SWAMI VIVEKANAND COLLEGE OF COMPUTER SCIENCE

B.C.A. SEM - VI

SUBJECT – Network Security (603)

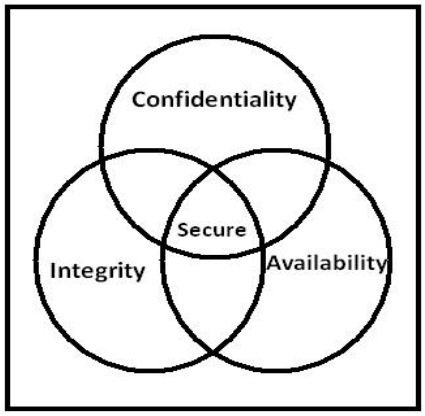
Unit - 1

UNIT – Network Security Fundamental

- Concept of Computer Security, Challenges of Computer Security.
- The OSI Security Architecture.
- Types of Security Attacks: Active Attacks and Passive attacks
- Security Services: Authentication, Access Control, Data Confidentiality, and Data Integrity.
- A Model for Network Security.

1.1 Concept of Computer Security

- **Computer security** allows you to use the computer while keeping it safe from threats. Computer security can be defined as controls that are put in place to provide confidentiality, integrity, and availability for all components of computer systems. These components include information / data, software, hardware, firmware, Telecommunication etc.
- There are three **goals** (Objects) of computer security.
    1. Confidentiality
    2. Integrity
    3. Availability



- **Confidentiality:** This term covers two related concepts
    - ✓ *Data confidentiality:* Assures that private or confidential Information is not made available or disclosed to unauthorized individuals.
    - ✓ *Privacy:* Assures that individuals control or influence what Information related to them may be collected and stored and by whom and to whom that information may be disclosed.
- **Integrity:** This term covers two related concepts
    - ✓ *Data integrity:* Assures that information and programs are changed only in a specified and authorized manner.
    - ✓ *System integrity:* Assures that a system performs its intended function in an unaffected manner, free from deliberate or unauthorized manipulation of the system.
- **Availability:** Assures that systems work immediately and service is not denied to authorize users.

Challenges of Computer Security

- Computer security is both interesting and complex. Some of the reasons follow:

1. Computer security is not as simple as it might first appear to the beginner. The requirements seem to be simple; most of the major requirements for security services can be given understandable one-word labels: confidentiality, authentication, non repudiation, integrity. But the mechanisms used to meet those requirements can be quite complex.
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 counterintuitive. Typically, a security mechanism is, and it is not apparent from the declaration of a particular requirement that such precise measures are needed. It is only when the various aspects of the threat are considered that precise security mechanisms make sense.
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/ (Transmission Control Protocol/Internet Protocol) should mechanisms be placed].

5. Security mechanisms typically involve more than a particular algorithm or protocol. They also require that participants (members) be in control of some secret information (e.g., an encryption key), which raises questions about the creation, distribution, and protection of that secret information. There may also be a trust on communications protocols whose behavior 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.
6. Computer security is essentially a battle of wits between a guilty party 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 until a security failure occurs.
8. Security requires regular, even constant, monitoring, and this is difficult in today' short-term, overloaded environment.
9. Security is still too often an addition 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 to efficient and user-friendly operation of an information system or use of information. The difficulties just enumerated will be encountered in numerous ways.

1.2 The OSI Security Architecture.

- The OSI security architecture is useful to managers as a way of organizing the task of providing Security. The OSI security architecture focuses on security attacks, mechanisms, and services. These Can be defined briefly as follows:
  - ✓ **Security attack**: Any action that compromises the security of information owned by an organization.
  - ✓ **Security mechanism:** A process (or a device incorporating such a process) that is designed to detect, Prevent, or recover from a security attack.
  - ✓ **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.

Threat:

- ✓ A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. That is, a threat is a possible danger that might exploit vulnerability.

