# Information Security SEng 3084

## Chapter One

### Introduction

# Presentation outline

- Introduction and terminologies
- The cause of insecurity.
- Security goals
- Security breach levels
- The challenges of computer security
- The OSI security architecture
- Security attacks
- Common security threats
- Security services and mechanisms
- Security techniques

# Introduction and Terminology

## ❑ Definition of Security:

- This is the age of universal electronic connectivity, where the activities like **hacking, viruses, electronic fraud are very common.**
- **So security measures should be taken to solve such types of problems.**
- "The quality or state of being secure--to be free from danger" and to be protected from adversaries.
- It is a continuous process of protecting an object from attack.
- The object may be a person, an organization, or properties, files etc.

# Introduction and Terminology

## ❑ Definition of Security:

- The term, Computer Security, refers to the protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of information system resources (includes hardware, software, firmware, information/data, and telecommunications).
- This definition introduces three key objectives, CIA traid (Integrity, availability, and confidentiality) that are at the heart of computer security.
- **Security is about**
  - Threats (bad things that may happen, e.g. your money getting stolen)
  - Vulnerabilities (weaknesses in your defenses, e.g. your front door being made of thin wood and glass)
  - Attacks (ways in which the threats may be actualized, e.g. a thief breaking through your weak front door while you and the neighbors are on holiday)

# Introduction and Terminology

## ❑ Definition of Security:

- **Computer security** is about provisions and policies adopted to protect information and property from **theft, corruption, or natural disaster.**
  - while allowing the information and property to remain accessible and productive to its intended users.
- Security of computers against intruders (e.g. hackers) and malicious software (e.g. viruses).

# bing

- **Malicious software, or malware**, is a term for any kind of computer software with malicious(ተንኮለኛ) intent. Most online threats are some form of malware.
- Malware can take many forms, including viruses, worms, trojan horses, ransomware, and spyware[1]. Malware can invade(weeraruu), damage, or disable computers, computer systems, networks, tablets, and mobile devices. It can also steal, encrypt, or delete your data, alter or hijack core computer functions, and spy on your computer activity without your knowledge or permission[1]. Malware can be about making money off you, sabotaging your ability to get work done, making a political statement, or just bragging rights[1].
- **Windows Malicious Software Removal Tool (MSRT)** is a tool that helps keep Windows computers free from prevalent malware. MSRT finds and removes threats and reverses the changes made by these threats. MSRT is generally released monthly as part of Windows Update or as a standalone tool available here for download[2].

# Introduction and Terminology

## ❑ Definition of Security:

- "The most secure computers are those not connected to the Internet and shielded from any interference"

# bing

- - Information availability is the timely and reliable access to data and information services for authorized users[1]. It ensures that information and information systems are operational and accessible when needed.
- - Information integrity is the protection of data and information from unauthorized or accidental modification, destruction, or disclosure[1]. It ensures that information and information systems are accurate, complete, consistent, and trustworthy.
- - Information confidentiality is the protection of data and information from unauthorized disclosure or interception[1]. It ensures that information and information systems are only accessible to authorized users or processes.

# Introduction and Terminology

## ❑ Information Assurance (IA)

- It is the study of **how to protect your information assets from destruction, degradation, manipulation and exploitation.,** by insuring its confidentiality, integrity and availability.
- **How to recover should any of those happen.**
- It involves the **actions taken to protect and defend information and information systems**.
- This includes providing for restoration of information systems by incorporating protection, detection and reaction capabilities.
- IA is a multidisciplinary area of study and professional activity which aims to protect business by reducing risks associated with information and information systems by means of a comprehensive and systematic management of security countermeasures, which is driven by risk analysis and cost-effectiveness.

# Introduction and Terminology

## ❑ Information Assurance (IA)

- The definition declares two main drivers behind security decisions:
  - **Risk analysis** - IA does not attempt to eliminate all risks, the risks should be prioritized according to the organization's specifics, and reduced to an acceptable level.
  - **Cost-effectiveness** - IA does not attempt to achieve security at any price, but in a most efficient and cost-effective way.
- Generally, Information Assurance is a broad field that **there is no universally accepted definition.**
- Information assurance encompasses a broader scope than **information security, network security,** and **computer security.**

# Introduction and Terminology

## ❑ Information Assurance (IA)

- The U.S Department of Defense (DoD) breaks down IA into three basic elements — people, technology, and operations.
  - **People** are the most crucial aspect of IA. The challenge is to provide the right amount and type of training to all the people and to develop a human resources strategy that brings the right people to bear at the right time and place.
  - **Operation** consists of two main aspects: **system management** and **situation awareness.** Operations **also include the security procedures required to ensure that system defences quickly adapt in response to changing threats.**
  - The element of **Technology** includes all tools /hardware or software/ which are used to protect information and information systems: within the network at large; at the enclave boundary; and within the computing environment of an enterprise.

# bing

- **Information Assurance (IA)** is the practice of assuring information and managing risks related to the use, processing, storage, and transmission of information and information systems[2]. Information Assurance includes protection of the integrity, availability, authenticity, non-repudiation and confidentiality of user data[2].
- IA also encompasses physical and digital protections, as well as business aspects such as privacy, regulatory and standards compliance, auditing, business continuity, and disaster recovery[2]. IA is an interdisciplinary field that requires expertise in various domains such as business, accounting, user experience, fraud examination, forensic science, management science, systems engineering, security engineering, and criminology[2].
- IA is different from information security (IS), which is a subset of IA that focuses on **the creation and application of security controls** to protect information and information systems. IA is more concerned with the business level and strategic risk management of information and related systems[2].
- IA is also related to information risk management (IRM), which is the process of identifying, assessing, and mitigating risks to information and information systems. IA is the desired outcome of IRM[2].

# Introduction and Terminology

## ❑ Information Security

- It refers to the processes and methodologies which are designed and implemented to protect information or data:-
  - From unauthorized access, use, misuse, disclosure(ይፋ ማድረግ), destruction(ጥፋት፣), modification, or disruption(መቋረጥ).
  - Information can be printed, electronic, or any other form of confidential, private and sensitive information or data.
- It is concerned with the confidentiality, integrity and availability of data regardless of the form the data may take: electronic, printed, or other forms.
- It means **protecting information and information systems from illegal operations.**
- Information security is also about working with employees and management to make sure that everyone is aware of current threats and how they can protect their information and systems.

# Introduction and Terminology

## ❑ Information Security

- The terms information security, computer security and network security are frequently used interchangeably.
- These fields are interrelated often and share the common goals of protecting the confidentiality, integrity and availability of information; however, there are some subtle differences between them.
  - **Information security**: refers to the processes and methodologies that are designed and implemented to protect print, electronic, or any other form of confidential, private and sensitive information or data from unauthorized access, use, misuse, disclosure, destruction, modification, perusal, inspection, recording or disruption.
  - **Computer security**: is the generic name for the collection of tools designed to protect the processed and stored data and to hinder hackers.
  - **Network security**: is the generic name for the collection of tools designed to protect data during their transmission over a collection of interconnected networks.

# The Causes of insecurity

- The insecurity of computer systems and networks goes much further than the well-known computer viruses, and has now **become a priority.**
- In the networked world, the new generation of criminals does not need to have physical contact with the victim.
- Data can be easily copied, transmitted, modified or destroyed.
- As a result, the scene of crime is a particularly difficult one: there are no traces, identification of the culprits is nearly impossible, apprehension even more so and the legal framework does not make adequate provision for justice in this kind of crime.
- The real-time nature of the Internet adds a further dimension to crime.
- While many causes exist for security problems, at **least three types of fundamental weaknesses open the door to security problems**.
  - **Technology weakness**
  - **Policy weakness**
  - **Configuration weakness**

# Computer Security… Vulnerabilities

- Types of Vulnerabilities
  - Physical vulnerabilities (e.g. Computer can be stolen)
  - Natural vulnerabilities (e.g. Earthquake)
  - Hardware and Software vulnerabilities (e.g. Failures)
  - Media vulnerabilities (e.g. Hard disks can be stolen)
  - Communication vulnerabilities (e.g. Wires can be tapped)
  - Human vulnerabilities (e.g. Insiders)

## ❑ Computer Security… Consequences of risks

- Failure/End of service.
- Reduction of QoS (quality of service), down to Denial of Service (DoS)
- Trust decrease from partners (client, providers, share-holders)
- Human consequences (personal data, sensitive data - medical, insurances, …)

# bing

- There are different types of vulnerabilities that can affect the security of information and information systems. Some of the common types are:
- - **Software vulnerabilities**: These are flaws or weaknesses in the software products that can be exploited by cybercriminals to compromise the system or data. Software vulnerabilities can result from programming errors, design flaws, or unpatched software[1].
- **- Network vulnerabilities**: These are flaws or weaknesses in the network infrastructure that can allow cybercriminals to gain unauthorized access and cause harm. Network vulnerabilities can include poorly-protected wireless access, misconfigured firewalls, weak encryption, or exposed ports[2].
- **- Physical vulnerabilities**: These are flaws or weaknesses in the physical security of the system or data that can allow cybercriminals to access them through physical means. Physical vulnerabilities can include unlocked doors, camera blind spots, inadequate documentation, or stolen devices[3].
- **- Human vulnerabilities**: These are flaws or weaknesses in the human behavior or awareness that can allow cybercriminals to manipulate or deceive them into compromising the system or data. Human vulnerabilities can include phishing, social engineering, weak passwords, or insider threats[3].

# Security Goals

- **Security is expressed in terms of**

1. **Confidentiality (Privacy)**

- It requires that the **message must only be viewed and accessible by authorized parties.**
- It also requires that the system should **verify the identity of a user.**
- Only authorized people or systems can access protected data which refers to **Data Confidentiality.**
- The other confidentiality is in terms of **Privacy,** which assures that **individuals control or influence what information be collected and stored** **and** **by whom and to whom that information m be disclosed**

- Measures how secure is the information?
- How secured the data need to be?
- **Best methods:**
  - Physical protection
    - Locking the door, fence, security camera…
  - Electronic protection
    - Encryption, password, firewall, authentication…

**Failure of confidentiality occurs when someone can obtain and view the data.**

# Security Goals

- **Security is expressed in terms of:**

1. **Confidentiality (Privacy)**

- An organization needs to guard against malicious actions that endanger the confidentiality of its information.
- Confidentiality **not only applies to the storage of information but also applies to the transmission of information.**
- **When we send a piece of information to be stored in a remote computer or when we retrieve a piece of information from a remote computer, we need to conceal (cover) it during transmission.**

➢ There are many countermeasures that organizations put in place to ensure confidentiality.

- **Passwords, access control lists and authentication procedures** use software to control access to resources, volume and file encryption, and Unix file permissions.
- These access control methods are complemented by the use encryption to protect information that can be accessed despite the controls, such as emails that are in transit.

# Bing... privacy vs confidentiality

- Confidentiality and privacy are related but distinct concepts that often apply to information security. According to one source[1], the difference between confidentiality and privacy can be stated as follows:
- - Confidentiality is about the data, and privacy is about the individual.
- - Confidentiality is the assurance that only authorized parties can access data, and privacy is the ability of an individual to be forgotten, or free from public attention.
- - Confidentiality is focused on preventing access of data by unauthorized parties, and privacy is focused on preventing identification of individuals by data.
- Some examples of confidentiality and privacy are:
- - Confidentiality: Encrypting data before sending it over the internet, using passwords or biometrics to restrict access to data, classifying data according to its sensitivity and applying different levels of protection.
- - Privacy: Anonymizing or de-identifying data before sharing it with others, allowing individuals to opt out of data collection or request deletion of their data, complying with privacy laws and regulations such as GDPR or HIPAA

# Security Goals

- **Security is expressed in terms of:**

**2. Integrity**

- Integrity means that **changes need to be done only by authorized entities** and **through authorized mechanisms.**
- For example, in a bank when a customer deposits or withdraws money, the balance of his account needs to be changed.
- Information needs to be changed constantly.
- Integrity violation is not necessarily the result of a malicious act; an interruption in the system, such as a power surge(የኃይል መጨመር) may also create unwanted change in some information.
- Integrity covers two related concepts these are **Data integrity** which **Assures that information (both stored and in transmitted packets) and programs are changed only in a specified and authorized manner.**
- The other is **System integrity** which **Assures that a system performs its intended function in an unimpaired (undamaged) manner**, free from deliberate or inadvertent unauthorized manipulation of the system.

# Security Goals

- **Security is expressed in terms of:**

2. **Integrity**

- It requires that **messages should be modified or altered only by authorized parties.**
- Modification includes writing, changing, deleting, and creating the message that is supposed to be transmitted across the network.
- Integrity guarantees that no modification, addition, or deletion is done to the message.(by unauthorized user jechuu qaba ture)

Failure of integrity occurs if someone modifies the data being stored in or transmit.

# Security Goals

- **Security is expressed in terms of:**

3. **Availability (Denial of Service)**
   - The information created and stored by an organization **need to be available to authorized entities.**
   - **Availability measures protect timely and un-interrupted access to the system.**
   - It requires that computer and network assets are only available to authorized parties.
   - ***Computer and network should provide*** *all the designated services* ***in the presence of all kinds of security attack.***
   - **threats to availability are mostly non-malicious in nature**, its **hardware failures**, **unscheduled software downtime** and **network bandwidth issues**.
   - How much uptime is the system providing the service?
   - Is the data accessible by users at all times?
   - Failure of availability occurs if the data cannot be accessed by the end users. (by authorized user jechuudha)

# Security Goals

- **Security is expressed in terms of:**

4. **Non-repudiation**
   - Non-repudiation **prevents either sender or receiver from denying a transmitted message.**
   - This capability is crucial to e-commerce.
   - Without it an individual or entity can deny **that he, she or it is responsible for a transaction, therefore not financially liable.**
5. **Authentication**
   - Authentication is a **foundations of security**. (ማረጋገጥ የደህንነት መሰረት ነው።)
   - In its absence, security properties can be violated.
   - Assures that a communication is authentic.
   - The property of being genuine and being able to be **verified and trusted; confidence in the validity of a transmission, a message, or message originator.**
   - This means **verifying that users** are who they are and that **each input arriving at the system came from a trusted source.**

# Security breach levels

- There are **three levels** of impact on organizations or individuals should there be a breach of security (i.e., a loss of confidentiality, integrity, or availability).
- These levels are: **Low level, moderate level and high level.**

1. **Low: The loss could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.**

- A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might:
  - Cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced.
  - Result in minor damage to organizational assets.
  - Result in minor financial loss; or
  - Result in minor harm to individuals.

# Security breach levels

2. **Moderate: The loss could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.**

- A serious adverse effect means that, for example, the loss might:
  - Cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced;
  - Result in significant damage to organizational assets;
  - Result in significant financial loss; or
  - Result in significant harm to individuals that does not involve loss of life or serious, life threatening injuries.

# Security breach levels

3. **High: The loss could be expected to have a severe(ከባድ) or catastrophic(አስከፊ) adverse effect on organizational operations, organizational assets, or individuals.**

- A severe or catastrophic adverse effect means that, for example, the loss might:
  - Cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions;
  - Result in major damage to organizational assets;
  - Result in major financial loss; or
  - Result in severe or catastrophic harm to individuals involving loss of life or serious, life threatening injuries.

# The Challenges of Computer Security

- **Computer and network security is both fascinating(ማራኪ) and complex. Some of the reasons follow:**

1. Security is not as simple as it might first appear to the novice. The requirements seem to be straightforward; indeed, most of the major requirements for security services can be given self explanatory, one-word labels: confidentiality, authentication, nonrepudiation, or integrity. But the mechanisms used to meet those requirements can be quite, complex, and understanding them may involve rather subtle(ረቂቅ) reasoning.
2. In developing a particular security mechanism or algorithm, one must always consider potential attacks on those security features. In many cases, successful attacks are designed by looking at the problem in a completely different way, therefore exploiting an unexpected weakness in the mechanism.
3. Because of point 2, the procedures used to provide particular services are often counter intuitive. Typically, a security mechanism is complex, and it is not obvious from the statement of a particular requirement that such elaborate measures are needed. It is only when the various aspects of the threat are considered that elaborate security mechanisms make sense.

# The Challenges of Computer Security

4. Having designed various security mechanisms, it is necessary to decide where to use them. This is true both in terms of physical placement (e.g., at what points in a network are certain security mechanisms needed) and in a logical sense (e.g., at what layer or layers of an architecture such as TCP/IP should mechanisms be placed).

5. Security mechanisms typically involve more than a particular algorithm or protocol. They also require that participants be in possession of some secret information (e.g., an encryption key), which raises questions about the creation, distribution, and protection of that secret information. There also may be a reliance on communications protocols whose behaviour may complicate the task of developing the security mechanism. For example, if the proper functioning of the security mechanism requires setting time limits on the transit time of a message from sender to receiver, then any protocol or network that introduces variable, unpredictable delays may render such time limits meaningless.

# The Challenges of Computer Security

6. **Computer and network security is essentially a battle of wits between a perpetrator(ወንጀለኛ) (criminal) who tries to find holes and the designer or administrator who tries to close them.** The great advantage that the attacker has is that he or she need only find a single weakness, while the designer must find and eliminate all weaknesses to achieve perfect security.
7. There is a natural tendency on the part of users and system managers to perceive little benefit from security investment until a security failure occurs.
8. **Security requires** regular, even constant, monitoring(hordoffi), and this is difficult in today's short-term, overloaded environment.
9. Security is still too often an afterthought to be incorporated into a system after the design is complete rather than being an integral part of the design process.
10. Many users and even security administrators view strong security as an impediment(እንቅፋት) to efficient and user-friendly operation of an information system or use of information.

# The OSI Security Architecture

- The OSI security architecture **focuses on security attacks, mechanisms, and services.** These can be defined briefly as
  1. **Security attack:** Any action that compromises (balaadhaaf saaxilu) the security of information owned by an organization.
  2. **Security mechanism:** A process (or a device incorporating such a process) that is designed **to detect, prevent, or recover** from a security attack.
  3. **Security service:** A processing or communication service **that enhances** the security of the data processing systems and the information transfers of an organization.
- **The services are intended to counter security attacks**, and they make use of one or more security mechanisms to provide the service.

# Security Attacks

- **Security attacks** can be characterized as the **different sorts of systematic activities** aimed at decreasing or corrupting the security.
- From this perspective, **an attack can be defined as a systematic threat generated by an entity in an artificial, deliberate (beekaa) and intelligent way.**
- The terms threat (a **possible danger that might exploit a vulnerability**) and attack (a deliberate attempt to evade(miliquu) security services) are commonly used to mean more or less the same thing.
- Conceptually, the security attacks can be classified into two types that are active and passive attacks where the attacker gains illegal access to the system's resources.

  **A. Passive attacks**

  **B. Active attacks**

# bing

- Attack and threat are two related but distinct concepts in information security. According to one source[1], the difference between attack and threat can be stated as follows:
- - Attack is intentional, threat can be intentional or unintentional.
- - Attack is malicious, threat may or may not be malicious.
- - Attack is an objective to cause damage, threat is a circumstance that has the ability to cause damage.
- - Attack has a high chance of information alteration and damage, threat may or may not alter or damage information.
- - Attack is comparatively easy to detect, threat is comparatively hard to detect.

Some examples of attacks and threats are:

- - Attack: A hacker exploits a vulnerability in a system and steals confidential data or disrupts the service.
- - Threat: A natural disaster such as a flood or an earthquake that damages the infrastructure and affects the availability of data and systems.

