Cybersecurity

AL Mansour University College

Digital Media Department

4th Class

Lecturer Mustafa Muhanad

-5-

2.1 Cyber Security Vulnerabilities

Vulnerability is, in broad terms, a weak spot in your defense. The term cybersecurity vulnerability refers to any kind of exploitable weak spot that threatens the cybersecurity of an organization.

The following subjects are effecte on vulnerabilities of Cybersecurity

1) Vulnerabilities in Software

2) System administration

3) Complex Network Architectures

4) Poor Cyber Security Awareness

1) Vulnerabilities in Software

Software vulnerability can be seen as a flaw, weakness, or even an error in the system that can be exploited by an attacker to alter the normal behavior of the system Because the number of software systems increases every day also the number of vulnerabilities is increased.

2) System administration

A security systems administrator is someone who gives expert advice to companies regarding their internal security procedures and can also help to detect any weaknesses in a company's computer network that may make them vulnerable to cyber-attacks.

Security systems administrators are a company’s first step in monitoring suspicious activity either within the local network or from outside internet traffic.

A security systems administrator's responsibilities :

1. Defending systems against unauthorized access

2. Performing vulnerability and penetration tests and Identifying threats and working on steps to defend against them

3. Monitoring traffic for suspicious activity

4. Configuring and supporting security tools (firewalls, antivirus, and IDS/IPS software)

5. Implementing network security policies, and providing technical security advice

6. Analyzing and establishing security requirements

7. Identifying threats and working on steps to defend against them

8. Consulting with staff, managers, and executives on best security practices

3) Complex Network Architectures

Complex networks have more entryways and points of interaction than ever for cybercriminals to target, making it more likely they will be able to find a vulnerability to exploit, that inconsistent security measures can slip, and that threats can spread rapidly once the perimeter has been compromised.

Improving Complex Network Security Network security refers to any activities designed to protect the confidentiality, integrity, and availability of the network, as well as the information assets that rely upon it.

What are the network security fundamental objectives?

• To protect the network itself;

• To reduce the vulnerability of computer systems and applications to threats originating from the network.

• To protect data during transmission across the network.

Cybercriminals are continuously searching for weaknesses in an organization's Internet-facing network protection devices give example? (e.g. firewalls). These devices protect an organization from threats that emanate from the Internet.

4) Poor Cyber Security Awareness

Cyber security awareness is the combination of both knowing and doing something to protect a business's information assets.

When an enterprise's employees are cyber security aware?

it means they understand what cyber threats are, the potential impact a cyber-attack will have on their business and the steps required to reduce risk and prevent cyber-crime infiltrating their online workspace.

2.2 Cyber Security Safeguards

Cybersecurity safeguards protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for an information system. Safeguards may include:

- Security features
- Management constraints
- Personnel security, and security of physical structures, areas, and devices.

Authentication, Access control, and **Audit** together provide the foundation for information and system security. Authentication, Access control, and auditing are the three basic types of security controls to ensure information confidentiality, integrity, and availability.

- Authentication establishes the identity of one party to another. Most commonly authentication establishes the identity of a user to some part of the system, typically using a password. More generally, authentication can be computer-to-computer or process-to-process and mutual in both directions.

- Access control: Access control is a fundamental component of data security that dictates who's allowed to access and use company information and resources.

- Through authentication and authorization, access control policies make sure that users have appropriate access to company data.

- Access control usually requires authentication as a prerequisite.

Some examples of virtual and physical access control systems include:

- Login credentials (such as usernames and passwords).
- PINs and One-Time Passwords (OTPs).
- Virtual Private Network (VPN) access to internal networks.

• The Audit process gathers data about activity in the system and analyzes it to discover security violations or diagnose their cause.

• Analysis can occur offline after the fact or online in real-time.

• The process is usually called intrusion detection.

2.3 Biometrics

Biometric is the methodological study of measuring and analyzing biological data for

• authentication or identification

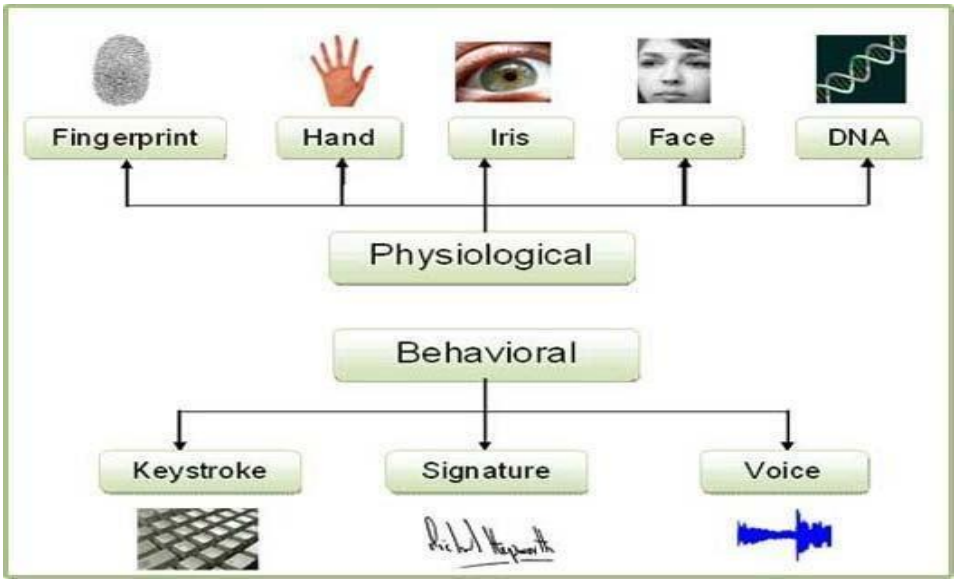
• encryption

• physical acess

Biometric technology is ancient Egyptian times technology. The word " biometric" is originated from the Greek words 'bios' (life) and 'metric 'or 'metrikos' (measure), which directly translates into "life measurement".

▪ **Physical characteristics:** include Face, Fingerprint, DNA, Ear, Iris, Retina, and Hand geometry, they are associated with the shape or measurements of the human body.

▪ **Behavioral characteristics:** include Signature, Voice, and Gait and they are associated with the behavior or dynamic measurements of an individual.



Categories of Biometrics

Two general uses of biometrics are identification and verification.

During these processes, a biometric data sample is compared against the respective biometric data of every person enrolled in the database or against a single reference template of a particular enrolled individual to confirm the identity of that person respectively.

When a biometric system correctly identifies a person, then the result of the identification process is a true positive.

whereas if the system correctly rejects a person as not matching the respective enrolled template, the result is a true negative.

Examples of Popular Biometric Security

- Facial Recognition
- Iris Scanning
- Retinal Scan
- Fingerprinting
- Voice Recognition
- Vein Recognition
- Hand Geometry

The following are some application of Biometric Security Systems

- Banking
- Business Security
- Self Check-In
- Device Security
- Money Security
- Home Security