Emerging issues in computer science

Week 4: Cyber Security and Privacy Challenges

Lecturer: Ikwap Flavia Agatha

Lecture learning out come

- By the end of the class you will be able to:
- Understand the Concept of information security and Cybersecurity
- Comprehend the history of computer security and how it evolved into information security
- Understanding the Cyber security Fundamentals
- Understand the manifestation of attacks
- Understanding the common security attacks
- Understanding the different technologies and mechanised developed to control attacks

Introduction

- Information security: a “well-informed sense of assurance that the information risks and controls are in balance.” —Jim Anderson, Innovant (2002)
- Information security began with Rand Report R-609 (paper that started the study of computer security) Scope of computer security grew from physical security to include:
- Safety of data
- Limiting unauthorized access to data
- Involvement of personnel from multiple levels of an organization

History

- The penetration of the Internet into the commercial phase (1984-1989), facilitated by the upgrading of backbone links, the writing of new software programs and the growing number of interconnected international networks: saw the rise in computer connections however at this point in time security was treated as a low priority

The Present

- The Internet brings millions of computer networks into communication with each other—many of them unsecured

  Today: many devices are connected to the internet, the internet has become a “a bee hive of activities” causing so many security and privacy concerns

- Ability to secure a computer’s data is influenced by the security of every computer to which it is connected

What is Security?

- security is “the quality or state of being secure—to be free from danger.” In other words, protection against adversaries—from those who would do harm, intentionally or otherwise—is the objective. National security, for example, could be a multilayered system that protects the sovereignty of a state, its assets, its resources, and its individuals. Achieving the acceptable level of security
- An organization requires different levels of security
- Physical security, to shield physical things, objects, or areas from unauthorized access and misuse

Different levels of security

- Personnel security, to shield the individual or cluster of people
- Operations security, to shield the small print of a specific operation or series of activities
- Communications security, to shield communications media, technology, and content
- Network security, to shield networking elements, connections, and contents
- Information security, to shield the confidentiality, integrity and convenience of knowledge assets, whether or not in storage, processing, or transmission. It's achieved via the applying of policy, education, coaching and awareness, and technology.

What is Information Security?

- The protection of information and its critical elements, including systems and hardware that use, store, and transmit that information
- Necessary tools: policy, awareness, training, education, technology
- C.I.A. triangle was standard based on confidentiality, integrity, and availability
- C.I.A. triangle now expanded into list of critical characteristics of information

Critical Characteristics of Information

- The value of information comes from the characteristics it possesses:
- Availability
- Accuracy
- Authenticity
- Confidentiality
- Integrity
- Utility
- Possession

Components of an Information System

- Information System (IS) is entire set of software,
- hardware, data, people, procedures, and networks necessary to use information as a resource in the organization

Securing Components

- Computer can be subject of an attack and/or the object of an attack
- When the subject of an attack, computer is used as an active tool to conduct attack
- When the object of an attack, computer is the entity being attacked

Cyber Security - Cyber Security Basics:

- Cyber security is the most concerned matter as cyber threats and attacks are overgrowing.
- Attackers are now using more sophisticated techniques to target the systems. Individuals, small-scale businesses or large organization, are all being impacted. So, all these firms whether IT or non-IT firms have understood the importance of Cyber Security and focusing on adopting all possible measures to deal with cyber threats

What is cyber security?

- "Cyber security is primarily about people, processes, and technologies working together to encompass the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, etc."
- OR
- Cyber security is the body of technologies, processes, and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access.

- OR
- Cyber security is the protection of Internet-connected systems, including hardware, software, and data from cyber attacks.
- It is made up of two words one is cyber and other is security.
- Cyber is related to the technology which contains systems, network and programs or data.
- Whereas security related to the protection which includes systems security, network security and application and information security.

Cyber security Fundamentals (Principles)

- **Confidentiality:**

Confidentiality is about preventing the disclosure of data to unauthorized parties.

It also means trying to keep the identity of authorized parties involved in sharing and holding data private and anonymous.

- Often confidentiality is compromised by cracking poorly encrypted data, Man-in-the-middle
- (MITM) attacks, disclosing sensitive data.
- Standard measures to establish confidentiality include:
- Data encryption
- Two-factor authentication
- Biometric verification
- Security tokens

Integrity

- Integrity refers to protecting information from being modified by unauthorized parties.
- Standard measures to guarantee integrity include:
- Cryptographic checksums
- Using file permissions
- Uninterrupted power supplies
- Data backups

Availability

- Availability is making sure that authorized parties are able to access the information when needed.
- Standard measures to guarantee availability include:
- Backing up data to external drives
- Implementing firewalls
- Having backup power supplies
- Data redundancy

Security Attack

- Any action that compromises the security of information owned by an organization Information security is about how to prevent attacks,
- or failing that, to detect attacks on information-based
- systems
- Often threat & attack used to mean same thing
- There are a wide range of attacks
- Can focus of generic types of attacks
- Passive
- Active

- Attack Manifestation:

