Unit 1 - Introduction

DR. VASUDHA ARORA

VASUDHA.ARORA@GDGU.ORG, VASUDHARORA6@GMAIL.COM

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

GD GOENKA UNIVERSITY, GURUGRAM

Introduction to Security

The art of war teaches us to rely not on the likelihood of the enemy's not coming, but on our own readiness to receive him; not on the chance of his not attacking, but rather on the fact that we have made our position unassailable.

Security

Security Consists of measures to detect, correct and prevent security violations that involve transmission of information

Why do we need Security???

Increased reliance on Information technology with or without the use of networks

- *The use of IT has changed our lives drastically.*
- *We depend on E-mail, Internet banking, and several other governmental activities that use IT*
- *Increased use of E-Commerce and the World wide web on the Internet as a vast repository of various kinds of information (immigration databases, flight tickets, stock markets etc.)*

Aspects of Security

consider 3 aspects of information security:

- **Security service (Principles of Security)**
- **Security attack**
- **Security mechanism**

Principles of Security(Security Services)

The Principles of Security can be classified as follows:

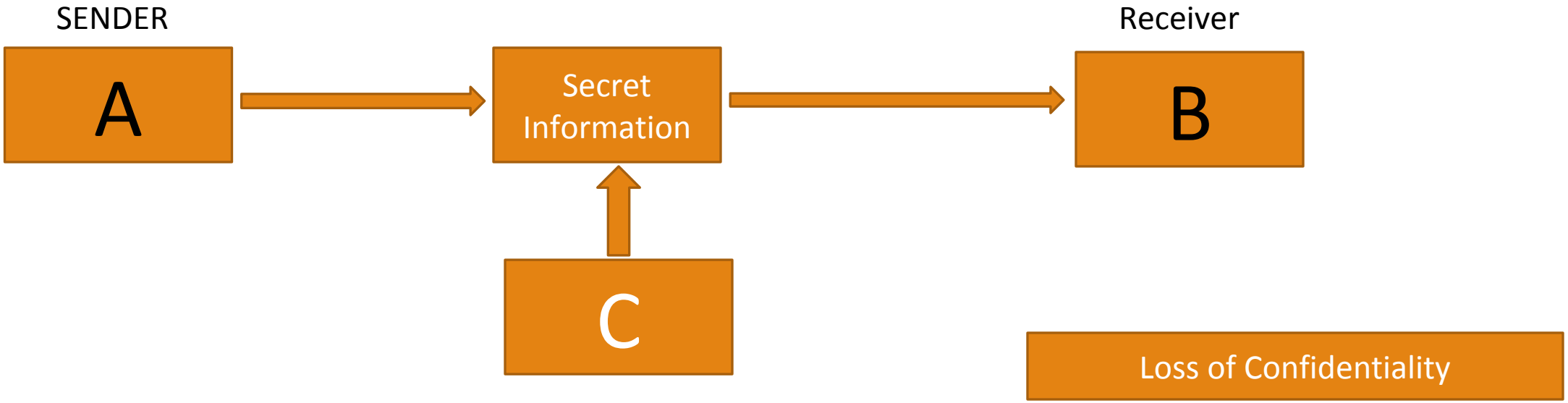
- Confidentiality
- Authentication
- Integrity
- Non Repudiation
- Access Control
- Availability

Confidentiality

The degree of confidentiality determines the secrecy of the information.

The principle specifies that only the sender and receiver will be able to access the information shared between them.

Confidentiality compromises if an unauthorized person is able to access a message.



Confidentiality

For example, let us consider sender A wants to share some confidential information with receiver B and the information gets intercepted by the attacker C. Now the confidential information is in the hands of an intruder C.

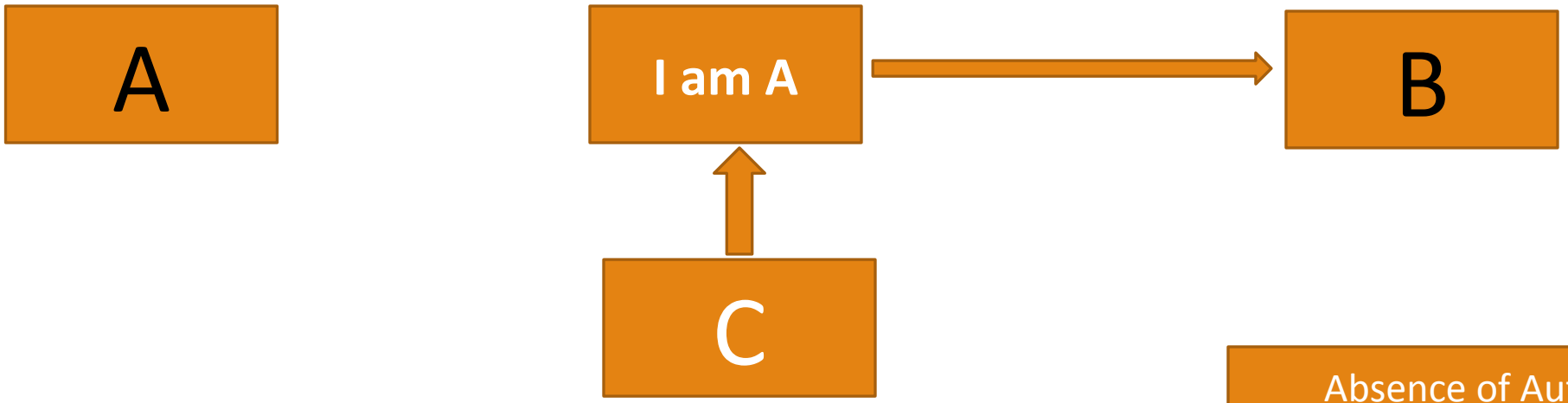
Loss of Confidentiality leads to **INTERCEPTION ATTACK**

Authentication

Authentication mechanism helps to establish **“Proof of identities**”.