Attack:

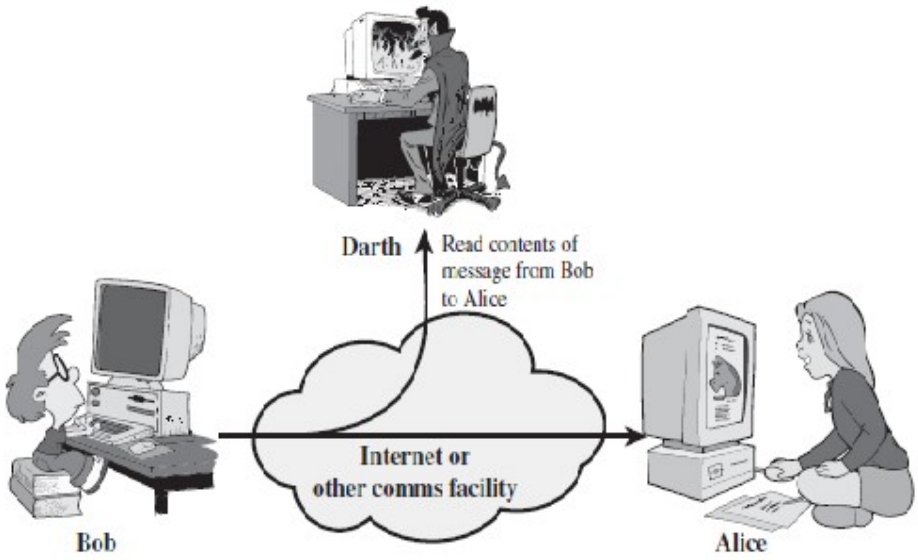
- ✓ An assault on system security that derives from an intelligent threat; that is, an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.

1.3 Types of Security Attacks: Active Attacks and Passive attacks

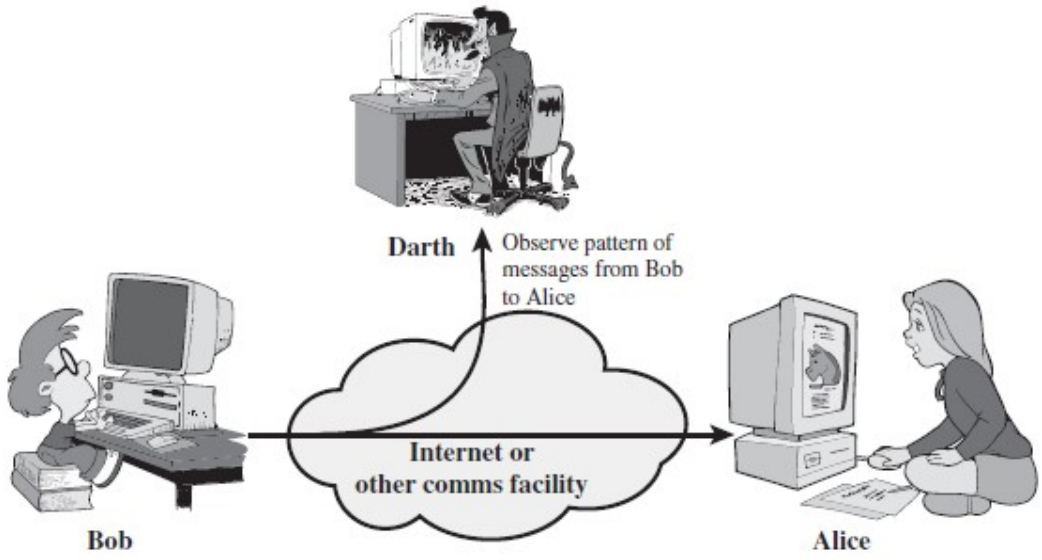
A useful means of classifying security attacks is in terms ***passive attacks*** and ***active attacks***.

(1) Passive Attacks:

- ✓ A passive attack attempts to learn or make use of information from the system but does not affect system resources.
- ✓ Passive attacks are in the nature of eavesdropping on, or monitoring of, transmissions. The goal of the opponent is to obtain information that is being transmitted. Two types of passive attacks are…
  - ***release of message contents***
  - ***traffic analysis***
- ✓ The *release of message contents* is easily understood. A telephone conversation, an electronic mail message, and a transferred file may contain sensitive or confidential information. We would like to prevent an opponent from learning the contents of these transmissions.
- ✓ A second type of passive attack, *traffic analysis*, is subtler. Suppose that we had a way of masking the contents of messages or other information traffic so that opponents, even if they captured the Message, could not extract the information from the message. The common technique for masking contents is encryption Passive attacks are very difficult to detect because they do not involve any alteration of the data.