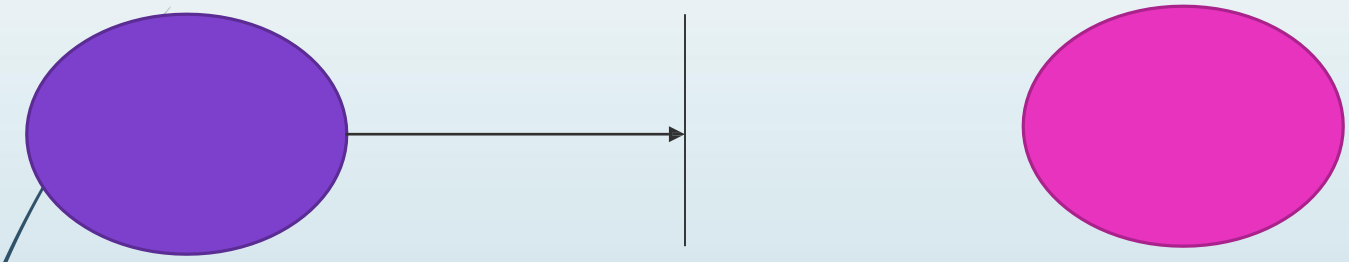
Normal Information flow

Information source

Destination

Security Attack

Interruption by an attacker



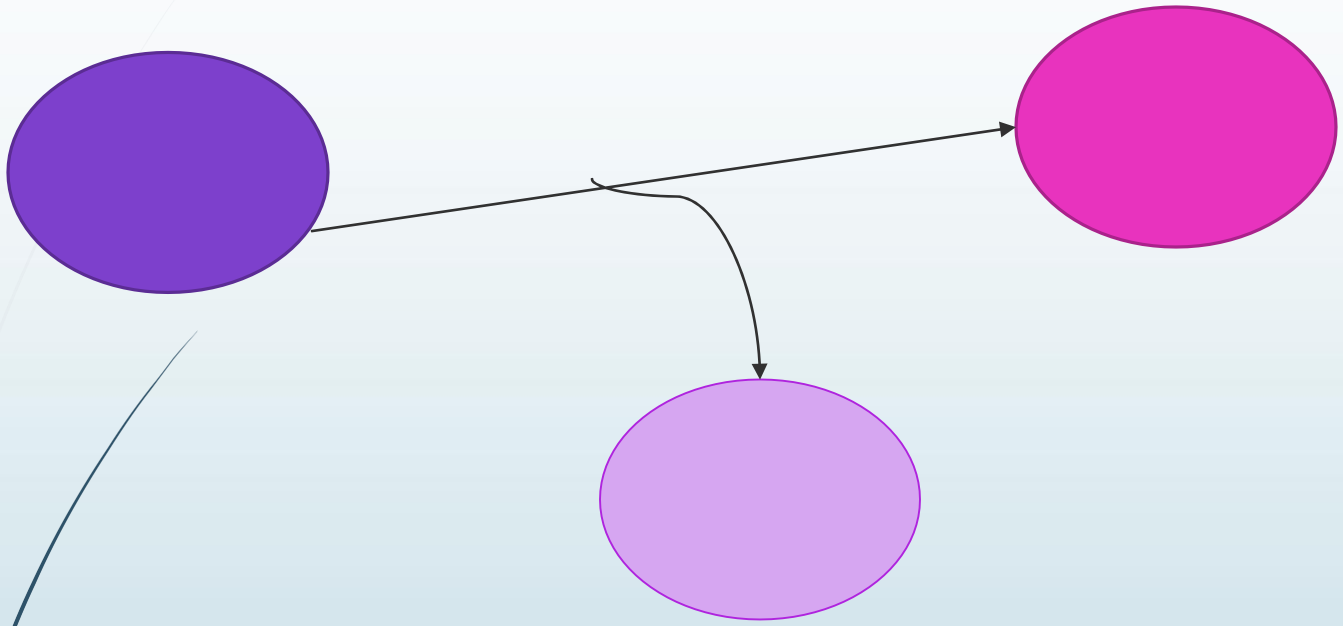
Information Source

Destination

Interruption by an attacker

- An asset of the system is destroyed or becomes unavailable or unusable. It is an attack on availability.
- Destruction of hardware
- Jamming wireless signals
- Disabling file management systems