Authentication is the mechanism to identify the user or system or the entity.

It ensures the identity of the person trying to access the information.



Authentication

The authentication is mostly secured by using **username and password**.

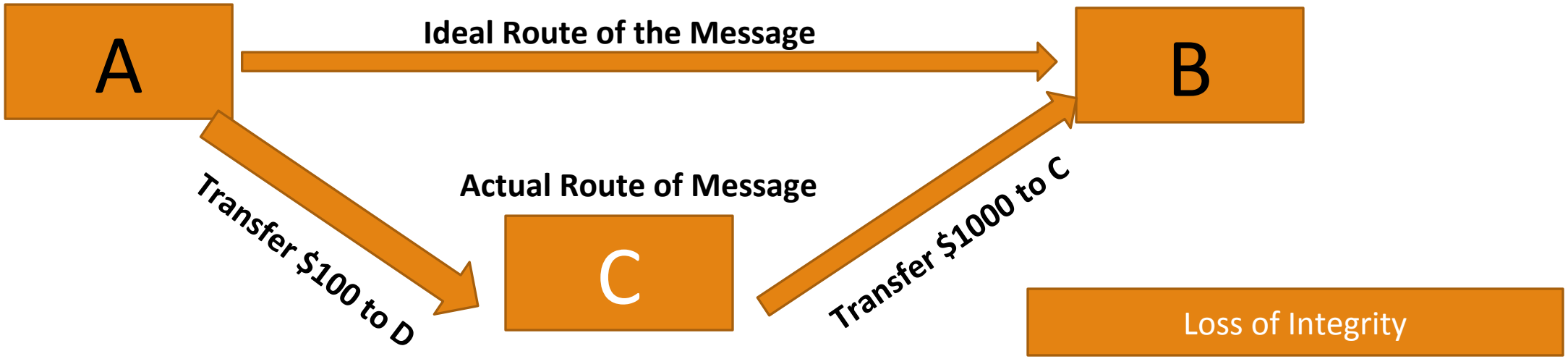
The authorized person whose identity is preregistered can prove his/her identity and can access the sensible information.

Absence of Authentication leads to **Fabrication Attack**

Integrity

Integrity gives the assurance that the information received is exact and accurate.

If the content of the message is changed after the sender sends it but before reaching the intended receiver, then it is said that the **integrity** of the message is lost.



Integrity

Data Sent Should be exactly same as data received.

There should be no modifications in data.

Here bot User A and User B are unaware of about this change.

This type of attack due to loss in Integrity of Data is known as **Modification Attack**.

Non-Repudiation

Non-repudiation is a mechanism that prevents the denial of the message content sent through a network.

In some cases the sender sends the message and later denies it.

But the non-repudiation does not allow the sender to refuse the receiver.

The principle of Non Repudiation defeats such possibilities of denying something having done it.

Access Control

The principle of access control is determines '**Who**' can access '**What**' by role management and rule management.

Role management determines who should access the data while **rule management** determines up to what extent one can access the data.

The information displayed is dependent on the person who is accessing it.

Based on the information gathered from Role management and Rule management an access control matrix is prepared which lists the users against the list of resources they can access.

Availability

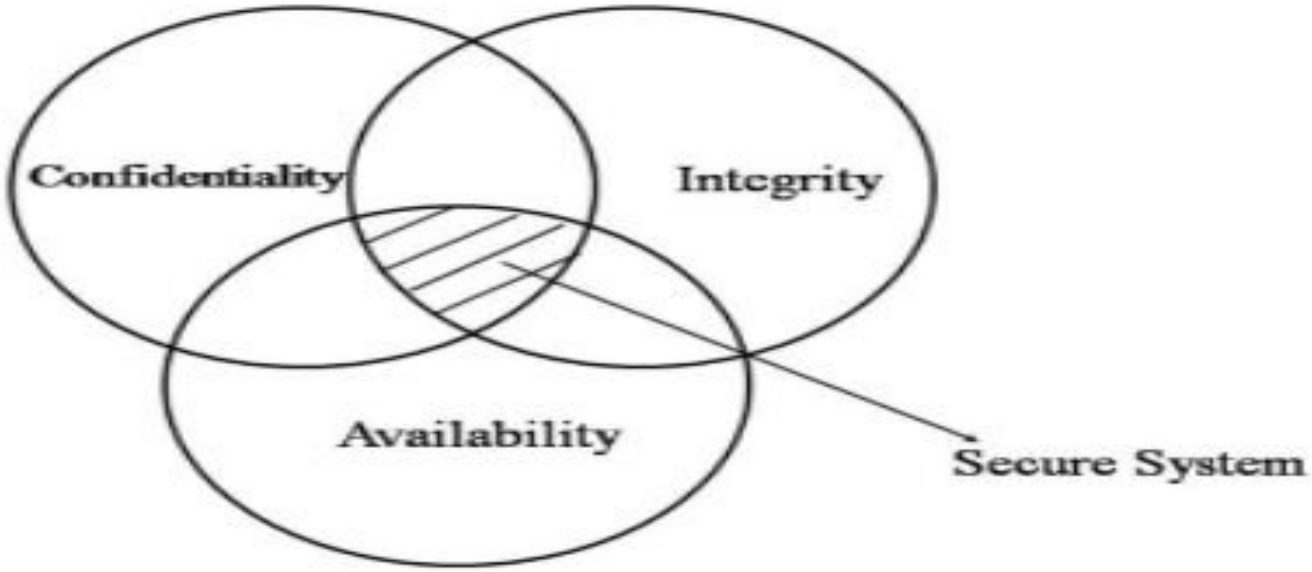
The principle of availability states that the resources will be available to authorize party at all times.