# bing

- Malicious software can be used for both passive and active attacks. A passive attack is a type of cyberattack that involves the use of malicious software, such as spyware, malware, and other malicious programs, to monitor, intercept, or eavesdrop on data transmissions without altering or affecting them[3]. A passive attack is an attack on the confidentiality of the data. For example, an attacker can use spyware to steal sensitive information from a user's computer or network.
- An active attack is a type of cyberattack that involves the use of malicious software, such as viruses, ransomware, keyloggers, trojans, worms, and other malicious programs, to alter, destroy, or disrupt the normal operation of a system or network[1]. An active attack involves the attacker taking direct action against the target system or network, and can be more dangerous than passive attacks[2]. An active attack can be an attack on the integrity, availability, or authentication of the data.
- For example, an attacker can use **ransomware** to encrypt the data on a user's computer or network and demand payment for decryption.

# bing

- **Keyloggers** are a type of spyware that can record and steal what you type on your computer or mobile device. Keyloggers can be used for legitimate purposes, such as monitoring employees or troubleshooting issues, but they can also be used for malicious purposes, such as stealing passwords, credit card numbers, or other sensitive information[1].
- Keyloggers can be either hardware devices that are attached to the keyboard or software programs that run in the background[2].
- Keyloggers can capture every keystroke you enter, as well as take screenshots, record audio, or track your web browsing activity[3]. Keyloggers can be hard to detect and remove, so it is important to protect yourself from this threat.

# Security Attacks

- **Passive attacks**
- A passive attack attempt to learn or make **use of the information without changing the content** of the message and disrupting the operation of the communication.
- A passive attack is one where the attacker **only monitors(hordofuu)** the communication channel.
- A passive attacker **only threatens the confidentiality of data**.
- Due to passive attack, there is **no any harm to the system**.
- The goal of the opponent is **to obtain information** that is being transmitted.
- Passive attacks are in the **nature of eavesdropping** on, or monitoring of, transmissions.
- The attacker **observes** the content of messages or **copy** the content of messages.
- The eavesdropper does **not make any changes** to the data or the system.

# Security Attacks

- **Passive attacks**
- **Passive attacks are very difficult to detect.**
  - Message transmission apparently normal.
  - No alteration of the data.
  - Neither the sender nor receiver is aware that a third party has read the messages or observed the traffic pattern.
- **Emphasis on prevention rather than detection** by means of encryption.
- These types of attacks **threaten the confidentiality of information**.
- Two types of passive attacks are related to **message contents and traffic analysis:**

# Security Attacks

- **Passive attacks**

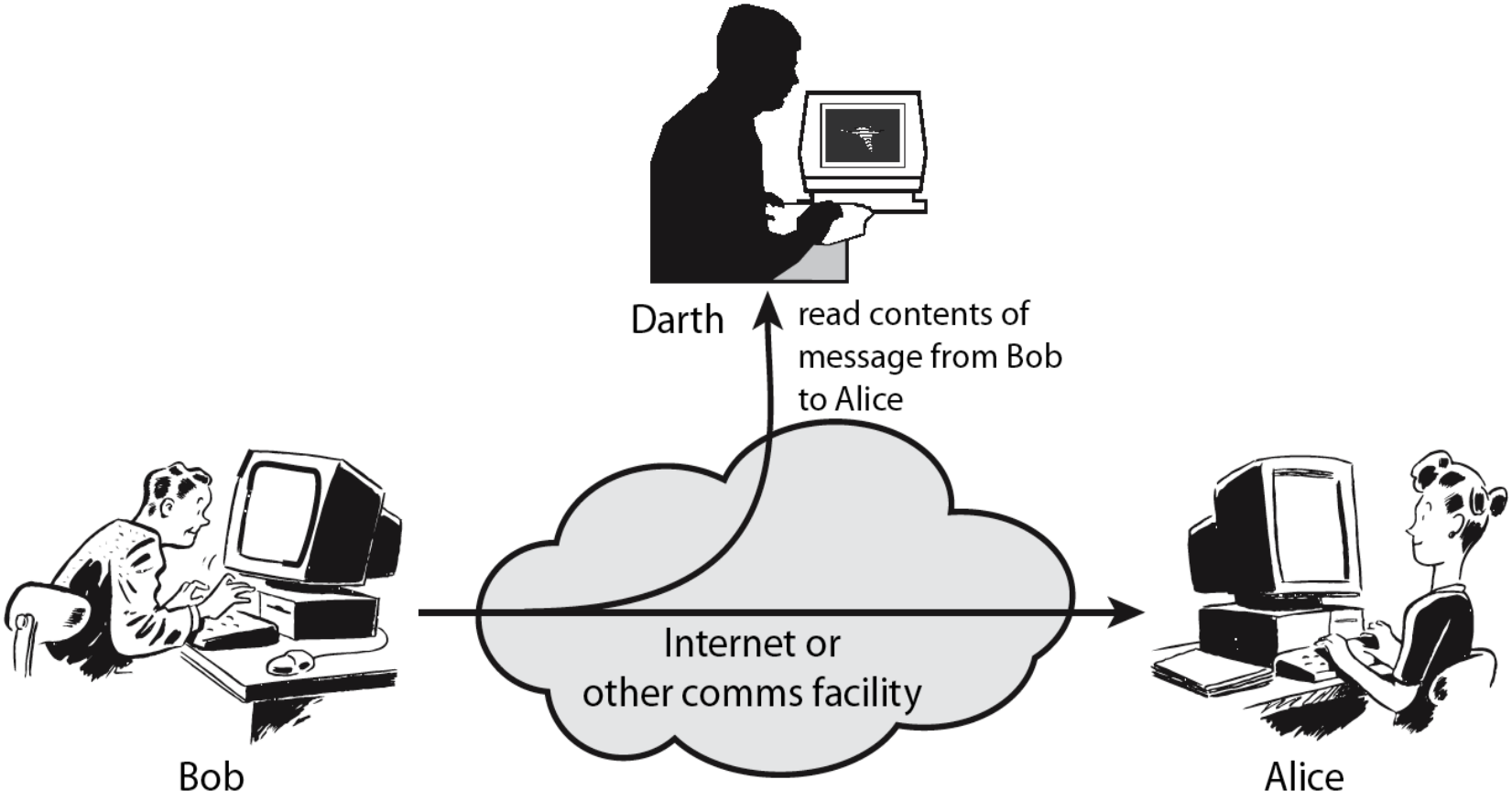
1. **Eavesdropping(dhageefataa) / Snooping:** (secretly listen to a communication)

- The majority of network communications occur in an unsecured or "clear text" format, which allows an attacker who has gained access to data paths in the network to **"listen in"** or interpret (read) the data exchanged over the network.
- The ability of an eavesdropper to monitor the network is generally the biggest security problem.
- Without strong encryption services that are based on cryptography, the data can be read by others as it traverses the network.
- **Snooping** refers to unauthorized access to or interception of data.
- For example, a file transferred through the internet may contain confidential information.
- An unauthorized entity may intercept the transmission and use the contents for his own benefit.

# Security Attacks

- **Passive attacks**

1. **Eavesdropping / Snooping:** (secretly listen to a



# Security Attacks

- **Passive attacks**

**2. Traffic Analysis:**

- An unauthorized entity can obtain some other **type information by monitoring online traffic.**
- For example, he can find the **email id** of the sender or the receiver, he can collect pairs of request and response to help him guess the nature of transaction **Traffic analysis:**
- It refers to the process of intercepting and examining messages in order to deduce information from patterns in communication.
- It can be performed even when the messages are encrypted and cannot be decrypted.
- In general, the greater the number of messages observed, or even intercepted and stored, the more can be inferred from the traffic.

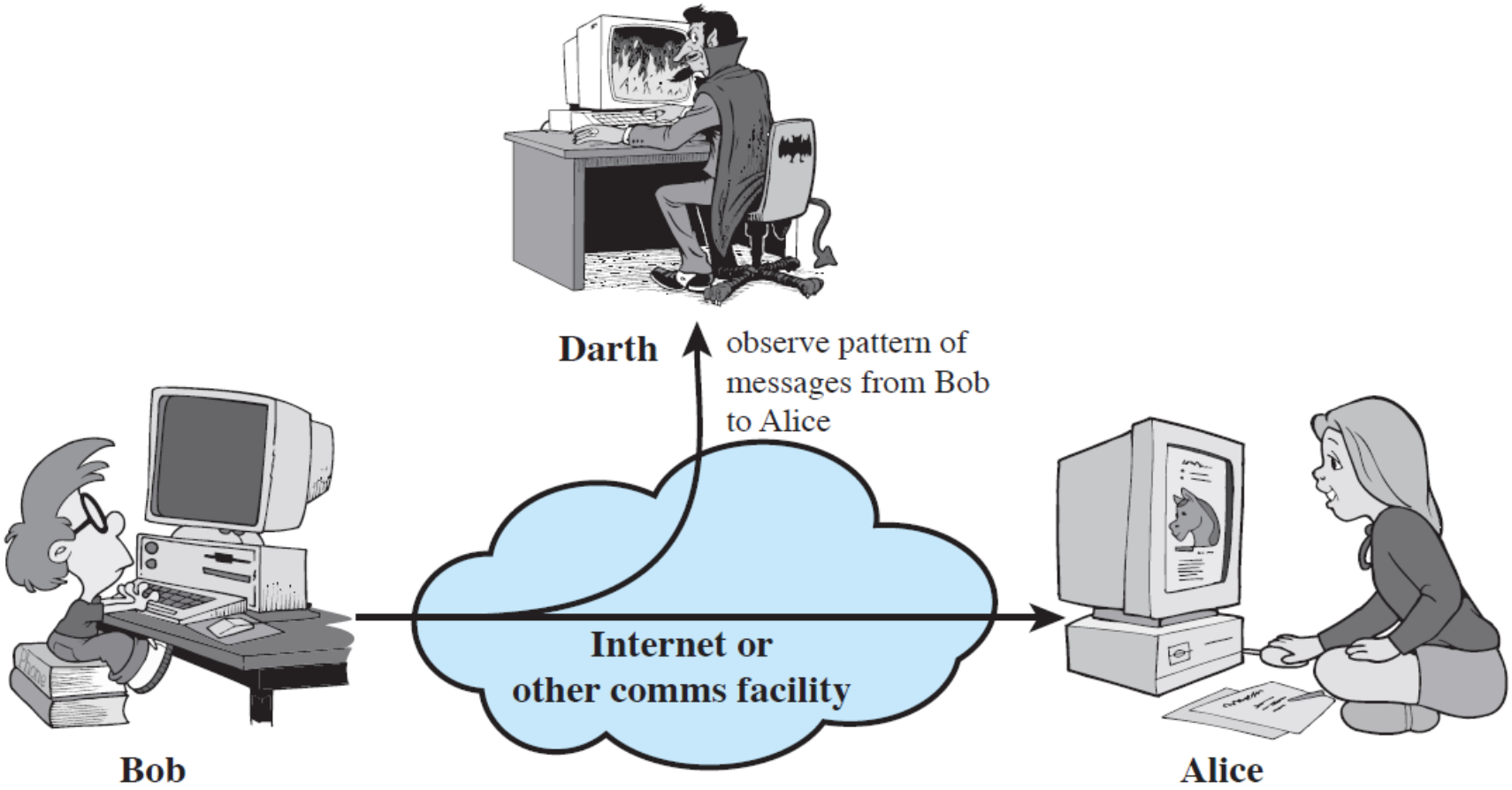
# bing

- That is correct. Traffic analysis can be performed even when the messages are encrypted and cannot be decrypted. Traffic analysis does not rely on the contents of the messages, but on the patterns and characteristics of the data packets, such as their source, destination, frequency, size, or duration. Traffic analysis can be used to infer information about the communication or the network activity without reading the contents of the data packets. For example, traffic analysis can reveal who is communicating with whom, how often, how long, or what type of service they are using. Traffic analysis can also identify the type, location, or activity of the devices or users on the network.

# Security Attacks

- **Passive attacks**

## 2. Traffic Analysis:



# bing

- Traffic analysis and sniffing are both types of passive security attacks that involve capturing and analyzing the data packets passing through a network[1]. However, they differ in their scope and purpose. Traffic analysis focuses on the patterns and characteristics of the data packets, such as their source, destination, frequency, size, or duration[2]. Traffic analysis can be used to infer information about the communication or the network activity without reading the contents of the data packets[2].
- Sniffing focuses on the contents of the data packets, such as their headers, payloads, or protocols[3]. Sniffing can be used to steal sensitive information, such as login credentials, email messages, financial data, or trade secrets[3]. Both traffic analysis and sniffing can be performed on any type of network, such as wired, wireless, or public networks[13]. Both traffic analysis and sniffing can be prevented by using encryption, authentication, and noise generation techniques to protect the data and the network[3].

# Security Attacks

- **Active attacks**
- Attempts to interrupt, modify, delete, or fabricate messages or information thereby disrupting normal operation of the network.
- **Active attacks try to alter system resources or affect their operation.**
  - Modification of data, or creation of false data
- An active attacker **threatens data integrity, authentication as well as confidentiality.**
- The most important thing is that, in active attack, Victim gets informed about the attack.
- Active attacks involve some modification of the data stream or the creation of a false stream and can be **divided into six categories:**

# bing

- Active attacks are security attacks in which an attacker attempts to alter, destroy, or disrupt the data or the normal operation of a system or network[1]. There are many types of active attacks, but some of the most common ones are[2][3]:
- - **Masquerade attack**: An attack in which an intruder pretends to be another user or entity to gain access or privileges that they are not authorized for. For example, an attacker may use a stolen login ID and password to access a system or network.
- - **Modification of messages attack**: An attack in which an intruder alters the data packets passing through a network, such as changing their contents, headers, or addresses. For example, an attacker may modify the amount or destination of a money transfer request.
- - **Repudiation attack**: An attack in which an intruder denies their involvement in a communication or transaction, or denies the validity of a message or document. For example, an attacker may forge a digital signature or tamper with a log file to avoid accountability.

# bing

- - **Replay attack**: An attack in which an intruder captures and resends a data packet that was previously sent by a legitimate user or entity. For example, an attacker may replay an authentication message to gain access to a system or network.
- - **Denial-of-service (DoS) and distributed denial-of-service (DDoS) attack**: An attack in which an intruder overwhelms the resources of a system or network and prevents it from responding to legitimate requests. For example, an attacker may flood a server with bogus requests or packets to cause slowdowns, errors, or outages.
- - **Zero-day exploit**: An attack in which an intruder exploits a previously unknown vulnerability in a system or network before a patch or solution is available. For example, an attacker may use a zero-day exploit to compromise the security of any system or network that has the vulnerability.

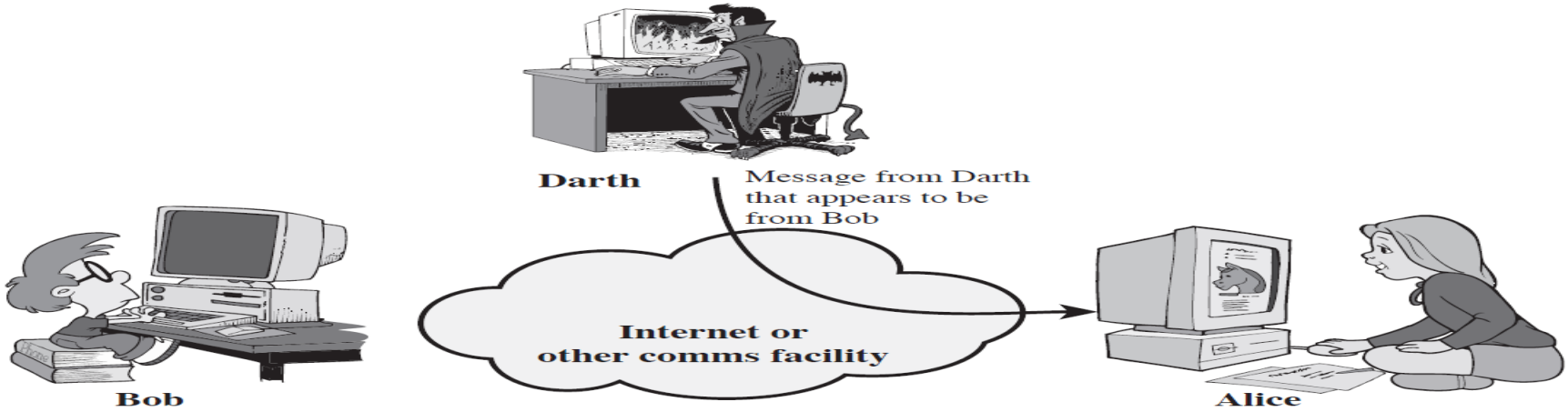
# Security Attacks

- **Active attacks**

1. **Masquerade**: It is a type of attack where the attacker pretends(ያስመስላል) to be an authorized user of a system in order to gain access to it or to gain greater privileges than they are authorized for.

- **Masquerading** or **spoofing**, happens when the **attacker impersonates(ያስመስላል) somebody else.**
- For example, the attacker might steal the bank card and PIN of a

Customer and pretend that he is that customer.



# bing

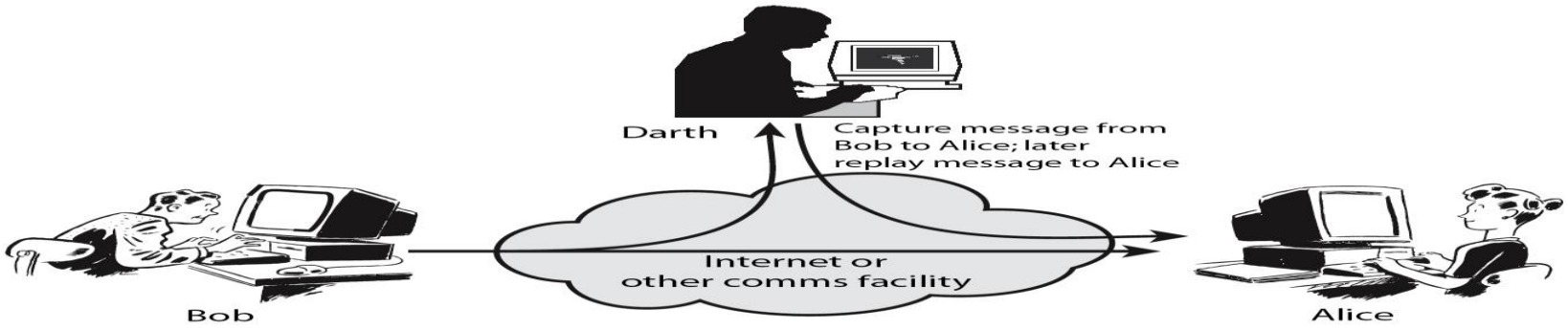
- Spoofing is a type of security attack in which an attacker pretends to be someone or something else to deceive the victim or gain their trust[1].
- Spoofing can involve changing or faking the email address, sender name, phone number, or website URL of the attacker to make it look like it belongs to a legitimate or trusted entity[2].
- Spoofing can be used to launch phishing attacks, which are attempts to trick the victim into revealing sensitive information or installing malware.
- Spoofing can also be used to bypass access controls, impersonate services, or redirect traffic[3].
- Spoofing can be prevented by using encryption, authentication, and verification techniques to protect the communication and the network[2].

# Security Attacks

- **Active attacks**

2. **Replay**: In this kind of attack, a **valid data transmission is maliciously or fraudulently repeated or delayed.**

- This is carried out either by the originator or by an adversary (opponent) who intercepts the data and retransmits them, **possibly as part of a masquerade attack.**
- **The attacker obtains a copy of a message sent by the user and later tries to reply it.**
- For example, a person sends a request to his bank to ask for payment to the attacker who has done job for him. The attacker intercepts the message and sends it again to receive another payment from the bank.



