Physical and Biometric security

Access Control

- Two parts to access control…
- **Authentication:** Are you who you say you are?
  - Determine whether access is allowed or not
  - Authenticate human to machine
  - Or, possibly, machine to machine
- **Authorization:** Are you allowed to do that?
  - Once you have access, what can you do?
  - Enforces limits on actions
- Note: "access control" often used as synonym for authorization

Objectives

- Distinguish between logical and physical security, and explain the reasons for placing equal emphasis on both
- Recognize the importance of the Physical Security domain
- Outline the major categories of physical security threats

Objectives cont.

- Classify the techniques to mitigate risks to an organization’s physical security
- Classify the five main categories of physical security controls
- Identify how to use smart cards for physical access control
- Categorize the different types of biometric access controls and determine their respective strengths and weaknesses

Introduction

- To protect logical systems, the hardware running them must be physically secure
- Physical security deals with who has access to buildings, computer rooms, and the devices within them

Understanding the Physical Security Domain

- Four focus areas
  - How to *choose a secure site* (location) and guarantee the correct design
  - How to *secure a site* against unauthorized access
  - How to *protect equipment* against theft
  - How to *protect the people and property* within an installation

Physical Security Threats

- **Weather:** Tornadoes, hurricanes, floods, fire, snow, ice, heat, cold, humidity, and so forth
- **Fire/chemical:** Explosions, toxic waste/gases, smoke, and fire
- **Earth movement:** Earthquakes, and mudslides
- **Structural failure:** Building collapse because of snow/ice or moving objects (cars, trucks, airplanes, and so forth)
- **Energy:** Loss of power, radiation, magnetic wave interference, and so forth
- **Biological:** Virus, bacteria, infestations of animals or insects.
- **Human:** Strikes, sabotage, terrorism, and war

Providing Physical Security

- Five Areas of Physical Security
  - Educating personnel
  - Administrative controls
  - Physical security controls
  - Technical controls
  - Environmental/Life-safety control

Educating Personnel

- An educated staff is the best weapon a company can have against illegitimate and accidental acts by others
  - Being mindful of physical and environmental considerations required to protect the computer systems
  - Adhering to emergency and disaster plans
  - Monitoring the unauthorized use of equipment and services
  - Recognizing the security objectives of the organization
  - Accepting individual responsibilities associated with their own security as well as the equipment they use

Administrative Access Controls

- Restricting Work Areas
- Escort Requirements and Visitor Control
- Site Selection
  - Visibility
  - Locale considerations
  - Natural disasters
  - Transportation

Physical Security Controls

- **Perimeter Security Controls**
  - Controls on the perimeter of the data center are designed to prevent unauthorized access to the facility
  - Include gates, fences, turnstiles, and mantraps
- **Badging**
  - The photo identification badge is a perimeter security control mechanism that not only authenticates an individual but also continues to identify the individual while inside the facility
- **Keys and Combination Locks**
  - Keys and combination locks are the least complicated and least expensive devices

Physical Security Controls

- **Security Dogs**
  - Dogs are a highly effective and threatening perimeter security control when handled properly and humanely
- **Lighting**
  - Lighting is another form of perimeter protection that discourages intruders or other unauthorized individuals from entering restricted areas

Technical Controls

- The more prominent technical controls include
  - Smart/Dumb cards
  - Audit trails/access logs
  - Intrusion detection
  - Biometric access controls

Technical Controls cont.

- Smart Cards
  - Similar to a credit card but it has a semiconductor chip
  - The smart card has many purposes
    - Storing value for consumer purchases
    - Medical identification
    - Travel ticketing and identification
    - Building access control
  - The smart card can facilitate file encryption and digital signature
  - The use of smart cards with biometrics authentication can be extremely effective

Technical Controls cont.

- Audit Trails/Access Logs
  - Should contain
    - The user ID or name of the individual who performed the transaction
    - Where the transaction was performed
    - The time and date of the transaction
    - A description of the transaction—what function did the user perform, and on what
  - The retention period of the audit logs, recovery time, and the integrity of the data must also be considered and the logging system designed appropriately.

Technical Controls cont.

