School of Computing Science and Engineering

Course Code : BCA3010 Course Name: Network Security

# UNIT I

# Introduction: Basic Terminology

Name of the Faculty: Dr. S.Vijayalakshmi Program Name: BCA3010

# Introduction of Network Security

While computer systems today have some of the best security systems ever, they are more vulnerable than ever before. This vulnerability stems from the world-wide access to computer systems via the Internet. Computer and network security comes in many forms, including encryption algorithms, access to facilities, digital signatures, and using fingerprints and face scans as passwords. network security engineers, analysts, and administrators are held responsible for the safety of the IT network

# Definition of network security

A set of rules and configurations designed to protect the integrity, confidentiality and accessibility of computer networks and data using both software and hardware technologies

# Network security

**Example of Network Security**

✓password protection:-in which the user of the network oneself choose.

**Network security protect different vulnerabilities of the system like :-**

✓User

✓Location

✓Data

✓Devices

✓applications

# Network Security

The main task of network security is protecting huge stored data and network in layers that ensures a bedding of rules and regulations that have to be acknowledged before performing any activity on the data.

The main three level are :-

✓Physical

✓Technical

✓Administrative

# Physical Network Security

This level protect the data and network though unauthorized personnel from acquiring the control over the confidentiality of the network

# Technical Network Security

This level protect the data stored in the network or data involved in transitions through the network. The two main purpose of this level are:-

❑ protection from the unauthorized users

❑ protection from malicious activities

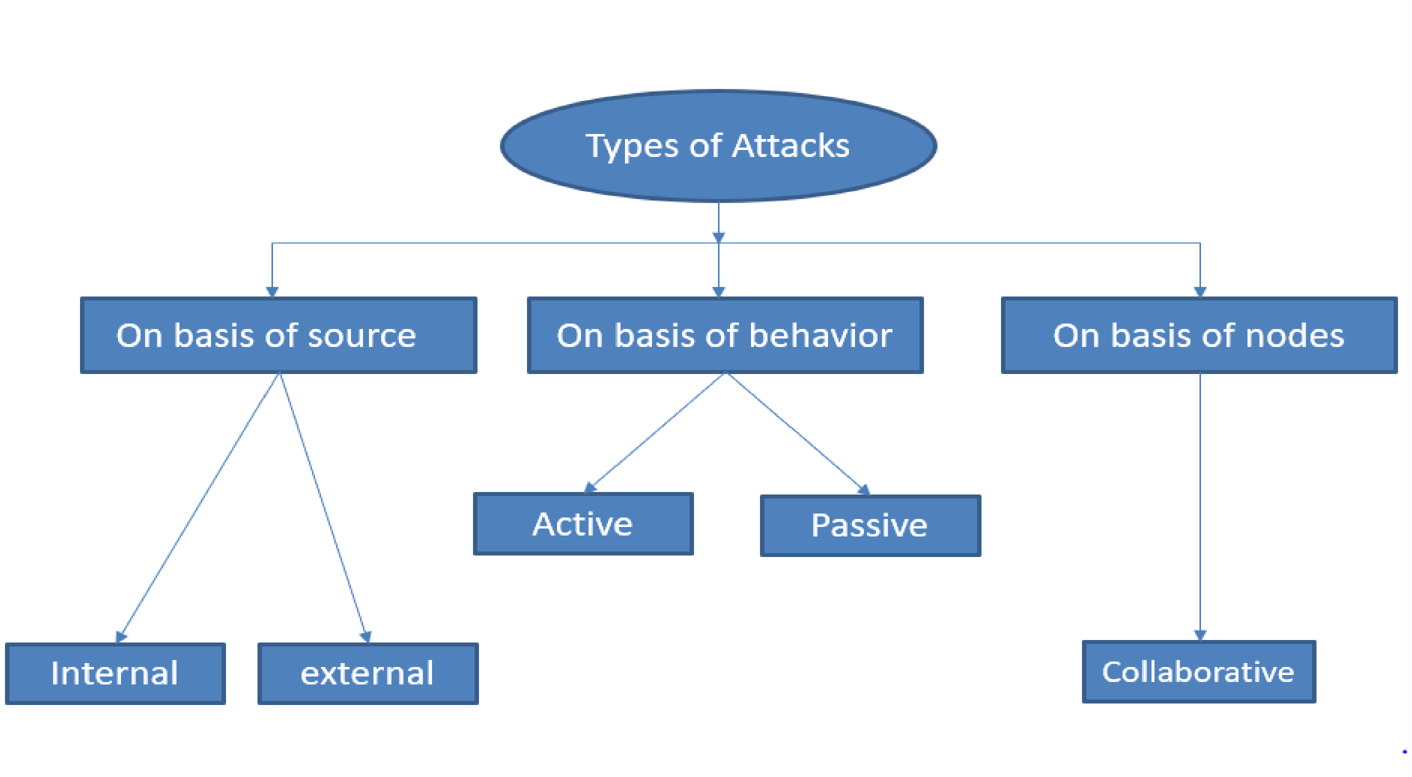
# Administrative Network Security

- ❑ This level protects user behavior like how the permission has been granted and how the authorization process takes place
- ❑ It also ensures the level of sophistication the network might need for protecting it through all the attacks
- ❑ Suggest necessary amendments that have to be done over the infrastructure

# Network Attack

A network attack is an attempt to gain unauthorized access to an organization’s network, with the objective of stealing data or perform other malicious activity.