# bing

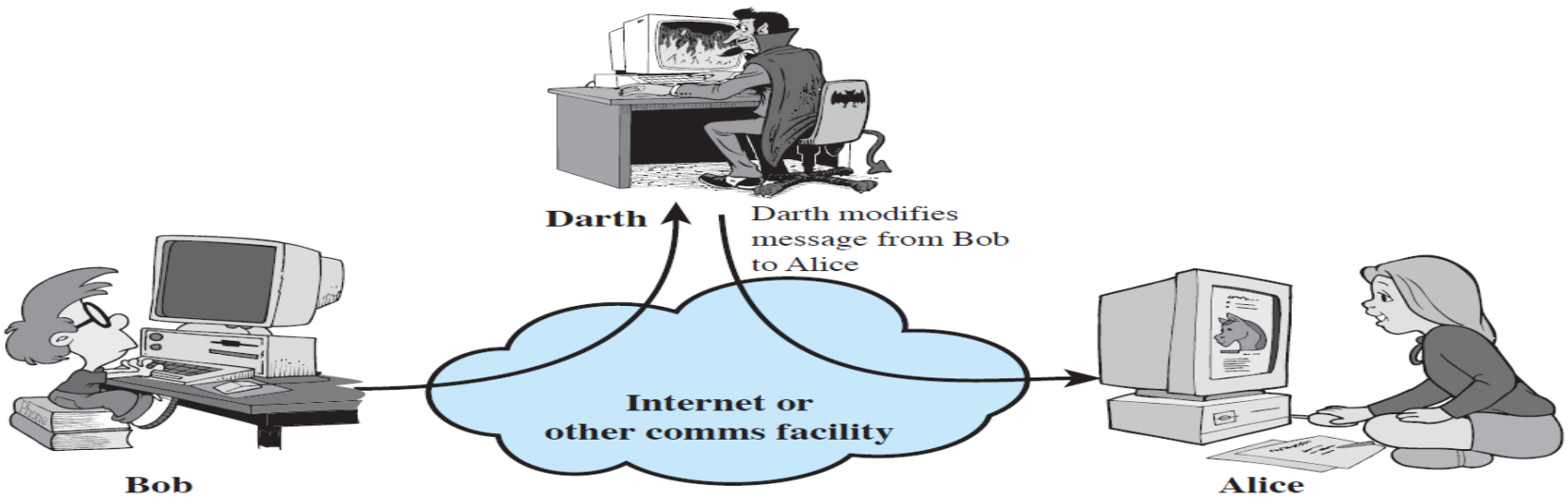
- A replay attack is a type of security attack in which an attacker captures and resends a data packet that was previously sent by a legitimate user or entity[1].
- A replay attack can be used to gain unauthorized access to a system or network, or to impersonate a user or entity[2]. For example, an attacker may replay an authentication message to gain access to a system or network, or replay a money transfer request to cause double spending[3].
- A replay attack can be prevented by using encryption, authentication, and verification techniques to protect the data and the network[12]. For example, a session ID, a timestamp, or a nonce can be used to ensure that each data packet is unique and valid for only one transaction[23].

# Security Attacks

- **Active attacks**

3. **Modification of messages:** The attacker **removes a message from the network traffic, alters it, and reinserts it.**

- **Modification:** After intercepting or accessing information, the attacker modifies the information to make it beneficial to himself. For example, a customer sends a message to a bank to do some transaction, and the attacker intercepts the message and changes the type of transaction to benefit him.



# bing

- Modification of messages is a type of active security attack in which an attacker alters the data packets passing through a network, such as changing their contents, headers, or addresses[1]. Modification of messages can be used to compromise the integrity, authenticity, or functionality of the data or the system[2].
- For example, an attacker may modify the amount or destination of a money transfer request, or alter the commands or programs on a target machine(ajjaja hin taane hojachiisuf command jijira)[3].
- Modification of messages can be prevented by using encryption, authentication, and verification techniques to protect the data and the network[12].
- For example, a message digest, a digital signature, or a checksum can be used to ensure that the data has not been tampered with[23].

# Security Attacks

- **Active attacks**

4. **Repudiation**: It is performed by one of the parties in the communication: the sender or the receiver.

- The sender of the message might later **deny that he has sent the message**; the receiver of the message might later **deny that he has received the massage.**
- For example, customer ask his Bank "To transfer an amount to someone" and later on the sender(customer) deny that he had made such a request. This is repudiation.

# Security Attacks

- **Active attacks**

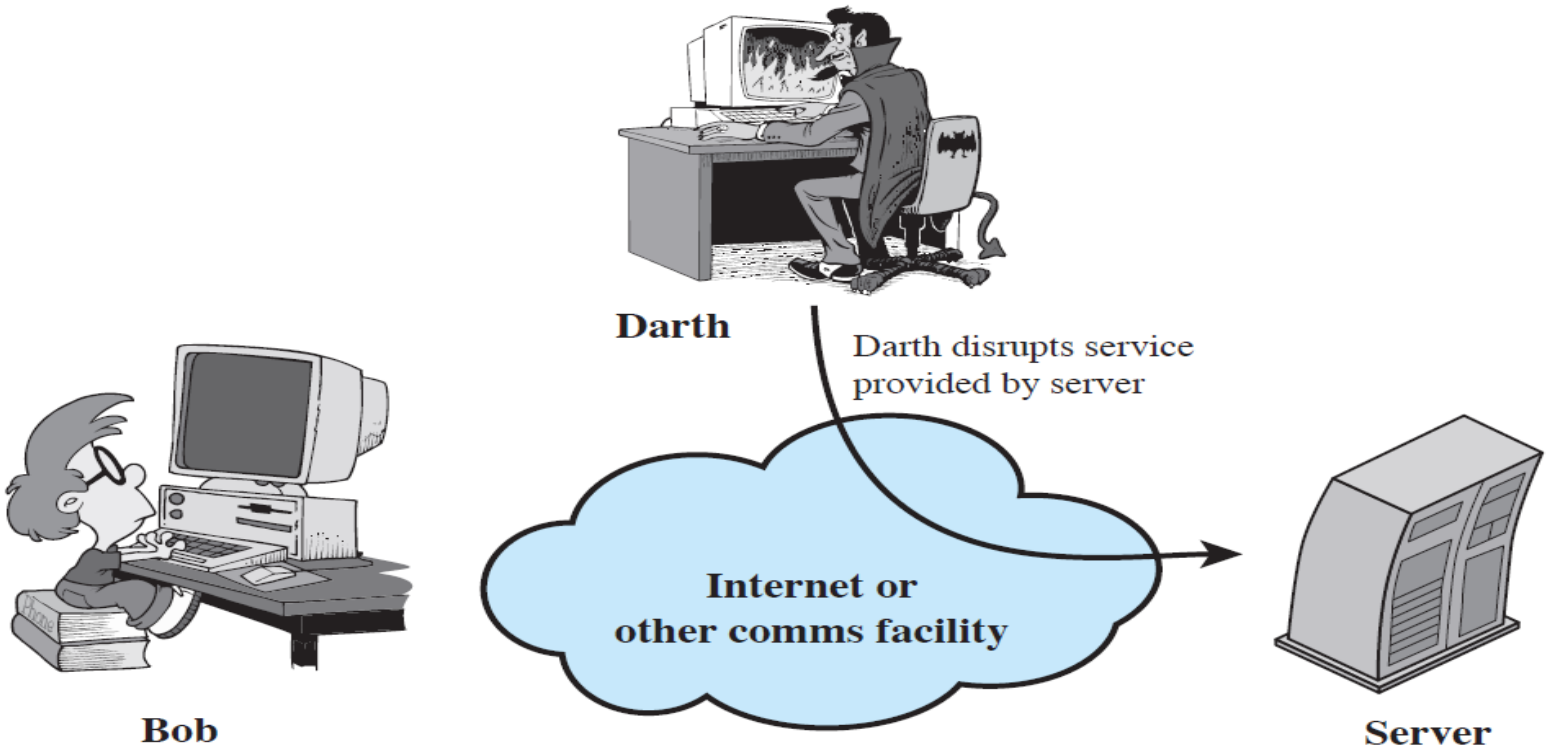
5. **Denial of service (DoS)**

- In a DoS attack, an attacker attempts to prevent legitimate users **from accessing information or services.**
- **This attack threatens availability.**
- It may **slow down or totally interrupt the service of a system.**
- The attacker can use several strategies to achieve this.
  - He may send **so many fake (bogus) requests to a server** that the server crushes because of heavy load.
  - The attacker may **intercept and delete a server's response to a client,** making the client believe that the server is **not responding.**

# Security Attacks

- **Active attacks**

5. **Denial of service (DoS)**



# Security Attacks

- **Active attacks**

6. **Advanced Persistent Threat (APT):** It is a network attack in which an unauthorized person gains access to a network and stays there undetected for a long period of time.

- The intention of an APT attack is to steal data rather than cause damage to the network or organization.
- APT attacks target organizations in sectors with high-value information, such as national defense, manufacturing and the financial industry.

❑ Generally:-

- An active attack usually requires more effort and often more dangerous implication.
- When the hacker attempts to attack, the victim gets aware of it.
- The active attacks can be in the form of **interruption**, **modification** and **fabrication**.

# bing

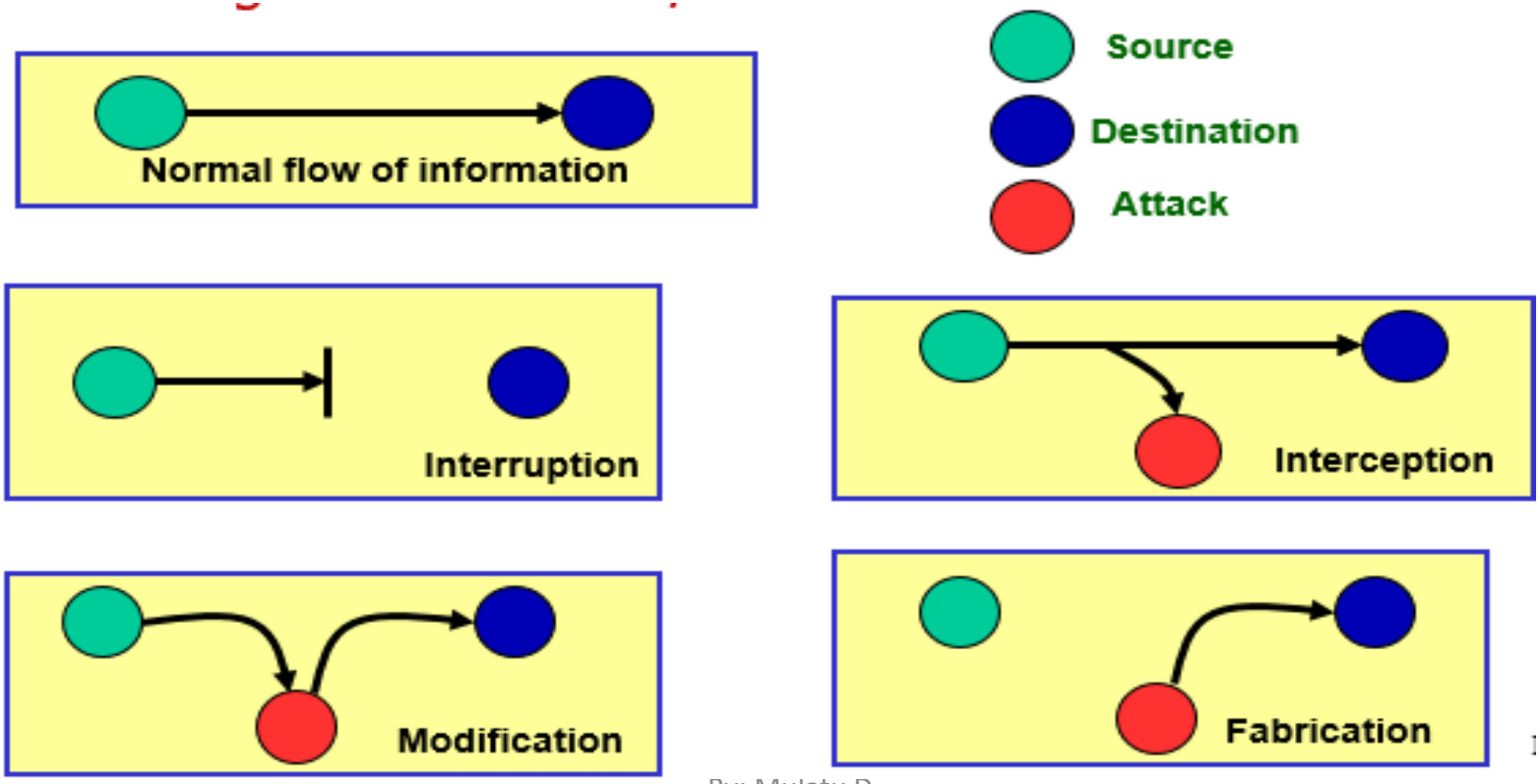
- An advanced persistent threat (APT) is a type of cyberattack in which the attacker gains and maintains unauthorized access to a targeted network for a long period of time, usually with the intention of stealing sensitive data or conducting espionage[1]. APTs are sophisticated, stealthy, and often sponsored by nation-states or organized groups[2]. APTs use various techniques to infiltrate, expand, and persist in the network, such as exploiting vulnerabilities, using malware, phishing, social engineering, or compromising insiders[3]. APTs can cause significant damage to the victims, such as intellectual property theft, data breaches, sabotage, or disruption of critical services[3].

# bing

- An APT can be considered both an active and a passive attack, depending on the stage and the objective of the attack. An active attack is one that attempts to alter or affect the system or data, while a passive attack is one that only observes or monitors the system or data. In general, an APT starts as a passive attack, where the attacker tries to gain access and reconnaissance without being detected. Then, it becomes an active attack, where the attacker tries to expand, persist, and exfiltrate data or cause damage. However, an APT can also switch between active and passive modes depending on the situation and the goal of the attacker.

# Security Attacks

- **Active attacks**
- **Interruption:** An attack on availability
- **Modification:** An attack on integrity
- **Fabrication:** An attack on authenticity, cause DOS



# bing

The types of active attacks you listed are:

- - **Interruption**: An attack on availability that prevents normal access or use of the system or network.

For example, a denial-of-service (DoS) attack that floods the target with unwanted traffic or requests[2].

- - **Modification**: An attack on integrity that alters the data or messages in transit or at rest.

For example, a message modification attack that changes the packet header addresses or the content of the message[2].

- - **Fabrication**: An attack on authenticity that creates or inserts false data or messages into the system or network. For example, a masquerade attack that impersonates a legitimate user or system to gain access or privileges[2].
- - **Replay**: An attack on freshness that captures and resends a valid message or data at a later time.

For example, a session hijacking attack that steals a user's session ID and uses it to access their account[2].

# Security Attacks

- **Comparison between Active attacks and passive**

| BASICS FOR COMPARISION | ACTIVE ATTACK | PASSIVE ATTACK |
|---|---|---|
| Basic | Tries to change the system resources or affect their operation. | Tries to read or make use of information from the system but does not influence system resources. |
| Modification in information | Occurs | Does not occur |
| Harm to the system | Always causes damage to the system. | Always causes damage to the system. |
| Threat to | Integrity and availability | Confidentiality |
| Attack awareness | The entity (victim) gets informed about the attack. | The entity is unaware of the attack. |
| Task performed by the attacker | The transmission is captured by physically controlling the portion of a link | Just need to observe the transmission. |
| Emphasis on | Detection | Prevention |

# Security Services and Mechanism

## ❑ Security Services:

ITU-T (International Telecommunication Union – Telecommunication Standardization Sector (ITU-T) has defined **five services** relating to the security goals and attacks:

### 1. Data Confidentiality:

- This service is designed to protect data from disclosed attacks.
- The services encompasses confidentiality of the whole message or part of a message and also protection against traffic analysis.
- It is designed to protect against **snooping and traffic analysis** attack .

### 2. Data Integrity

- This is designed to **protect the data from modification, insertion, deletion, and replaying by an adversary**.
- It may protect the whole message or the part of the message.

# Security Services and Mechanism

## ❑ Security Services:

ITU-T has defined **five services** relating to the security goals and attacks:

### 3. Authentication

- This service provides the authentication of the party at the other end of the line.
- **In connection-oriented communication, it provides authentication of the sender or receiver during the connection establishment**.
- **In connectionless communication**, **it authenticates the source of the data.**

### 4. Access Control

- This service provides protection against unauthorized access **to data**.
- access includes reading, writing, modifying, executing programs and so on.

5. **Non-repudiation:** This service protects against repudiation by either the sender or the receiver of the data. In non-repudiation with proof of the origin, the receiver of the data can later prove the identity of the sender if denied. In non-repudiation with proof of the delivery, the sender of the data can later prove that data were delivered to the intended recipient

# Security Services and Mechanism

- (ITU-T) provides some security mechanisms to implement those services.

## ❑ Security Mechanism:

- Security mechanism is a process that **implements** security services based on hardware (technical), software (logical), physical or administrative approach.
- **Security mechanisms** support the security services and execute specific activities for the protection against attacks or attack results.
- The security mechanisms are divided into those that are implemented in a specific protocol layer and those that are not specific to any particular protocol layer or security service.
- Security Mechanisms that are specific to a particular OSI security service or protocol layer:

# Security Services and Mechanism

- (ITU-T) provides some security mechanisms to implement those services.

## ❑ Security Mechanism:

### 1 Encipherment

- **is a mechanism** aimed at protecting a message's information content by using mathematical algorithms that transform data into a form that is **not readable** by unauthorized subjects.
- This is used either **to protect the confidentiality of data units** and **traffic flow information** or to support or complement**(itti guutuu)** other security mechanisms.
- **This is hiding or covering data can provide confidentiality**.
- **Two techniques, cryptography** and **steganography**, are used for enciphering.

# Security Services and Mechanism

- (ITU-T) provides some security mechanisms to implement those services.

❑ **Security Mechanism:**

**2 Digital signature**

- This is a means by which the sender can electronically sign the data and the receiver can electronically verify the signature.
- The receiver uses the **sender's public key** to prove that the message is indeed signed by the sender who claims to have sent the message.
- Public and private keys can be used.

3 **Access Control** covers a variety of mechanisms that **enforce access rights to resources**. **This mechanism involves authorization to access some resources.** Access control used methods to prove that a user has access right to the data or resources owned by a system. **Examples of proofs are passwords and PINs.**

# Security Services and Mechanism

- (ITU-T) provides some security mechanisms to implement those services.

## ❑ Security Mechanism:

### 4 Data integrity

- Covers a variety of mechanisms used to **assure the integrity of a data unit or stream of data units.**
- The data integrity mechanism appends to the data **a short check value** that has been created by a specific process from the data itself.
- Data integrity is preserved by comparing **check value received** to the **check value generated.**

### 5 Authentication Exchange

- is a mechanism intended to ensure the identity of an entity by means of information exchange.
- **Two entities exchange some messages to prove their identity to each other.**

# Security Services and Mechanism

- (ITU-T) provides some security mechanisms to implement those services.

❑ **Security Mechanism:**

**6 Traffic Padding**

- This means **inserting some bogus (fake) data into the data traffic** to thwart(ማደናቀፍ) adversary's attempt to use the traffic analysis.

**7 Routing Control**

- This means selecting and **continuously changing different available routes** between the sender and the receiver to prevent the opponent from eavesdropping on a particular route.

**8 Notarization**

- This means **selecting a third trusted party to control the communication between two entities.** This can be done **to prevent repudiation.**

# Security techniques

- The actual implementation of security goals needs some techniques.

- Two techniques are prevalent today: **Cryptography and Steganography**

- **i. Cryptography:** involves the following mechanisms.

**a. Symmetric-key** ( **secret key cryptography**)

- An entity can send a message to another entity over an insure channel with the assumption that an **adversary can not understand the content by simply snooping over the channel**.
- **The sender** encrypts the message using encryption algorithm**.**
- **The receiver** decrypts the message using decryption algorithm**.**
- **A single secret key is used for both encryption and decryption.**
- E.g. AES, DES, RC4 and RC6[1].