- Intrusion Detection
  - **Perimeter intrusion detectors**
    - These devices are based on dry contact switches or photoelectric sensors. An alarm is set off when the switches are disturbed or the beam of light is broken
  - **Motion detectors**
    - These devices detect unusual movements within a well-defined interior space, including
      - Wave pattern detectors that detect changes to light-wave patterns
      - Audio detectors that passively receive un-usual sound waves and set off an alarm

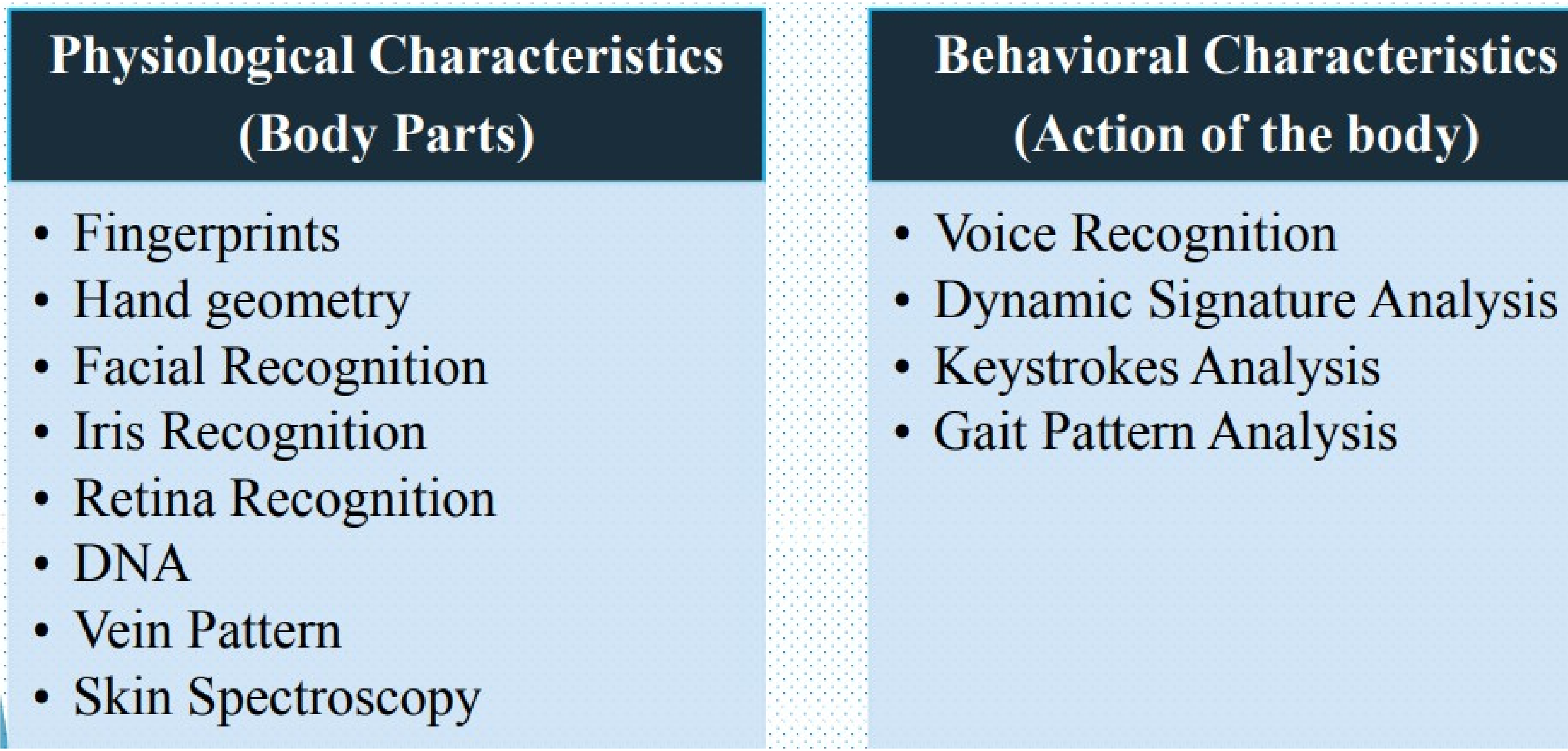
Technical Controls cont.