Information will not be useful if it is not available to be accessed.

Systems should have sufficient availability of information to satisfy the user request.

Attack on Availability is called **Interruption Attack**

CIA Triad



Security Attacks

Any action that compromises the security of information owned by an organization

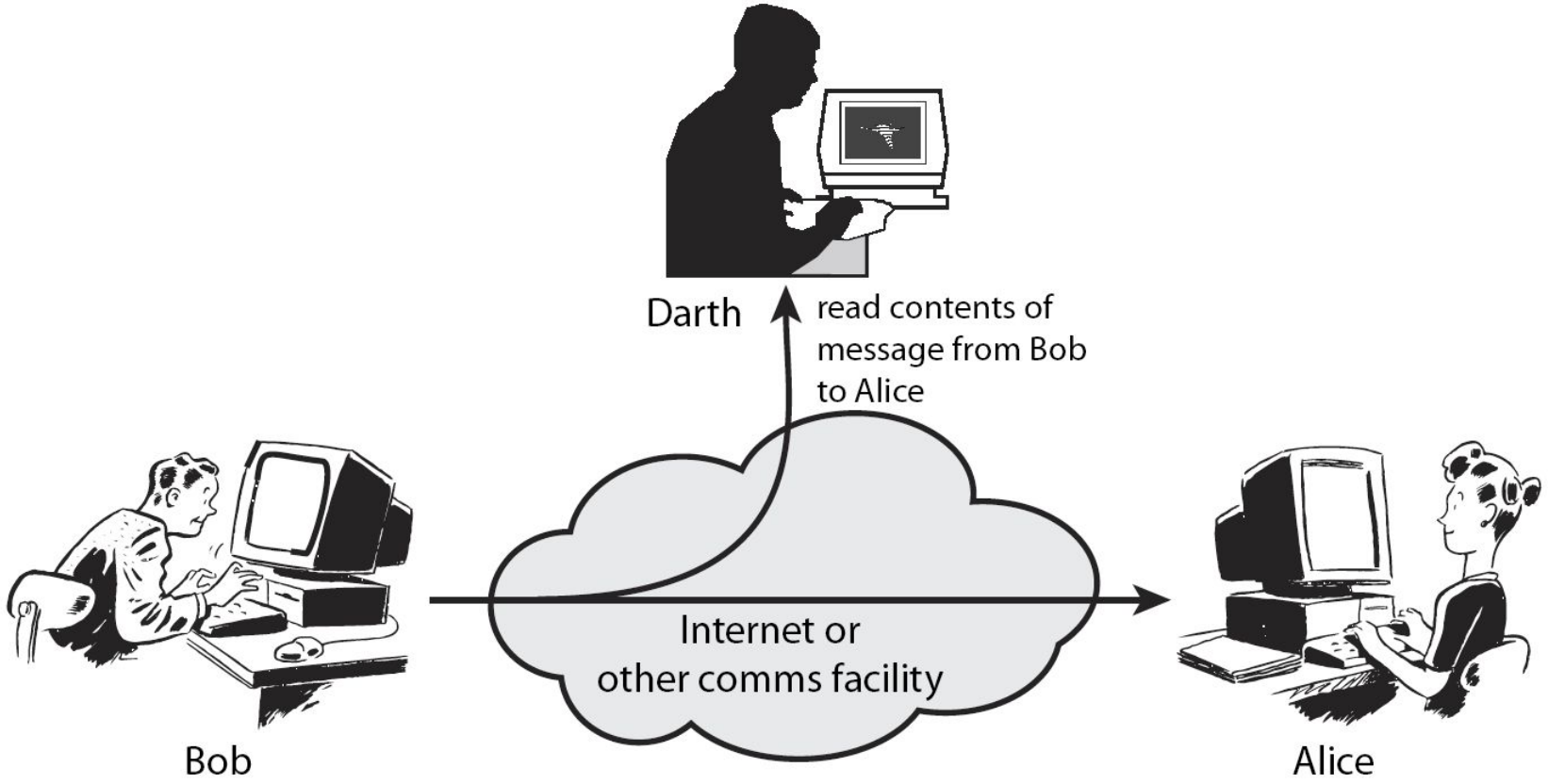
Information security is about how to prevent attacks, or failing that, to detect attacks on information-based systems