# Security techniques

Two techniques are prevalent today: **Cryptography and Steganography**

**i. Cryptography:** involves the following mechanisms.

**b. Asymmetric-key** (**public key cryptography**)

- first there are two key instead of one: one public key and the other private key.
- **the sender** first encrypts the message by using the receiver 's public key.
- **to decrypt the message,** the receiver uses his own private key.
- E.g. RSA, Diffie-Hellman key exchange,DSA, ElGamal and PKCS[1]..

# Security techniques

Two techniques are prevalent today: **Cryptography and Steganography**

## ii. Steganography

- Cryptography is **secret writing**, steganography is **covered writing**.

- Steganography means concealing(dhoksuu) the message itself by covering it with something else.

- E.g. image over text

# bing

- Cryptography and Steganography are two techniques that are used to protect the confidentiality and integrity of data.
- **Cryptography** is the method of hiding information in a particular form so that only the sender and intended recipient can read and understand it[12].
- **Steganography** is the method of hiding information within another non-secret document, image, video, etc. so that it cannot be visualized[23].
- Cryptography scrambles the data using encryption algorithms and keys, while steganography embeds the data using various techniques such as modifying the least significant bits of pixels or frequencies[24].
- Cryptography and Steganography can be used separately or together to achieve different levels of security and secrecy[5].

# bing

- There are various types of steganography that use different mediums to hide information. Some of the common types are:

- - Text steganography: It involves hiding data within text files, such as by using invisible characters, changing the font size or color, or embedding data behind each nth letter of each word[13].
- - Image steganography: It involves hiding data within image files, such as by modifying the least significant bits of pixels, using color palettes, or embedding data in the image header[12].
- - Audio steganography: It involves hiding data within audio files, such as by using low-bit encoding, phase coding, spread spectrum, or echo hiding[12].
- - Video steganography: It involves hiding data within video files, such as by using discrete cosine transform, motion vector technique, or masking and filtering[12].
- - Network steganography: It involves hiding data within network protocols or packets, such as by using timing channels, header fields, or covert channels[12].

- These types of steganography can be used to conceal information from unauthorized parties and avoid detection[12].

# Review Questions

1. Define what information, computer and network security mean?
2. Discuss about goals of security
3. Discuss about the attacks in relation with goals.
4. What do we mean by an attack is active or passive? Give examples for each.
5. Discuss on the security services provided by ITU-T organization.
6. Discuss on the security mechanisms provided by ITU-T organization.
7. What are the actual techniques that can be implemented for security? Discuss about them.

# bing

- Information security, computer security and network security are related but distinct concepts in the field of cybersecurity. According to one source[1], they can be defined as follows:
- - Information security is the protection of information from unauthorized access, use, modification, or disclosure, regardless of where the information is stored or how it is processed[1].
- - Computer security is the protection of computer systems and devices from unauthorized access, use, modification, or damage, including hardware, software, data, and networks[1].
- - Network security is the protection of network devices and resources from unauthorized access, use, modification, or damage, including routers, switches, firewalls, servers, and data[1].
- Information security is a broader term that encompasses computer security and network security, as well as other aspects of cybersecurity such as application security, cloud security, or mobile security[1]. Computer security and network security are more specific terms that focus on the security of different components of information systems. All three concepts are important for ensuring the confidentiality, integrity, and availability of information and systems..

# bing

- The goals of security are the desired outcomes or objectives of implementing security measures to protect information and systems from threats and attacks. The goals of security can vary depending on the context, scope, and nature of the information and systems involved, but they are generally based on the principles of confidentiality, integrity, and availability (CIA) triad[1].
- - Confidentiality is the goal of ensuring that information is only accessible to authorized parties and preventing unauthorized disclosure or leakage of information[1].
- - Integrity is the goal of ensuring that information is accurate, consistent, and trustworthy and preventing unauthorized modification or corruption of information[1].
- - Availability is the goal of ensuring that information and systems are accessible and functional for authorized parties and preventing unauthorized denial or disruption of service[1].
- These goals form the basis of all security programs and information assurance[1]. Information assurance ensures that user data is protected both in transit and throughout storage[2]. To achieve these goals, security measures can include various types of security, such as network security, computer security, application security, cryptography, incident response, vulnerability management, and disaster recovery[3].

# bing

- The attacks in relation with goals are the actions or attempts that aim to compromise or violate one or more of the security goals of confidentiality, integrity, and availability (CIA) triad[1]. The attacks can be classified into two main types: active and passive[2].
- - Active attacks are those that try to alter or affect the system or data, such as modifying, deleting, or disrupting information or services[2]. Active attacks can target any of the security goals, but they usually affect the integrity and availability of information and systems[2]. Some examples of active attacks are viruses, worms, trojans, denial-of-service (DoS) attacks, ransomware, or phishing[2].
- - Passive attacks are those that only observe or monitor the system or data, such as eavesdropping, snooping, or intercepting information[2]. Passive attacks do not affect the system or data directly, but they can compromise the confidentiality of information and lead to further active attacks[2]. Some examples of passive attacks are traffic analysis, wiretapping, port scanning, or keylogging[2].
- To prevent or mitigate these attacks, security measures can include various types of security, such as network security, computer security, application security, cryptography, incident response, vulnerability management, and disaster recovery[3].

# bing

- An attack is active or passive depending on whether it tries to alter or affect the system or data, or only observes or monitors the system or data. Here are some examples for each type of attack:
- - Active attacks: These are attacks that try to modify, delete, or disrupt information or services. For example, a virus that infects and corrupts files, a worm that spreads and consumes network bandwidth, a trojan that opens a backdoor for remote access, a denial-of-service (DoS) attack that floods a server with requests and makes it unavailable, a ransomware that encrypts data and demands payment for decryption, or a phishing email that tricks users into revealing their credentials or installing malware.
- - Passive attacks: These are attacks that only eavesdrop, snoop, or intercept information. For example, a traffic analysis that reveals the source and destination of packets, a wiretapping that captures the content of communications, a port scanning that probes for open ports and services on a host, or a keylogging that records the keystrokes of a user.

# bing

- The security services provided by ITU-T organization are the technical methods and processes that ensure the protection of information and communication systems from threats and attacks. ITU-T is the Telecommunication Standardization Sector of the International Telecommunication Union (ITU), which is a specialized agency of the United Nations for information and communication technologies (ICTs)[1]. ITU-T develops and maintains international standards (called Recommendations) for various aspects of ICTs, including security[2].
- According to ITU-T Recommendation X.800[3], security services are classified into five categories:
- - Authentication: The security service that verifies the identity or role of an entity involved in a communication or data exchange[3].
- - Access control: The security service that controls the access rights and privileges of entities to resources or services[3].
- - Data confidentiality: The security service that protects data from unauthorized disclosure or leakage[3].
- - Data integrity: The security service that protects data from unauthorized modification or corruption[3].
- - Non-repudiation: The security service that provides proof of the origin or delivery of data and prevents the denial of previous actions or commitments[3].
- ITU-T provides various Recommendations for implementing these security services, such as X.509 for public key infrastructure (PKI), X.805 for security architecture, X.1051 for cybersecurity information exchange, X.1361 for distributed ledger technology security, and X.1601 for cloud computing security.

# bing

- The security mechanisms provided by ITU-T organization are the specific methods or techniques that implement the security services to protect information and communication systems from threats and attacks. ITU-T is the Telecommunication Standardization Sector of the International Telecommunication Union (ITU), which is a specialized agency of the United Nations for information and communication technologies (ICTs)[1]. ITU-T develops and maintains international standards (called Recommendations) for various aspects of ICTs, including security[2].
- According to ITU-T Recommendation X.800[3], security mechanisms are classified into two categories:
- - Specific security mechanisms: These are mechanisms that provide a specific security service or function, such as encryption, digital signature, authentication exchange, or access control[3].
- - Pervasive security mechanisms: These are mechanisms that apply to more than one aspect of security or that are not associated with any particular security service, such as trusted functionality, security labels, event detection, security audit trails, or security recovery[3].
- ITU-T provides various Recommendations for specifying these security mechanisms, such as X.509 for public key infrastructure (PKI), X.805 for security architecture, X.1051 for cybersecurity information exchange, X.1361 for distributed ledger technology security, and X.1601 for cloud computing security..

# bing

- The actual techniques that can be implemented for security are the specific methods or tools that apply the security mechanisms to achieve the security services and goals. There are many types of security techniques that can be used for different purposes and scenarios, such as protecting hardware, software, networks, and data from threats and attacks. For example[1]:
- - Physical security techniques include such things as data center perimeter fencing, locks, guards, access control cards, biometric access control systems, and surveillance cameras that prevent unauthorized physical access to resources or systems[1].
- - Cryptographic security techniques include such things as encryption, decryption, digital signature, hashing, and key management that protect the confidentiality, integrity, and non-repudiation of data in transit or at rest[1].
- - Network security techniques include such things as firewalls, intrusion detection and prevention systems (IDS/IPS), virtual private networks (VPN), secure sockets layer (SSL), transport layer security (TLS), and network access control (NAC) that protect the network devices and resources from unauthorized access, use, modification, or damage[2].
- - Computer security techniques include such things as antivirus software, antimalware software, patch management, backup and recovery, secure boot, secure erase, and password management that protect the computer systems and devices from unauthorized access, use, modification, or damage[3].
- - Application security techniques include such things as secure coding practices, code analysis tools, penetration testing tools, web application firewalls (WAF), input validation, output encoding, and encryption that protect the applications from vulnerabilities and attacks.
- - Data security techniques include such things as data masking, data anonymization, data encryption, data classification, data retention policies, and data loss prevention (DLP) tools that protect the data from unauthorized disclosure or leakage.

# Thank you

# ???

# Software Security
# SEng 3071

## Chapter Two
## Classical Encryption Techniques

# Presentation outline

- Introduction and terminologies
- Mono-alphabetic substitution ciphers
- Polyalphabetic substitution ciphers
- Transposition ciphers

# Basic Cryptography Techniques

- Purpose of cryptography
  - Secure stored information - regardless if access obtained.
  - Secure transmitted information - regardless if transmission has been monitored.

# Basic Cryptography Techniques

- Cryptography
- Cryptography has five components:
  1. Plaintext: This is what you want to encrypt.
  2. Cipher text: The encrypted output.
  3. Encryption algorithm: The sequence of data processing steps that go into transforming **plaintext into cipher text.**
  4. Secret Key: is used to set some or all of the various **parameters** used by the encryption algorithm.
  5. Decryption algorithm: The sequence of data processing steps that go into transforming **cipher text back into plaintext.**
     - Enciphering or encryption: The process by which plaintext is converted into cipher text.
     - Deciphering or decryption: Recovering plaintext from cipher text.

# Basic Cryptography Techniques

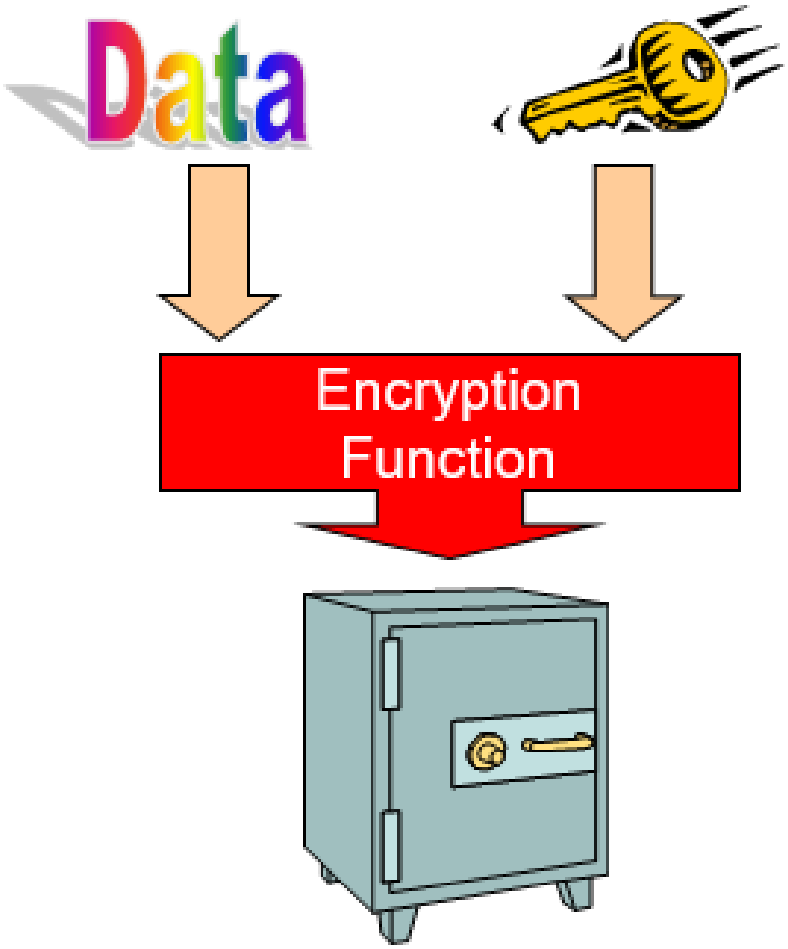
- Cryptography
- **Keys**
- A key can be thought of as simply a collection of bits.
- The more bits, the stronger the key.
- **Lengths** vary depending on the encryption algorithm.
- Keys are tied to specific encryption algorithms.
- e.g. 128 bits is long for some algorithms, but short for others.

# Basic Cryptography Techniques

- **Cryptography**
- Plain text is converted to cipher text by making use of an algorithm and key.
  - Algorithm is publicly known
  - Key is held private
- **Three Main Categories**
  - Secret Key
    - **single key is used to encrypt and decrypt information**
  - Public/Private Key
    - **two keys are used: one for encryption (public key) and one for decryption (private key**)
  - One-way Function
    - information is encrypted to produce a "digest" of the original information that can be used later to prove its authenticity.
    - Does not have any decryption mechanism.

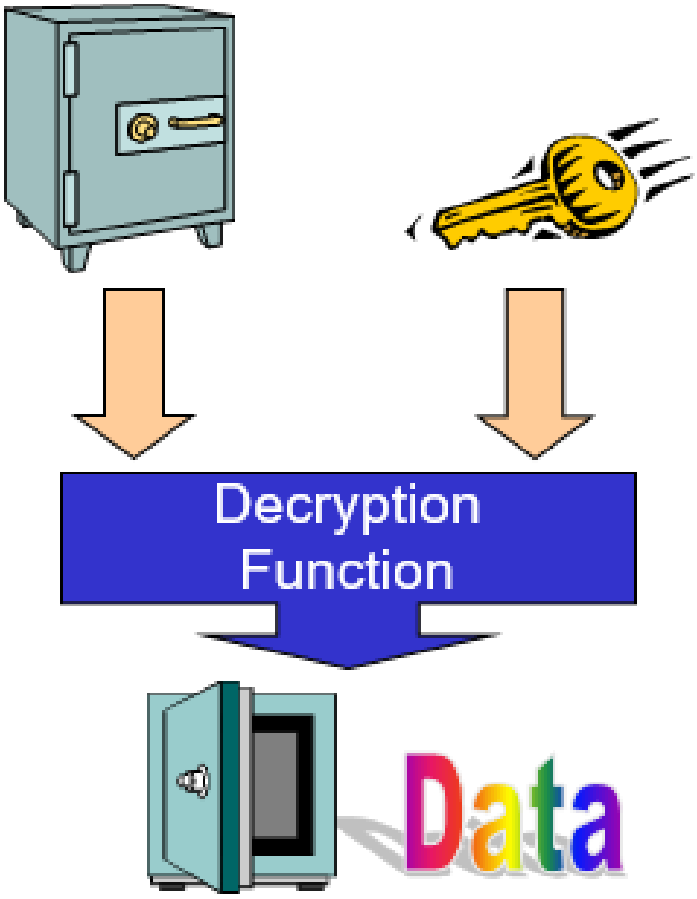
# Basic Cryptography Techniques

- **Encryption**
- Encryption is the process of taking some data and a key and feeding it into a function and getting encrypted data out.
- Encrypted data is, in principle, unreadable unless decrypted.



# Basic Cryptography Techniques

- **Decryption**
- Decryption is the process of taking encrypted data and a key and feeding it into a function and getting out the original data.
- Encryption and decryption functions are linked.

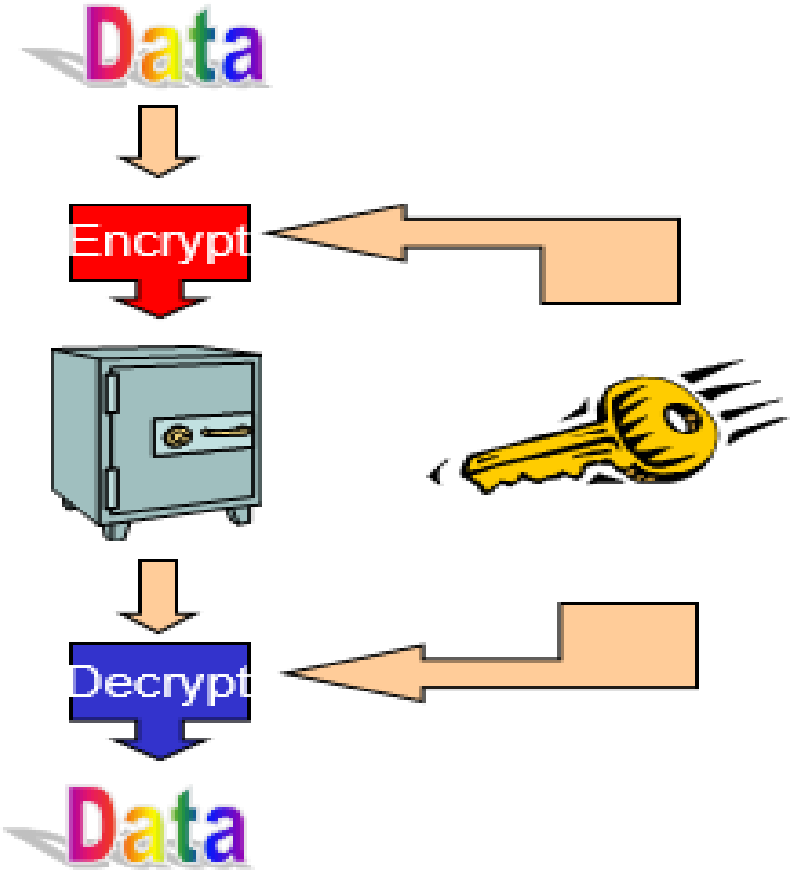


# Encryption Techniques

There are three encryption techniques

1. Symmetric Encryption

- Encryption and decryption algorithms that use the same key are called symmetric.
- Sender and receive have the same secret key that will encrypt and decrypt plain text.
- **Strength of encryption technique depends on key length.**



# Encryption Techniques

- Secret Key (Symmetric)
- Known symmetrical algorithms
  - Data Encryption Standard (DES)
    56 bit key
  - Triple DES, DESX, GDES, RDES
    168 bit key
  - Advanced Encryption Standard (AES)
    128, 192, 256 bit key
  - RC2, RC4, RC5
    variable length  up to 2048 bits
  - IDEA - basis of PGP
    128 bit key
  - Blowfish, Twofish
    variable length up to 448 bits

# Encryption Techniques

## 2. Asymmetric Encryption

- Encryption and decryption algorithms that use a key pair are called asymmetric.
  - Keys are mathematically linked
  - Example: RSA, DH, Elgamal…

- **NB. Algorithm**
  - **Symmetric**: $K_1 = K_2$
  - **Asymmetric:** $K_1 \neq K_2$

## ENCRYPTION

### Message 1

Central to the growth of e-commerce and e-governance is the issue of trust in electronic environment.