Security Attack-Interception



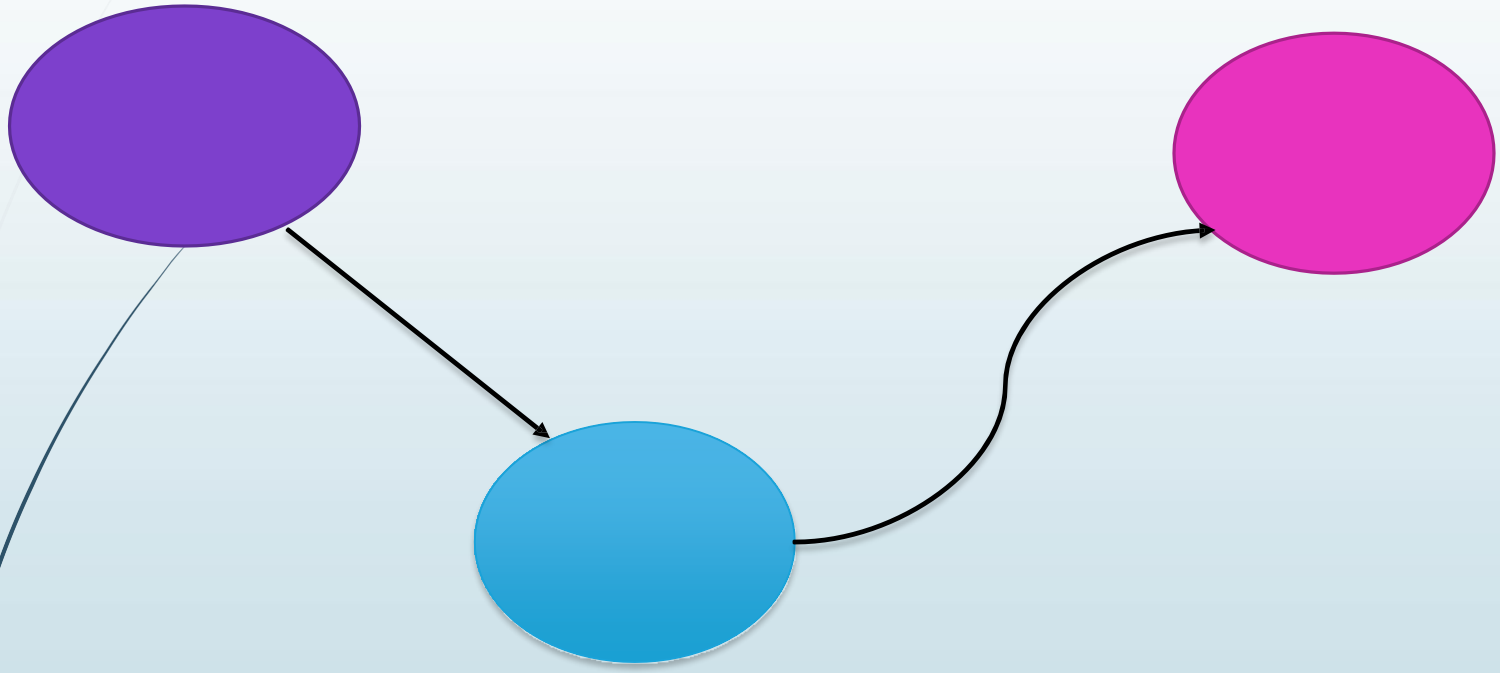
- Information Source

Destination

INTERCEPTION

- An unauthorized party gains access to an asset. Attack on confidentiality.
- Examples:
  - Wire tapping to capture data in a network.
  - Illicitly copying data or programs
  - Eavesdropping
  - Capture data in a network, copying file