- Alarm systems
  - Sets off an alarm to alert guard on the premises or in a remote location
- Biometrics
  - Biometrics authentication uses physiological or behavioral characteristics such as the human face, eyes, voice, fingerprints, hands, signature, and even body temperature
  - Biometric is data stored and used for the authentication procedure

Environmental/Life-Safety Controls

- The three most critical areas are
  - Power (electrical, diesel)
  - Fire detection and suppression
    - Fire types
    - Fire detectors
    - Fire-extinguishing systems
  - Heating, ventilation, and air conditioning (HVAC)

Biometric



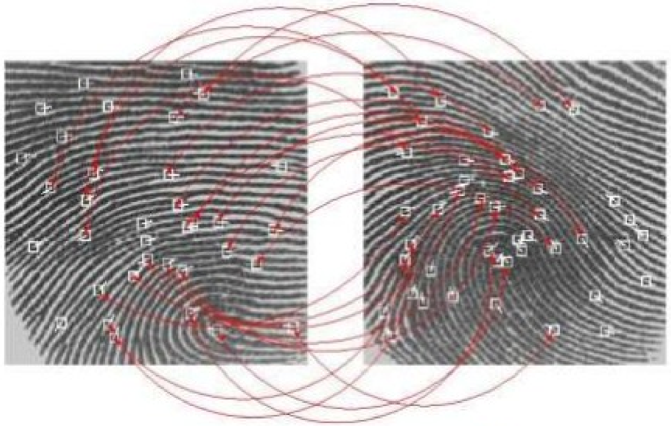
Physiological Characteristics (Body Parts)	Behavioral Characteristics (Action of the body)
• Fingerprints	• Voice Recognition
• Hand geometry	• Dynamic Signature Analysis
• Facial Recognition	• Keystrokes Analysis
• Iris Recognition	• Gait Pattern Analysis
• Retina Recognition	
• DNA	
• Vein Pattern	
• Skin Spectroscopy	

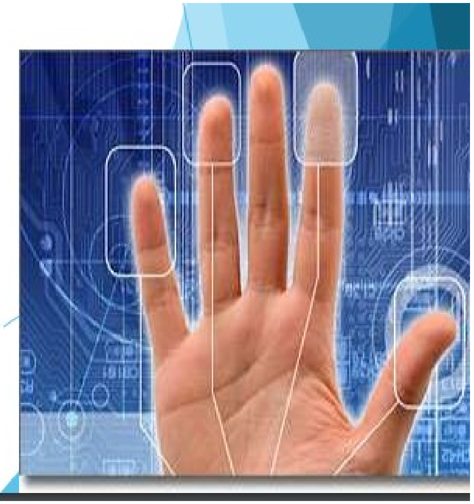
Fingerprint recognition

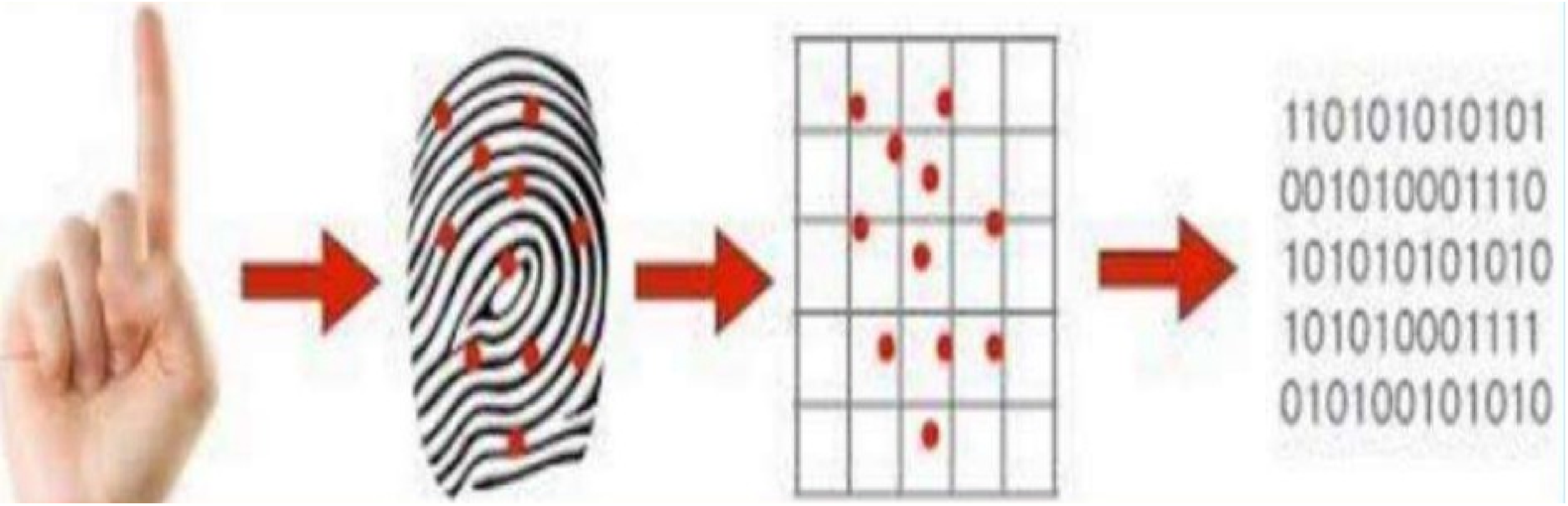
Level 1 : Identify the pattern of Fingerprint

