جامعة المستقبل
AL MUSTAQBAL UNIVERSITY

قسم الامن السيبراني

Department of Cyber Security

Subject: Principles of Cyber Security

Class: 1st

Lecture: (3)

Digital Privacy and Cybersecurity

Lecturer: Msc :najwan thaeer ali

Digital privacy: refers to the set of principles, policies, and practices aimed at safeguarding individuals' personal information within digital environments. It focuses on the processes through which data are collected, stored, processed, shared, and utilized by organizations, governmental entities, and online platforms. Personal data may encompass names, identification numbers, browsing histories, biometric information, and patterns of online behavior.

- **Ensuring digital privacy involves empowering individuals with control over their personal data and protecting** such information from unauthorized access, misuse, or exploitation, in accordance with established legal and ethical frameworks for data protection.

Lecture Objectives

1. **Understand the concept of digital privacy and its importance in protecting personal data in digital environments.**

2. **Explain the role of cybersecurity measures in preventing unauthorized access, misuse, and data breaches.**

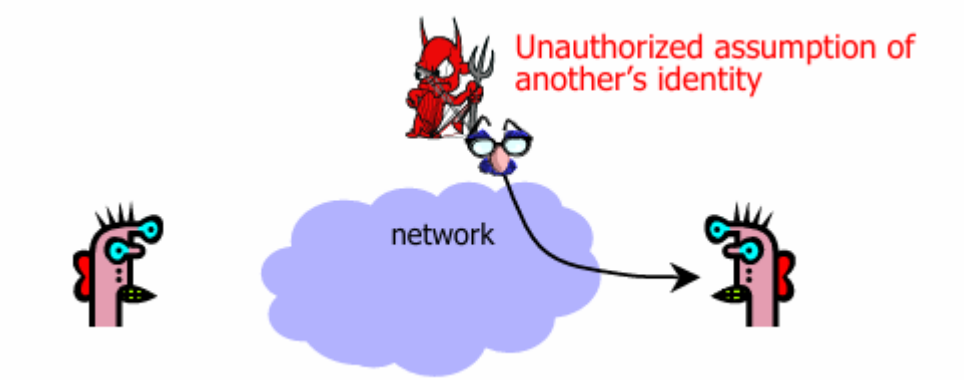
Key aspects of digital privacy include:

1. **Data Protection: Safeguarding personal data from leaks, breaches, and unauthorized sharing.**
2. **User Consent: Ensuring individuals are informed and agree to how their data is used.**
3. **Privacy Policies and Regulations: Compliance with laws such as GDPR and other national data protection frameworks.**
4. **Anonymity and Confidentiality: Protecting user identity and sensitive communications online.**

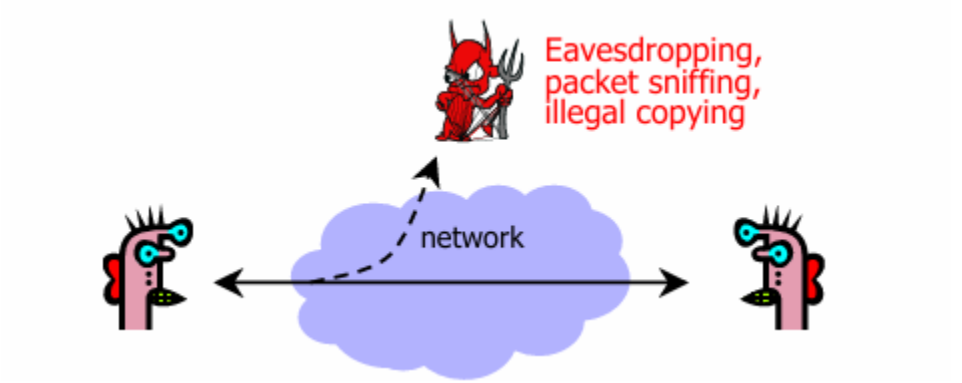
👌 Relationship Between Digital Privacy and Cybersecurity

Aspect	Security	Privacy
Definition	Protecting systems and data from unauthorized access, threats, or attacks.	The right of individuals to control their personal information and its use.
Focus	Technical protection of information systems (firewalls, encryption, access).	Ethical and legal protection of personal data and user rights.
Scope	Concerned with data integrity, confidentiality, and availability.	Concerned with data collection, sharing, and consent.
Target	Protects organizations, networks, and systems.	Protects individuals and their personal information.