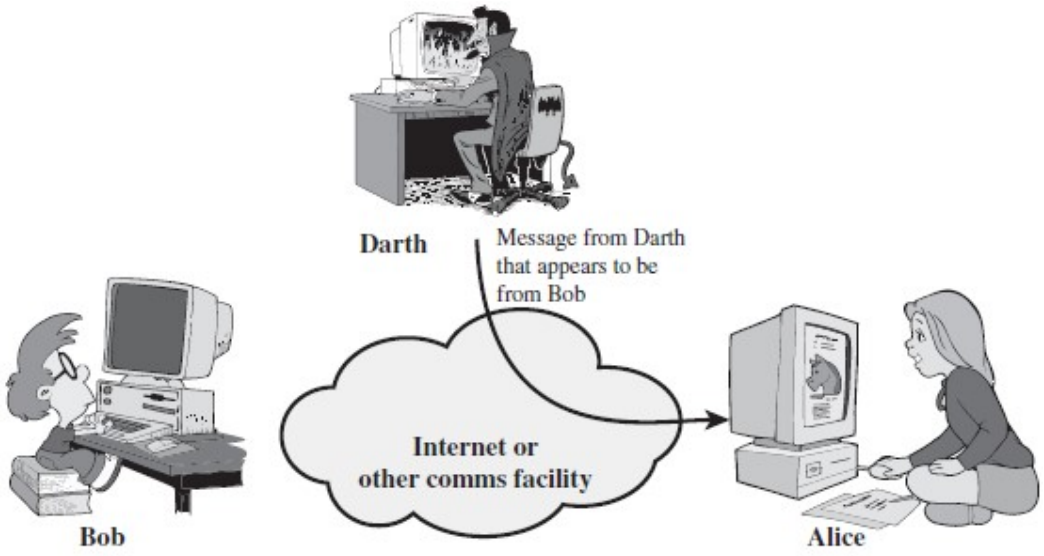
[Release of Message Contents]



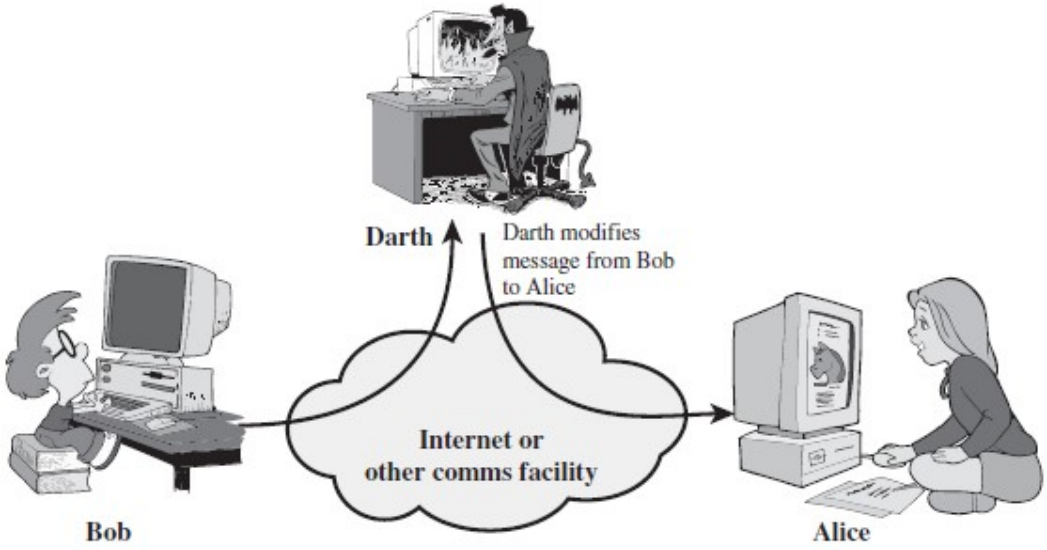
[Traffic Analysis]

(2) Active Attacks:

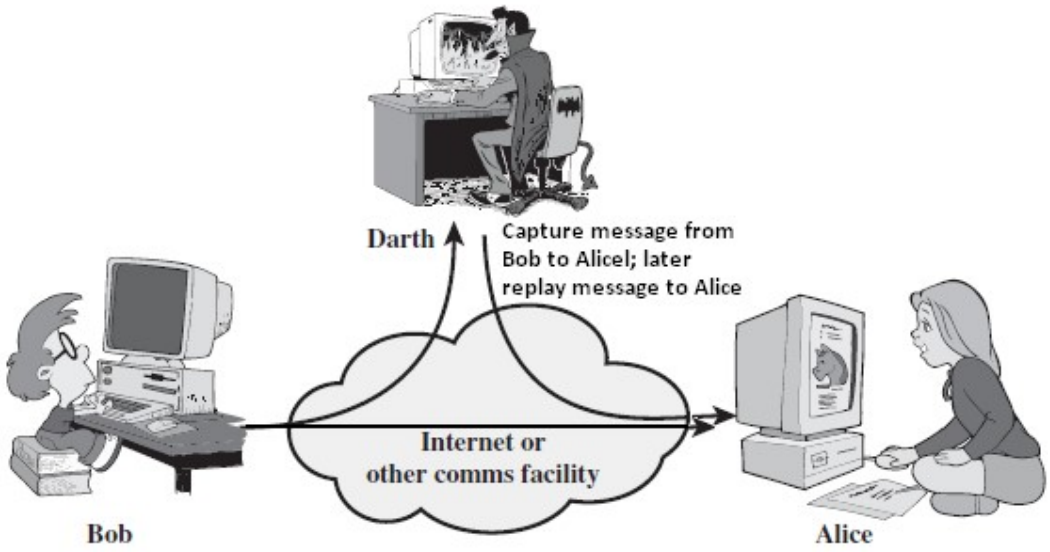
- ✓ Active attacks involve some modification of the data stream or the creation of a false stream and can be subdivided into four categories:
  - ***Masquerade***
  - ***Replay***
  - ***Modification of messages***
  - ***Denial of service.***
- ✓ A *masquerade* takes place when one entity pretends to be a different entity. A masquerade attack usually includes one of the other forms of active attack. For example, authentication sequences can be captured and replayed after a valid authentication sequence has taken place, thus enabling an authorized entity with few privileges to obtain extra privileges by impersonating an entity that has those privileges.
- ✓ *Replay* involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect.
- ✓ *Modification of messages* simply means that some portion of a legitimate message is altered, or that messages are delayed or reordered, to produce an unauthorized effect.
- ✓ The *denial of service* prevents or inhibits the normal use or management of communications facilities. This attack may have a specific target; for example, an entity may suppress all messages directed to a particular destination (e.g., the security audit service).
- ✓ Active attacks present the opposite characteristics of passive attacks. Whereas passive attacks are difficult to detect, measures are available to prevent their success. On the other hand, it is quite difficult to prevent active attacks absolutely.



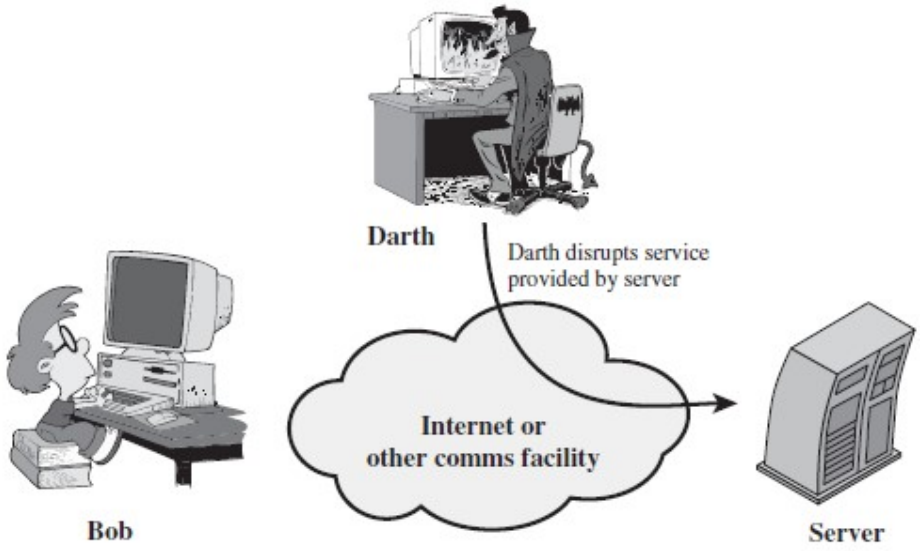
[Masquerade]



[Modification of messages]



[Replay]



[Denial of service]

