Chapter 2

Organizational Security

2.1 and 2.4 Password Selection

- **A Password is a word or string of characters used for user authentication to prove identity.**
- Computer intruders depend on poor passwords to gain unauthorized access to a system or network.

- Password Problems:
  1. Users choose passwords that are easy to remember and often choose the same sequence of characters as they have for their user IDs.
  2. Users also frequently select names of family members, their pets, or their favorite sports team for their passwords.

Example of Bad Password

- The following are examples of badly chosen passwords that can be easily guessed or cracked using password crackers freely available on the Internet.

1. "password" - the most easily guessed password
2. "administrator" - a login name
3. "cisco" - a vendor's name
4. "aaaaaaaa" - repeating the same letter
5. "abcdefgh" - consecutive letters
6. "23456789" - consecutive numbers
7. "qwertyui" - adjacent keys on the keyboard.
8. "computer" - a dictionary word
9. "computer12" - simple variation of a dictionary word

Component of Good Password

- Be at least ten characters.
- Longer usually means better. If you choose your characters wisely, you can make stronger passwords using fewer characters.
- Include a mix of lower case and upper case letters.
- Include at least one number
- Include at least one special character, Most English keyboards have over 30 special characters. When selecting special characters, try to use ones that are comfortable for you to type.
- If you will access a site on a device that does not have a keyboard, try using special characters your device supports.

Component of Good Password

- Dictionary words should be avoided.
- Internet searches for any part of the password should not return any meaningful results.
- Do not use series like abc or 123 or 321.
- Avoid character substitution (like P@$$W0RD) for dictionary words.
- Don't use recently used password.
- It should not be same as username.

Rules That Can Be Followed

- DON'Ts,

1. Do not use your login name in any form (as-is, reversed, capitalized etc.)
2. Do not use your first, middle or last name in any form.
3. Do not use your spouse's or child's name.
4. Do not use other information easily obtained about you. This includes ID card numbers, license numbers, telephone numbers, birth dates, the name of the street you live on, and so on.
5. Do not use a password that contains all digits, or all the same letters.
6. Do not use consecutive letters or numbers like "abcdefgh" or "23456789".

Component of Good Password

- Dictionary words should be avoided.
- Internet searches for any part of the password should not return any meaningful results.
- Do not use series like abc or 123 or 321.
- Avoid character substitution (like P@$$W0RD) for dictionary words.
- Don't use recently used password.
- It should not be same as username.

Rules That Can Be Followed

- DON'Ts,

1. Do not use your login name in any form (as-is, reversed, capitalized etc.)
2. Do not use your first, middle or last name in any form.
3. Do not use your spouse's or child's name.
4. Do not use other information easily obtained about you. This includes ID card numbers, license numbers, telephone numbers, birth dates, the name of the street you live on, and so on.
5. Do not use a password that contains all digits, or all the same letters.
6. Do not use consecutive letters or numbers like "abcdefgh" or "23456789".

7. Do not use adjacent keys on the keyboard like "qwertyui".
8. Do not use a word that can be found in an English dictionary.
9. Do not use a word in reverse that can be found in an English dictionary.
10. Do not use a simple variation of anything described in 1-10 above. Simple variations include appending or prepending digits or symbols, or substituting characters, like 3 for E, $ for S, and 0 for O.
11. Do not reuse recently used passwords.
12. Do not use the same password for everything; have one password for non-critical activities and another for sensitive or critical activities.

Password Protection

- Password is the main defense against intruders and hackers.
- Generally computers storing sensitive or important data are kept password protected.
- Multiuser system also contains username and password.
- The password provides authentication to the user ID of the person logging on to the system.
- The ID provides security in the following ways:
  1. The ID determines whether the user is authorized to gain access to a system.
  2. The ID determines the privileges given to the user.
- Security of important data can be break if someone steals your password.
- So there is a greater need to protect our password .

The Vulnerability of Passwords

- When password is stored only as plain texts, it is vulnerable(weak) to the attacks.
- Vulnerability is a weakness which allows an attacker to avoid system's security.
- There are two general classifications of password weakness:
- **Organizational or user weakness:**
- This includes lack of password policies in organization.
- Lack of security for user.
- **Technical weakness:**
- This includes weak encryption methods and unsecure storage of password on computer system.

The Vulnerability of Passwords

- A number of possible weakness arise from the use of password:
  - They could be guessed
  - They could be forgotten
  - They could be shared
- To avoid the problem with vulnerabilities , the password is first encrypted and stored in the password file.
- These password files are encrypted using key which is derived from password itself.
- For each password different key is generated. Then password is encrypted using DES algorithm.
- Encryption makes password invisible and prevents from brute force attack.

