UNIT- 1

Chapter 1: Attacks on Computers and Computer Security

① Introduction

Computer Security or cybersecurity is the protection of computer systems and networks from information disclosure, theft of or damage to their hardware, software, or data, as well as from the misdirection of the services they provide.

→ Computer security is the process of preventing and detecting unauthorized use of your computer system.

Network security consists of the policies, processes to prevent, detect & monitor unauthorized access, misuse, modification of a computer network and network-accessible resources.

Threat :- A potential for violation of security, which exists when there is a circumtance, capability, action, or event that could breach security and cause harm.

Attack :- An assault on system security that derives from an intelligent threat; that is, an intelligent act that is a deliberate attempt to evade security services and & violate the security policy of a system.

② The need for security

The network needs security against attackers and hackers. Network security includes the security of data or information i.e., to protect the information from unauthorized access and loss.

→ Here network security not only means security in a single network rather in any network or network of networks

* The information security is needed for the following given reasons:-

→ To protect the secret information from unwanted editing, accidently or intentionally by unauthorized users

→ To protect the information from loss and make it to be delivered to its destination properly.

→ To restrict a user to send some message to another user with name of a third one.

* Computer security means to protect your computer system from unwanted damages caused due to network. The need of computer security from Hackers are as follows:-

→ It should be protected from replicating and capturing viruses from infected files.

→ It needs a proper protection from worms.

→ There is a need of protection from Trojan Horses as they are enough dangerous for your computer.

When Computer applications were developed to handle financial & personal data, the security is needed. people realized that data on Computers was extremely important aspect of modern life. Two typical examples of such security mechanisms were as follows:

→ provide a user id and password to every user and use that information to authenticate a user.

→ Encode information stored in the database in some fashion so that it is not visible to users who do not have the right permissions.

③ Security Approaches

In present scenario Security of the system is the sole priority of any organization. The main aim of any organization is to protect their data from attackers.

* Security Models :- An organization can take several approaches to implement its security model.

- No security: In this simplest case, the approach could be a decision to implement no security at all.
- Security through obscurity :- In this model, a system is secure simply because nobody knows about its existence and contents. This approach cannot work for too long, as there are many ways an attacker can come to know about it.
- Host security: In this scheme, the security for each host is enforced individually. This is a very safe approach, but the trouble is that it cannot scale well. The complexity and diversity of modern sites/organizations makes the task even harder.
- Network security: Host security is tough to achieve as organizations grow and become more diverse. In this technique, the focus is to control network access to various hosts and their services, rather than individual host security. This is a very efficient and scalable model.

* Security Management Practices :- A good security policy and its proper implementation go a long way in ensuring sufficient security management practices. A good security policy generally takes care of four key aspects:

- Affordability :- Cost and effort in security implementation.
- Functionality :- Mechanism of providing security
- Cultural issues :- Whether the policy work well with people's expectations, working style and beliefs.
- Legality :- Whether the policy meets the legal requirements.

④ Principles of Security

The principles of security can be classified as follows:

1. Confidentiality
2. Authentication
3. Integrity
4. Non-Repudiation
5. Access control
6. Availability

* **Confidentiality**:- The principle of Confidentiality specifies that only the Sender and the intended receiver(s) should be able to access the contents of a message.

→ Confidentiality gets compromised if an unauthorized person is able to access a message.

For example:- Let us consider sender A wants to sends a message to receiver B. Another user C gets access to this message, which is not desired and therefore, defects the purpose of confidentiality. The message is accessed by C without the permission of A and B. This type of attack is called as interception.

- Interception causes loss of message Confidentiality.

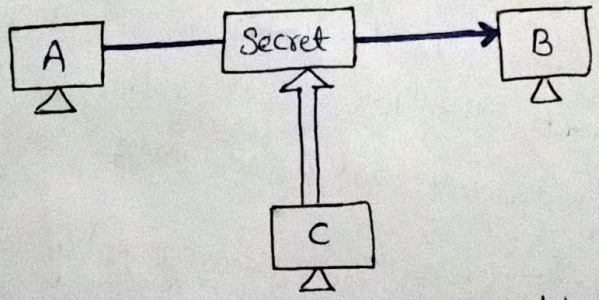

Fig:- Loss of confidentiality

* **Authentication**:- Authentication mechanism help establish proof of identities. It ensures the identity of the person trying to access the information.

For example:- Suppose that user C sends an electronic document over the Internet to user B. The trouble is that user C had posed as user A, when she sent this document to user B.