Have a wide range of attacks

Generic types of attacks

- passive
- active

Passive Attacks



Passive Attacks

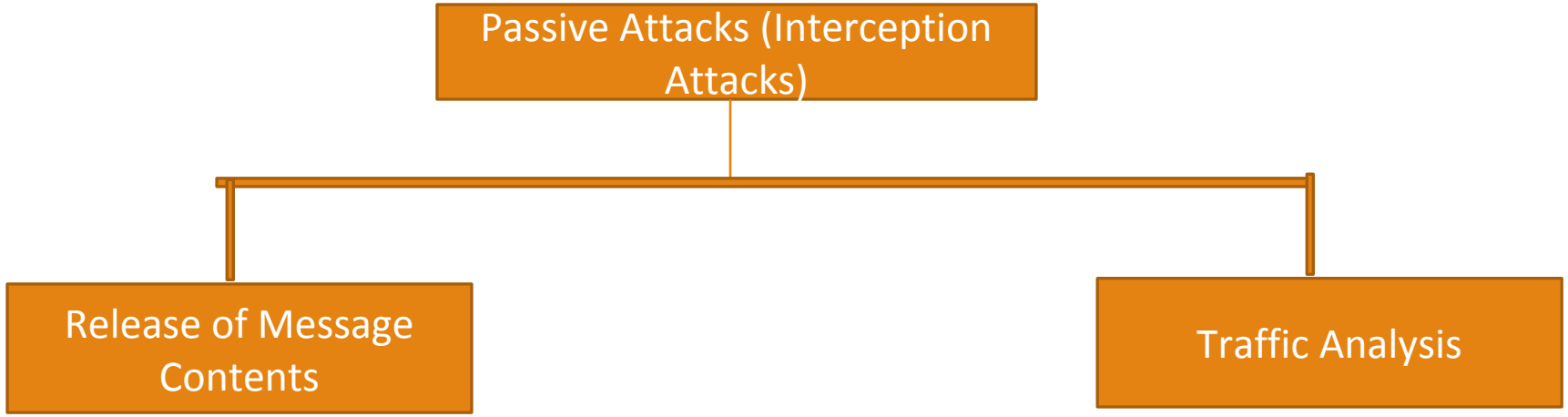
Passive attacks are those wherein the attacker indulges in evesdropping or monitoring the data transmission i.e

The attacker aims to obtain information in transit.

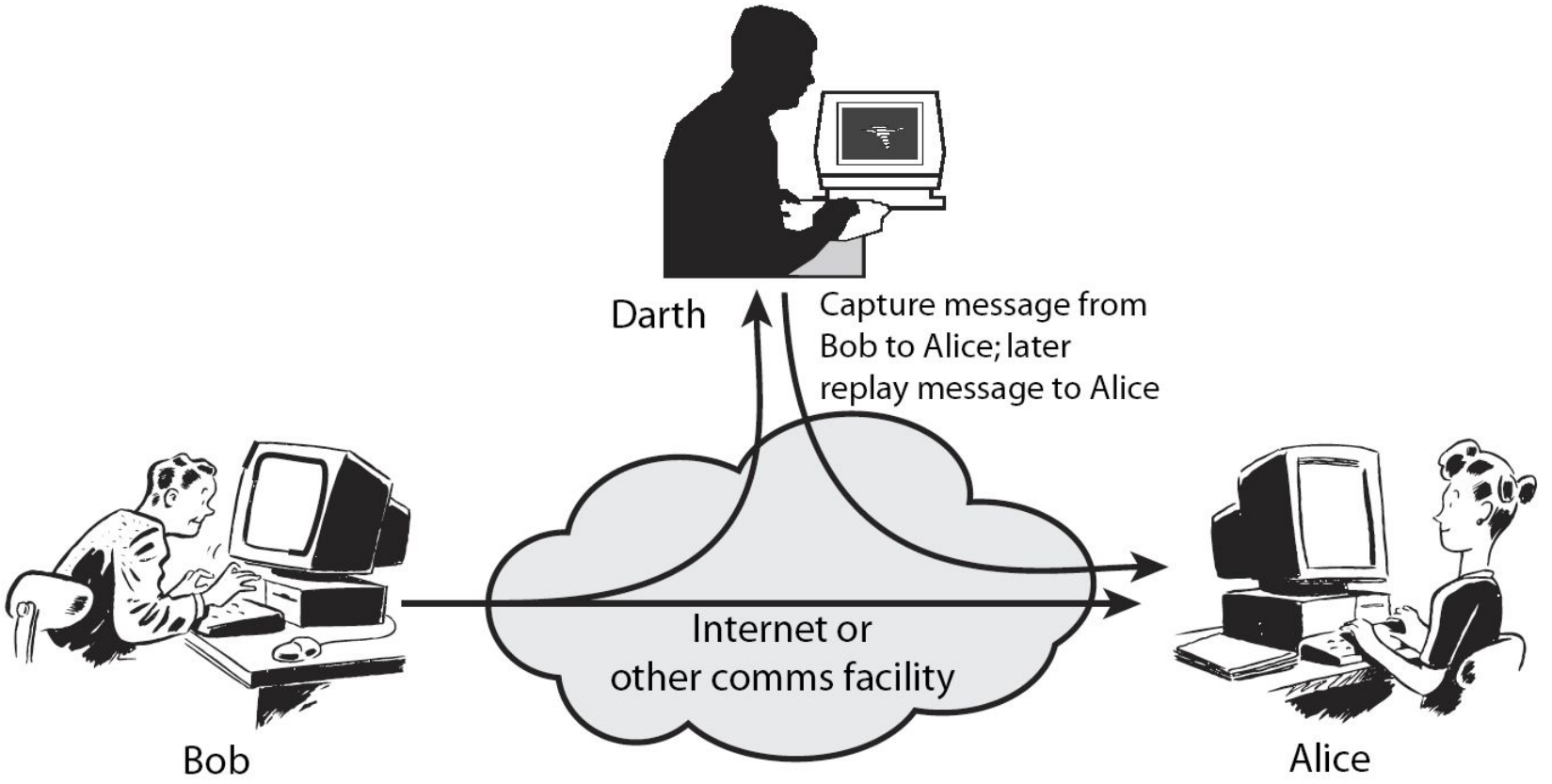
The term Passive indicates that the attacker does not attempt to perform any modifications in data, Therefor Passive attacks are harder to detect

Thus general approach to deal with Passive attacks is prevention rather than detection or corrective actions.