Password Selection Strategies

- If password is randomly selected than it would be hard to remember.
- If it is easily guessable than it would be cracked by an attacker.
- So the goal of password selection is, it should not be easily guessable and it should be easy to memorize.
- Different password selection strategies are:

1. **User education**
2. **Computer generated passwords**
3. **Reactive password checking**
4. **Proactive password checking**

1. User education:

- The user education policies tells user the importance of using hard to guess password and provides guidelines for selecting strong password.
- This policies makes user aware of easily guessed password and also tells them about strong password.
- Guidelines for selecting strong password are given to users.
- Like: use some capital letters in between or use some digits etc.
- This technique fails because many users don't follow the guidelines.

2. Computer generated passwords:

- This strategy let the computer to create password.
- If the passwords are quite random in nature, users will not be able to remember them.
- Even if the password is pronounceable, the user may have difficulty remembering it and so be attracted to write it down.
- In general, computer-generated password schemes have a history of poor acceptance by users.
- FIPS PUB 181 defines one of the best-designed automated password generators.

3. Reactive password checking:

- A reactive password checking strategy is one in which the system periodically runs its own password cracker to find guessable passwords.
- The system cancels any passwords that are guessed and notifies the user.
- Drawbacks are that it is resource intensive.
- Any existing passwords remain vulnerable until the reactive password checker finds them.

4. Proactive password checking:

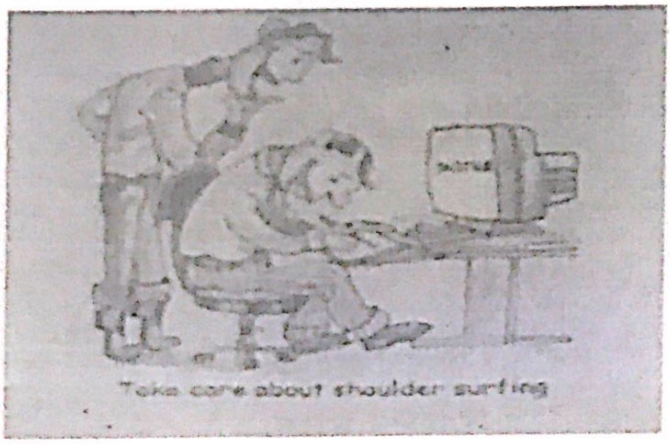
- The most promising approach to improved password security is a proactive password checker
- In this strategy a user is allowed to select his or her own password, but the system checks to see if it is allowable and rejects it if not.
- Sometime system may provide facility to select password which is easy to remember and still hard to crack.
- It also provides some guidelines for password selection.

2.1.1 Human Attacks

1. Shoulder surfing
2. Piggybacking
3. Dumpster diving
4. Installing unauthorized hardware and software
5. Access by non-employees

1. Shoulder Surfing

- It is direct observation technique, such as **looking over someone's shoulder to get information.**
- It is commonly used to obtain password, PINs, security codes and similar data.
- Shoulder surfing is a procedure in which attackers position themselves in such a way that they can observe the authorized user entering the correct access code.



1. Shoulder Surfing

- When a person types in his or her password, someone might be able to **see what is typed** and **steal the password** by looking over the person's shoulder, or by indirect monitoring using a camera.
- It is **effective in crowded places.**
- In crowded places, it is easy to observe following activities:
  - Fill a form
  - Enter password at cyber café
  - Enter a code at public place
  - Enter PIN number at ATM center.
- To avoid shoulder surfing, add cover to block the view of your access, be aware with your environment.

2. Piggybacking (Tailgating)

- Piggybacking is **"unauthorized entry" to a system by using an authorized person's access.**
- Here Attacker Follow The Authenticate User.
- Piggybacking is the way of **closely following a person who has just used an access card or PIN to get physical access** to a room or building.
- People are often in a hurry not follow good physical security procedures, Attackers know this and may attempt to exploit this characteristic in a human behavior.
- **Piggybacking can be done electronically and physically.**
- In electronic piggybacking , if user fails to terminate session than attacker takes advantage of active session.

2. Piggybacking (Tailgating)

- In physical piggybacking, person follow authorized user to get entry in restricted area.
- An attacker slip behind legal employee and gaining access to a secure area which needs some type of biometric or any security.
- It is one of the form of social engineering attack.

Prepared By: Chirag Patel, KDP, Patan

3. Dumpster Diving

- Dumpster Diving is **the process of digging through a company's trash bins or dumpsters to gain information.**
- **Attackers need some information before launching an attack**, A common place to find this information is to go through the target's trash.
- If the attackers are fortunate and the target's security procedures are very poor, attackers may find user ids and passwords.

3. Dumpster Diving

- In Dumpster Diving ,the Attackers or Hackers are looking for,
  1. Phone List
  2. Memos
  3. Policy Manuals
  4. Calendars of event
  5. System Manuals
  6. Print Outs
  7. Disk Tapes, CD,DVD
  8. Old hard drives
- Many people forget to erase or destroy the stored information completely from the waste materials and attackers use those information.
- The Best thing about this is that is LEGAL!
- To avoid it, sensitive material or information should be burnt or torn before going for waste.