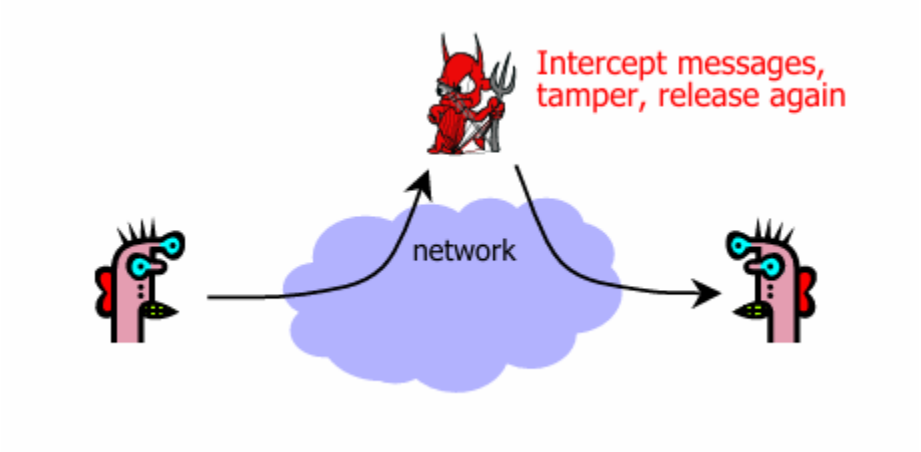
Attack on Authenticity :Authenticity is identification and assurance of origin of information



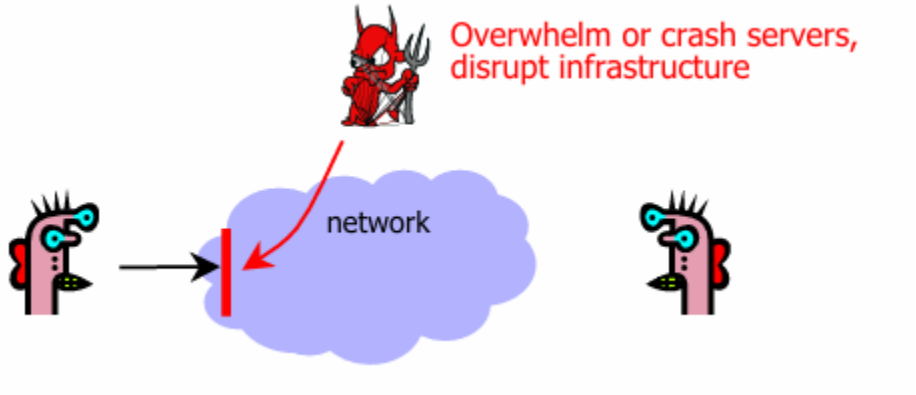
Attack on Confidentiality: Confidentiality is concealment of information



Attack on Integrity : Integrity is prevention of unauthorized changes



Attack on Availability :Availability is ability to use information or resources desired



Summary of Attacks

- **Eavesdropping:** Unauthorized monitoring of communication between parties to obtain sensitive information without their knowledge.
- **Packet Sniffing:** Intercepting and analyzing data packets transmitted over a network to extract confidential data such as passwords or personal information.
- **Illegal Copying:** Unauthorized duplication or theft of transmitted data, leading to data leakage and violations of digital privacy.

Reference

- Stallings, W. (2023). *Cryptography and Network Security: Principles and Practice* (8th ed.). Pearson Education.
- Whitman, M. E., & Mattord, H. J. (2022). *Principles of Information Security* (7th ed.). Cengage Learning.