# Network Security Services



Network Attacks

# On basis of source

**External Attacks**

External attacks are caused by the nodes which are not a part of the network. External attackers are the aims to cause congestion, propagate fake routing information or disturb nodes from providing services.

**Internal Attacks**

Internal attacks are caused by the nodes which are a part of the network. Internal attacks, in which the adversary wants to gain the normal access to the network and participate the network activities, either by some malicious impersonation to get the access to the network as a new node or by directly compromising a current node and using it as a basis to conduct its malicious behaviors.

# On basis of Behaviors

**Active Attacks**

Active attack tries to change the system resources or affect their operation. Always causes damage to the system.

Some active attacks are

✓**Spoofing attack**:-When a malicious node miss-present his identity, so that the sender change the topology

# On basis of Behaviors

✓**Wormhole attack**:- This attack is also called the tunnelling attack. In this attack an attacker receives a packet at one point and tunnels it to another malicious node in the network.

✓**Modification**:-When malicious node performs some modification in the routing route, so that sender sends the message through the long route. This attack cause communication delay occurred between sender and receiver.

# On basis of Behaviors

✓**Denial of services**:- In denial of services attack, malicious node sending the message to the node and consume the bandwidth of the network. The main aim of the malicious node is to be busy the network node. If a message from unauthenticated node will come, then receiver will not receive that message because he is busy and beginner has to wait for the receiver response.

# On basis of Behaviors

✓***Sinkhole***

Sinkhole is a service attack that prevents the base station from obtaining complete and correct information. In this attack, a node tries to attract the data to it from his all neighbouring node. Selective modification, forwarding or dropping of data can be done by using this attack.

# On basis of Behaviors

- ✓***Sybil***

This attack related to the multiple copies of malicious nodes. The Sybil attack can be happen due to malicious node shares its secret key with other malicious nodes. In this way the number of malicious node is increased in the network and the probability of the attack is also increases. If we used the multipath routing, then the possibility of selecting a path malicious node will be increased in the network

# On basis of Behaviors

## Passive Attacks

Attackers gain access to a network and can monitor or steal sensitive information, but without making any change to the data, leaving it intact.

# Some passive attacks

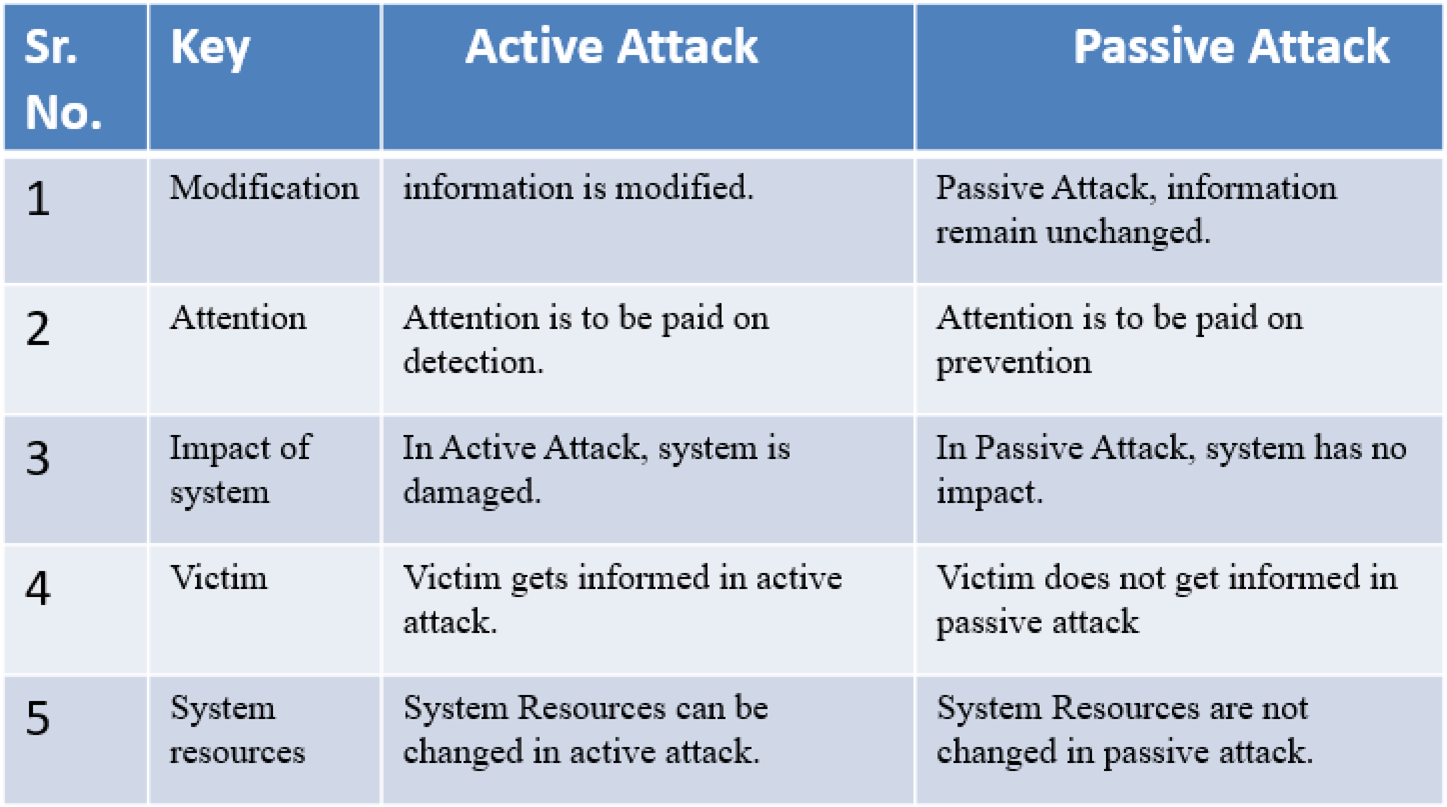
✓***Traffic analysis***:- In the traffic analysis attack, an attacker tries to sense the communication path between the sender and receiver. An attacker can found the amount of data which is travel from the route of sender and receiver. There is no modification in data by the traffic analysis.