4. Installing unauthorized hardware and software

- Organizations should have a policy to restrict normal users from installing software and hardware on their systems.
- Example:
  - A user Install games on their System, Unfortunately not all games come in a wrapped packages.
  - The Problem is That user don't always know where the software originally came from and what may be inside it.
  - Many individuals have innocently installed what seemed to be an safe game, but a piece of malicious code attached to game can do many things.
  - It includes opening a backdoor that allows attackers to connect to and control the system from the internet.
- Because of these, Many organizations do not allow their users to load software or install new hardware without the knowledge of administrators.

5. Access by Non-employees

- If an attacker gains access to a facility, there are chances of obtaining enough information to enter in computer systems and networks.
  - Many organizations require employees to wear identification badges at work.
  - This method is easy to implement and may be a warning to unauthorized individuals.
  - Only legal employees should be allowed to use resources in their proper time.

2.2 People as a Security Tool

1. Security Awareness

- Organizations can counter potential social engineering attacks by conducting an active security awareness program for the organization's security goals and policies.
  - The training will vary depending on the organization's environment and the level of threat.
- An important element that should be stressed in the training on social engineering is the type of information that the organization considers sensitive and that may be the target of a social engineering attack.

2. Individual User Responsibilities

- Certain responsibilities that should be adopted by all users include,
  1. Locking the door to the office or workspace.
  2. Not leaving sensitive information unprotected inside the car.
  3. Securing storage media containing sensitive information.
  4. Tearing paper containing organizational information before discarding it.
  5. Don't give sensitive information to unauthorized individuals.
  6. Not discussing sensitive information with family members.
  7. Protecting laptops that contain sensitive or important organization information.
  8. Being aware of who is around when discussing sensitive corporate information.
  9. Enforcing good password security practices, which all employees should follow.
  10. Cultivating an environment of trust in the office and an understanding of the importance of security.

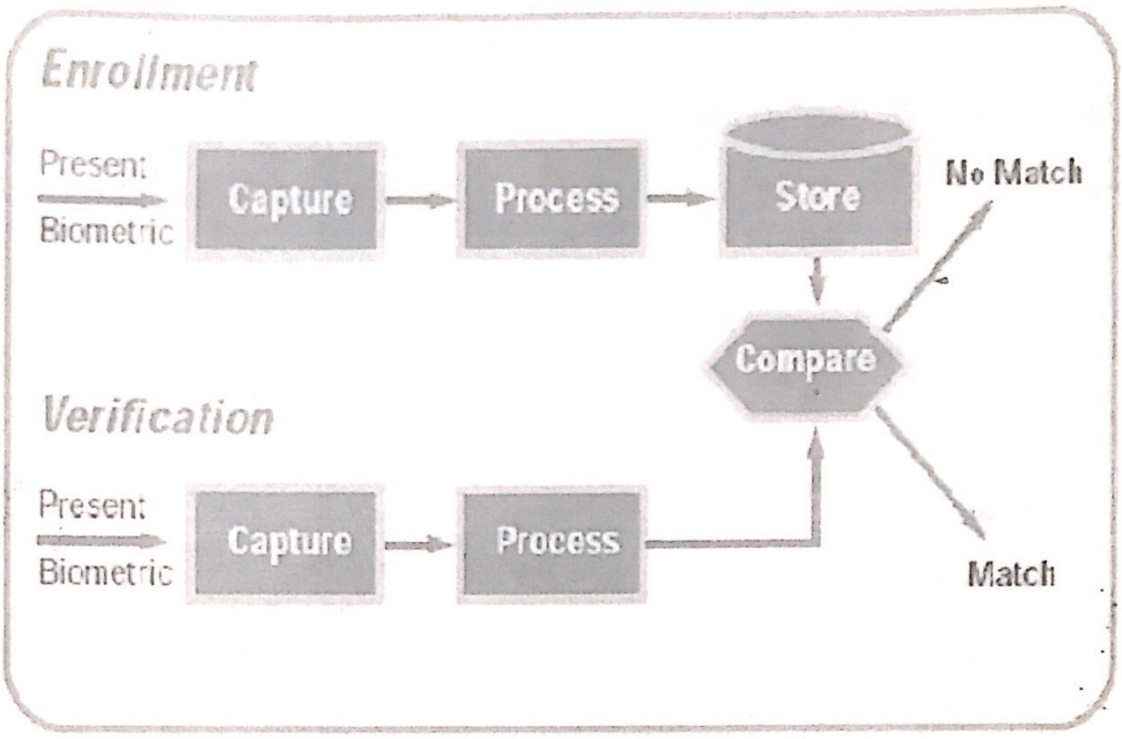
2.3 Physical Security

- Physical security is the protection of Data, Software, Hardware or Any Network from physical attacks or physical events that could cause serious damage to Organization.
- The main goal physical security is to provide a safe environment to the organization.
- **Access Control:**
  - It Restrict the entry and exit of personal (often equipment and media) from an area, such as an office, data center, or Room containing LAN server.
  - Locks and login credentials are two mechanisms of access control.
  - Traditional access control systems provide a proximity card or a smart card to gain access to a protected resource.