Passive Attacks



Active Attacks



Active Attacks

Based on :

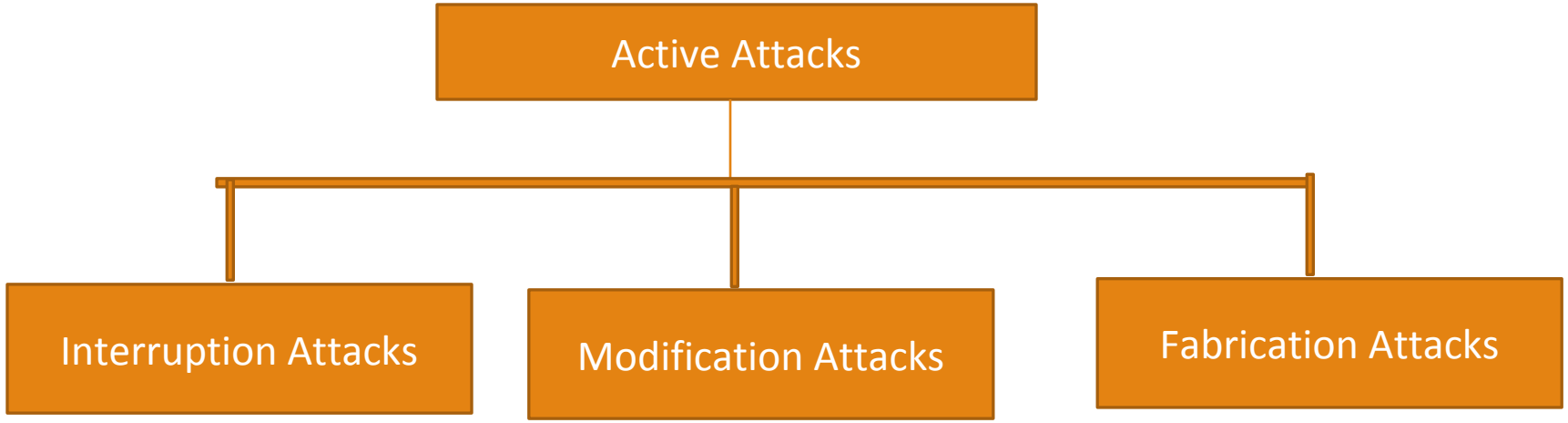
- Modification of the original Message in some manner, or
- Creation of a false message

These attacks can not be prevented

They can be prevented with some effort

Attempts can be made to recover from them

Active Attacks



Masquerade Attack

Replay Attack
Alteration of Messages

DoS Attack

Security Threats

Virus

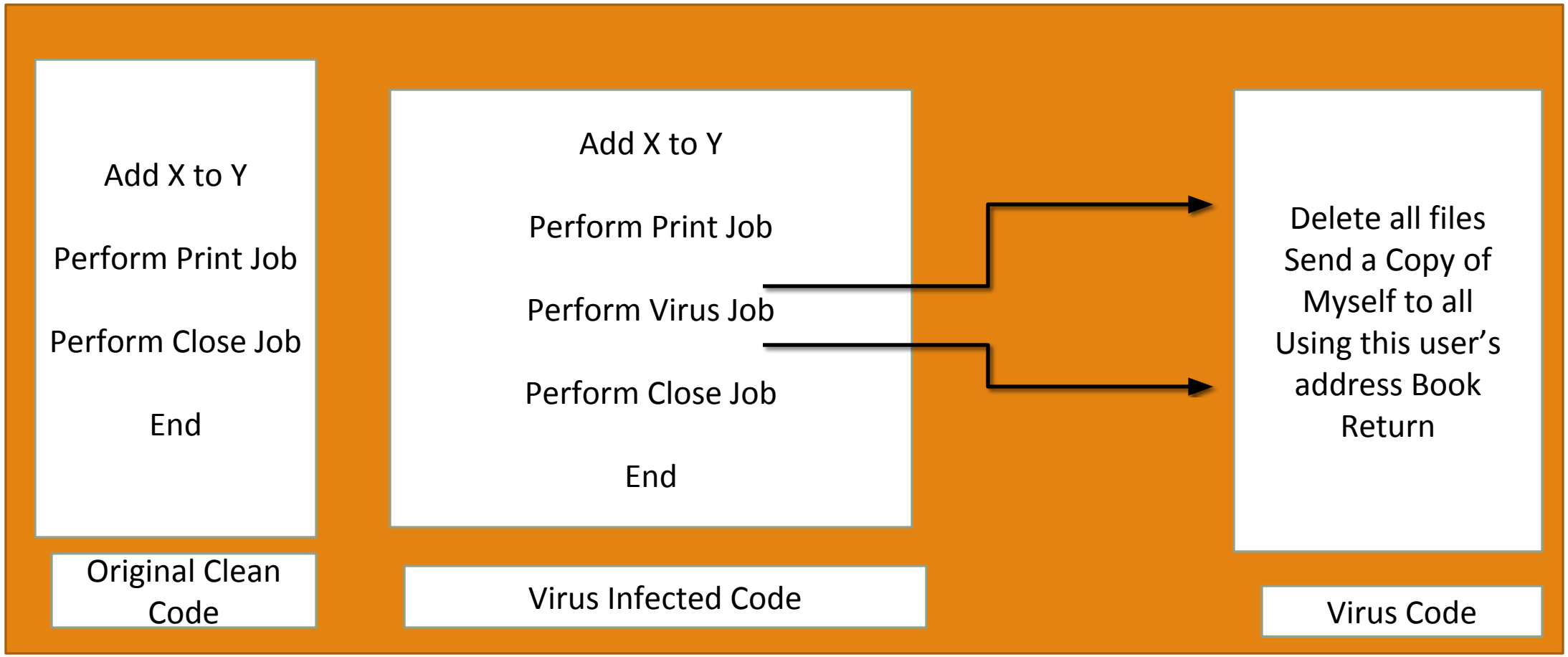
A Virus is a piece of Program Code that attaches itself to legitimate program code and runs when the legitimate code runs.