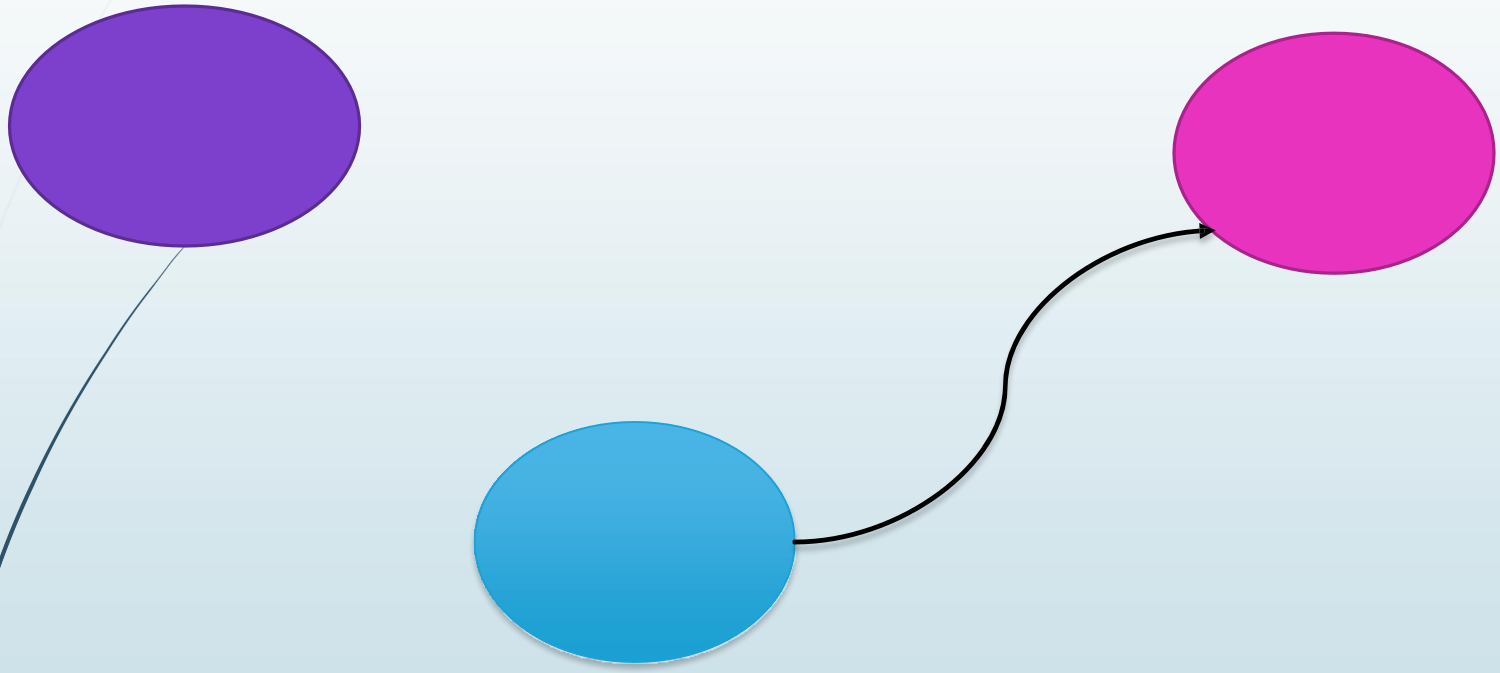
Security Attack-Modification



MODIFICATION

- When an unauthorized party gains access and tampers an asset. Attack is on Integrity.
- Changing value of data, modify message
- **Examples:**
  - Changing data file
  - Altering a program and the contents of a message

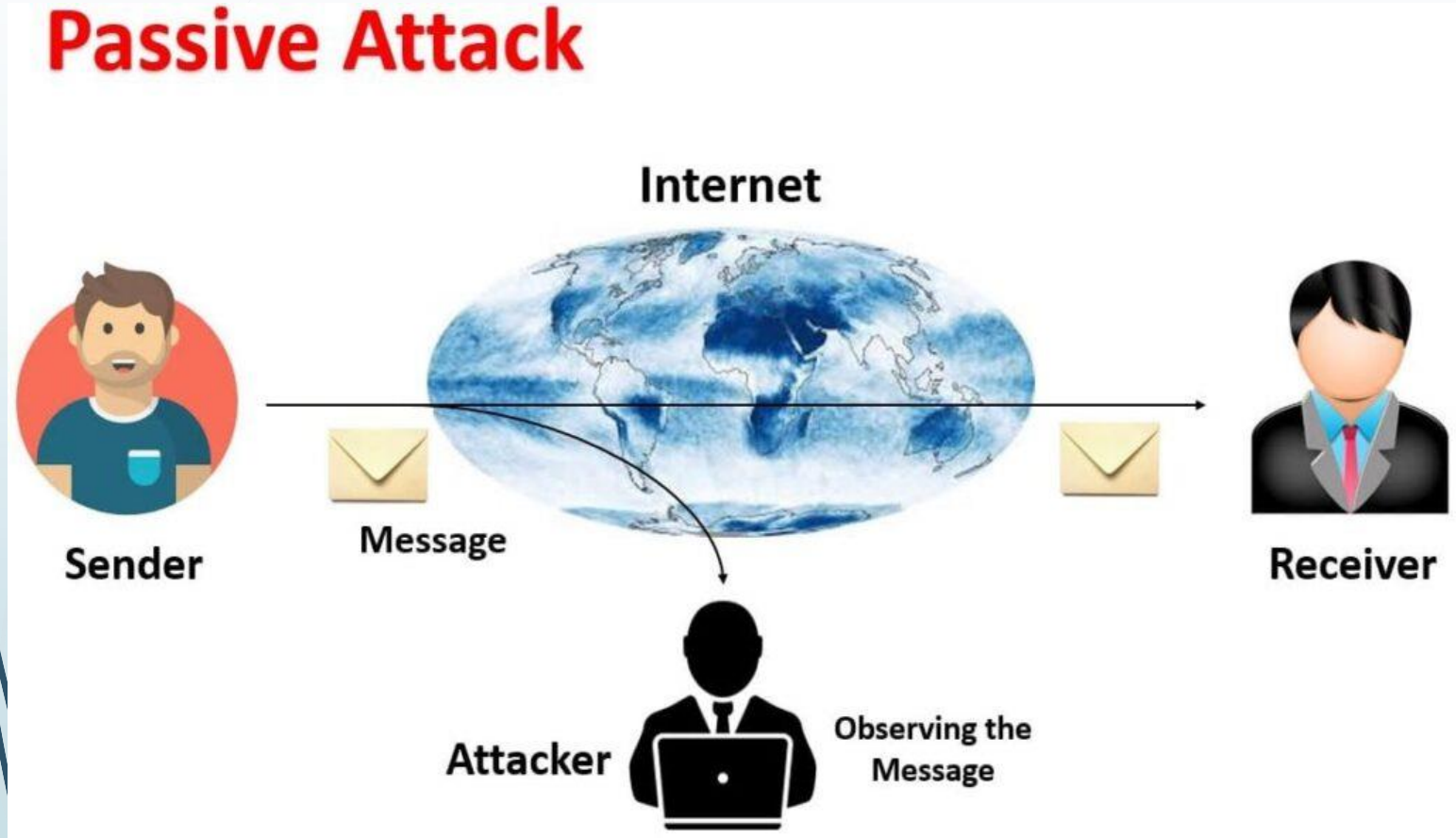
Security Attack-Fabrication



FABRICATION

- An unauthorized party inserts a counterfeit object into the system. attack on authenticity. also called impersonation
- Examples:
  - hackers gaining access to a personal email and sending message
  - insertion of records in data files
  - insertion of spurious messages in a network
  - Inserts object into system
  - Attack on authenticity
  - Addition records to a file, insert message