Biometrics

- **Biometric is the science and technology of measuring and analyzing biological data.**
- Biometric technologies **measure and analyze human body characteristics**, such as **DNA, finger print, eye retinas, voice and face recognition etc.**
- Those characteristics are then used for authentication.

- Working of biometric system,



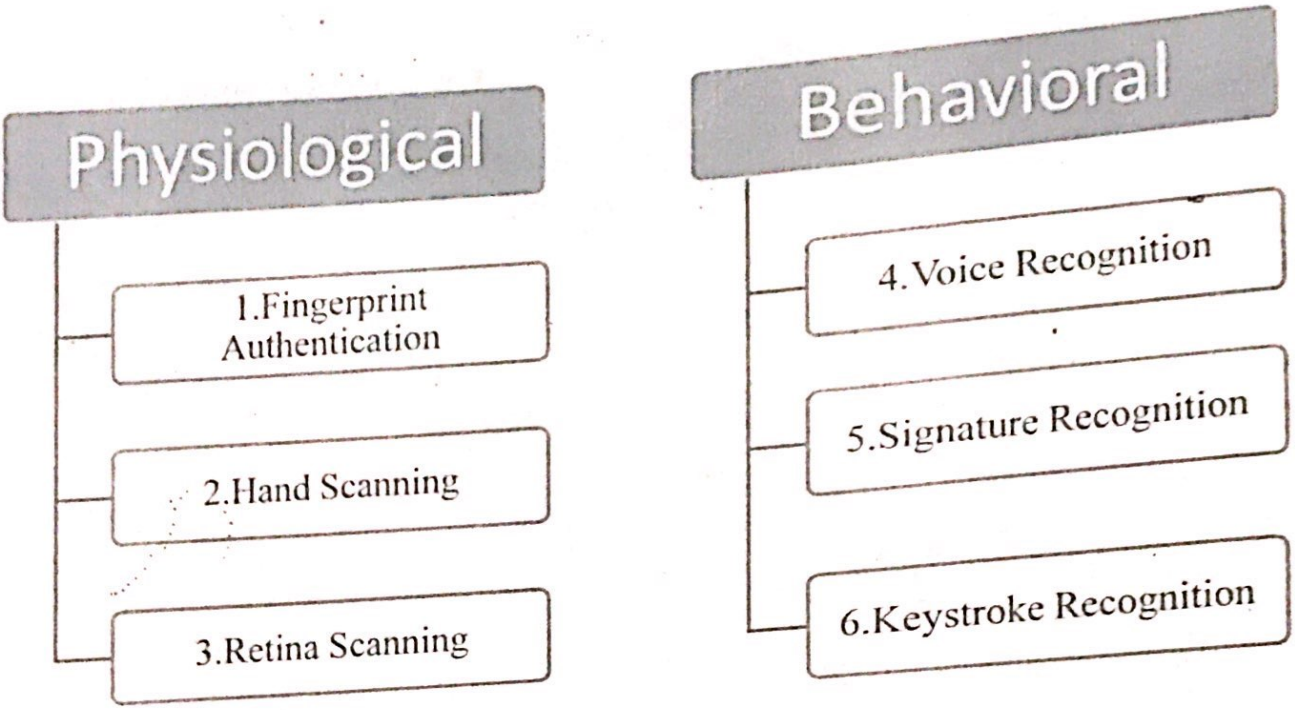
- The Process are done in following steps,

1. The Biometric sensor **capture** the users physiological or behavioral characteristic pattern, this pattern is captured and sent to the Processing Module.

2. **Processing** Module performs a comparison between the biometrics pattern **stored** in the database and the information pattern just received from the sensor.

3. Results are then transmitted to the application which grants or denies access based upon the results of the comparison.