### Encrypted Message 1

**9a46894335be49f0b9cab28d755aaa9cd985**
**71b275bbb0adb405e6931e856ca3e5e569e**
**dd135285482**

### Message 2

The Internet knows no geographical boundaries. It has redefined time and space. Advances in computer and telecommunication technologies have led to the explosive growth of the Internet. This in turn is affecting the methods of communication, work, study, education, interaction, leisure, health, governance, trade and commerce.

### Encrypted Message 2

**a520eecb61a770f947ca856cd675463f1c95**
**a9a2b8d4e6a71f80830c87f5715f5f593349**
**8dd7e**
**67c3**

Same Key
SYMMETRIC

Different Keys
[Keys of a pair – Public and Private]
ASYMMETRIC
[PKI]

## DECRYPTION

### Encrypted Message 1

**9a46894335be49f0b9cab28d755aaa9cd98571b275bbb0adb405e6931e856ca3e5e569edd135285482**

### Message 1

Central to the growth of e-commerce and e-governance is the issue of trust in electronic environment.

### Encrypted Message 2

**a520eecb61a770f947ca856cd675463f1c95a9a2b8d4e6a71f80830c87f5715f5f59334978dd7e97da0707b48a1138d77ced56feba2b467c398683c7dbeb86b854f120606a7ae1ed934f5703672adab0d7be66dccde1a763c736cb9001d0731d541106f50bb7e54240c40ba780b7a553bea570b99c9ab3df13d75f8ccfdddeaaf3a749fd1411**

### Message 2

The Internet knows no geographical boundaries. It has redefined time and space. Advances in computer and telecommunication technologies have led to the explosive growth of the Internet. This in turn is affecting the methods of communication, work, study, education, interaction, leisure, health, governance, trade and commerce.

# Encryption Techniques

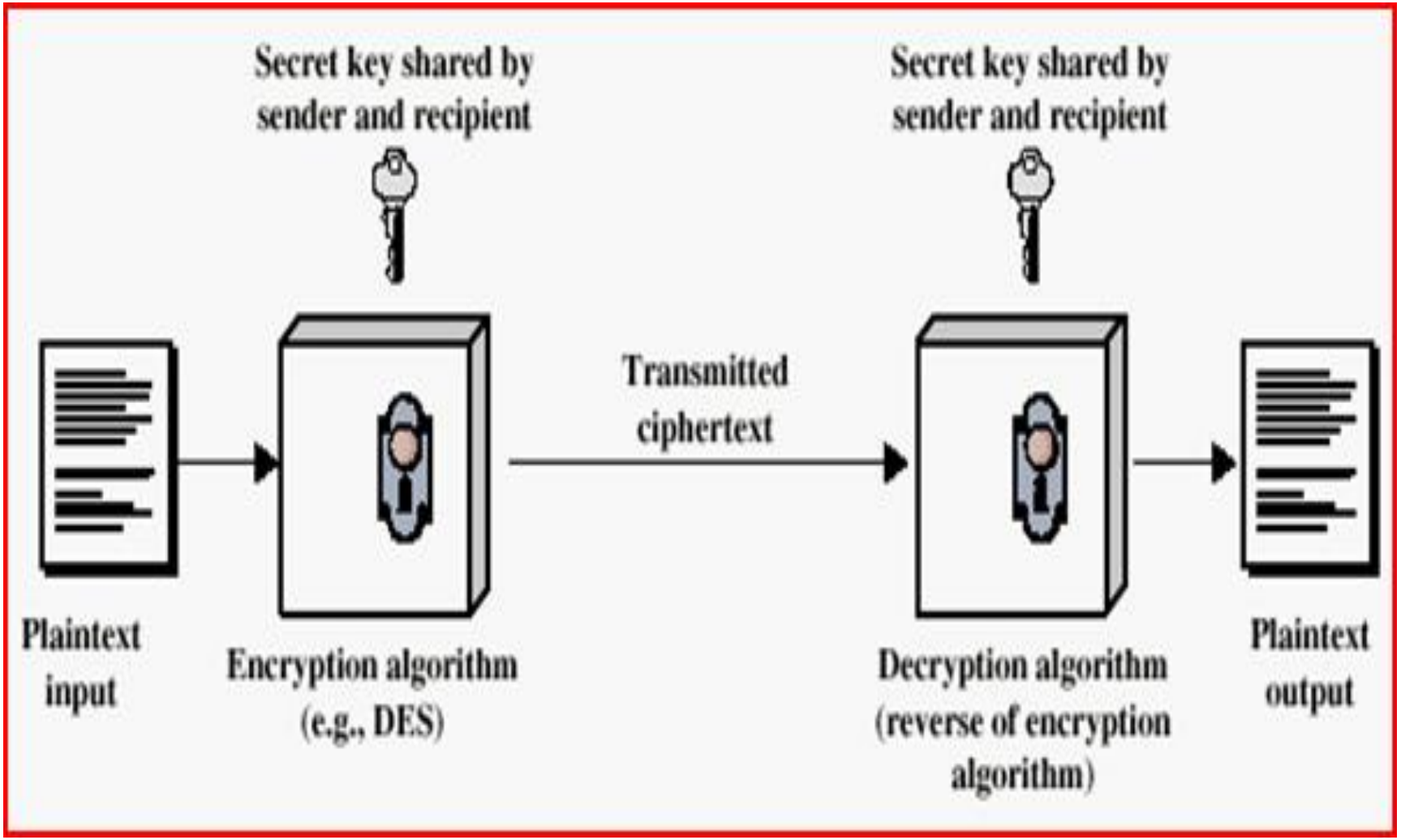
## 3. One-Way Function

- It is easy to compute but it is very **difficult to compute their reverse function.**
- Thus having a data X it is easy to calculate f(X) but, knowing the value of f(X) it is difficult to calculate the value of X.
- non-reversible "quick" encryption
- produces a fixed length value called a *hash* or *message digest.*
- used to authenticate contents of a message.
- There is no a mathematical prove that one-way functions exist, in practical application functions that have behave similarly as real one-way functions are used.
- Common message digest functions
  - MD4 and MD5
    - produces 128 bit hashes

The MD5 algorithm produces a 128-bit (16-byte) hash value. This value is typically represented as a 32-digit hexadecimal number.

# Cryptography

- Simplified Encryption Model:



# Classical Encryption Techniques

- Two building blocks of all classical encryption techniques are
  1. SUBSTITUTION and
  2. TRANSPOSITION.

- Substitution means replacing an element of the plaintext with an element of cipher text.
  - each element in the plaintext (bit, letter, group of bits or letters) is mapped into another element
- Transposition means **rearranging** the order of appearance of the elements of the plaintext.
- Transposition is also referred to as permutation.

# Classical Encryption Techniques

- Substitution techniques: example: Caesar cipher
- This is the earliest known example of a substitution cipher.
- **Each character in the plain-text is replaced by a letter some fixed number of positions down the alphabet. E.g, with a left shift 3, D will be replace by A, E will be become B and so on.**

| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

**Encryption**

| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| + 3 | + 3 | + 3 | + 3 | + 3 | + 3 | + 3 | + 3 | + 3 | + 3 | + 3 | + 3 | + 3 | + 3 | + 3 | + 3 | + 3 | + 3 | + 3 | + 3 | + 3 | + 3 | + 3 | + 3 | + 3 | + 3 |
| D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C |

- **Example**
- **plaintext:** are you ready
- **ciphertext:** duh brx uhdgb

- **Plain**: ABCDEFGHIJKLMNOPQRSTUVWXYZ
- **Cipher**: DEFGHIJKLMNOPQRSTUVWXYZABC

# Classical Encryption Techniques

- Substitution techniques: example: Caesar cipher
- If we represent each letter of the alphabet by an integer that corresponds to its position in the alphabet, the formula for replacing each character 'P' of the plaintext with a character "C" of the cipher-text can be expressed as
  - $C = E(3, P) = (P + 3) \bmod 26$
- A more general version of this cipher that allows for any degree of shift would be expressed by
  - $C = E(k, P) = (P + k) \bmod 26$
- The formula for decryption would be
  - $P = D(k, C) = (C - k) \bmod 26$
- In these formulas, 'k' would be the secret key.
- The symbols 'E' and 'D' represent encryption and decryption.

# Classical Encryption Techniques

- WEAKNESSES OF THE CAESAR CIPHER
- The Caesar Cipher is a secret key cryptosystem;
  - that is, revealing the enciphering key makes decryption simple.
- In the Caesar cipher, the shift value is the enciphering key.
- Anyone knowing it can immediately decrypt, so it must be protected from unauthorized persons.
- Exhaustive Key Search. There is yet another method for breaking the Caesar cipher:
- Simply try all the possible keys!
- After all, there are only 26 possible keys in the ordinary alphabet, and this kind of attack is called an exhaustive search.
- An exhaustive search is rarely effective against all but the simplest of cryptosystems.
- Seeing that the Caesar cipher is so vulnerable, we attempt to see stronger cryptosystems.

# Substitution ciphers

- A substitution cipher is one in which the letters of plaintext are replaced by other letters or by numbers or symbols.
- Substitution ciphers can be categorized as either
  - a. Mono-alphabetic ciphers
  - b. Poly-alphabetic ciphers

## A. Mono-alphabetic ciphers

E.g. MY NAME ---------- NZ OBNF

- In this case**, a character ( or symbol) in the plaintext is always changed to the same character (or symbol) in the ciphertext regardless of its position or text.**
- For example, if the algorithm says that **letter A in the plaintext is changed to letter D, every letter A is changed to letter D.**
- The relationship in between plaintext and ciphertext is **one-to-one.**
- Now have a total of 26! $=4*10^{26}=2^{88}$ possible key
- This coming from limitation of caser cipher, since only used 26 possible key.

# Substitution ciphers

- The group of mono-alphabetic ciphers includes:
    - i. Additive ciphers or Caesar ciphers
    - ii. Multiplicative ciphers
    - iii. Affine ciphers

# Substitution ciphers (Mono-Alphabetic)

## 1. Additive ciphers:

- This is the simplest mono-alphabetic cipher.
- We assume that the plaintext contains the lowercase characters (a to z) and the ciphertext contain the upper text characters (A to Z) as follows:

| | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Plaintext → | a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |
| Ciphertext → | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |

- In the Figure, each character is assigned an integer in $Z_{26}$ .
- The secret key is also an integer in $Z_{26}$
- The encryption algorithm adds the key to the plaintext characters and the decryption algorithm subtracts the key from the ciphertext characters.

# Substitution ciphers (Mono-Alphabetic)

## 1. Additive ciphers:

- Then the algorithm can be expressed as follows:

  For each plaintext letter $P$, substitute the ciphertext letter $C$:

  ($a$ mod $n$ is the remainder when $a$ is divided by $n$. E.g. 11 mod 7 = 4)

❖ The encryption algorithm is

$C = E(k, P) = (P + k) \bmod 26$ ; **where *k* takes a value in the range 1 to 25.**

❖ The decryption algorithm is simply

$P = D(k, C) = (C - k) \bmod 26$ ; **where *k* takes a value in the range 1 to 25.**

# Substitution ciphers (Mono-Alphabetic)

## 1. Additive ciphers:

Exercise: Use the additive cipher with key =15 to encrypt the message "hello".

Soln. : We apply the encryption algorithm to the plaintext character by character

Plaintext : h → 07 Encryption: (07+15) mod 26 Ciphertext: 22→ W

Plaintext : e → 04 Encryption: (04+15) mod 26 Ciphertext: 19 → T

Plaintext : l → 11 Encryption: (11+15) mod 26 Ciphertext: 00 → A

Plaintext : l → 11 Encryption: (11+15) mod 26 Ciphertext: 00 → A

Plaintext : o → 14 Encryption: (14+15) mod 26 Ciphertext: 03 → D

# Substitution ciphers (Mono-Alphabetic)

## 2. Multiplicative cipher:

- In this cipher, the encryption algorithm specifies the **multiplication of the plaintext by the key and the decryption algorithm specifies the division of the ciphertext by the key.**
- Since operations are in $Z_{26,}$ decryption here means multiplying by the multiplicative inverse of the key.
  - The general multiplicative encryption algorithm is

$C = E(k, P) = (P * k) \bmod 26$ ; where $k$ takes on a value in the range 1 to 25.

  - The general multiplicative decryption algorithm is

$P = D(k, C) = (C * k^{-1}) \bmod 26$ ; where $k$ takes on a value in the range 1 to 25.

# Substitution ciphers (Mono-Alphabetic)

## 2. Multiplicative cipher:

Exercise: Use the multiplicative cipher with key =7 to encrypt the message "hello".;

Soln. : We apply the encryption algorithm to the plaintext character by character

Plaintext : h → 07 Encryption: (07*07)mod 26 Ciphertext: 23→ X

Plaintext : e → 04 Encryption: (04*07)mod 26 Ciphertext: 02 →C

Plaintext : l → 11 Encryption: (11*07)mod 26 Ciphertext: 25 → Z

Plaintext : l → 11 Encryption: (11*07)mod 26 Ciphertext: 25→ Z

Plaintext : o → 14 Encryption: (14*07)mod 26 Ciphertext: 20 → U

So, the result is "XCZZU"

# Substitution ciphers (Mono-Alphabetic)

## 3. Affine cipher:

- Affine cipher is a combination of additive and multiplicative ciphers with a pair of keys.
- The first key is used with multiplicative cipher and the second key is used with the additive cipher.
- Affine cipher is actually two ciphers applied one after the other.
- In the affine cipher, the relations between the plaintext and ciphertext are

$C = E(k_1, k_2; P) = (P * k_1 + k_2) \bmod 26$ and $P = D(C; k_1, k_2) = ((C - k_2) * k_1^{-1}) \bmod 26$

# Substitution ciphers (Poly-alphabetic)

## B. Polyalphabetic cipher

- In this kind of cipher, **each occurrence of the same character have a different substitute.**
- **The relationship between the characters in the plaintext and the characters in ciphertext is one-to-many.**
- For example, 'a' could be enciphered as 'D' in the beginning, but as 'N' in the middle…..
- Polyalphabetic ciphers have the advantage of hiding the letter frequency of the underlying language.
- To create a polyalphabetic cipher, we need to make each ciphertext character dependent on both the plaintext character and the position of the plaintext character.
- We need to have a key stream k= ($k_1$, $k_2$, $k_3$,…) in which $k_i$ is used to encipher the $i^{th}$ character in the plaintext to create the $i^{th}$ character in the ciphertext.

# Substitution ciphers (Poly-alphabetic)

- The group of polyalphabetic ciphers includes:

  a) Auto key cipher
  b) Play fair cipher
  c) Vegenere cipher
  d) Hill cipher
  e) Rotor cipher
  f) Enigma machine

# Substitution ciphers (Poly-alphabetic)

## 1. Auto key cipher

- In this cipher, the key is a stream of sub keys, in which each sub key is used to encrypt the corresponding character in the plaintext.
- **The first sub key is a predetermined value agreed upon by the sender and the receiver.**
- **The second sub key is the value of first plaintext character (between 0 and 25).**
- **The third sub key is the value of second plaintext character and so on.**
- The name of the cipher auto key implies that the sub keys are automatically generated from the plaintext cipher characters during the encryption process.

$P=P_1P_2P_3\ldots$ $C=C_1C_2\ C_3\ldots$ $k=k_1P_1P_2\ldots$

**Encryption: $C_i = (P_i + k_i) \bmod 26$**

**Decryption: $P_i = (C_i - k_i) \bmod 26$**

# Substitution ciphers (Poly-alphabetic)

## 1. Auto key cipher

- **N.B Auto key added at the first of the sub keys.**
- E.g. Encrypt HELLO using K = N
- Given plain text = HELLO and Key = NHELL
- **Lets Encrypt**
- Plain text (P) : H E L L O
- Corresponding number: 7 4 11 11 14
- Key (K): N H E L L
- Corresponding number: 13 7 4 11 11
- Apply the formula: 20 11 15 22 25
- Corresponding Letter: U L P W Z
- Cipher text: ULPWZ

# Substitution ciphers (Poly-alphabetic)

## 1. Auto key cipher

- Example: Encrypt the plaintext "attack is today" using the initial key value $k_1 = 12$.
- Sol: Here enciphering is done character by character.
- Each character in the plaintext is first replaced by its integer value as shown in the figure. The first sub-key is added to create the first ciphertext character.

| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Plaintext: | a | t | t | a | c | k | i | s | t | o | d | a | y |
| P's Values: | 00 | 19 | 19 | 00 | 02 | 10 | 08 | 18 | 19 | 14 | 03 | 00 | 24 |
| Key stream: | 12 | 00 | 19 | 19 | 00 | 02 | 10 | 08 | 18 | 19 | 14 | 03 | 00 |
| C's Values: | 12 | 19 | 12 | 19 | 02 | 12 | 18 | 00 | 11 | 7 | 17 | 03 | 24 |
| Ciphertext: | M | T | M | T | C | M | S | A | L | H | R | D | Y |

- **Nb. Encryption: $C_i = (P_i + k_i) \bmod 26$**
- **Decryption: $Pi = (Ci - Ki) \bmod 26$**
- We note that the cipher is polyalphabetic because the three occurrences of "a" in the plaintext are encrypted differently. The three occurrences of the "t" are enciphered differently.

# Substitution ciphers (Poly-alphabetic)

## 2. Vegenere cipher

- This cipher was designed by Blaise de Vegenere, a sixteenth century French mathematician.
- A Vegenere cipher uses a different strategy to create the key stream.
- The key stream is a repetition of an initial secret key stream of length m, where we have $1 \leq m \leq 26$.
- The cipher can be described as follows where $(k_1, k_2, \ldots, k_m)$ is the initial secret key agreed by the sender and the receiver.

❖ $P = P_1 P_2 \ldots \quad C = C_1 C_2 \ldots \qquad K = [(k_1, k_2, \ldots, k_m), (k_1, k_2, \ldots, k_m), \ldots]$

- Encryption: $C_i = (P_i + k_i) \bmod 26$
- Decryption: $P_i = (C_i - k_i) \bmod 26$

# Substitution ciphers (Poly-alphabetic)

## 2. Vegenere cipher

- The difference between the Vegenere cipher and the other two polyalphabetic ciphers is that the Vegenere key stream does not depend on the plaintext characters; **it depends only on the position of the character in the plaintext.**
- In other words, the key stream can be created without knowing what the plaintext is.
- Example: Encrypt the message "she is listening" using the 6-character keyword "PASCAL".
- Sol.: The initial key stream is (15, 0, 18, 2, 0, 11). The key stream is

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Plaintext: | s | h | e | i | s | l | i | s | t | e | n | i | n | g |
| P's values: | 18 | 07 | 04 | 08 | 18 | 11 | 08 | 18 | 19 | 04 | 13 | 08 | 13 | 06 |
| Key stream: | *15* | *00* | *18* | *02* | *00* | *11* | *15* | *00* | *18* | *02* | *00* | *11* | *15* | *00* |
| C's values: | 07 | 07 | 22 | 10 | 18 | 22 | 23 | 18 | 11 | 6 | 13 | 19 | 02 | 06 |
| Ciphertext: | H | H | W | K | S | W | X | S | L | G | N | T | C | G |

# Substitution ciphers (Poly-alphabetic)

## 2. Vegenere cipher

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Plaintext: | s | h | e | i | s | l | i | s | t | e | n | i | n | g |
| P's values: | 18 | 07 | 04 | 08 | 18 | 11 | 08 | 18 | 19 | 04 | 13 | 08 | 13 | 06 |
| Key stream: | *15* | *00* | *18* | *02* | *00* | *11* | *15* | *00* | *18* | *02* | *00* | *11* | *15* | *00* |
| C's values: | 07 | 07 | 22 | 10 | 18 | 22 | 23 | 18 | 11 | 6 | 13 | 19 | 02 | 06 |
| Ciphertext: | H | H | W | K | S | W | X | S | L | G | N | T | C | G |

**How to convert cipher text into original text**

7 7 22 10 18 22

H H W K S W

P A S C A L

150182011

Plain text =c-k mod26

7-15=-8+26=18 do like this to all

# **Transposition Techniques** (Ciphering with Transposition)

- A transposition cipher does not substitute one symbol for another (as in substitution cipher), but changes the location of these symbols.
- **Transposition is performing some sorts of permutation on the plain text letter.**
- **Re-arrangement of letters of the plain text.**
- **EXAMPLE:- NAME------MEAN**
- This is how a pure permutation cipher could work:
  - You write your plaintext message along the rows of a matrix of some size.
  - You generate ciphertext by reading along the columns.
  - The order in which you read the columns is determined by the encryption key.