→ How would user B know that the message has come from user C, who is posing as user A?

This type of attack is called as fabrication.

- Fabrication is possible in absence of proper authentication mechanisms.

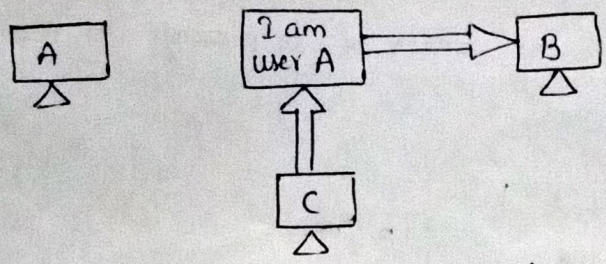

Fig:- Absence of authentication

* Integrity:- When the contents of a message are changed after the sender sends it, but before it reaches the intended receiver, we say that the integrity of the message is lost.

For example:- User C tampers with a message originally sent by user A, which is actually destined for user B. User C somehow manage to access it, change its contents and send the changed message to user B.

→ User B has no way of knowing that the contents of the message were changed after user A had sent it. User A does not know about this change. This type of attack is called as modification.

- Modification causes loss of message integrity.

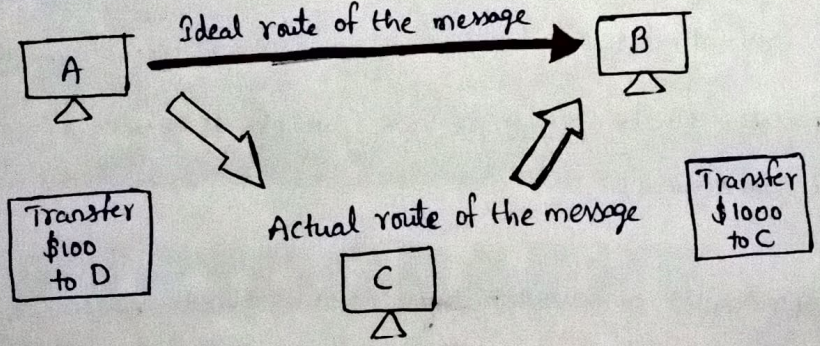

Fig:- Loss of Integrity

* Non-repudiation:- There are situations where a user sends a message and later on refuses that she had sent that message.

For example:- User A could send a funds transfer request to bank B over the Internet. After the bank performs the funds transfer as per A's instructions, A could claim that she never sent the funds transfer instruction to the bank!

Thus, A denies, her funds transfer instruction. The principle of non-repudiation defeats such possibilities of denying something, having done it.

Non-repudiation does not allow the sender of a message to refute the claim of not sending that message.

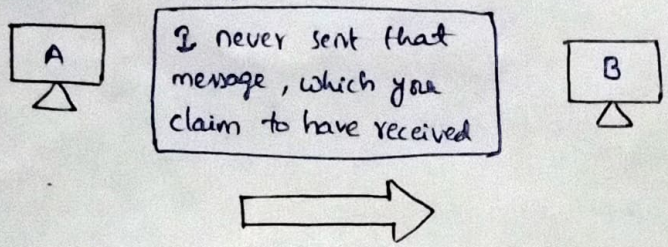

Fig:- Establishing non-repudiation

* Access Control:- The principle of access control determines who should be able to access what.

For example:- we should be able to specify that user A can view the records in a database, but cannot update them. User B might be allowed to make updates as well. An access control mechanism can be set up to ensure this.

- Access control is broadly related to two areas: < role management, rule management

Role management:- It concentrates on the user side (which user can do what)

Rule management:- It focuses on the resources side (which resource is accessible and under what circumstances).

* Availability:- The principle of availability states that resources (i.e., information) should be available to authorized parties at all times.

For example:- Due to the intentional actions of an unauthorized user C, an authorized user A may not be able to connect a Server Computer B. This would defeat the principle of availability. Such an attack is called as interruption.

