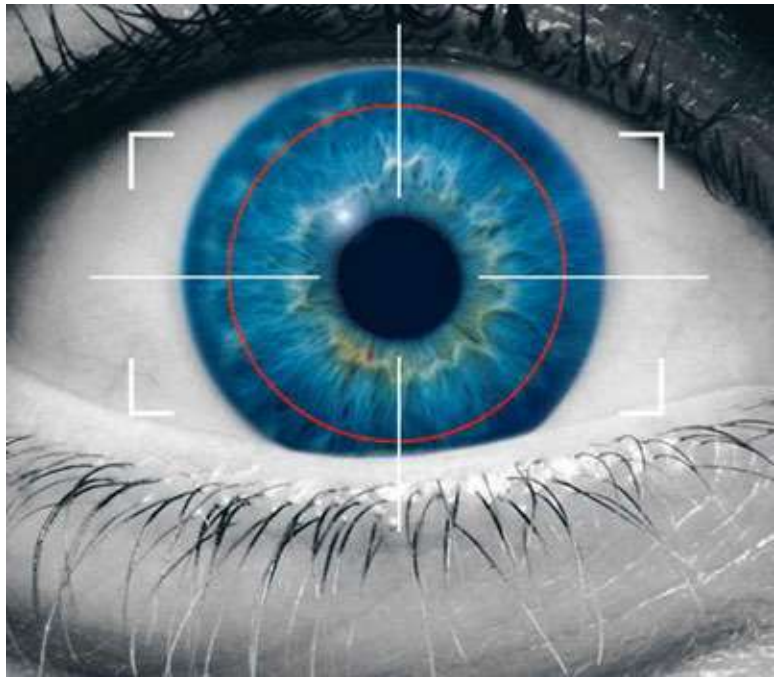
Your finger doesn’t have to be attached to your hand

Forged Fingers

- Fingerprints, and biometric traits in general, may be unique but they are no secret
- You are leaving your fingerprints in many places
- Rubber fingers that defeat most commercial fingerprint recognition systems can be fabricated quite easily
  - If authentication takes place in the presence of security personnel this would be a minor issue
  - When authenticating remote users additional precautions have to be taken to counteract this type of fraud
  - Gummy Bears and 3D printing have made fingerprint duplication easier
- User acceptance: so far fingerprints have been used to trace criminals

Iris Matching

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

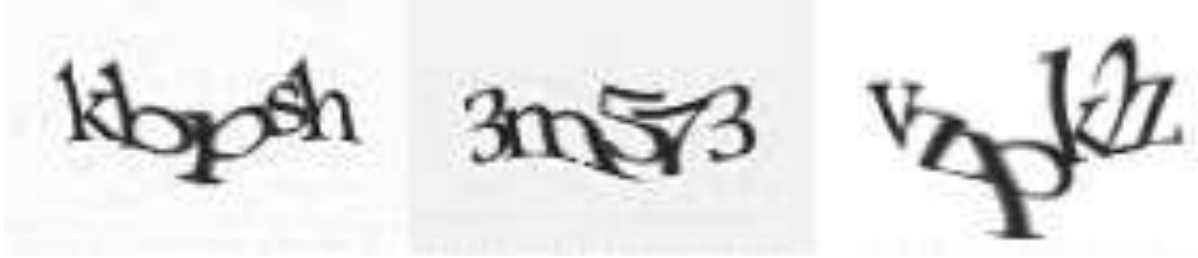


Revoking Biometrics

- 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

Research Subjects Needed

- A fellow graduate student needs subjects for an experiment on alternate password systems
- Participation requires:
  - two surveys which take about 4 minutes
  - reading a tutorial
  - logging into a system once a day for 9 days
- Participants will receive a **Starbucks Gift Card** for completing this study
- Email gridauthexperiment@gmail.com if you are interested