A computer virus is a small program written to alter the way a computer operates, without the permission or knowledge of the user.

A virus must meet two criteria:

- It must execute itself. It will often place its own code in the path of execution of another program.
- It must replicate itself. For example, it may replace other executable files with a copy of the virus infected file. Viruses can infect desktop computers and network servers alike.

Virus


Add X to Y
Perform Print Job
Perform Close Job
End
Original Clean Code
Add X to Y
Perform Print Job
Perform Virus Job
Perform Close Job
End
Virus Infected Code
Delete all files
Send a Copy of Myself to all Using this user's address Book
Return
Virus Code

Virus

Viruses can also be triggered by specific Events(e.g. 12:00 PM daily)

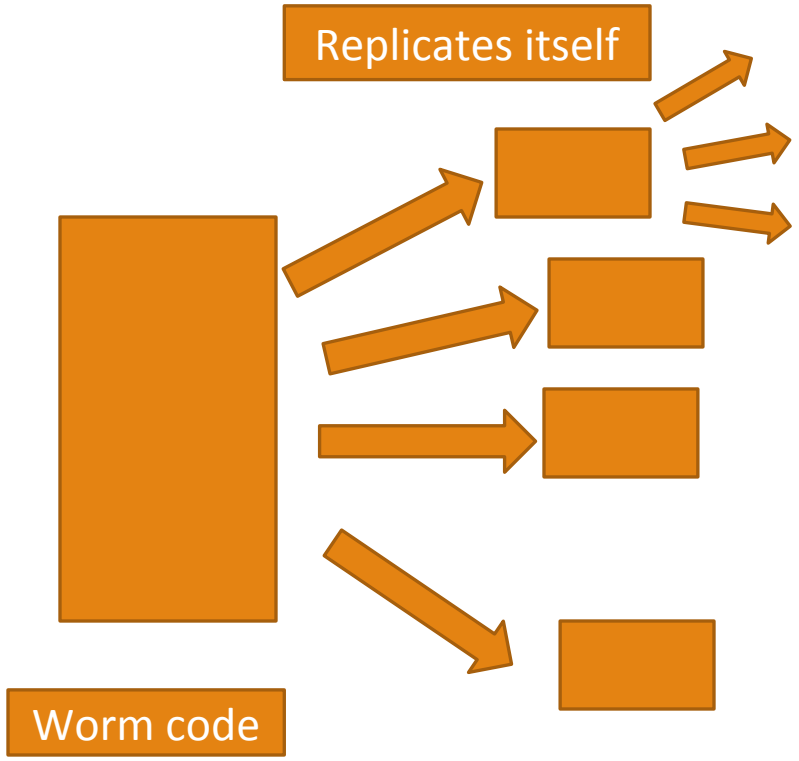
Some viruses are programmed to damage the computer by damaging programs, deleting files, or reformatting the hard disk.

Others are not designed to do any damage, but simply to replicate themselves and make their presence known by presenting text, video, and audio messages.

Usually Viruses cause damage to the computer systems to the extent that it can be repaired.

Worms

Similar in concept to a Virus, a worm is different in implementation.



WORM

Worm

Worms are programs that replicate themselves from system to system without the use of a host file.

This is in contrast to viruses, which requires the spreading of an infected host file.

Although worms generally exist inside of other files, often Word or Excel documents, there is a difference between how worms and viruses use the host file. Usually the worm will release a document that already has the "worm" macro inside the document. The entire document will travel from computer to computer, so the entire document should be considered the worm.

PrettyPark.Worm is a particularly prevalent example.

Trojan Horse

The term comes from the a Greek story of the Trojan War, in which the Greeks give a giant wooden horse to their foes, the Trojans, ostensibly as a peace offering. But after the Trojans drag the horse inside their city walls, Greek soldiers sneak out of the horse's hollow belly and open the city gates, allowing their compatriots to pour in and capture Troy.

A destructive program that masquerades as a benign application.

Unlike viruses, Trojan horses do not replicate themselves but they can be just as destructive.

Trojan Horses attempt to reveal confidential information to an attacker.

Trojan Horse

User id: XXXX
Pswd: YYYYYY

Login Code

Trojan Code
Login COde

Attacker

User id: XXXX
Pswd: YYYYYY

Introduction to Computer Networks and OSI Security Architecture

DR. VASUDHA ARORA

VASUDHA.ARORA@GDGU.ORG, VASUDHARORA6@GMAIL.COM

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

GD GOENKA UNIVERSITY, GURUGRAM

What is Computer Network

A Computer network consists of two or more autonomous computers that are linked(connected) together in order to:

- Share resources (files, printers, modems, fax machines).
- Share Application software like MS Office.
- Allow Electronic communication.
- Increase productivity (makes it easier to share data amongst users).