- Interruption puts the availability of resources in danger

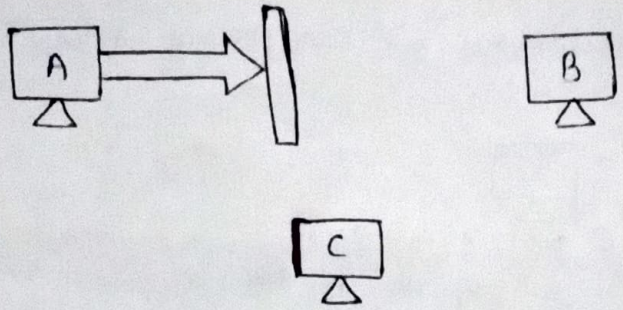

Fig:- Attack on availability

⇒ The OSI security model focuses on security attacks, mechanisms, and services. The OSI standard for security model defines seven layers of security in the form of:

- Authentication
- Access control
- Non repudiation
- Data Integrity
- Confidentiality
- Availability
- Notarization or Signature

⑤ Types of Attacks

The attacks are grouped into two types: passive attacks and active attacks

* Passive attacks :- Passive attacks are in the nature of eavesdropping or monitoring of data transmission. The attacker aims to obtain information that is in ~~trans~~ transit.

→ Passive attacks do not involve any modifications to the contents of an original message.

- Two types of passive attacks are: release of message contents, traffic analysis

(i) Release of message contents :- It is quite simple to understand. A telephone conversation, an email message and a file may contain sensitive or confidential information. The contents of the message are released against our wishes to someone else.

Using certain security mechanisms, we can prevent release of message contents.

(i) Traffic Analysis :-

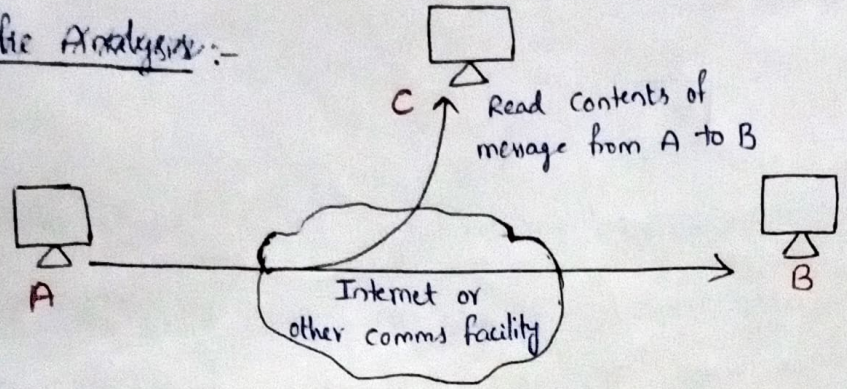

Fig:- Release of message contents

(ii) Traffic Analysis :- Suppose that we had a way of masking (encryption) the contents of message, so that the attacker even if captured the message could not extract any information from the message.

→ The opponent could determine the location and identify of communicating hosts and could observe the frequency and length of messages being exchanged.

This information might be useful in guessing the nature of the communication that was taking place.

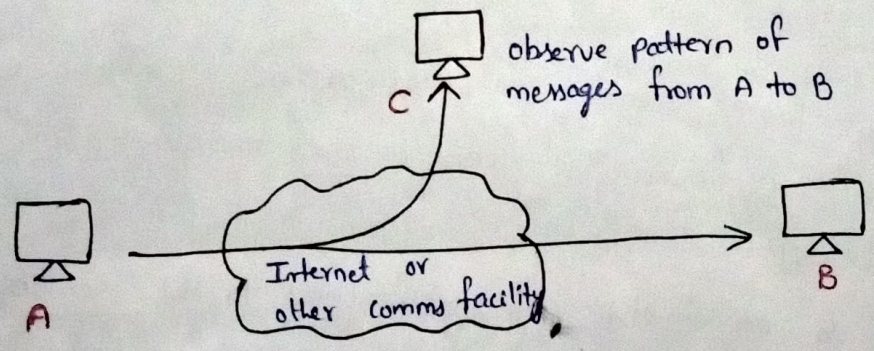

Fig:- Traffic analysis

* Active Attacks :- The Active attacks are based on modification of the original message in some manner or the creation of a false message.

→ In active attacks, the contents of the original message are modified in some way.

- The active attacks are divided into four categories: Masquerade, replay, modification of messages, and denial of service (DOS).

(i) Masquerade :- Masquerade is caused when an unauthorized entity pretends to be another entity. In this attacks, an entity poses as another entity. The attack may involve capturing the user's authentication sequence.

For example :- User C might pose as user A and send a message to user B. User B might be led to believe that the message indeed came from user A.