Level 2 : Based on ridge characteristics i.e. ridge minutiae

Level 3 : Based on shape, size of ridges and pores

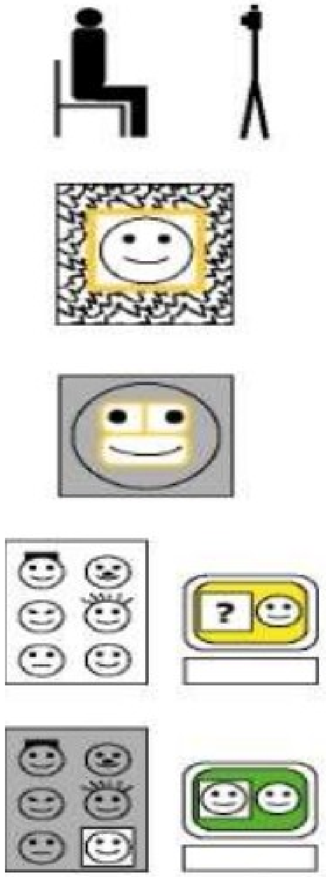


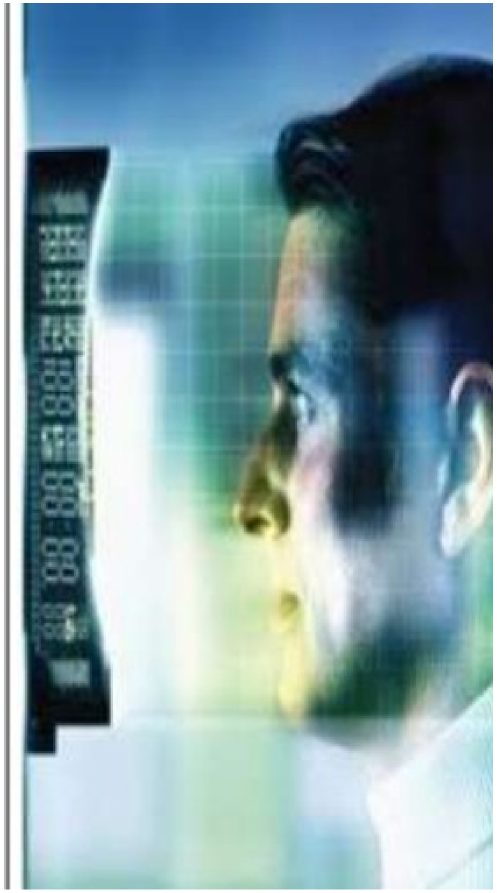



110101010101
001010001110
101010101010
101010001111
010100101010

Face Recognition

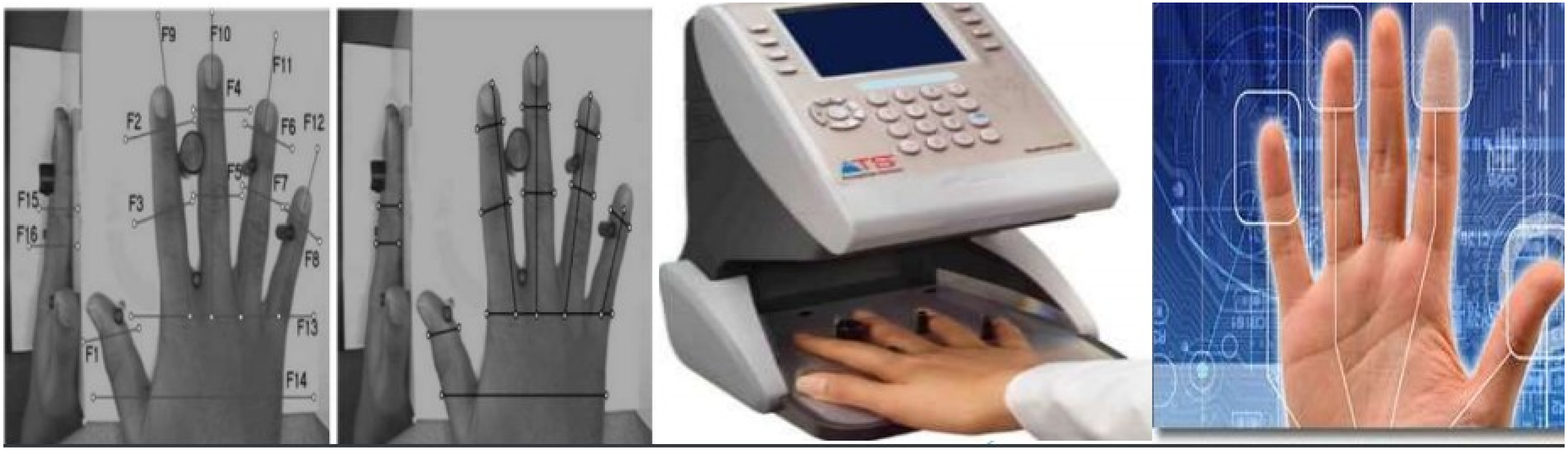