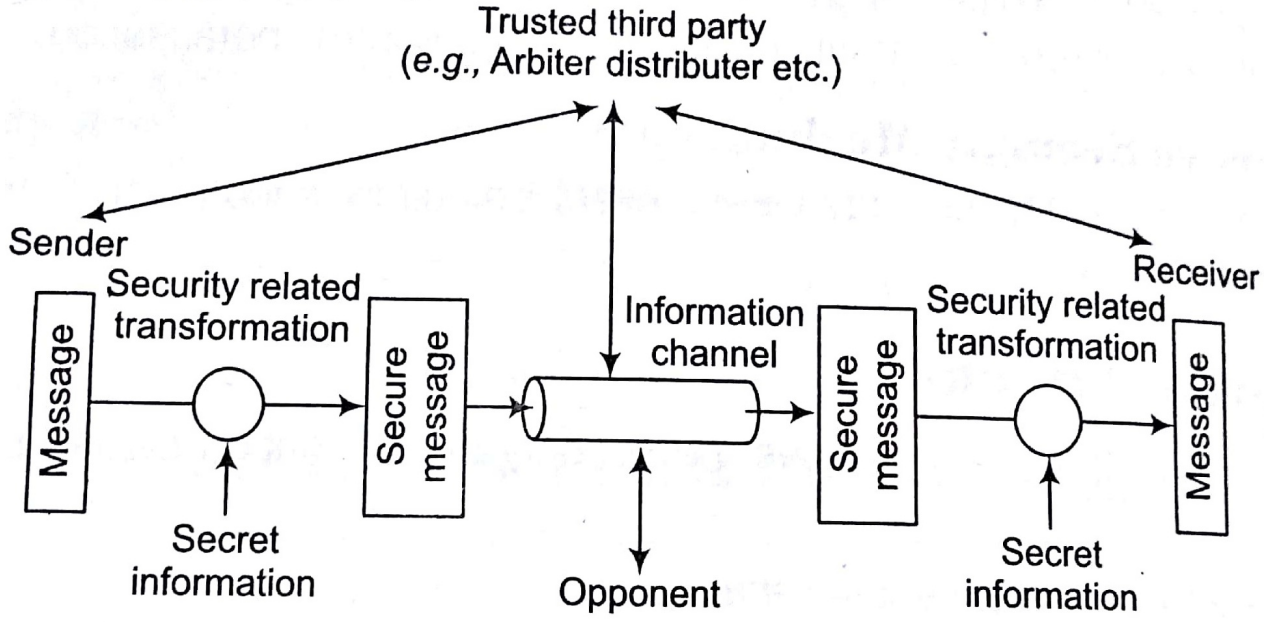
1.4 SECURITY SERVICES

- ***Security service*** as a service provided by a protocol layer of communicating open systems, which ensures adequate security of the systems or of data transfers. Also defines ***security services*** as a processing or communication service that is provided by a system to give a specific kind of protection to system resources. Security Services implement security policies and are implemented by security mechanisms.
- Security service divide into five categories and fourteen specific services are following.

1. **AUTHENTICATION:** The assurance that the communicating entity is the one that it claims to be.
    a. **Peer Entity Authentication:** Used in association with a logical connection to provide confidence in the identity of the entities connected.
    b. **Data Origin Authentication:** In a connectionless transfer, provides assurance that the source of received data is as claimed.
2. **ACCESS CONTROL:** The prevention of unauthorized use of a resource (i.e., this service controls who can have access to a resource, under what conditions access can occur, and what those accessing the resource are allowed to do.)
3. **DATA CONFIDENTIALITY:** The protection of data from unauthorized disclosure.
    a. **Connection Confidentiality:** The protection of all user data on a connection.
    b. **Connectionless Confidentiality:** The protection of all user data in a single data block
    c. **Selective-Field Confidentiality:** The confidentiality of selected fields within the user Data on a connection or in a single data block.
    d. **Traffic Flow Confidentiality:** The protection of the information that might be derived from observation of traffic flows.
4. **DATA INTEGRITY:** The assurance that data received are exactly as sent by an authorized entity (i.e., contain no modification, insertion, deletion, or replay).
    a. **Connection Integrity with Recovery:** Provides for the integrity of all user data on a connection and detects any modification, insertion, deletion, or replay of any data within an entire data sequence, with recovery attempted.
    b. **Connection Integrity without Recovery:** As above, but provides only detection without recovery.
    c. **Selective-Field Connection Integrity:** Provides for the integrity of selected fields within the user data of a data block transferred over a connection and takes the form of determination of whether the selected fields have been modified, inserted, deleted, or replayed.
    d. **Connectionless Integrity:** Provides for the integrity of a single connectionless data block and may take the form of detection of data modification. Additionally, a limited form of replay detection may be provided.
    e. **Selective-Field Connectionless Integrity:** Provides for the integrity of selected fields within a single connectionless data block; takes the form of determination of whether the selected fields have been modified.
5. **NONREPUDIATION:** Provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication
    a. **Nonrepudiation, Origin:** Proof that the message was sent by the specified party.
    b. **Nonrepudiation, Destination:** Proof that the message was received by the specified party.