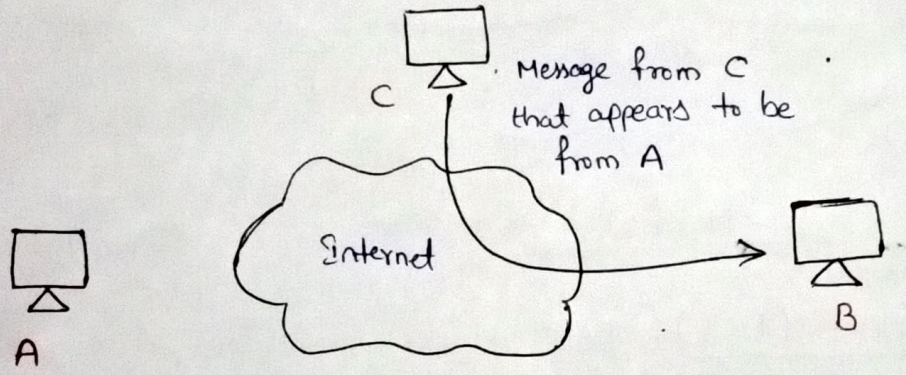

Fig :- Masquerade

(ii) Replay :- Replay involves the passive capture of a data unit and its subsequent retransmission to produce an unathorized effect. A user captures a sequence of events or some data units and re-sends them.

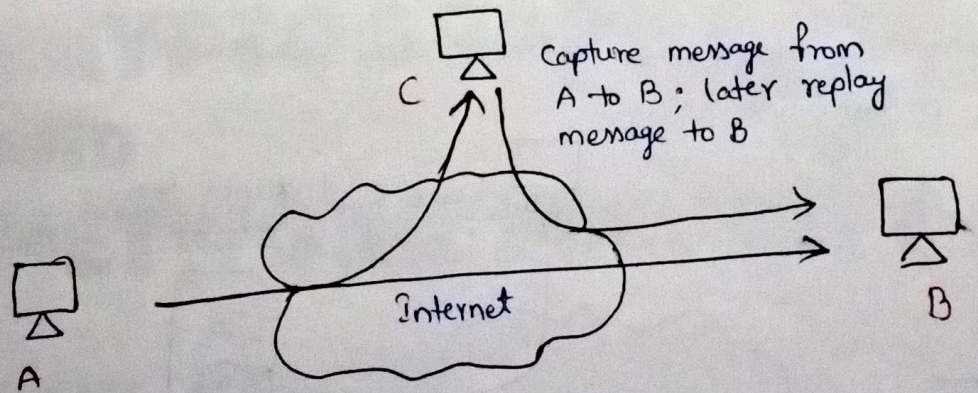

Fig :- Replay

(iii) Modification of messages :- Modification of messages simply means that some portion of a message is altered or that messages are delayed or reordered, to produce an unauthorized effect.

For example :- Suppose User A sends an email message Transfer $1000 to D's account to bank B. User C might capture this and change it to Transfer $10000 to C's account.

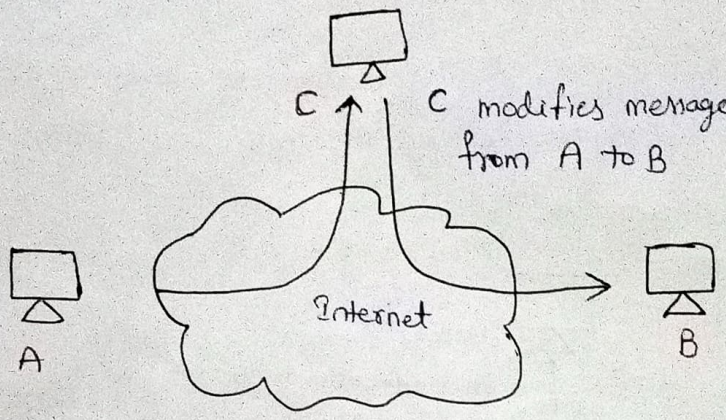

Fig:- Modification of messages

(iv) Denial of Service (DOS) :- Dos attacks make an attempt to prevent legitimate users from accessing some services, which they are eligible for.

→ This attack may have a specific target. For example; an entity may supress all messages directed to a particular destination.

→ Service denial is the disruption of an entire network.

→ Disabling the network or by overloading it with messages so as to degrade performance.