Passive Attack



https://usemynotes.com/computer-network-attacks/

Passive Attacks

- The goal : obtain information that is being transmitted.
- Release of message content
- Telephone conversation, e-mail message, transferred file
- Traffic analysis
- Encrypt message, masking so opponent couldn’t extract the information.
- But could determine the location and identity of communicating host

Active Attacks

https://techdifferences.com/difference-between-active-and-passive-attacks.html

Active Attacks

- Involve modification of data or the creation of false Data Subdivided into 4 categories
- Masquerade : one entity pretends to be a different entity
- Replay : passive capture of data and its subsequent retransmission to produce an unauthorized effect
- Modification of message :
- legitimate message is altered
- Denial of Service : prevents or inhibits the normal use or management of communications facilities
- Degrade performance

Cyber security and privacy challenges / Concerns

- A number of challenges are on the increase due to complexity of technology, growing volume of data, and the continuous evolution of cyber threats. Some key challenges include:
- **Data Breaches**: Access of data without authorization, such as personal, financial, or business information, can lead to identity theft, financial loss, and a loss of trust. .
- **Privacy Concerns**: With the increasing amount of personal data being collected by organizations, there are significant concerns about how this data is used, shared, and protected. Individuals worry about unauthorized tracking, surveillance, and misuse of their personal information by companies or governments.
- **Insider Threats**: Employees, contractors, or anyone with authorized access to a system can intentionally or unintentionally cause harm by leaking sensitive information, misusing data, or introducing malware into systems.

Cyber security and privacy challenges / Concerns

- **Complexity of Compliance**: Many organizations must adhere to strict privacy regulations like GDPR, HIPAA, or CCPA, which can be difficult to navigate and comply with. Ensuring data protection and privacy while following legal frameworks across different regions is a complex challenge.
- **Cloud Security**: Continuous migration to cloud computing, comes with risks related to data storage, access, and management. Cloud providers need to guarantee security to clients by implementing strong security practices and have data properly encrypted is critical.

Cyber security and privacy challenges / Concerns

- **Securing IoT Devices**: The growing number of Internet of Things (IoT) devices creates new vulnerabilities as many of these devices have weak security or lack necessary updates, making them attractive targets for cybercriminals.
- **User Awareness and Behavior**: Many security breaches occur due to human error, such as weak passwords, falling for phishing scams, or failing to update software. Improving user education and awareness is a significant challenge in maintaining security.
- **Advanced Persistent Threats (APTs)**: These are long-term, targeted attacks often orchestrated by skilled hackers or state-sponsored groups. APTs can infiltrate systems undetected and steal valuable data over extended periods, making detection and mitigation difficult.

Common Cyber attacks

- **Man-in-the-Middle (MitM) Attacks**: Attackers intercept and manipulate communications between two parties, often to steal sensitive data, such as login credentials, during transmission.
- **SQL Injection**: Cybercriminals insert malicious SQL code into input fields of websites or applications, allowing them to manipulate databases, steal data, or execute unauthorized commands.
- **Cross-Site Scripting (XSS)**: Attackers inject malicious scripts into websites that can execute on a user's browser, often leading to stolen data, unauthorized actions, or compromised accounts.
- **Credential Stuffing**: Attackers use previously stolen or leaked username and password combinations to gain unauthorized access to other accounts where users have reused credentials.

Common Cyber attacks

- **Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) Attacks**: Attackers flood a network or system with an overwhelming amount of traffic to disrupt its normal operation and make it unavailable to legitimate users.
- **Zero-Day Exploits**: Cybercriminals take advantage of vulnerabilities in software or hardware that are unknown to the vendor or security community, and for which no fix or patch exists.
- **Insider Threats**: Employees, contractors, or trusted individuals with access to a company's systems or data intentionally or unintentionally cause harm, such as leaking sensitive information or compromising security.
- **Social Engineering**: Manipulating people into divulging confidential information or performing actions that compromise security, often through psychological manipulation rather than technical means.

Common Cyber attacks

- **Phishing**: Cybercriminals use deceptive emails, websites, or messages that appear to be from legitimate sources to trick individuals into revealing personal information, such as login credentials or credit card numbers.
- **Ransomware**: A type of malicious software that encrypts a victim's files or locks them out of their system, demanding a ransom payment for the decryption key to regain access to the files.
- **Malware**: Malicious software such as viruses, worms, Trojans, and spyware designed to disrupt, damage, or gain unauthorized access to systems or steal sensitive data.

Security technologies and Mechanisms used to prevent attacks

- **VPNS**
- VPN stands for "Virtual Private Network", VPNs establish a protected network connection when using public networks. VPNs encrypt your internet traffic and disguise your online identity. This makes it more difficult for third parties to track your activities online and steal data. The encryption takes place in real time.