# **Transposition Techniques** (Ciphering with Transposition)

- **EXAMPLE:- NAME------MEAN**
- This have 4! Number of cypher can be generated from the plain text NAME.
- 4!=24
- MEAN, EAMN, AENM, MNEA……

# **Transposition Techniques** (Ciphering with Transposition)

- **There Are Two Types Of Transposition Cyphers.**
- **Key less transposition cypher**
  - The message is converted to cipher text by either of two permutation techniques.

A. Text is written into a table **column-by-column (diagonally)** and is then transmitted **row by row.**

B. Text is written into a table **row-by-row** and is then transmitted **column-by-column.**

  - The first method is also popularly known as Rail-fence cipher
  - E.g. we need to send the message "DEFENDTHEEASTWALL"
  - Arrange into tables we get:-

| | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| D | | F | | N | | T | | E | | A | | T | | A | | L |
| | E | | E | | D | | H | | E | | S | | W | | L | |

  - Now the message is sent row-by-row, so cipher text is "DFNTEATALEEDHESWL"

# **Transposition Techniques** (Ciphering with Transposition)

- **There Are Two Types Of Transposition Cyphers.**
  - **Keyed transposition cypher**
    - In this approach, rather than permuting all the symbols together, **we divide the entire plaintext into blocks of predetermined size and then permute each block independently.**
    - The key is used as a position finder for the cipher text.
    - Consider a message "WE HAVE AN ATTACK"
    - **Both the sender and receiver previously agreed as block size = 5.**
      - So blocks would be:-

WEHAV

EANAT

TACKX

- The last character X is a bogus character so as to complete the

| 4 | 1 | 3 | 2 | 5 |
|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 |

**Cipher text= AWHEVAENATKTCAX**

**decryption**

## Group Assignment (15%)
## submission date 14/09/2014

1. What is biometric encryption and list types of biometric encryption techniques and discuses them
2. Write the following cipher techniques in detail with example.
   a. Playfair cipher
   b. Hill cipher
   c. Rotor cipher
   d. Enigma machine

# Thank you

# ???

# Software security
# SEng 3071

## Chapter 5

## Network Management Tools

# Presentation outline

- Network Management Tools
- Basic concepts of SNMP
- Proxies
- Distributed Network Management
- Message Processing Model
- User Security Model
- Access Control Processing
- Operating System Security
- Trusted Operating System:
- Developing a secured operating system

# Network Management Tools

## ❑ Network Management Tools

- Network management is the procedure of administering, managing and working a data network using a network management system.
- A network management tool allows you to identify problems, set configurations on the network and devices remotely, update configurations of critical network infrastructure devices, and monitor the status of the network and devices.
- Network management tools enable you to troubleshoot problems when they occur, remotely access devices as though you are on a network, and remotely manage the power of devices.
- In other words, you use a network management tool for all network management aspects.
- Furthermore, you use it to monitor performance in real-time and remotely perform actions to maintain the network and

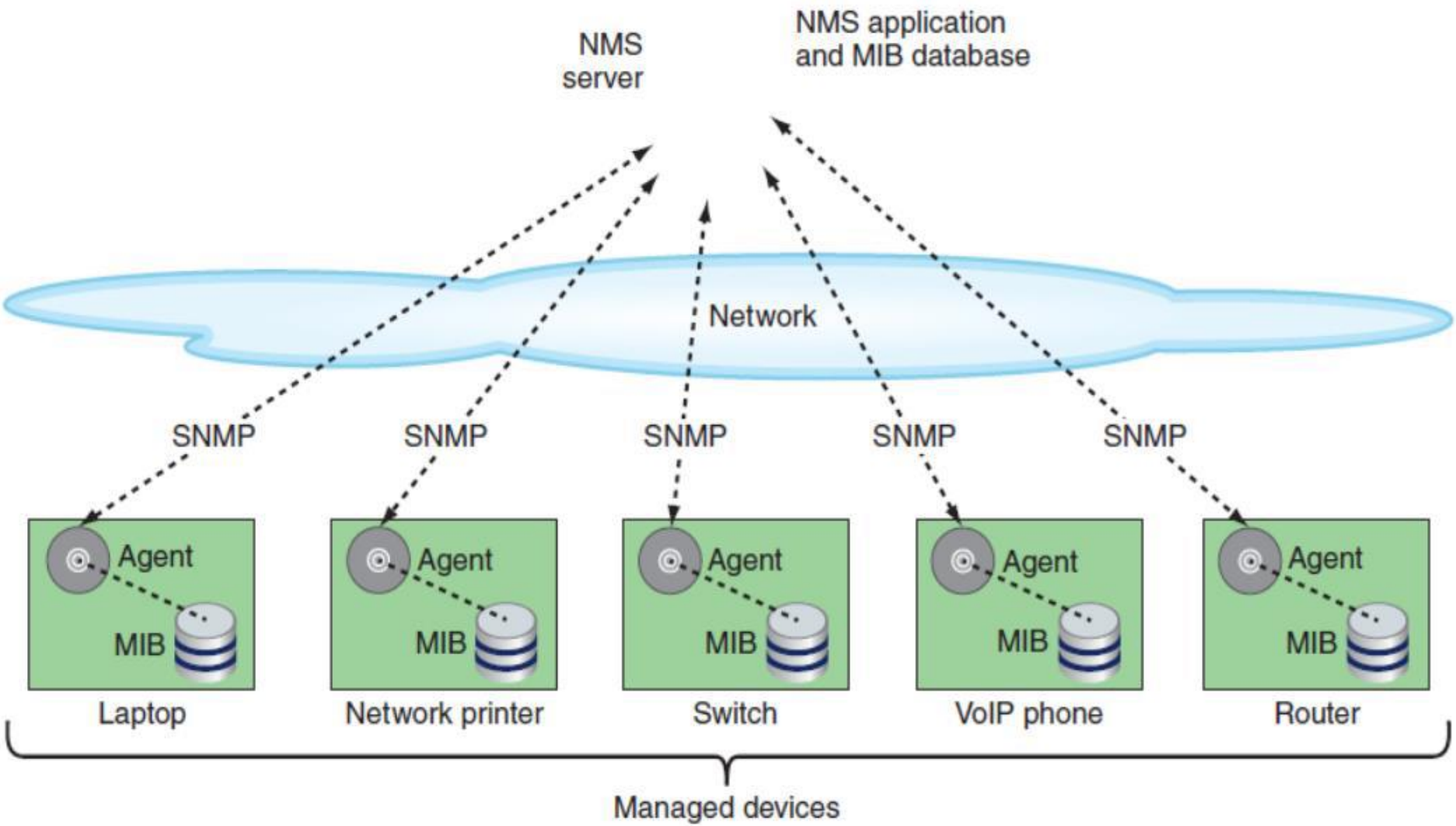
# Network Management Tools

## ❑ Basic concepts of SNMP

- **SNMP (Simple Network Management Protocol)**
- It is an Internet-standard **protocol** for handling devices on IP networks.
- Devices that typically provide SNMP include **routers, switches, servers, workstations, printers** and more.
- It is used mainly in the network management framework **to monitor network-attached computers** for conditions requiring regulatory attention.
- Network administrators use SNMP **to monitor and map network availability, performance, and error rates.**
- Is an Application Layer (Layer 7) protocol, using UDP (user data gram protocol) ports 161 and 162
- Facilitate the exchange of management information b/n network devices.

# Network Management Tools

## ❑ Basic concepts of SNMP



# Network Management Tools

## ❑ Basic concepts of SNMP

- Is used more for real-time network monitoring rather than retroactive analysis.
  - **Port 161 is used to send information from the manager to the installed agents.**
  - **Port 162 is used for agents to send messages to the manager.**
- SNMP facilitates the concept of manager and agent.
- A manager, generally **a host, controls and monitors a group of agents, usually routers.**
- The protocol is designed to monitor different devices and installed on various physical networks at the application level.

# Network Management Tools

## ❑ Basic concepts of SNMP

- An SNMP-managed network includes **three key components.**

1. **Network management system (NMS)**

- Executes **applications** that monitor and control managed devices.
- Executes monitoring applications, management processes and **controls managed devices.**
- A network might be managed by one or more management systems.
- **NMS server**:- At least one network management console, which may be a server or workstation, depending on the size of the network, **collects data from multiple managed devices at regular intervals** in a process called polling.

# Network Management Tools

## ❑ Basic concepts of SNMP

### 2. Agent

- An agent is a network-management **software** mechanism that consists of a managed device.
- Each managed device runs a network management agent, which is a software routine that **collects information about the device's operation and provides it to the NMS.**
- Resides on each managed device and translates local management information data, such as:
  - performance information or event and error information caught in software traps, into a readable form for the management system.
  - on a server, an agent can measure how many users are connected to the server or what percentage of the processor's resources are used at any given time. So as not to affect the performance of a device while collecting information, agents demand minimal

# Network Management Tools

## ❑ Basic concepts of SNMP

### 3. Managed Device

- It is a network node Such as a router, a switch, a computer, or a firewall that **executes** an SNMP interface that enables unidirectional (read-only) or bidirectional access to node-specific information.
- Managed devices collect and store management information, making it available through SNMP to other management systems having the same protocol compatibility.
- This can be any characteristic of the device that is monitored, including components such as a processor, memory, hard disk, or NIC, or intangibles such as performance or utilization.
- Each managed object is assigned an OID (object identifier), which is standardized across all NMSs.

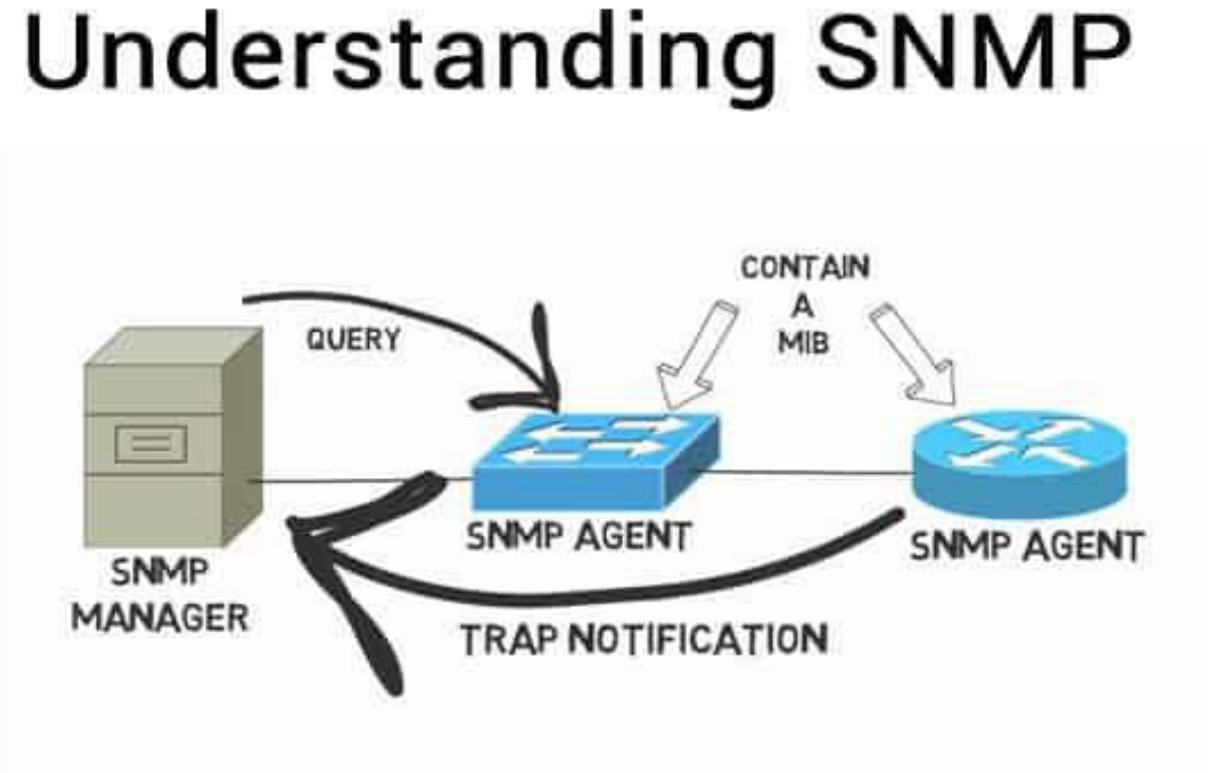
# Network Management Tools

## ❑ Basic concepts of SNMP

- **Three SNMP commands used to manage (monitored and controlled) devices:**
  - **Read, Write**, and **Trap.**
- The **read** command is used by an NMS to monitor managed devices.
  - This is performed by the NMS examining different variables that are maintained by managed devices.
- The **write** command is used by an NMS to control managed devices.
  - Using this command, the NMS can change the values of variables stored within managed devices.
- The **trap** command is used by NMS managed devices to report events to the NMS.
- NOTE:- Monitoring involves collecting and analyzing data from the devices. Controlling uses these findings to make changes.

# Network Management Tools

## ❑ Basic concepts of SNMP



# Network Management Tools

## ❑ Basic concepts of SNMP

- Versions of SNMP -Versions 1, 2, and 3.
- **Version 1 (1988), or SNMPv1,** Now rare
  - Is the initial implementation of the SNMP protocol. operates over protocols such as User Datagram Protocol (UDP), Internet Protocol (IP), and the OSI Connectionless Network Service (CLNS).
- **SNMPv2 –still widely used**
  - Revises SNMPv1 and includes improvements in the areas of performance, security, confidentiality, and manager-to-manager communications. SNMPv2 also defines two new operations: Get-Bulk and Inform.
  - The Get Bulk operation is used to retrieve large blocks of data efficiently.
  - The Inform operation allows one NMS to send trap information to another NMS and then to receive a response.

# Network Management Tools

## ❑ Basic concepts of SNMP

### Comparison between SNMP V1 and SNMP V2

| SNMPv1 PDU | SNMPv2 PDU | Direction | Description |
|---|---|---|---|
| GetRequest | GetRequest | Manager to agent | Request value for each listed object |
| GetRequest | GetRequest | Manager to agent | Request next value for each listed object |
| ------ | GetBulkRequest | Manager to agent | Request multiple values |
| SetRequest | SetRequest | Manager to agent | Set value for each listed object |
| ------ | InformRequest | Manager to manager | Transmit unsolicited information |
| GetResponse | Response | Agent to manager or Manage to manager (SNMPv2) | Respond to manager request |
| Trap | SNMPv2-Trap | Agent to manager | Transmit unsolicited information |

# Network Management Tools

## ❑ Basic concepts of SNMP

- **SNMPv3**
  - This version is similar to SNMPv2 and adds three additional security services **authentication, validation, and encryption** for messages exchanged between managed devices and the network management console.
  - SNMPv3 uses message integrity to ensure that a packet has not been tampered with in-transit.
  - SNMPv3 also utilizes **authentication,** which is used to determine whether the **message is from a valid source.**
  - SNMPv3 **provides encryption**, which is used to scramble the contents of a packet to prevent it from being seen by unauthorized sources.
  - Information is exchanged between a management station and an agent in the form of an SNMP message.

# Network Management Tools

## ❑ Proxies

- A proxy concept was developed **to accommodate devices that do not implement SNMP.**
- The SNMP agent acts as a proxy for one or more other devices; **it acts on behalf of those devices.**
- The management station **sends queries concerning a device to its proxy agent.**
- The proxy agent converts the query into the management protocol that is used by the device and when the reply arrives, it passes the reply back to the management station.
- It also sends a trap message when an event notification is transmitted to proxy agent from the device.
- For SNMPv2, proxy is the only means of managing the devices that do not implement SNMPv2. It also

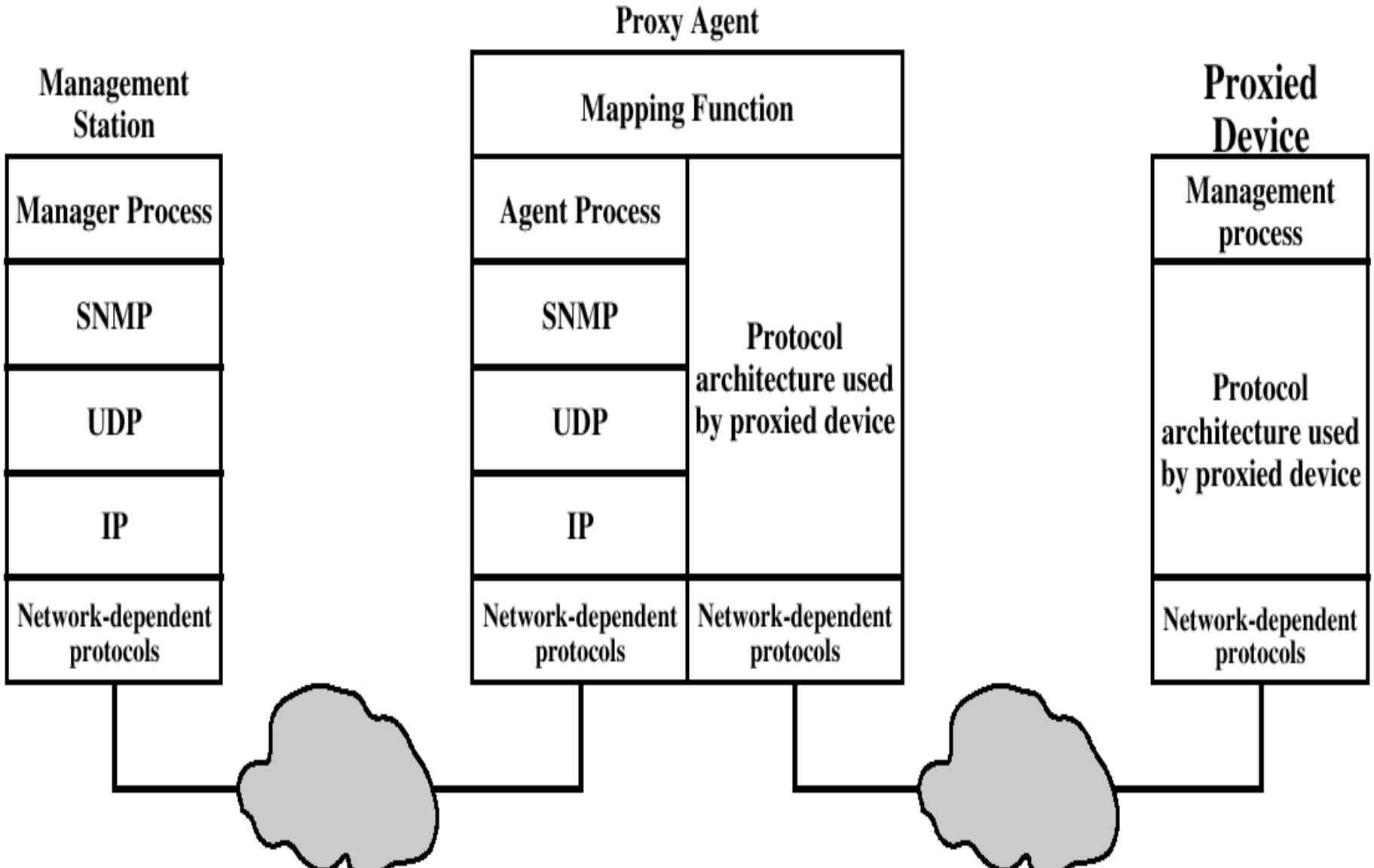
# Network Management Tools

## ❑ Proxies

- Proxy & Gateway Agents extend the capabilities of SNMP by allowing it to:
  - Manage a device that cannot support an SNMP agent
  - Manage a device that supports a non-SNMP management agent
  - Allow a non-SNMP management system to access an SNMP agent
  - Provide firewall-type security to other SNMP agents (UDP packet filtering)
  - Translate between different formats of SNMP messages (v1 and v2)
  - Consolidate multiple managed nodes into a single network address (also to provide a single trap destination)

# Network Management Tools

## ❑ Proxies



# Network Management Tools

## ❑ Distributed Network Management

- A traditional network management scheme involves a **host acting as a management station** and the **remaining devices acting as agents,** which for large networks with high traffic infeasible.
- In a **decentralized network management scheme, multiple top level management stations are present, referred to as management servers,** which manage a portion of total pool of agents.
- For many agents, the management server delegates responsibility to an intermediate manager who plays the role of manager to monitor and also agent to convey information to higher level management.
- SNMP supports either a highly centralized network management strategy or a distributed one.