- Capture Image
- Find Face in Image
- Features Extract (store template)
- Compare Template
- Declare Match





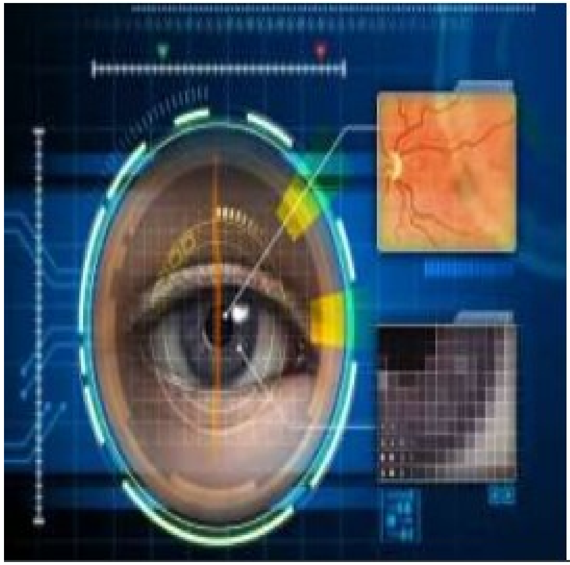
Hand Geometry

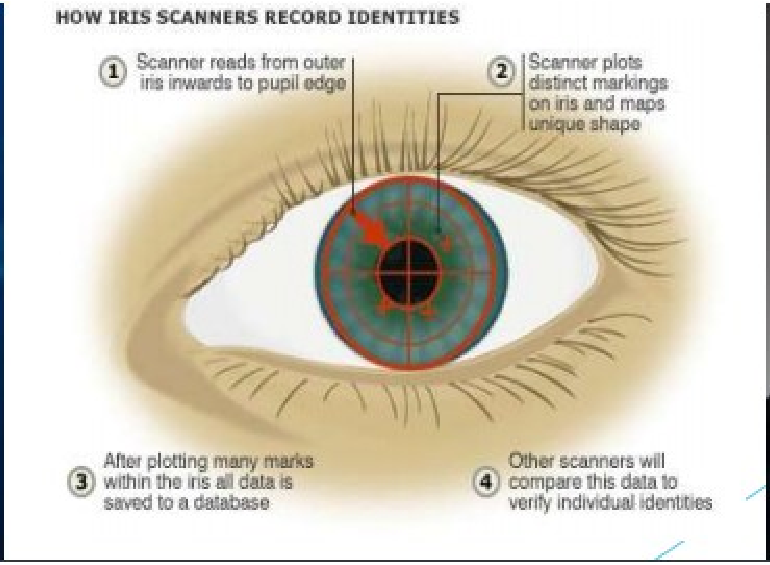
- Hand or fingers geometry is an automated measurement of many dimension of hand and fingers.



