جامعة المستقبل
AL MUSTAQBAL UNIVERSITY

قسم الامن السيبراني

Department of Cyber Security

Subject: Principles of Cyber Security

Class: 1st

Lecture: (1)

Introduction

Lecturer: Msc :Najwan thaeer ali

Overview

The lecture introduces the fundamentals of security.
It begins by examining the current challenges in computer security and explaining why achieving effective protection is so difficult.
Then, it describes information security in more detail to illustrate its importance and role in safeguarding systems and data.

Lecture Objectives

1. Explain the challenges of securing information

2. Define information security and explain why it is important

1-Challenges of Securing Information

Before introducing the topic of cybersecurity, it is important to emphasize a fundamental fact: **there is no such thing as 100% information security**, even when all security standards and best practices are fully implemented. This is due to the constantly evolving nature of cyber threats and the wide variety of attack techniques used by adversaries.

Modern users and systems face many types of attacks, including malware, phishing, denial-of-service attacks, and advanced persistent threats. Defending against all these attacks simultaneously is extremely difficult because each attack requires different detection and prevention mechanisms. As a result, securing information systems is a complex and ongoing process rather than a one-time solution.

Another major challenge in information security is **system overhead**. This refers to the additional burden placed on a system when multiple security mechanisms are implemented by the software designer, such as layered defenses, encryption techniques, firewalls, and multi-factor

authentication. While these measures significantly enhance security, they also consume system resources.

Consequently, increased security often leads to **slower system performance and delays in processing**, which may cause users to complain about the software or system. Therefore, one of the key challenges in cybersecurity is achieving a balance between strong security, acceptable system performance, and user convenience.

The attacker does not need to bypass all security mechanisms in place. Exploiting even a small weakness—such as bypassing 1% of the implemented security controls—is sufficient to compromise the system. This weakness or flaw in the security design, implementation, or configuration is referred to as a vulnerability.

Today's Security Attacks

Recent years have witnessed a significant increase in sophisticated security attacks, demonstrating that both digital and cyber-physical systems are vulnerable to exploitation.

One notable example involved a **Jeep Cherokee**, where two security researchers remotely accessed the vehicle's internal network from approximately 10 miles away. They were able to manipulate critical controls such as steering, braking, and acceleration. This incident highlighted serious vulnerabilities in connected and autonomous vehicle systems and raised major concerns about automotive cybersecurity.

In another case, a **United Airlines passenger** managed to tamper with the **Seat Electronic Box (SEB)** located under an aircraft seat. By accessing this component, the passenger attempted to connect to other onboard systems, exposing potential weaknesses in aircraft internal networks and emphasizing the importance of strict isolation between passenger-accessible systems and critical flight systems.

A large-scale example of a cyberattack is the **Yahoo data breach**, in which attackers gained unauthorized access to the company's web servers. As a result, **approximately half a billion user accounts** were compromised, including personal information such as names, email addresses, and encrypted passwords. This breach is considered one of the largest data breaches in history and demonstrates the severe consequences of server-side vulnerabilities.

Security statistics further confirm the **ongoing success of attackers**. For instance, between **2005 and 2017**, more than **907 million electronic data records in the United States** were breached. These figures clearly illustrate that security threats are persistent and continuously evolving, making information security a critical and ongoing challenge.