Benefits of a VPNs Connection

- **Access to regional conten**t: Regional web content is not always accessible from everywhere. Services and websites often contain content that can only be accessed from certain parts of the world. Standard connections use local servers in the country to determine your location.
- **Secure encryption:** To read the data, you need an encryption key, without one, it would take millions of years for a computer to decipher the code in the event of a brute force attack. With the help of a VPN, your online activities are hidden even on public networks.
- **Disguising your whereabouts:** VPN servers essentially act as your proxies on the internet. Because the demographic location data comes from a server in another country, your actual location cannot be determined.
- **Secure data transfer:** VPN services connect to private servers and use encryption methods to reduce the risk of data leakage.

Scanning and analysis tools

- Scanning and analysis tools are computer programs that are used to find vulnerabilities in systems, and security holes in individual system components. For examples, the vulnerabilities of specific hosts, routers, or even firewalls.
- **Categories of scanning and analysis tools**
- **Port scanners**
- Port scanners are tools used by both attackers and defenders to identify the computers that are active on a network, as well as the ports and services active on those computers.
- **Network mappers**
- Network mappers are tools that identify all systems connected to a network.

Scanning and analysis tools

- **OS detection tools**

 Tools that detect target host‘s operating system. Knowing a host‘s OS is critical to exploit the host‘s vulnerabilities. For example, the known bugs of that OS

- **Vulnerability scanners**

 Software tools that assess security vulnerabilities in network & hosts and produce a set of scan results.

Packet sniffers

A packet sniffer (sometimes called a network protocol analyzer) is a network tool that collects copies of packets from the network and analyzes them.

- **Wireless sniffers**

 A software or maybe hardware that is capable of capturing & decoding packets as they pass over airwaves.

Access controls

- Access control the selective method by which systems specify who may use a particular resource and how they may use it.
- Access control is the method by which systems determine whether and how to admit a user into a trusted area of the organization—that is, information systems, restricted areas such as computer rooms, and the entire physical location. Access control is achieved through a combination of policies, programs, and technologies

Access Control Mechanisms

- In general, all access control approaches rely on the following four mechanisms, which represent
- the four fundamental functions of access control systems:
- Identification: I am a user of the system.
- Authentication: I can prove I’m a user of the system.
- Authorization: Here’s what I can do with the system.
- Accountability: You can track and monitor my use of the system.

Biometric access control

- The use of physiological characteristics to provide authentication for a provided identification. Biometric means “life measurement” in Greek. Sometimes referred to as biometrics.
- Biometric access control relies on recognition—the same thing you rely on to identify friends, family, and other people you know
- Biometric authentication technologies include the following:
- Fingerprint comparison of the unauthenticated person’s actual fingerprint to a stored
- Fingerprint
- Palm print comparison of the unauthenticated person’s actual palm print to a stored palm print

Biometric access control

- Facial recognition using a photographic ID card, in which a human security guard
- compares the unauthenticated person's face to a photo
- Facial recognition using a digital camera, in which an unauthenticated person's face is compared to a stored image
- Retinal print comparison of the unauthenticated person's actual retina to a stored image
- Iris pattern comparison of the unauthenticated person's actual iris to a stored image
- Hand geometry comparison of the unauthenticated person's actual hand to a stored measurement

Encryption

- Encryption is the process of converting information or data into a code to prevent unauthorized access. It transforms readable data (plaintext) into an unreadable format (ciphertext) using an algorithm and a key. Only those with the appropriate decryption key can convert the cipher text back into its original, readable form.
- Encryption is widely used to protect sensitive information, such as passwords, personal data, and financial transactions, ensuring privacy and security when transmitting or storing data.