Iris Recognition

- Iris scanning measures the iris pattern in the colored part of the eye.

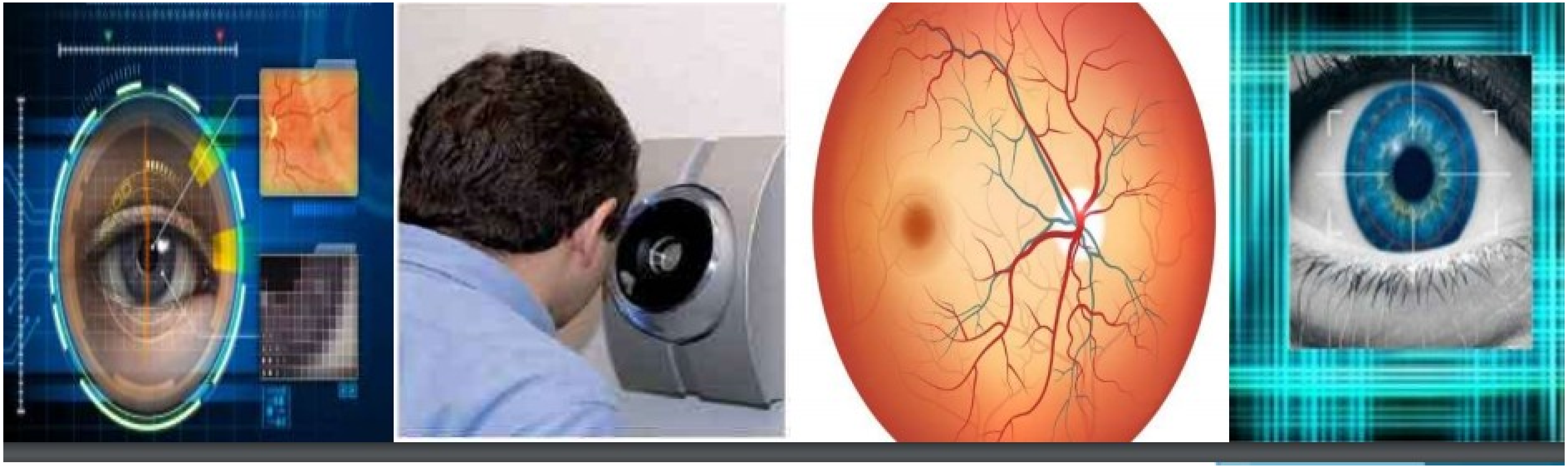




HOW IRIS SCANNERS RECORD IDENTITIES
1 Scanner reads from outer iris inwards to pupil edge
2 Scanner plots distinct markings on iris and maps unique shape
3 After plotting many marks within the iris all data is saved to a database
4 Other scanners will compare this data to verify individual identities