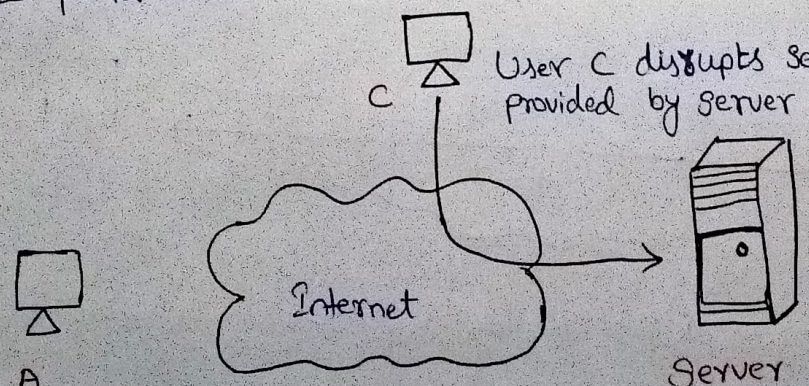

Fig:- Denial of Service

⑥ Security Services

A processing or communication service that enhances the security of the data processing systems and the information transfer of an organiza-tion.

→ The services are intended to counter security attacks, and they make use of one or more security mechanisms to provide the service.

X.800 divided these services into five categories: Authentication, Access control, Data Confidentiality, Data Integrity, and Nonrepudiation.

(i) Authentication :- The authentication service is concerned with assuring that a communication is authentic.

⇒ Two specific authentication services are defined in X.800

- Peer Entity Authentication :- provides for the confirmation of the identity of a peer entity in an association. It attempts to provide confidence that an entity is not performing either a masquerade or an ~~aut~~ unauthorized replay of a previous connection.
- Data origin authentication :- provides for the confirmation of the source of a data unit. It does not provide protection against the duplication (or) modification of data units.

(ii) Access Control :- The prevention of unauthorized use of a resource. This service Controls who can have access to a resource, under what conditions access can occur.

(iii) Data Confidentiality :- The protection of data from unauthorized disclosure. Confidentiality is the protection of transmitted data from passive attacks.

- Connection Confidentiality :- The protection of all user data on a connection
- Connectionless Confidentiality :- The protection of all user data in a single data block.
- Selective - Field Confidentiality :- The Confidentiality of selected fields within the user data on a connection or in a single data block.

- Traffic Flow Confidentiality :- The protection of the information that might be derived from observation of traffic flows.

(iv) Data Integrity :- The assurance that data received are exactly as sent by an authorized entity (i.e., contain no modification, insertion, deletion, or replay).

- 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.
- Connection Integrity without Recovery :- As above, but provides only detection without recovery.
- Selective-field Connection Integrity :- provides for the integrity of selected fields within the user data of a data block transferred over a connection.
- Connectionless Integrity :- provides for the integrity of selected fields within a single connectionless data block.

(v) Nonrepudiation :- Nonrepudiation prevents either sender or receiver from denying a transmitted message.

- Nonrepudiation, Origin :- proof that the message was sent by the specified party.
- Nonrepudiation, Destination :- proof that the message was received by the specified party.

⑦ Security Mechanisms

Security mechanisms : A process that is designed to detect, prevent, or recover from a security attack.

→ Security mechanisms are technical tools and techniques that are used to implement security services.

* Specific Security Mechanisms:- May be incorporated into the appropriate protocol layer in order to provide some of the osi security services.

- Encipherment:- The use of mathematical algorithms to transform data into a form that is not readily intelligible. The transformation and subsequent recovery of the data depend on an algorithm and zero or more encryption keys.
- Digital signature:- Digital signature is like a fingerprint or an attachment to a digital document that ensures its authenticity and integrity. It is a cryptographic output used to verify the authenticity of data.
- Access Control:- A variety of mechanisms that enforce access rights to resources.
- Data Integrity:- This security mechanism is used by appending value to data to which is created by data itself. when this data which is appended is checked and is the same while sending and receiving data integrity is maintained.
- Authentication Exchange:- A mechanism intended to ensure the identity of an entity by means of information exchange.
- Traffic padding:- The insertion of bits into gaps in a data stream to frustrate traffic analysis attempts.
- Routing Control:- Enables selection of particular physically secure routes for certain data & allows routing changes, especially when a breach of security is suspected.
- Notarization:- The use of a trusted third party to assure certain properties of a data exchange.

(8) A model for Network Security

A message is to be transferred from one party to another across some sort of Internet. A logical information channel is established by defining a route through the internet from source to destination

and by the cooperative use of communication protocols (e.g., TCP/IP).

When we use the protocol for this logical information channel the main aspect security has come. who may present a threat to confidentia-lity, authentication, and so on.