Biometrics Techniques

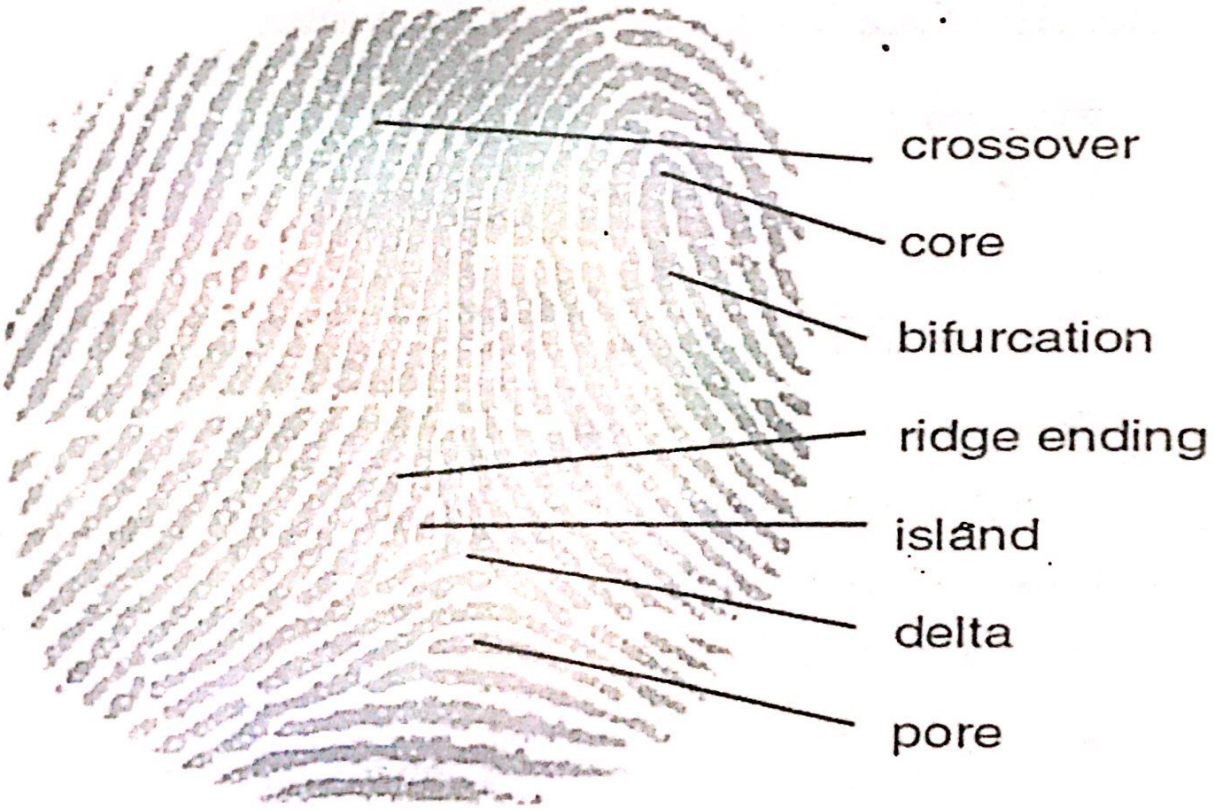


1.Fingerprint Authentication

- **"Fingerprint authentication"** describes the **process of finding a digital representation of a fingerprint** and **comparing it** to a stored digital version of a fingerprint.
- Everyone have **unique finger print**.
- Electronic fingerprint scanners capture digital "pictures" of fingerprints.
- These pictures are then **processed into digital templates** that contain the **unique extracted features** of a finger.