# Network Management Tools

## ❑ Distributed Network Management

- Distributed network management is the creation of multiple core locations that are used to administrate and control various resources of a computer network.

# Network Management Tools

## ❑ Message Processing Model

- The following five fields are generated by the message processing model on outgoing messages and process by the message processing model on incoming messages.

1. **Msg-Version:** set to SNMPv3
2. **Msg-ID:** identifier used between two SNMP entities to coordinate request and response messages and by the message processor to coordinate the processing of message by different subsystem models within the architecture.
3. **Msg-Max-Size:** conveys the maximum size of a message in octets supported by the sender of the message.
4. **Msg-Flags:** an octet string containing three flags in the least significant three bits: reportable-Flag, private-Flag, authenticated-Flag
5. **Msg-Security-Model:** an identifier that indicates **which security model was used by the sender to prepare this message and therefore which security model the receiver**

# Network Management Tools

## ❑ User Security Model

- USM provides authentication and privacy services for SNMP.
- USM supports privacy of messages.
- Uses DES technique for encrypting and decrypting SNMPv3 packets.
- In the same way as with authentication, the same secret privacy key is used to encrypt and decrypt messages on both sides.
- It is designed to protect:
  - Modification of information
  - Masquerade
  - Message stream modification
  - Disclosure
- This model is not intended to protect:
  - **Denial of service attacks:** an attacker may prevent exchanges between a manager and an agent.
  - **Traffic analysis:** an attacker may observer the general pattern of traffic between a manger and agents

# Network Management Tools

## ❑ Access Control Processing

- All of these parameters are needed to make the access control decision.
  - **Who:** the combination of security model and security Name define **the who of this operation**; it defines a given principal whose communications are protected by a given security model.
  - **Where:** the context Name specifies **where the desired management object is to be found.**
  - **Why:** the view type specifies **why access is requested:** for a read, write or notify operation.
  - **What**: the variable Name is an object identifier whose prefix identifies a specific object type and whose suffix identifies a specific object instance. The object type indicates **what type of management information is requested.**
  - **Which:** the object instance indicates **which specific**

# Network Management Tools

## ❑ Operating System Security

- Security refers to providing a protection system to computer system resources such as CPU, memory, disk, software programs and most importantly data/information stored in the computer system.
- If a computer program is run by an unauthorized user, then he/she may cause severe damage to computer or data stored in it.
- So a computer system must be protected against **unauthorized access, malicious access** to system memory, viruses, worms etc.
- We distinguish between protection and security:
    - Protection refers to a mechanism for controlling the access of programs, processes or users to the resources. It must provide means for specifying the controls to be imposed.
    - Security is a measure of confidence that the integrity

# Network Management Tools

## ❑ Operating System Security

- **Reasons for protection**
  - Prevent the mischievous, intentional violation of an access restriction
  - Ensure that each program component uses system resources only in ways consistent with system policies
  - Protection is strictly an internal problem and Security, however, requires also consideration of the external environment
  - A protection system is ineffective, for instance, if user authentication is compromised
  - A protection oriented system provides means to distinguish between authorized and unauthorized usage

# Network Management Tools

## ❑ Operating System Security

- **The Security Problem**
  - Security violations can be categorized as intentional or accidental.
  - It is easier to protect against accidental security violations
  - Protection methods mostly consider accidental security violations
  - A threat is a potential for a security violation
  - An attack is the attempt to break security. It includes Breach of confidentiality, Breach of integrity , Breach of availability, Theft of service and Denial of service

# Network Management Tools

## ❑ Operating System Security

- Every computer system and software design must handle all security risks and implement the necessary measures to enforce security policies.
- At the same time, it's critical to strike a balance because strong security measures might increase costs while also limiting the system's usability, utility, and smooth operation.
- As a result, system designers must assure efficient performance without compromising security.
- OS security refers to the processes or measures taken to protect the operating system from dangers, including viruses, worms, malware, and remote hacker intrusions.

# Network Management Tools

## ❑ Operating System Security

- Operating system security (OS security) is the process of ensuring OS integrity, confidentiality and availability.
- OS security refers to specified steps or measures used to protect the OS from threats, viruses, worms, malware or remote hacker intrusions.
- OS security encompasses **all preventive-control techniques**, which safeguard any computer assets capable of being stolen, edited or deleted if OS security is compromised.
- OS security may be approached in many ways, including adherence to the following:
  - Performing regular OS patch updates
  - Installing updated antivirus engines and software
  - Examining all incoming and outgoing network traffic through a firewall
  - Creating secure accounts with required privileges only (i.e.,

# Network Management Tools

## ❑ Trusted Operating System

- An OS is trusted if it can provide:-

1. **Memory Protection**
   - Each user's program must run in a portion of memory protected against unauthorized accesses.
2. **File Protection**
   - aims to prevent programs from replacing critical OS files
3. **General object access control**
   - Users need general objects, such as constructs to permit concurrency and allow synchronization
4. **User Authentication**
   - must identify each user who requests access and must ascertain that the user is actually who purports

# Network Management Tools

## ❑ Trusted Operating System

**The key features of a Trusted OS are:**

- **Identification and Authentication:-** who is requesting access to an object,
- **Mandatory access control (MAC):-** A central authority determines access, user cannot change access rights.
- **Discretionary access control (DAC):-** The owner can determine who should have access rights to an object and what those rights should be.
- **Object Reuse Protection:-** reuse objects rather than completely destroy them.
- **Complete Mediation:-** all accesses must be controlled and verified.
- **Trusted path:-** attackers can't intercept or modify information.
- **Accountability and Audit:-** protect the audit logs from outsiders, and record every security relevant event.



- **Audit Log Reduction:-** change the log location, or reduce the

# Network Management Tools

## ❑ Trusted Operating System

- **There are a few basic concepts that are fundamental when dealing with trusted OS:**

- **The kernel**:- is the part of the OS that performs the lowest-level functions
- **the security kernel:-** is responsible for enforcing the security mechanisms of the entire OS
- **The reference monitor (RM):-** is the part of the security kernel that controls access to objects.
- **The trusted computing base (TCB):-** is everything in the trusted OS necessary to enforce the security policy
- **Security Policy and Security Model**
- **A security policy** is a statement of the security we expect the system to enforce.
- The security can be expressed as a number of well-defined, consistent and implementable rules.



- **A security model** is a representation of the security policy for the

# Network Management Tools

## ❑ Trusted Operating System

## ❑ Developing a secured operating system

- The development of secure OS can be made in six steps:
  - Analyse of the system
  - Choose/define a security policy
  - Choose/create a security model (based on the policy)
  - Choose implementation method
  - Make a (conceptual) design
  - Verify the correctness of the design
  - Make an implementation
  - Verify the implementation
- There are feed-back loops between all of the above steps. Errors may occur in all above steps.

# Thank you

# ???

# Software security
# SEng 3071

## Chapter 6

## Malicious Software

# Presentation outline

- Malicious Software
- Viruses and related threats,
- How Malware Spreads?
- Preventive Measures
- Symptoms

# Malicious Software

## ❑ Malicious Software

- Malware, or malicious software, **is any program or file that is intentionally harmful to a computer, network or server.**
- A is software created **to disrupt computer operation, gather sensitive information, or gain access to private computer systems.**
- It can **appear in the form of code, scripts, active content, and other software.**
- Malware is **used primarily to steal sensitive personal, financial, or business information for the benefit of others.**
- Malware is sometimes used broadly against government or corporate websites to gather guarded information, or to disrupt their operation in general.
- However, malware is often used against individuals to gain

# Malicious Software

## ❑ Malicious Software

- Software which is used with the aim of attempting to breach a computer system's security **policy** with respect to **Confidentiality, Integrity or Availability.**
- Malware carries out many of the cyberattacks on the Internet, including nation-state cyberwar, cybercrime, fraud and scams.
- For example, Trojans can introduce a backdoor access to a government network to allow nation-state attackers to steal classified information.
- As the political and financial stakes become higher, the sophistication and robustness of both the cyber defence mechanisms and the malware technologies and operation models have also increased.

# Viruses and related threats

# Viruses and related threats

## ❑ Viruses

- **Viruses** A program or piece of code that is loaded onto your computer without your knowledge and runs against your wishes.
- Viruses can also **replicate** themselves.
- Viruses **copy** themselves to other disks to spread to other computers.
- All computer viruses are man-made.
- Examples of computer viruses are: –
  - **Macro virus**
  - **Boot virus**
  - **Logic Bomb virus**
  - **Directory virus**
  - **Resident virus**

# Viruses and related threats

## ❑ Viruses

- **Macro virus**
  - a computer virus written in the same macro language used to create software programs such as **Microsoft Excel or Word.**
  - It **centers on software applications** and does not depend on the operating system (OS).
  - As a result, it can infect any computer running any kind of OS, including Windows, mac OS and Linux.
- **Boot virus**
  - A boot sector virus is a type of virus that infects the boot sector of **floppy disks or the Master Boot Record** (MBR) of hard disks (some infect the boot sector of the hard disk instead of the MBR).
  - The **infected code runs when the system is booted from an infected disk,** but once loaded it will infect other

# Viruses and related threats

## ❑ Viruses

- **Logic Bomb virus**
  - A logic bomb is a set of instructions in a program carrying a malicious payload that can **attack an operating system, program, or network.**
- **Directory virus**
  - As its name would suggest, a directory virus attacks your computer by infiltrating its **directory.**
- **Resident virus**
  - A type of malware **that hides and stores itself within the computer's memory.**
  - Depending on the virus' programming, **it can then infect any file run by the computer.**
  - This type of virus even **attach itself to anti-virus applications, thereby allowing it to infect any file scanned by the program.**

# Viruses and related threats

## ❑ Trojan Horse

- A Trojan Horse Virus is a type of malware that downloads onto a computer disguised as a legitimate program.
- The delivery method typically sees an attacker use social engineering to hide malicious code within legitimate software to try and gain users' system access with their software.
- A Trojan Horse neither replicates nor copies itself, but causes damage or compromises the security of the computer.
- A Trojan Horse must be sent by someone or carried by another program and may arrive in the form of a joke program or software of some sort.
- **These are often used to capture your logins and passwords.**
- Example of Trojan Horses:-

# Viruses and related threats

## ❑ Worms

- A computer worm is a self-replicating computer program.
- A **computer worm** is a standalone malware computer program that replicates itself in order to spread to other computers.
- It often uses a computer network to spread itself, relying on security failures on the target computer to access it.
- It will use this machine as a host to scan and infect other computers.
- When these new worm-invaded computers are controlled, the worm will continue to scan and infect other computers using these computers as hosts, and this behaviour will continue.
- Computer worms use recursive methods to copy themselves without host programs and distribute themselves based on exploiting the advantages of exponential growth, thus

# Viruses and related threats

## ❑ Worms

- It uses a network to send copies of itself to other nodes (computers on the network) and it may do so without any user intervention.
- It does not need to attach itself to an existing program.
- The worms are largely spread through emails and message services.
- Once it takes control of a device, it will scan other systems connected to it and infect them.
- Many worms are designed only to spread, and do not attempt to change the systems they pass through. However, as the **Morris worm** and **Mydoom** showed, even these "payload-free" worms can cause major disruption by increasing network traffic and other unintended effects.

# Viruses and related threats

## ❑ Spyware

- Spyware is a type of malware installed on computers that **collects information about users without their knowledge.**
- **The presence of spyware is typically hidden from the user and can be difficult to detect.**
- Spyware programs lurk on your computer to steal important information, like your **passwords and logins** and **other personal identification information and then send it off to someone else.**
- Some Spyware can install malicious programs and change system settings.
- Unwanted computer program that stealthily spies activities on your system and reports everything to its creator.

# Viruses and related threats

## ❑ Zombie

- Zombie programs take control of your computer and use it and its internet connection to attack other computers or networks or to perform other criminal activities.

## ❑ Spam

- Any message (usually email) that delivers malware to your device. Unsuspecting readers who click on a link or open an email attachment end up with some type of malware including ransomware, Trojans, bots, info-stealers, crypto-miners, spyware, and key-loggers.
- A common delivery method is to include malicious scripts in an attachment of a familiar type like a Word document, PDF file, or PowerPoint presentation.
- Once the attachment is opened, the scripts run and retrieve the malware payload.

# Viruses and related threats

## ❑ Adware

- Adware (short for advertising-supported software) is a type of malware that automatically delivers advertisements.
- Adware is any software application in which an advertising banner or other advertising material displays or downloads while a program is running.
- The ads are delivered through **pop-up** windows or bars that appear on the program's user interface.
- Adware is commonly created for PCs, but mobile devices may also be targeted for adware exploits.
- Legitimate adware is deployed to help software developers recover development costs.
- It can also be used to reduce or eliminate the cost of software for users. But, in some cases, the ads contain **cybersecurity threats** or lead users to a malicious webpage.
- Common examples of adware include pop-up ads on websites and advertisements that are displayed by software.

# Viruses and related threats

## ❑ How Malware Spreads?

- Malware is a program that must be triggered or somehow executed before it can infect your computer system and spread to others.
- Here are some examples on how malware is distributed:_

  A. Social network

  B. Pirated software

  C. Removable media

  D. Emails

  E. Websites

# Symptoms of malwares

## ❑ Symptoms

- Increased CPU usage
- Slow computer or web browser speeds
- Problems connecting to networks
- Freezing or crashing
- Modified or deleted files
- Appearance of strange files, programs, or desktop icons
- Programs running, turning off, or reconfiguring themselves (malware will often reconfigure or turn off antivirus and firewall programs)
- Strange computer behaviour

# Symptoms of malwares

## ❑ Symptoms

- Emails/messages being sent automatically and without user's knowledge (a friend receives a strange email from you that you did not send)
- There seems to be a lot of network activity when you are not using the network
- The available memory on your computer is lower than it should be
- Programs or files appear or disappear without your knowledge
- File names are changed
- Homepage randomly changes.

# Preventive Measures

- **The following measures can be taken to avoid presence of malware in a system:-**

- Ensure the operating system and applications are up to date with patches/updates.
- Never open strange e-mails, especially ones with attachments.
- When you download from the internet, always check what you install.
- Do not simply click OK to dismiss pop-up windows. Verify the publisher before you install application.
- Install anti-virus software.
- Ensure you scan and update the antivirus programs regularly.
- Install firewall.
- Always enable and use security features provided by browsers and applications.
- Scan your hard drive for viruses monthly.
- Practice caution when working with files from unknown sources.

# Preventive Measures

## ❑ Anti-Malware Software

- The following software help remove the malwares from a system
  - Microsoft Security Essentials
  - Microsoft Windows Defender
  - AVG Internet Security
  - Spy-bot - Search & Destroy
  - Avast! Home Edition for personal use
  - Panda Internet Security
  - Mac-Scan for Mac OS and Mac OS X

# Thank you

# ???

# Software security SEng 3071

## Chapter 7

## Firewall

# Presentation outline

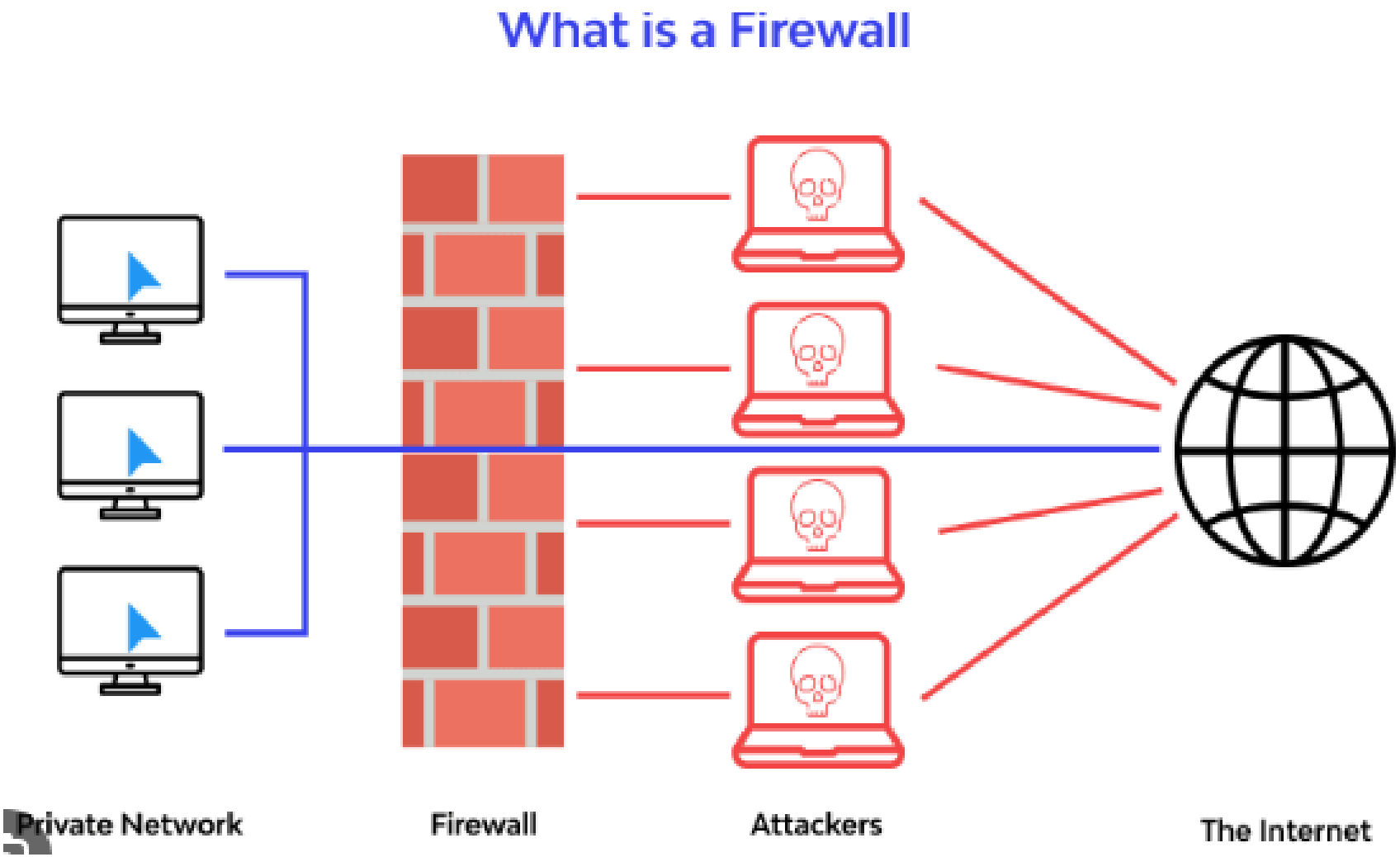
- Firewall
- What are Firewalls?
- Design principles of firewalls
- Firewall Characteristics
- Types of Firewalls

# Firewall

- One of the major challenges that companies face when trying to **secure** their sensitive data is **finding the right tools** for the job.
- Even for a common tool such as a firewall (sometimes called a network firewall), many businesses might not have a clear idea of how to find the right firewall (or firewalls) for their needs, how to configure those firewalls, or why such firewalls might be necessary.
- A complete network separation should be established between trusted and untrusted devices.
- Trusted devices should be behind a firewall.
- IT policy should be kept in mind before performing any major changes in the system.