IP Address (Internet Protocol address)

Also known as the Logical Address, the IP Address is the network address of the system across the network.

To identify each device in the world-wide-web, the Internet Assigned Numbers Authority (IANA) assigns an IPV4 (Version 4) address as a unique identifier to each device on the Internet.

The length of an IP address is 32-bits, hence, we have 2^{32} IP addresses available.

Type "ipconfig" in the command prompt and press 'Enter', this gives us the IP address of the device.

MAC Address (Media Access Control address)

Also known as physical address,

The MAC Address is the unique identifier of each host and is associated with its NIC (Network Interface Card).

A MAC address is assigned to the NIC at the time of manufacturing.

The length of the MAC address is : 12-nibble/ 6 bytes/ 48 bits

Type “ipconfig/all” in the command prompt and press ‘Enter’, this gives us the MAC address.

Port

A port can be referred to as a logical channel through which data can be sent/received to an application.

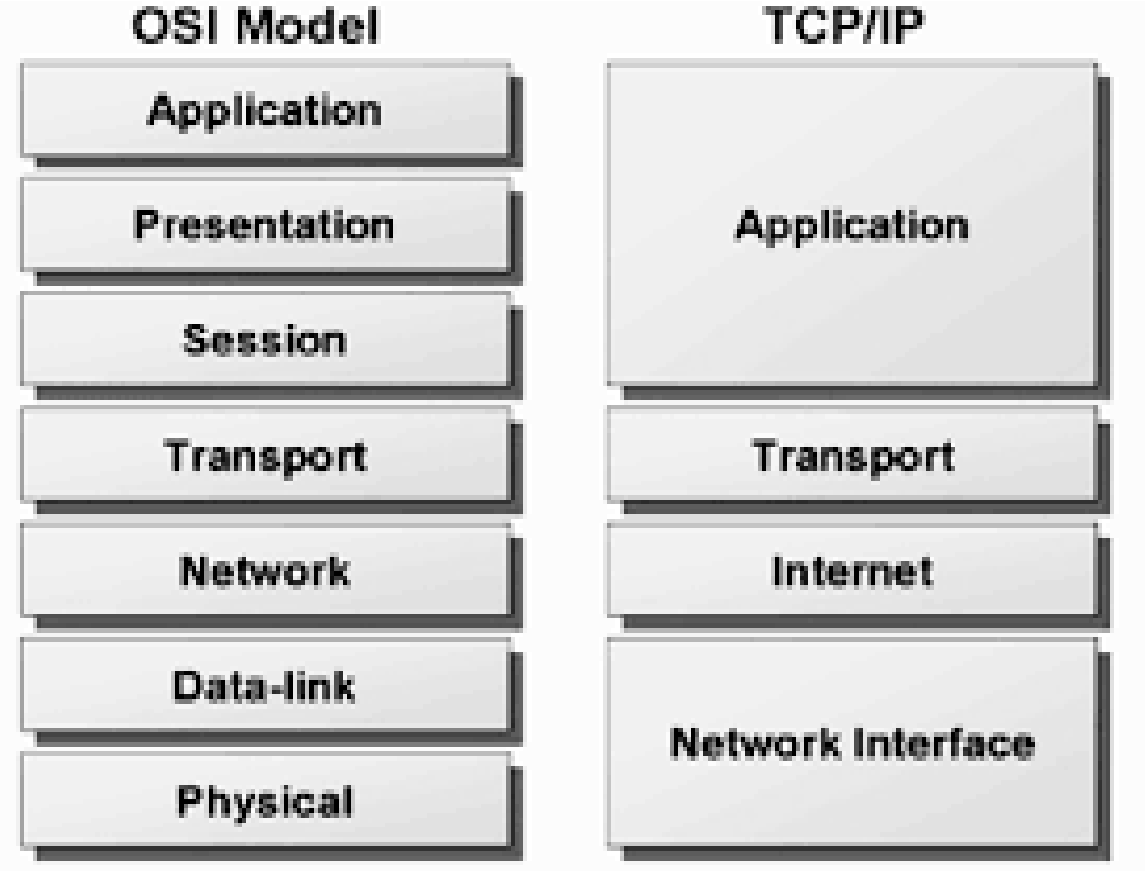
Any host may have multiple applications running, and each of these applications is identified using the port number on which they are running.

A port number is a 16-bit integer, hence, we have 2^{16} ports available.

Number of ports: 65,536

Well known Ports	0 – 1023
Registered Ports	1024 – 49151
Ephemeral Ports	49152 – 65535

OSI Vs TCP/IP


OSI Model
Application
Presentation
Session
Transport
Network
Data-link
Physical
TCP/IP
Application
Transport
Internet
Network Interface

OSI Model

The Open Systems Interconnection or **OSI Model** is a security framework which sets out recommendations for application security in terms of seven layers (three media, and four host layers), all of which must be secured for an application to be considered safe. Those layers are:

the physical layer

the data link layer

the network layer

the transport layer

the session layer

the presentation layer

the application layer

Implementing Security within the OSI Model

The Physical Layer

This is the media layer which gives technical specifications for physical and electrical data connections. It's also the medium through which physical communication occurs between various end points.

Security in the physical layer is easily threatened by accidental or malicious intent (e.g. unplugging of power or network cables) or environmental factors like power surges.

Denial of Service (DoS) for crucial applications and networks can result.

Biometric authentication, electromagnetic shielding, and advanced locking mechanisms are typically used to secure it.

Implementing Security within the OSI Model

The Data Link Layer

This media layer involves all the data packets which are moved by the physical layer.