1.Fingerprint Authentication

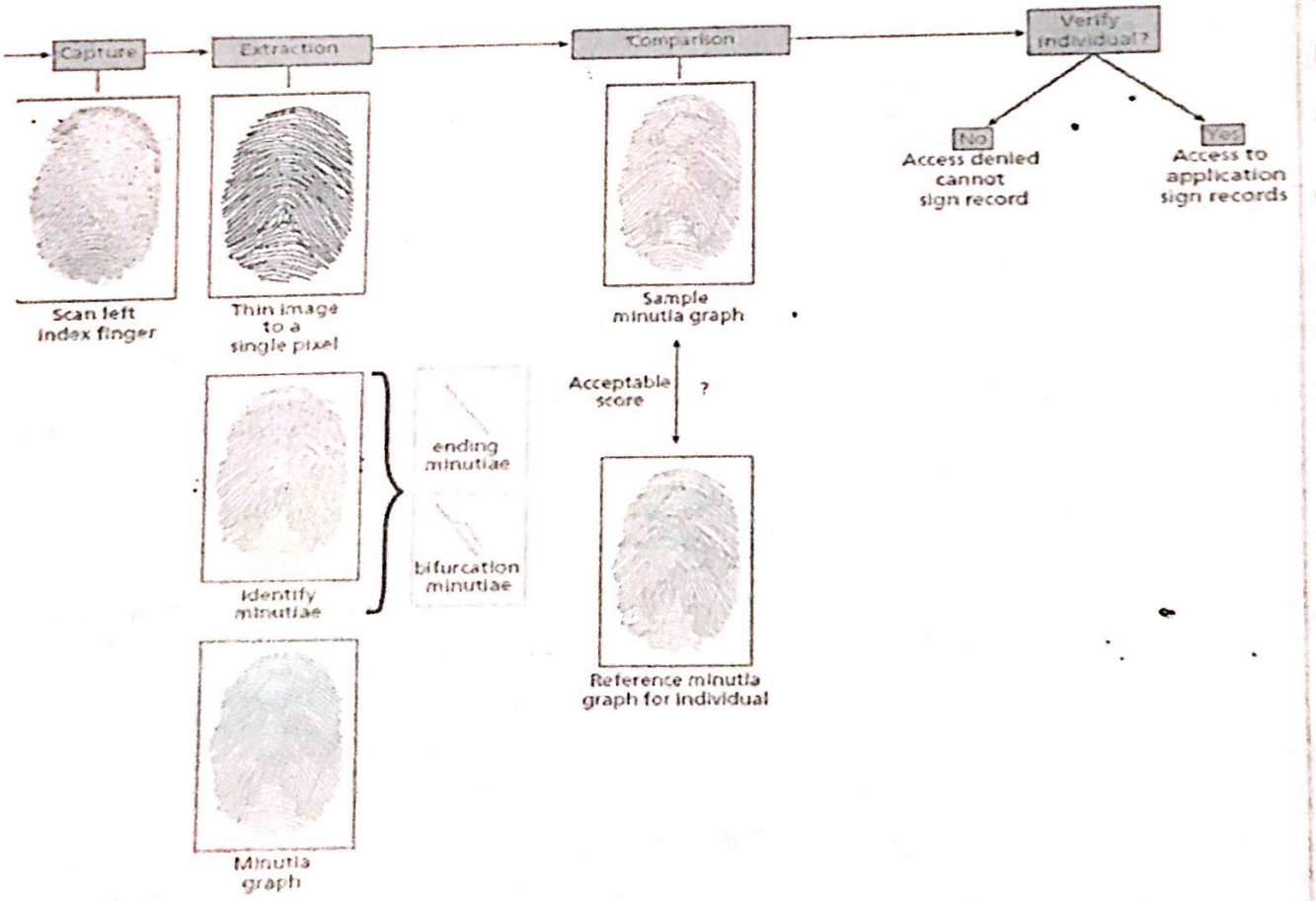
- These digital fingerprint templates can be stored in databases and used in place of traditional passwords for secure access.
- Instead of typing a password, users place a finger on an electronic scanner. The scanner compares the live fingerprint to the fingerprint template stored in a database to determine the identity and validity of the person requesting access.



Prepared By: Chirag Patel, KDP, Patan

- **Minutiae**
  - Uses the ridge endings and bifurcation's on a persons finger to plot points known as Minutiae.
  - The number and locations of the minutiae vary from finger to finger in any particular person, and from person to person for any particular finger.

Finger Image | Finger Image + Minutiae | Minutiae



Fingerprint scanning (Minutiae based approach)

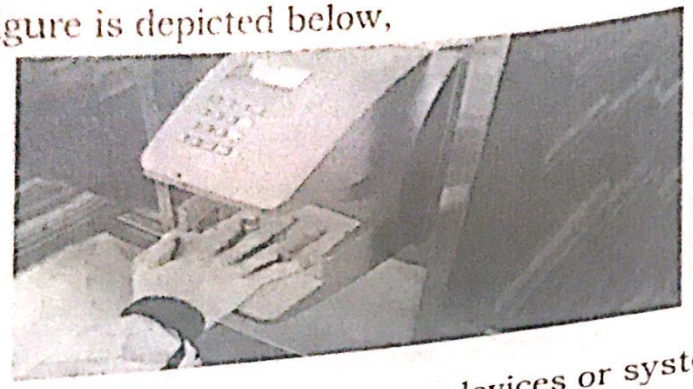
- Advantages:
  1. High Accuracy
  2. Easy to use
  3. Mature technology
  4. Small Storage space required of biometric template which is stored in database
  5. Low cost

- Disadvantages:
  1. It can make mistake with the dryness or dirty figures skin.

2. Hand scanning

- Hand geometry systems are commonly available in two main forms.
- Full hand geometry systems take an image of the entire hand for comparison.
- Two Finger readers take only image of two fingers of the hand.
- Usually a specialized reader device to measure parts such as length, width, thickness, and surface area of the hand and fingers.
- Hand recognition technology is currently one of the most installed biometrics discipline.

- The Basic figure is depicted below,



- Advantages:
  1. It Can be easily integrated into other devices or systems.
  2. Relatively simple.

- Disadvantages:
  1. Very Expensive
  2. It is not valid for arthritic person.

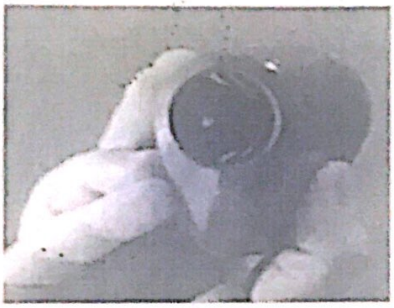
- Application:
  1. Widely used for identification and verification in criminal activities.
  2. Used in security access application.