1.5 A Model for Network Security

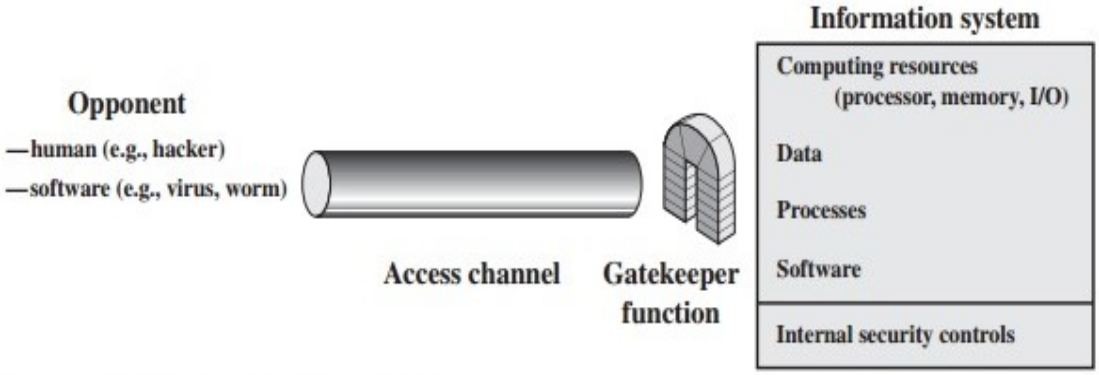
- A security-related transformation on the information to be sent. Examples include the encryption of the message, which scrambles the message so that it is unreadable by the opponent, and the addition of a code based on the contents of the message, which can be used to verify the identity of the sender.
- Some secret information shared by the two principals and, it is hoped, unknown to the opponent. An example is an encryption key used in conjunction with the transformation to scramble the message before transmission and unscramble it on reception.
- A trusted third party may be needed to achieve secure transmission. For example, a third party may be responsible for distributing the secret information to the two principals while keeping it from any opponent. Or a third party may be needed to arbitrate disputes between the two principals concerning the authenticity of a message transmission.
- This general model shows that there are four basic tasks in designing a particular security service:
  1. Design an algorithm for performing the security-related transformation. The algorithm should be such that an opponent cannot defeat its purpose.
  2. Generate the secret information to be used with the algorithm.
  3. Develop methods for the distribution and sharing of the secret information.
  4. Specify a protocol to be used by the two principals that makes use of the security algorithm and the secret information to achieve a particular security service.



A general Netwok Security Model (NSM)

- A general model of these other situations is illustrated by following Figure, which reflects a concern for protecting an information system from unwanted access. Most readers are familiar with the concerns caused by the existence of hackers, who attempt to penetrate systems that can be accessed over a network. The hacker can be someone who, with no malign intent, simply gets

satisfaction from breaking and entering a computer system. The intruder can be a disgruntled employee who wishes to do damage or a criminal who seeks to exploit computer assets for financial gain (e.g., obtaining credit card numbers or performing illegal money transfers).



[Network Access Security Model]

- Another type of unwanted access is the placement in a computer system of logic that exploits vulnerabilities in the system and that can affect application pro-grams as well as utility programs, such as editors and compilers. Programs can pre-sent two kinds of threats:
  - **Information access threats:** Intercept or modify data on behalf of users who should not have access to that data.
  - **Service threats:** Exploit service flaws in computers to inhibit use by legitimate users.

- Viruses and worms are two examples of software attacks. Such attacks can be introduced into a system by means of a disk that contains the unwanted logic con-cealed in otherwise useful software. They can also be inserted into a system across a network; this latter mechanism is of more concern in network security.

- The security mechanisms needed to cope with unwanted access fall into two broad categories. The first category might be termed a gatekeeper function. It includes password-based login procedures that are designed to deny access to all but authorized users and screening logic that is designed to detect and reject worms, viruses, and other similar attacks. Once either an unwanted user or unwanted software gains access, the second line of defense consists of a variety of internal controls that monitor activity and analyze stored information in an attempt to detect the presence of unwanted intruders.