Retina Recognition

- Images back of the eye and compare blood vessels with existing date

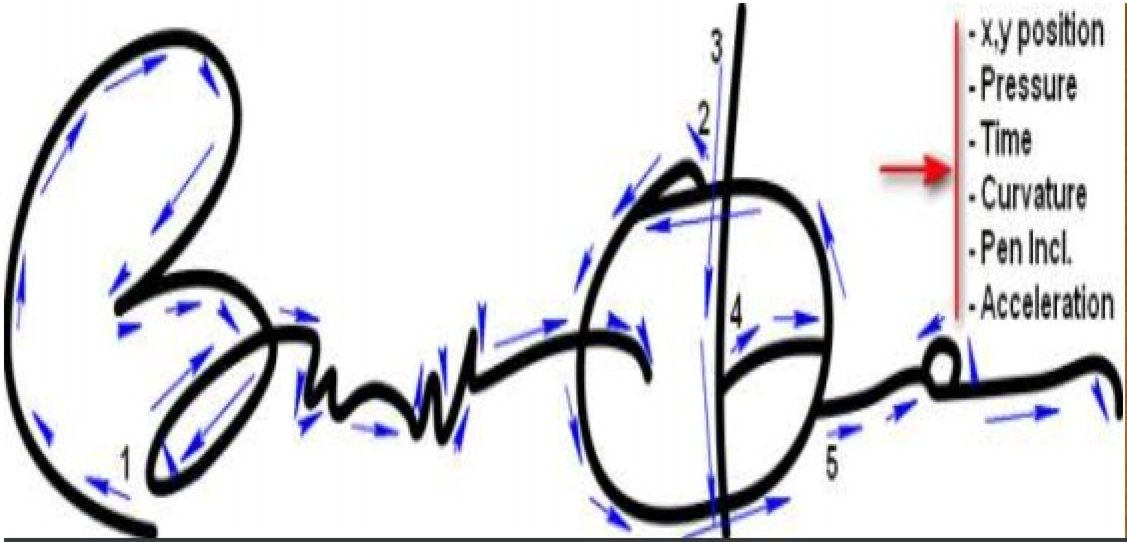


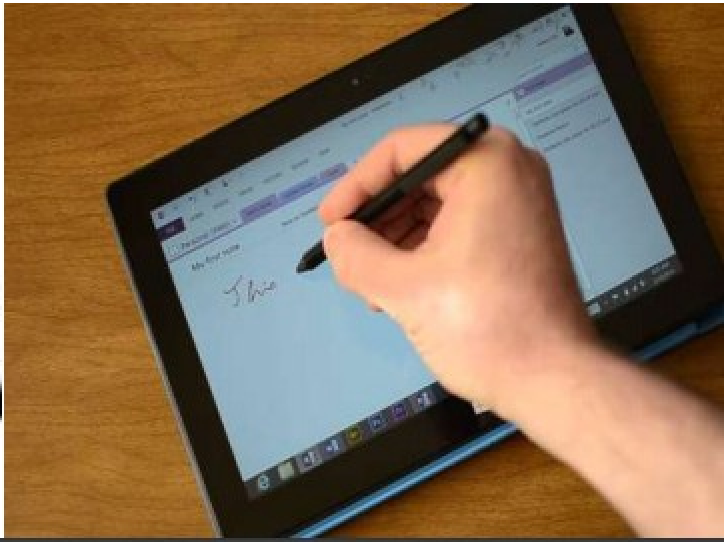
Voice/Speaker Recognition

- Voice or speaker recognition uses vocal characteristics to recognize individual.
- A telephone or microphone can act as a sensor

Signature Verification

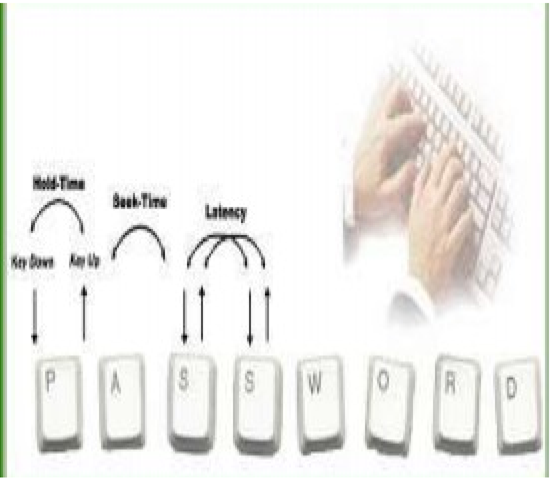
- An automated method of measuring an individual signature.
- This technology examine speed, direction, pressure of stylus while writing, the time that the stylus is in and out of contact with the paper/tablet





Keystrokes Dynamics

- Keystrokes dynamics is an automated method of examining an individual’s keystrokes on a ‘keyboard’.
- This technology examine such as speed, pressure, total time taken to type particular words and time elapsed between hitting certain keys.



Biometric still in developing stage

- Scent (smell)
- Ear Shape
- Fingernail bed
- Facial 3D

Discussion Question

- What are the advantages and disadvantages of each type of biometric security?

Sample answer

Advantages of Fingerprint Biometrics

- Fingerprint pattern stable through out the lifetime
- Fingerprints are unique in nature
- It is easily analyzed and compare
- Inexpensive device
- Oldest form of biometrics

Limitations of Fingerprint Biometrics

- Wet or moist fingers, cut fingers, or dirt or grease can sometimes affect the authentication process.
- It is not right tool for those persons who working in chemical labs.

Summary

- Physical security is often underemphasized by security experts when discussing strategies for protecting critical resources
- Physical security domain includes traditional safeguards against intentional and unintentional threats
- Physical security addresses the following areas
  - Educating personnel
  - Administrative controls
  - Physical controls
  - Technical controls
  - Environmental/Life-safety controls