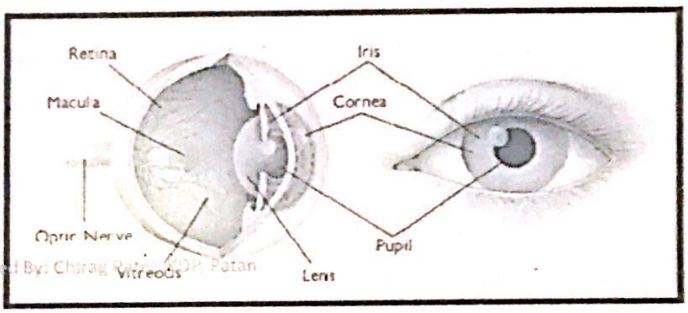
3. Retina scanning

- Retinal Scan technology is based on **the blood vessel pattern** in the retina of the eye and it provides unique basis for identification.
- The pattern of blood vessels that spread out from the optic nerve and spread throughout the retina depends on individuals and never changes.
- No two retinas are the same, even in identical twins, Exceptions include diabetes and infectious diseases.
- The Technique that is used are shown below,

Technique

- Step1:
  - Person looks into a focusing camera at close range for several seconds.
- Step 2:
  - Low power InfraRed Waves (~7mW) is directed into the pupil .
- Step 3:
  - Resulting picture is captured by the camera
- Step 4:
  - Image processing filters out relevant feature points.
- Step 5:
  - Pattern is matched against stored templates.





3. Retina scanning

- Advantages:
  1. Very High Accuracy
  2. There is no known way to replicate a retina.
- Disadvantages:
  1. Very Expensive
  2. Time consuming process.
  3. Inconvenient for persons with eyeglasses
- Application:
  1. UID aadhar authentication.
  2. Secure identity management.

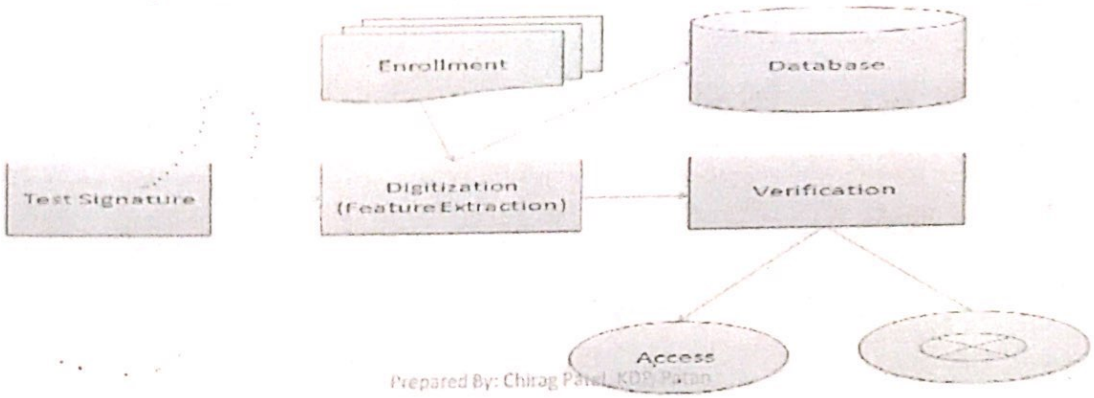
4. Voice Recognition

- Voice Recognition is method that examines the unique characteristics of user's voice.
- In it, a telephone or microphone can be used as server. It makes it relatively cheap and easily deployable technology.
- How Voice Recognition is Performed??
  - The first step is for the user to speak into a microphone.
  - The electrical signal from the microphone is converted in to digital data by an "analog-to-digital (A/D) converter", and is stored in memory.
  - To check voice input, the computer try to match the input with a digital voice sample, or template stored in memory.
- Sometimes there may be a problem with performance due to noise effect.

- Advantages:
  1. High Social Acceptability
  2. Low cost
  3. Usable over existing telephone system
  4. Good for remote access and monitoring
  5. Verification is about five seconds
- Disadvantages:
  1. Less Accuracy
  2. A persons voice can be easily recorded and used for authentication.
  3. The human voice's tremendous variability, due to colds etc.
- Applications:
  1. Generally used in automated phone system.
  2. Can be used in services like google voice etc.

5. Signature Recognition

- Signature Verification is a method of examining an individual's hand written signature.
- The technology examines the behavioral components of the signature such as speed, direction, pressure of writing, time that the stylus is in and out of contact, total time of signature etc.
- Its least reliable technique of identification.
- Forgers may have many ways to reproduce duplicate signature.
- The basic process are shown below,



- Advantages:
  1. High Social Acceptability
  2. Low cost
  3. Verification is about five seconds

- Disadvantages:
  1. Less Accuracy
  2. Chance of reproduction of the signature.