Efforts to bypass virtual Local Area Network or VLAN security protocols and the spoofing of network interface identifying MAC addresses are typical vulnerabilities of this layer,

Successful exploits can go on to compromise the security of the network layer.

Filtering MAC addresses and ensuring that all wireless applications have authentication and encryption built in are common security strategies for this layer.

Implementing Security within the OSI Model

The Network Layer

This final media layer governs the routing, control, and addressing of data and traffic on the network.

A major threat to application security in this layer is IP address or packet spoofing, where data packets originating from malicious sources are disguised so that they appear to come from legitimate addresses within the network.

Route and anti-spoofing filters in conjunction with strongly configured firewalls can best provide security in this layer.

Implementing Security within the OSI Model

The Transport Layer

This host layer is a logical zone in which the transfer of data sequences of various lengths occurs.

Smooth data flows with error control and measures ensuring segmentation and desegmentation are the mark of a strong transport layer protocol such as TCP or Transmission Control Protocol.

Security here is dependent on limiting access to the transmission protocols and their underlying information, together with strong firewall protection.

Implementing Security within the OSI Model

The Session Layer

The second of the host layers governs the interaction between local and remote applications.

It creates, manages, and terminates connections between machines on demand (i.e., per session).

The session layer is susceptible to brute force attacks and may be breached if authentication protocols are weak.

To ensure security, authentication should take place through the exchange of encrypted passwords (which must be safely stored),

and timers should be put in place to limit the number of attempts that may be made to establish a session.

Implementing Security within the OSI Model

The Presentation Layer

This logical or host layer uses a number of conversion methods to standardize data to and from various local formats, as information is transferred from the application layer to the network.

Input from users (which should have been cleaned up before it passes on to functions) should be segregated from program control functions, to avoid malicious inputs that might lead to system crashes or exploits.

Implementing Security within the OSI Model

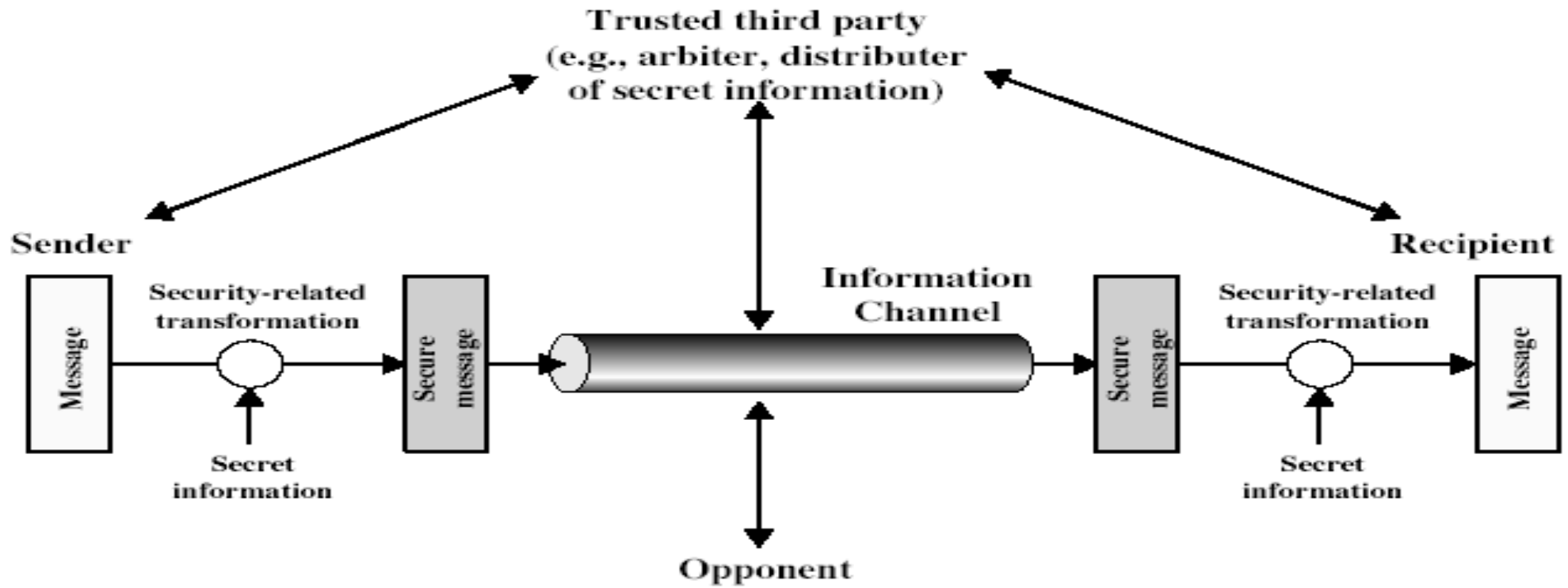
The Application Layer

The final host layer is the one closest to the end user – and the one which presents potential intruders with the biggest attack surface.

The application layer includes the user interface and various other critical functions, and if successfully exploited entire networks may be shut down in a Denial of Service attack, user data may be stolen, and individual applications may fall under an intruder's control.

Secure application development practices are the safest way to guarantee that applications are able to sanitize user input, detect malicious activity, and securely handle and transfer sensitive information.

Model for Network Security



Model for Network Security

using this model requires us to:

1. design a suitable algorithm for the security transformation
2. generate the secret information (keys) used by the algorithm
3. develop methods to distribute and share the secret information
4. specify a protocol enabling the principals to use the transformation and secret information for a security service