→ All the techniques for providing security have two components:

i) A security-related transformation on the information to be sent. Example include the encryption of the message.

ii) Some secret information shared by the two parties and, it is hoped, unknown to the opponent. An example is an encryption key used.

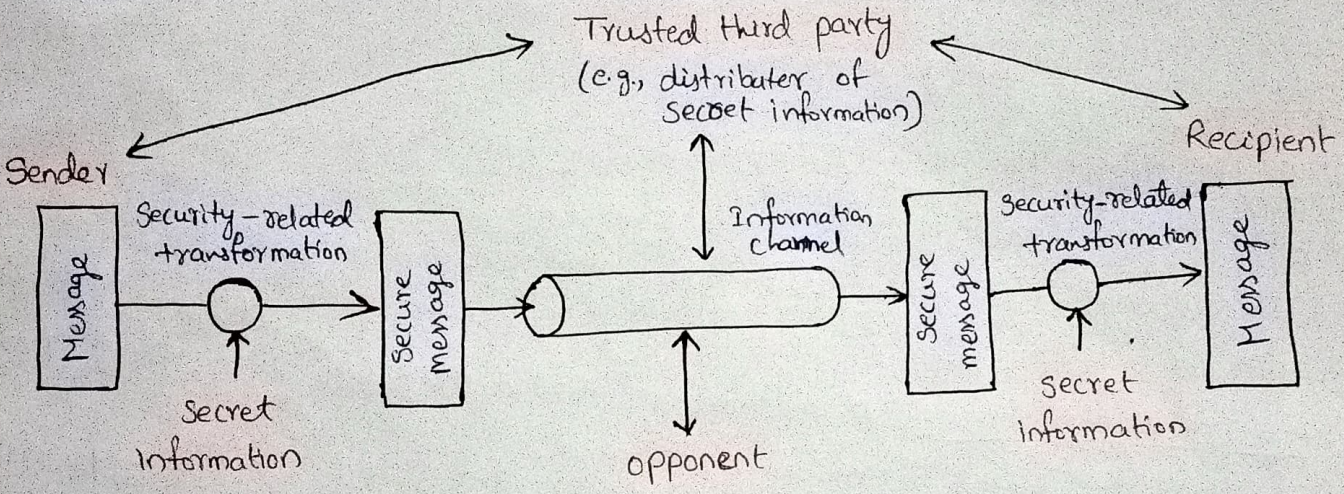

Fig:- Model for Network Security

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 parties.

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 transfor-mation.
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 parties that makes use of the security algorithm and the secret information to achieve a particular security service.

A general model is shown in figure, which reflects a concern for protecting an information system from unwanted access.

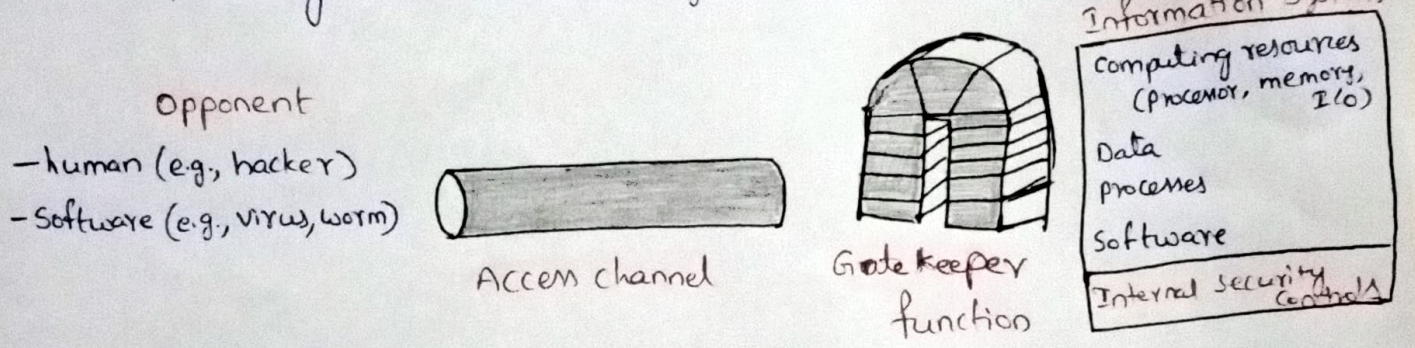

fig:- Network Access Security Model.

The security mechanisms needed to cope with unwanted access fall into two categories:

1. Select appropriate gatekeeper functions to identify users.
2. Implement security controls to ensure only authorized users access designated information or resources.