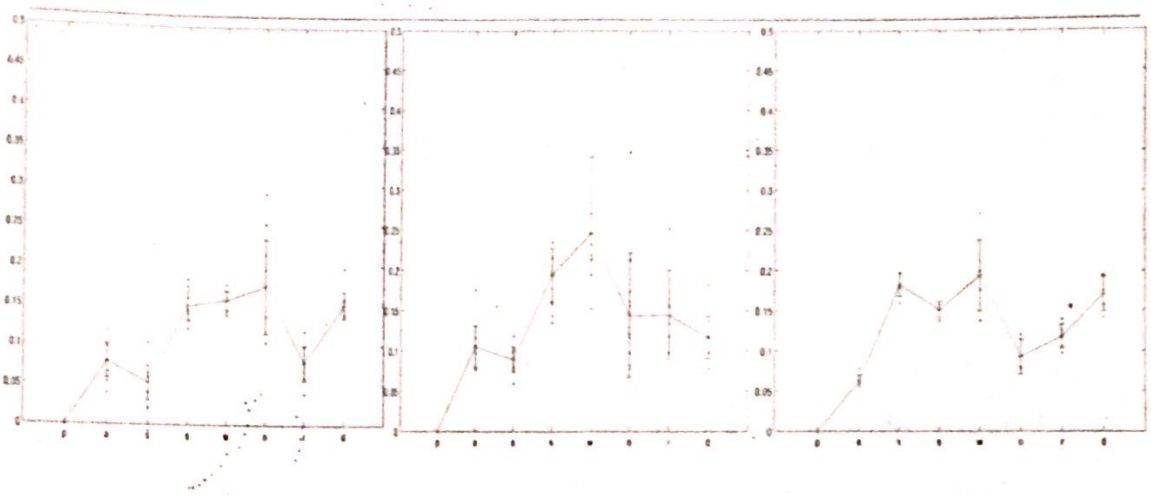
- Application:
  1. Used for authentication at banking places.
  2. Also used in medical science.

6. Keystroke Recognition

- Keystroke dynamics is a biometric based on guess that **different people type in uniquely characteristic manners.**
- The way and the manner in which we type on our computer keyboard varies from individual to individual and is considered to be a unique behavioral biometric.
- This technology identifies people based on dynamics like- speed and behavior of typing, total timing for typing particular password, user taking time between hitting certain keys etc.
- Keystroke Recognition is probably one of the easiest biometrics forms to implement and manage because there is no need to install any new hardware and even software.

- **Features:**
  - **Often used**
    - Latency between keystrokes
    - Duration of keystroke, hold-time
  - **Rarely used**
    - Overall typing speed
    - Frequency of errors
    - Habit of using additional keys (numpad etc)
    - Capital letters (order of releasing shift and letter)
    - Force of hitting keys (special keyboard needed)

- **Example:**
  - Inactivity between keystrokes when writing "password" by three persons



- Advantages:
  1. High Social Acceptability
  2. Low cost
  3. It uses existing hardware

- Disadvantages:
  1. Less Accuracy

- Application:
  1. Generally used for authentication purpose together with user id/password.
  2. It is also used in specific form of investigation.

Physical Barrier

- Physical barriers are used in physical security to define boundaries, prevent access and restrict particular area.
- We should select and install proper barriers to keep attackers out.
- Two general types of barriers are there,
  1. Manmade barriers
  2. Natural barriers
- Manmade barriers includes fences and walls, doors, gates, sealing etc.
- Natural barriers include rocks, forests, water features etc., that are difficult to cross or difficult to attack.
- Barriers must be tested and maintained regularly.

Prepared By: Chirag Patel, KDP, Patan

ASSIGNMENT -2
Semester- 5
Subject: Computer and Network Security(3350704)
Computer Department, KDP, Patan

UNIT - 2 : Organizational Security Date:

NO.	QUESTIONS	MARKS	YEAR						
1	Define: Biometrics.	2			2016		2018		
2	List various methods of Biometrics Access. Explain any two in Brief.	4				2016		2018	
3	What is Biometrics ? write a short note on finger prints.	4	2014				2018		
4	Write short note on Piggybacking.	3		2015	2016	2017	2018		
5	Write short note on Dumpster diving.	3		2015	2016		2018		
6	Explain Shoulder surfing.	3		2015	2016		2018		
7	Write a component of a good password. Or list out component of good password.	2	2014	2015					
8	Explain components of a good password.	4			2016		2018		
9	List out password selection strategies. Or identify different password selection strategies.	2				2016	2017	2018	
10	Explain" computer generated passwords" selection strategy.	3	2014						
11	Describe password and Explain characteristic of good password.	3			2016				
12	Explain password protection.	3		2015					2018

C. D. PATEL
Lecturer,
Computer department.