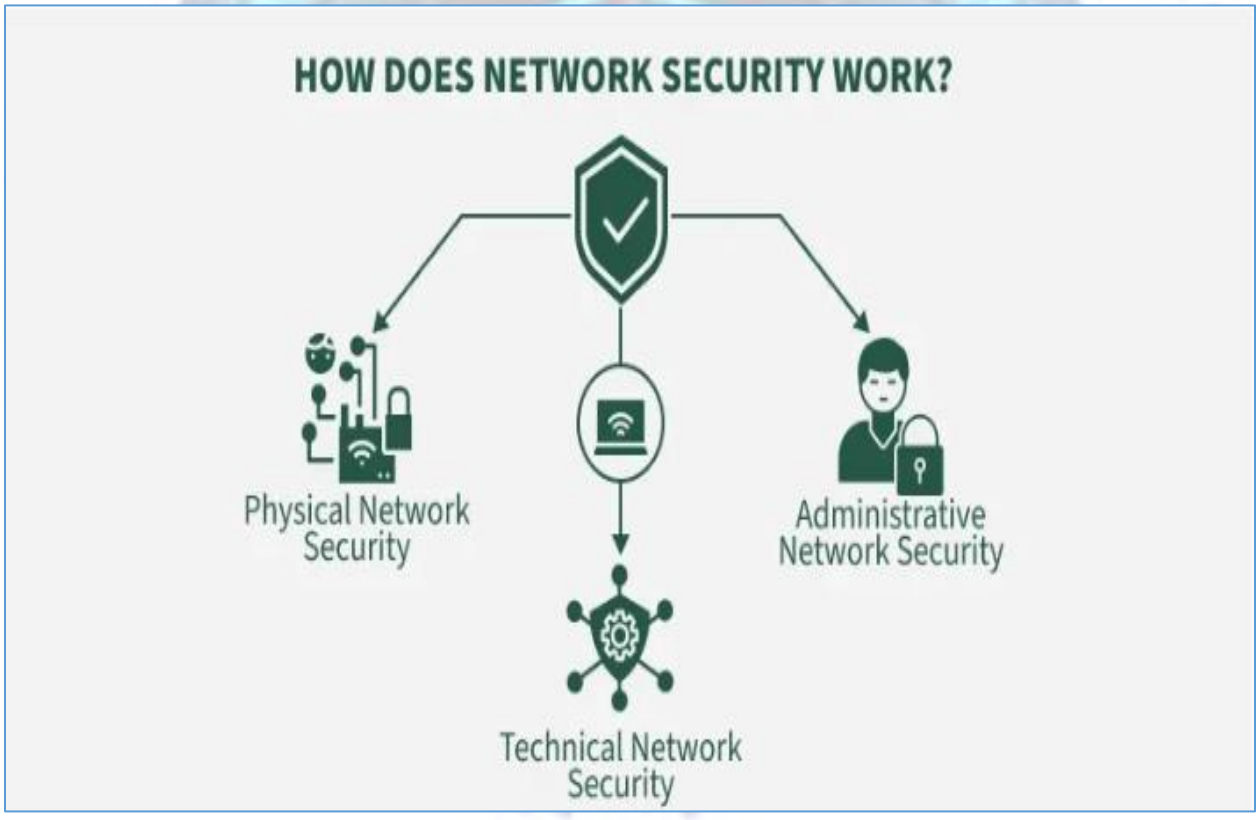

Figure: How Network Security Works: Physical, Technical, and Administrative Layers

Reasons for Successful Attacks

Discuss the following reasons behind successful attacks:

1. Widespread vulnerabilities
2. Configuration issues
3. Poorly designed software
4. Hardware limitations
5. Enterprise-based issues

Difficulties in Defending against Attacks

Describe the following difficulties in defending against attacks:

1. Universally connected devices
2. Increased speed of attacks
3. Greater sophistication of attacks
4. Availability and simplicity of attack tools
5. Faster detection of vulnerabilities
6. Delays in security updating
7. Weak security update distribution
8. Distributed attacks
9. Use of personal devices

2- What Is Information Security?

Understanding why information security is important today and identifying who the attackers are is highly beneficial, as it increases awareness of potential threats. In addition, becoming familiar with the terminology used in information security can be very helpful when designing and implementing effective defenses for computer systems.

Understanding Security

Security can be defined as a state of freedom from danger or risk. This state or condition exists as a result of establishing, implementing, and maintaining appropriate protective measures.

Defining Information Security

Definition: What is Cyber security?

Cyber security refers to a set of practices, technologies, and processes that are designed to protect systems, networks, software, devices, and data from digital attacks, unauthorized access, damage, or theft.

Main Objectives of Cyber security:

1. **Protecting Information (Confidentiality, Integrity, and Availability):**
    A. **Confidentiality:** Ensuring that information is accessible only to authorized users and preventing unauthorized access to data.
    B. **Integrity:** Maintaining the accuracy, consistency, and completeness of data, and preventing unauthorized alteration or destruction.
    C. **Availability:** Ensuring that authorized users can access information and systems reliably and when required.

2. **Defending Against Security Threats, such as:**
    a. **Malware**, including viruses and ransomware.
    b. **Hacking** and other forms of unauthorized access.
    c. **Denial-of-Service (DoS/DDoS) attacks** that disrupt system availability.
    d. **Phishing** and **social engineering** attacks aimed at deceiving users into revealing sensitive information.