# Firewall

- **What are Firewalls?**



# Firewall

- **What are Firewalls?**
- A firewall is a type of **cybersecurity tool** that is used to **filter traffic** on a network.
- **A Firewall is a network security device that monitors and filters incoming and outgoing network traffic based on an organization's previously established security policies.**
- At its most basic, a firewall is essentially the **barrier that sits between a private internal network and the public Internet.**
- The primary **goal** of a firewall is to **block malicious traffic requests** and **data packets** while allowing legitimate traffic through.
- Firewalls can be software, hardware, or cloud-based, with each type of firewall having its own unique pros and cons.
- Firewalls can be an **effective means of protecting a local system or network of systems from network-based**

# Firewall

- **Design principles of firewalls**
- A **Firewall** is a hardware or software to prevent a private computer or a network of computers from unauthorized access, it acts as a filter to avoid unauthorized users from accessing private computers and networks.
- It is a vital component of network security. It is the first line of defense for network security.
- It filters network packets and stops malware from entering the user's computer or network by blocking access and preventing the user from being infected.

# Firewall

- **Design principles of firewalls**

1. **Different Requirements:** Every local network or system has its threats and requirements which needs different structure and devices. All this can only be identified while designing a firewall. Accessing the current security outline of a company can help to create a better firewall design.
2. **Outlining Policies:** Once a firewall is being designed, a system or network doesn't need to be secure. Some new threats can arise and if we have proper paperwork of policies then the security system can be modified again and the network will become more secure.
3. **Identifying Requirements:** While designing a firewall data related to threats, devices needed to be integrated, Missing resources, and updating security devices. All the information collected is combined to get the best results. Even if one of these things is misidentified leads to security issues.

# Firewall

- **Design principles of firewalls**

4. **Setting Restrictions:** Every user has limitations to access different level of data or modify it and it needed to be identified and taken action accordingly. After retrieving and processing data, priority is set to people, devices, and applications.
5. **Identify Deployment Location:** Every firewall has its strengths and to get the most use out of it, we need to deploy each of them at the right place in a system or network. In the case of a packet filter firewall, it needs to be deployed at the edge of your network in between the internal network and web server to get the most out of it.

# Firewall

- **Design principles of firewalls**

## 6. Developing Security Policy

- Security policy is a very essential part of firewall design.
- Security policy is designed according to the requirement of the company or client to know which kind of traffic is allowed to pass.
- Without a proper security policy, it is impossible to restrict or allow a specific user or worker in a company network or anywhere else.
- A properly developed security policy also knows what to do in case of a **security breach.**
- Without it, there is an increase in risk as there will not be a proper implementation of security solutions.

# Firewall

- **Design principles of firewalls**

**7. Simple Solution Design**

- If the design of the solution is complex. then it will be difficult to implement it.
- If the solution is easy. then it will be easier to implement it. A simple design is easier to maintain. we can make upgrades in the simple design according to the new possible threats leaving it with an efficient but more simple structure.
- The problem that comes with complex designs is a configuration error that opens a path for external attacks.

# Firewall

- **Design principles of firewalls**

## 8. Choosing the Right Device

- Every network security device has its purpose and its way of implementation. if we use the wrong device for the wrong problem, the network becomes vulnerable.
- If the outdated device is used for a designing firewall, it exposes the network to risk and is almost useless.
- Firstly the designing part must be done then the product requirements must be found out, if the product is already available then it is tried to fit in a design that makes security weak.

## 9. Layered Defense

- A network defense must be multiple-layered in the modern world because if the security is broken, the network will be exposed to external attacks. Multilayer security design can be set to deal with different levels of threat. It gives an edge to the security design and finally neutralizes the attack on

# Firewall

- **Design principles of firewalls**

**10. Consider Internal Threats**

- While giving a lot of attention to safeguarding the network or device from external attacks.
- The security becomes weak in case of internal attacks and most of the attacks are done internally as it is easy to access and designed weakly.
- Different levels can be set in network security while designing internal security.
- Filtering can be added to keep track of the traffic moving from lower-level security to higher level.

# Firewall

- **Characteristics of Firewall**

- **Physical Barrier:** A firewall does not allow any external traffic to enter a system or a network without its allowance. A firewall creates a choke point for all the external data trying to enter the system or network and hence can easily block access if needed.
- **Multi-Purpose:** A firewall has many functions other than security purposes. It configures domain names and Internet Protocol (IP) addresses. It also acts as a network address translator. It can act as a meter for internet usage.
- **Flexible Security Policies:** Different local systems or networks need different security policies. A firewall can be modified according to the requirement of the user by changing its security policies.
- **Security Platform:** It provides a platform from which any alert to the issue related to security or fixing issues can be accessed. All the queries related to security can be kept under check from one place in a system or network.
- **Access Handler:** Determines which traffic needs to flow first according to priority or can change for a particular network or

# Firewall

- **Advantages of Characteristics**

- **Blocks infected files:** in internet we encounter many unknown threats. Any file might have malware in it. The firewall neutralizes this kind of threat by blocking file access to the system.
- **Stop unwanted visitors:** A firewall does not allow a cracker to break into the system through a network. A strong firewall detects the threat.
- **Safeguard the IP address:** A network-based firewall like an internet connection firewall(ICF). Keeps track of the internet activities done on a network or a system and keeps the IP address hidden so that it can not be used to access sensitive information against the user.
- **Prevents Email spamming:** In this too many emails are sent to the same address leading to the server crashing. A good firewall blocks the spammer source and prevents the server from crashing.
- **Stops Spyware:** If a bug is implanted in a network or system it tracks all the data flowing and later uses it for the wrong purpose. A firewall keeps track of all the users accessing the

# Firewall

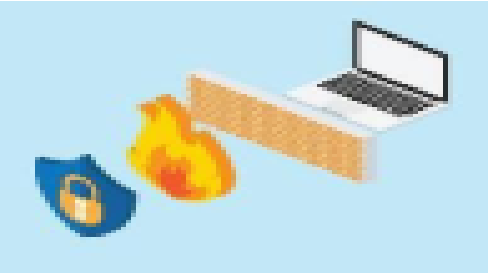
- **Firewalls have their limitations, including the following:**

1. The firewall cannot protect against attacks that bypass the firewall.
2. The firewall does not protect against internal threats, such as a disgruntled employee or an employee who unwittingly cooperates with an external attacker.
3. The firewall cannot protect against the transfer of virus-infected programs or files. Because of the variety of operating systems and applications supported inside the perimeter, it would be impractical and perhaps impossible for the firewall to scan all incoming files, email, and messages for viruses.
4. Firewalls are not able to stop the users from accessing the data or information from malicious websites, making them vulnerable to internal threats or attacks. It does not prevent misuse of passwords and attackers with modems

# Firewall

- **Types of Firewalls**
- Firewall types can be divided into several different categories **based on their general structure and method of operation.** Here are eight types of firewalls:
  - Packet-filtering firewalls
  - Circuit-level gateways
  - State-full inspection firewalls
  - Application-level gateways (a.k.a. proxy firewalls)
  - Next-gen firewalls
  - Software firewalls
  - Hardware firewalls
  - Cloud firewalls

# Firewall (Types)



## ❑ Packet-Filtering Firewalls

- A packet filtering firewall is the most basic type of firewall.
- It acts like a management program that monitors network traffic and filters incoming packets based on configured security rules.
- These firewalls are designed to block network traffic IP protocols, an IP address, and a port number if a data packet does not match the established rule-set.
- While packet-filtering firewalls can be considered a fast solution without many resource requirements, they also have some limitations.
- As the most "basic" and oldest type of firewall architecture, packet filtering firewalls basically **create a checkpoint at a traffic router or switch.**

# Firewall (Types)

## ❑ Circuit-Level Gateways

- Circuit-level gateways work by verifying the transmission control protocol (TCP).
- **A circuit-level gateway** firewall helps in providing the security between **UDP** and **TCP** using the connection.
- This TCP check is designed **to make sure that the session the packet is from is legitimate.**
- While extremely resource-efficient, these firewalls **do not check the packet itself.**
- So, if a packet held malware, but had the right TCP handshake, it would pass right through.
- This is why circuit level gateways are not enough to protect your business by themselves.

# Firewall (Types)

## ❑ State-full Inspection Firewalls

- These firewalls combine both **packet inspection technology and TCP handshake verification** to create a level of protection greater than either of the previous two architectures could provide alone.
- is a kind of firewall that keeps track and **monitors the state of active network connections** while analyzing incoming traffic and looking for potential traffic and data risks.
- A state-full firewall collects data regarding every connection made through it.
- However, these firewalls put more of a strain on computing resources as well.
- This may slow down the transfer of legitimate packets compared to the other solutions.

# Firewall (Types)

## ❑ Proxy Firewalls (Application-Level Gateways/Cloud Firewalls)

- A proxy firewall, also known as an application firewall or a gateway firewall, **limits the applications that a network can support, which increases security levels but can affect functionality and speed.**
- These firewalls are delivered via a cloud-based solution or another proxy device.
- Rather than letting traffic connect directly, **the proxy firewall first establishes a connection to the source of the traffic and inspects the incoming data packet.**
- This check is similar to the state-full inspection firewall in that it looks at both the packet and at the TCP handshake protocol.
- However, proxy firewalls may also perform deep-layer packet inspections, checking the actual contents of the information packet to verify that it contains no malware.

# Firewall (Types)

- **Proxy Firewalls (Application-Level Gateways/Cloud Firewalls)**

- Once the check is complete, and the packet is approved to connect to the destination, the proxy sends it off.
- This creates an extra layer of separation between the "client" (the system where the packet originated) and the individual devices on your network—obscuring them to create additional anonymity and protection for your network.
- If there's one drawback to proxy firewalls, it's that they can create significant slowdown because of the extra steps in the data packet transferal process.

# Firewall (Types)

## ❑ Next-Generation Firewalls

- Many of the most recently-released firewall products are being touted as "next-generation" architectures.
- However, there is not as much consensus on what makes a firewall truly next-generation.
- Some common features of next-generation firewall architectures include **deep-packet inspection (checking the actual contents of the data packet), TCP handshake checks, and surface-level packet inspection.**
- Next-generation firewalls may include other technologies as well, such as **intrusion prevention systems** (IPSs) that **work to automatically stop attacks against your network.**
- The issue is that **there is no one definition of a next-generation firewall,** so it's important to verify what specific capabilities such firewalls have before investing in one.

# Firewall (Types)

## ❑ Software Firewalls

- Software firewalls include any type of **firewall that is on a local device rather than a separate piece of hardware** (a cloud server).
- The big benefit of a software firewall is that it is highly useful for creating defense in depth by isolating individual network **endpoints from one another.**
- However, maintaining individual software firewalls on different devices can be difficult and time consuming.
- Furthermore, not every device on a network may be compatible with a single software firewall, which may mean having to use several different software firewalls to cover every asset.

# Firewall (Types)

## ❑ Hardware Firewalls

- Hardware firewalls use a physical appliance that acts in a manner **similar to a traffic router to intercept data packets and traffic requests before they're connected to the network's servers.**
- Physical appliance-based firewalls like this excel at perimeter security by making sure malicious traffic from outside the network is intercepted before the company's network endpoints are exposed to risk.
- The major weakness of a hardware-based firewall, however, is that it is often easy for insider attacks to bypass them.
- Also, the actual capabilities of a hardware firewall may vary depending on the manufacturer, some may have a more limited capacity to handle simultaneous connections than others.

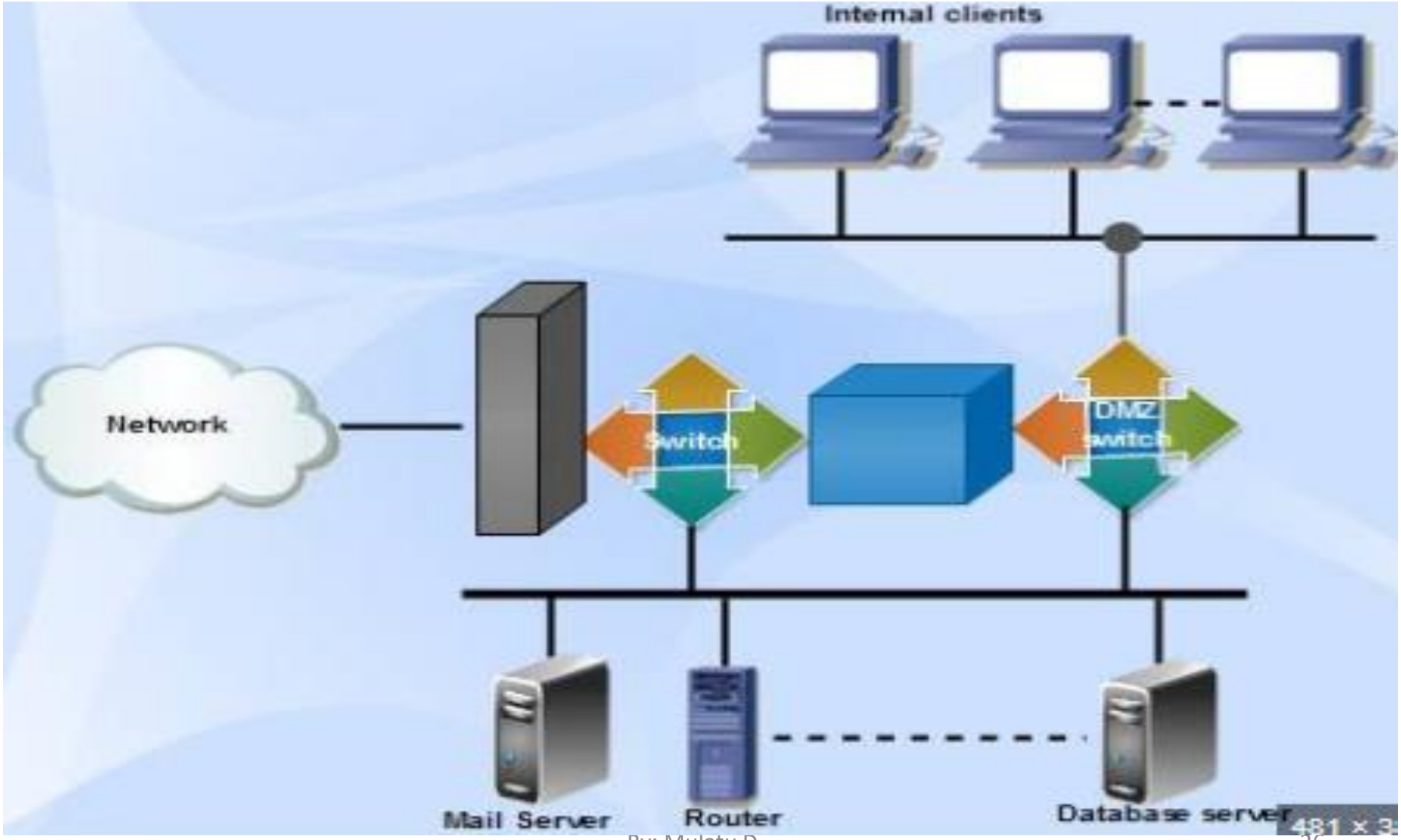
# Firewall (Types)

## ❑ Cloud Firewalls

- Whenever a cloud solution is used to deliver a firewall, it can be called a cloud firewall, or firewall-as-a-service (FaaS).
- Cloud firewalls are considered synonymous with proxy firewalls by many, since a cloud server is often used in a proxy firewall setup (though the proxy doesn't necessarily have to be on the cloud, it frequently is).
- The big benefit of having cloud-based firewalls is that they are very easy to scale with your organization.
- As your needs grow, you can add additional capacity to the cloud server to filter larger traffic loads.
- Cloud firewalls, like hardware firewalls, excel at perimeter security.

# Firewall

## ❑ Firewall Architectures



# Firewall

## ❑ Firewall Architectures

- Firewall architecture is built upon four primary components, **network policy, advanced authentication, packet filtering, and application gateways.** Let us look at each component in detail.

### 1. Network policy

- The design, installation, and use of a firewall in a network are largely influenced by two levels of network policy, the higher-level policy and the lower-level policy.

A. The **higher-level** policy is an issue-specific network access policy that defines services that are allowed or explicitly denied from the restricted network, how they would be used, and the conditions for exceptions to this policy.

B. The **lower-level** policy discloses how the firewall will handle access restriction and service filtration defined in the higher-level policy.

# Firewall

## ❑ Firewall Architectures

- These policies are briefly explained below.

## ❑ Service access policy

- The service access policy focuses on internet-specific usage issues and all outside network accesses (i.e., dial-in policy, SLIP, and PPP connections). For a firewall to be successful, the service access policy must be realistic and sound and should be drafted before implementing a firewall. A realistic policy is one that provides a balance between protecting the network from known risks while still providing users access to network resources.
- A firewall can implement several service access policies. However, a typical policy may be to allow no access to a site from the internet but allow access from the site to the internet. Firewalls often implement service access policies that allow some user access from the internet to selected internal hosts.

# Firewall

- **Firewall Architectures**
- **Firewall design policy**

- The firewall design policy is specific to the firewall and defines the rules used to implement the service access policy.
- One cannot design this policy in a vacuum isolated from understanding firewall capabilities and limitations and **threats and vulnerabilities** associated with TCP/IP.
- Firewalls generally implement one of two basic design policies, **permit** any service unless it is expressly denied and **deny** any service unless it is explicitly permitted.
- A firewall that implements the first policy allows all services to pass into the site by default, except services that the service access policy has identified as disallowed. The second policy follows the classic access model used in all areas of information security, where the second policy denies all services by default but then passes those services

# Firewall

## ❑ Firewall Architectures

### 2. Advanced authentication

- Advanced authentication measures such as smartcards, authentication tokens, biometrics, and software-based mechanisms are designed to tackle weak traditional passwords.
- Given the problems posed by passwords on the internet, an internet-accessible firewall that does not use or does not contain the hooks to use advanced authentication may be regarded as irrelevant in the current setting.
- Some of the more popular advanced authentication devices in use today are called **one-time password systems.** A smartcard or authentication token, for example, generates a response that the host system can use in place of a traditional password. Because the token or card works in conjunction with software or hardware on the host, the generated response is unique for every login.

# Firewall

## ❑ Firewall Architectures

### 3. Packet filtering

- IP packet filtering is accomplished using a **packet filtering** router that filters packets as they pass between the router's interfaces.
- A packet-filtering router usually can filter IP packets based on source IP address, destination IP address, TCP/UDP source port, or destination port.
- Not all packet filtering routers currently filter the source TCP/UDP port.
- However, more vendors are starting to incorporate this capability.
- Some routers examine which of the router's network interfaces a packet arrived at and then use this as an additional filtering criterion.

# Firewall

## ❑ Firewall Architectures

### 4. Application gateways

- To counter the weaknesses associated with packet filtering routers, firewalls need to use software applications to forward and filter connections for services such as TELNET and FTP.
- Such an application is referred to as a proxy service, while the host running the proxy service is referred to as an application gateway.

# Thank you

# ???