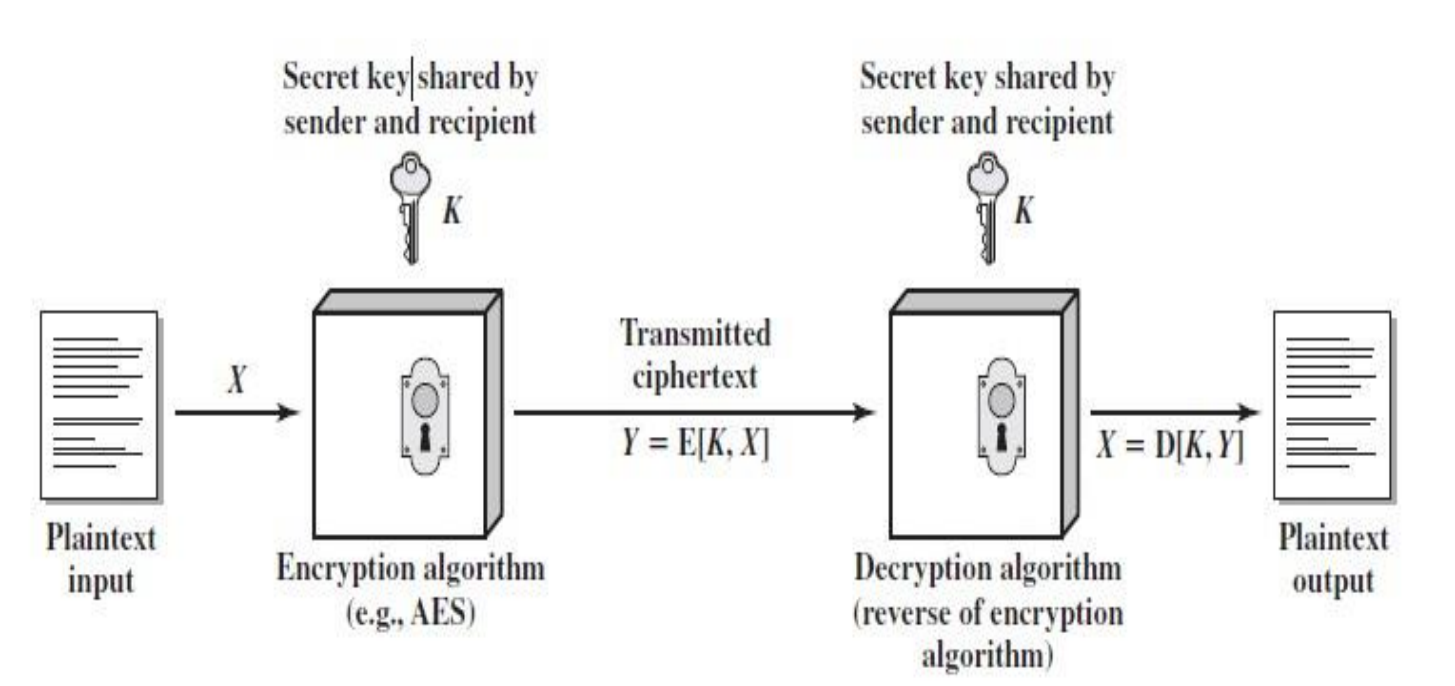
For example:

- When you use your credit card to make an online purchase, your payment details are encrypted to keep them safe from hackers.
- When you send a message on a secure messaging platform, it might be encrypted so that only you and the recipient can read it.

Encryption Types
symmetric encryption scheme

- **Plaintext:** This is the original message or data that is fed into the algorithm as input.
- **Encryption algorithm:** The encryption algorithm performs various substitutions and transformations on the plaintext.
- **Secret key:** The secret key is also input to the algorithm. The exact substitutions
- and transformations performed by the algorithm depend on the key.
- **Cipher text:** This is the scrambled message produced as output. It depends on
- the plaintext and the secret key. For a given message, two different keys will
- produce two different ciphertexts.
- **Decryption algorithm:** This is essentially the encryption algorithm run in
- reverse. It takes the ciphertext and the same secret key and produces the original
- plaintext.

symmetric encryption scheme



- (Stallings, 2011)

symmetric encryption scheme

- The most commonly used symmetric encryption algorithms are block ciphers.

A **block cipher** processes the plaintext input in fixed-sized blocks and produces a

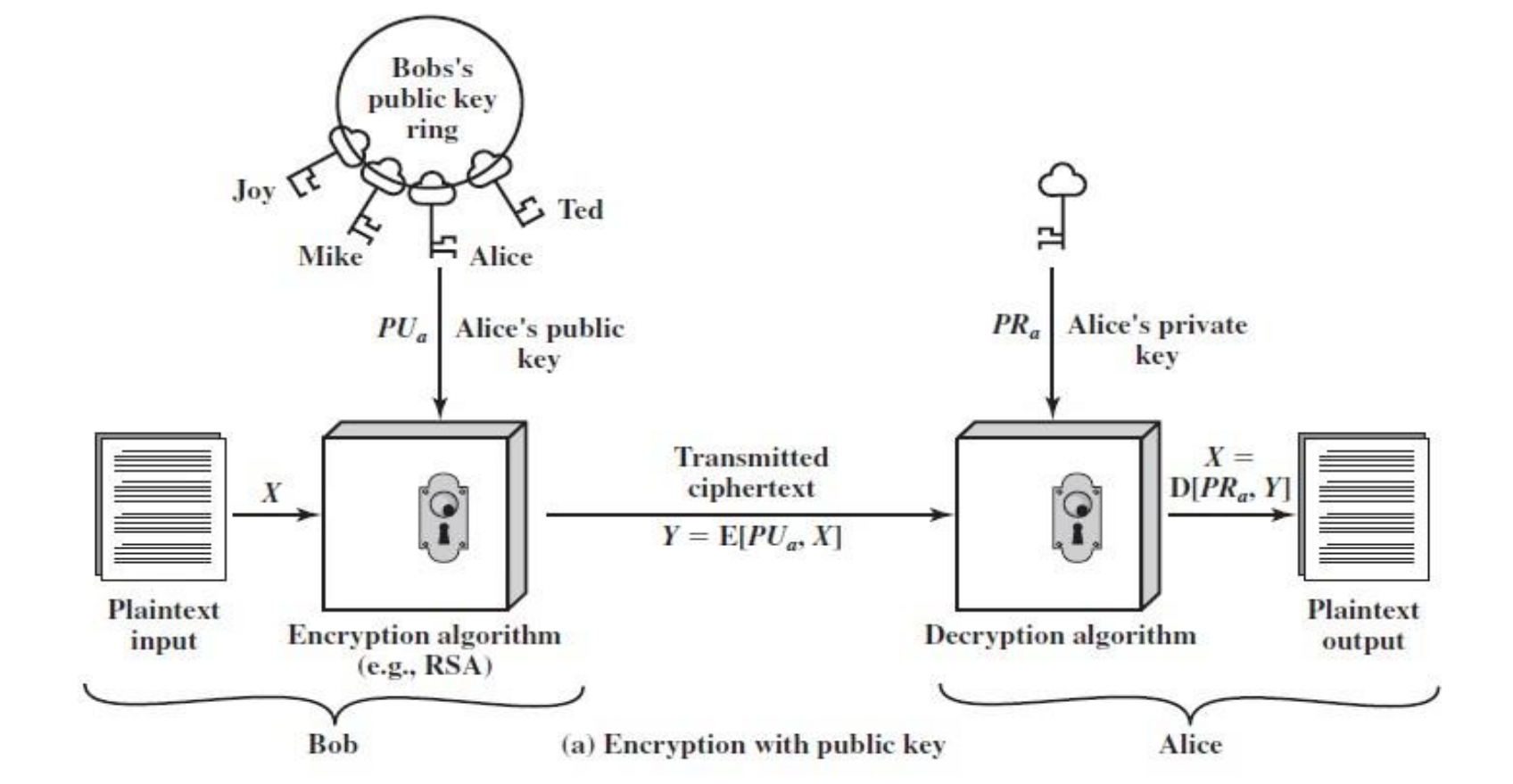
- Block of cipher text of equal size for each plaintext block.
- Three most important symmetric block ciphers:

- Data Encryption Standard
- (DES),
- triple DES (3DES), and Advanced Encryption Standard (AES).

Public-key encryption scheme

- **Plaintext:** This is the readable message or data that is fed into the algorithm as input.
- **Encryption algorithm:** The encryption algorithm performs various transformations on the plaintext.
- **Public and private key:** This is a pair of keys that have been selected so that if one is used for encryption, the other is used for decryption. The exact transformations performed by the encryption algorithm depend on the public or private key that is provided as input.
- **Cipher text:** This is the scrambled message produced as output. It depends on
- Plaintext and the key. For a given message, two different keys will produce two different cipher texts.
- **Decryption algorithm:** This algorithm accepts the cipher text and the matching key and produces the original plaintext.

Public-key encryption



(Stallings, 2011)

Other Techniques

- **Honey Pots:** Honey pots are decoy systems designed to lure potential attackers away from critical systems and encourage attacks against themselves. These systems are created for the sole purpose of deceiving potential attackers, they are also known as **decoys, lures, and fly-traps.**
- **Firewalls: A firewall** Acts as barriers between trusted internal networks and untrusted external networks, monitoring and controlling incoming and outgoing network traffic. It works by Block unauthorized access to systems and networks while allowing legitimate communication.

Other Techniques

- **Multi-Factor Authentication (MFA):** Requires two or more forms of verification before granting access (e.g., something you know, something you have, or something you are).
- **Regular Software Updates and Patching:** Keeping software, operating systems, and applications up to date with the latest security patches.
- **Intrusion Detection and Prevention Systems**
- intrusion detection and prevention system (IDPS) The general term for a system that can both detect and modify its configuration and environment to prevent intrusions. An IDPS encompasses the functions of both intrusion detection systems and intrusion prevention technology.
- Intrusion detection system (IDS) A system capable of automatically detecting an intrusion into an organization’s networks or host systems and notifying a designated authority.

Other Techniques

- **Regular Backups:** Regularly backing up critical data to ensure it can be recovered in case of data loss due to an attack (e.g., Ransomware).
- **User Education and Awareness Training**
- Providing staff and users adequate training about common cyber security threats like phishing, social engineering, and safe internet practices.
- **Secure Software Development Practices:** Integrating security measures and testing throughout the software development lifecycle (SDLC).
- **Antivirus and Anti-malware Software:** These help to Detect and remove malicious software (malware) such as viruses, ransomware, and spyware from systems.

Reference

- Alani, M. M. (2014). Securing the Cloud: Threats, Attacks and Mitigation Techniques.
- Journal of Advanced Computer Science and Technology, 1-12.
- Amara, N. (2017). Cloud Computing Security Threats and Attacks with their Mitigation Techniques. 2017
- International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, (pp. 1-9). Nanjing.
- Chandrasekaran, K. (2015). Essentials of Cloud Computing. Newyork: CRC.
- Ertaul, L. (2010). Security Challenges in Cloud Computing. Istanbul.
- BHUSHAN, M. (2017). *Fundamental of cyber security.* India: BPB Publications.
- Stallings, W. (2011). *NETWORK SECURITY ESSENTIALS: APPLICATIONS AND STANDARDS.* Pearson Education, Inc., publishing as [Prentice Hall].

Next Lecture

Blockchain Technology and Crypto currencies