Information Security Terminology

a. Asset
An asset is any item of value to an organization that must be protected. Assets can include data, hardware, software, networks, systems, services, and even people or organizational reputation.

b. Threat
A threat is any potential event, action, or circumstance that could exploit a vulnerability and cause harm to an asset, such as data loss, system damage, or service disruption.

c. Threat Actor
A threat actor is an individual, group, or organization that carries out or intends to carry out an attack against an asset. Examples include hackers, cybercriminals, insiders, hacktivists, and nation-state actors.

d. Vulnerability
A vulnerability is a weakness or flaw in a system, application, network, or process that can be exploited by a threat actor to gain unauthorized access or cause harm.

e. Attack Vector
An attack vector is the method or pathway used by a threat actor to exploit a vulnerability and carry out an attack, such as phishing emails, malicious websites, or unsecured network ports.

f. Attack Surface
The attack surface refers to the total number of points where an unauthorized user could attempt to access or extract data from a system. A larger attack surface increases the likelihood of successful attacks.

g. Risk
Risk is the potential for loss or damage when a threat exploits a vulnerability. It is typically evaluated based on the likelihood of the event occurring and the impact it would have on the organization.

Risk Management Options

When dealing with information security risks, organizations can choose among several approaches:

a. Risk Acceptance
Risk acceptance involves acknowledging a risk and deciding to tolerate it without taking additional action, usually because the cost of mitigation outweighs the potential impact.

b. Risk Transference
Risk transference means shifting the impact of a risk to a third party, such as through insurance, outsourcing, or contractual agreements.

c. Risk Avoidance
Risk avoidance involves eliminating the risk entirely by removing the activity, system, or process that creates the exposure.

d. Risk Mitigation
Risk mitigation focuses on reducing the likelihood or impact of a risk by implementing security controls, such as firewalls, encryption, access controls, and security policies.

Understanding the Importance of Information Security

1. Protecting the personal and financial data of individuals and organizations from unauthorized access, misuse, or theft.
2. Safeguarding critical infrastructure, such as hospitals, energy systems, and communication networks, to ensure continuity and public safety.
3. Preventing financial losses and protecting organizational reputation that may result from security breaches and cyber attacks.
4. Ensuring compliance with applicable laws and regulations, such as the General Data Protection Regulation (GDPR) and national cyber security authorities (e.g., the NCA in Saudi Arabia).

Cyber security does not exist in a single place; rather, it can be identified across several interconnected levels:

1. Physical Level (Tangible Locations)

- **Data Centers:** Facilities where large volumes of data are stored, processed, and managed.
- **Server Rooms:** Located within companies and organizations to host critical systems and services.
- **Network Devices:** Such as routers, switches, and firewalls that control and secure data traffic.
- **End-User Devices:** Including computers, smartphones, tablets, and Internet of Things (IoT) devices such as smart cameras and smart appliances.
- **Critical Infrastructure:** Power plants, water management systems, communication networks, and financial institutions that rely heavily on secure digital systems.

2. Digital Level (Cyberspace)

- **Networks:** Local Area Networks (LANs), Wide Area Networks (WANs), and the internet as a whole.
- **Cloud Environments:** Platforms and services such as AWS, Microsoft Azure, and Google Cloud.
- **Applications and Software:** Ranging from operating systems (e.g., Windows, Linux) to everyday applications such as web browsers and mobile banking apps.
- **Data Itself:** Including how data is stored (encrypted or unencrypted), transmitted, and processed.

3. Human and Procedural Level

- **Organizational Policies and Procedures:** Security policies, incident response plans, standards, and employee training programs.
- **User Awareness and Behavior:** Such as thinking critically before clicking suspicious links and using strong, secure passwords.
- **Cyber security Teams (Security Operations Centers – SOC):** Teams that continuously monitor systems, detect threats, and respond to incidents.

In Summary: Cyber security Exists In

- Every environment where devices are connected to a network.
- Every process involving the storage, transmission, or processing of digital information.
- Every interaction between humans and machines within the digital world.

For Clarification with a Daily Example

When you make a financial transfer using your bank's mobile application, cybersecurity is involved at multiple stages:

1. **Your mobile device:** Protected by security measures such as passwords, PINs, or biometric authentication.
2. **The banking application:** Designed using secure coding practices and protected by features such as two-factor authentication.
3. **The network connection:** Secured through encrypted communication between your device and the bank's servers.
4. **The bank's servers:** Protected by firewalls, intrusion detection and prevention systems.
5. **The bank's databases:** Your financial information is stored securely using encryption and access controls.
6. **The bank's internal procedures:** Employees are trained and policies are enforced to ensure the protection of customer data.

(References).

1. **NIST – National Institute of Standards and Technology**
   https://www.nist.gov/cyberframework

2. **Cisco Networking Academy**
   Introduction to Cybersecurity
   https://www.netacad.com

3. **ISO/IEC 27001 Information Security Management**
   https://www.iso.org/isoiec-27001-information-security.html

4. **ENISA – European Union Agency for Cybersecurity**
   https://www.enisa.europa.eu