✓ ***Eavesdropping***:- This is a passive attack, which occurred in the mobile ad-hoc network. The main aim of this attack is to find out some secret or confidential information from communication. This secrete information may be privet or public key of sender or receiver or any secrete data.

# Some passive attacks

✓***Monitoring***:- In this attack in which attacker can read the confidential data, but he cannot edit the data or cannot modify the data.

# Difference between Active and Passive Attacks



| Sr. No. | Key | Active Attack | Passive Attack |
|---|---|---|---|
| 1 | Modification | information is modified. | Passive Attack, information remain unchanged. |
| 2 | Attention | Attention is to be paid on detection. | Attention is to be paid on prevention |
| 3 | Impact of system | In Active Attack, system is damaged. | In Passive Attack, system has no impact. |
| 4 | Victim | Victim gets informed in active attack. | Victim does not get informed in passive attack |
| 5 | System resources | System Resources can be changed in active attack. | System Resources are not changed in passive attack. |

# On basis of Nodes

**Collaborative attacks :-**

Collaborative attacks (CA) occur when more than one attacker or running process synchronize their actions to disturb a target network. Multiple attacks occur when a system is disturbed by more than one attacker, but not necessarily in collaboration.

Types of Collaborative attacks

- ✓**Direct Collaborative Attacks**
- ✓**Indirect Collaborative Attacks.**

# Some Other Types of Attacks

***Black hole attack*** :- Black hole attack is one of the advance attacking which attacker uses the routing protocol to advertise itself as having the best path to the node whose packets it want to intercept. An hacker use the flooding based protocol for listing the request for a route from the initiator, then hacker create a reply message he has the shortest path to the receiver . As this message from the hacker reached to the initiator before the reply from the actual node, then initiator wills consider that, it is the shortest path to the receiver. So that a malicious fake route is create.

# Some Other Types of Attacks

✓***Rushing attack***:- In rushing attack, when sender send packet to the receiver, then attacker alter the packet and forward to receiver. Attacker performs duplicate sends the duplicate to the receiver again and again. Receiver assumes that packets come from sender so the receiver becomes busy continuously.

# Some Other Types of Attacks

***Replay attack***:- It this attack a malicious node may repeat the data or delayed the data. This can be done by originator who intercept the data and retransmit it. At that time, an attacker an intercept the password.

***Byzantine attack***:- A set of intermediate node works between the sender and receiver and perform some changes such as creating routing loops, sending packet through non optimal path or selectively dropping packet, which result in disruption or degradation of routing services.

***Location disclosure attack***:- Malicious node collects the information about the node and about the route by computing and monitoring the traffic. So malicious node may perform more attack on the network.

# Some Other Types of Attacks

***Unauthorized access***

Unauthorized access refers to attackers accessing a network without receiving permission. Among the causes of unauthorized access attacks are weak passwords, lacking protection against social engineering, previously compromised accounts, and insider threats.

***Distributed Denial of Service (DDoS) attacks***

Attackers build botnets, large fleets of compromised devices, and use them to direct false traffic at your network or servers. DDoS can occur at the network level, for example by sending huge volumes of SYN/ACC packets which can overwhelm a server, or at the application level, for example by performing complex SQL queries that bring a database to its knees.

# Some Other Types of Attacks

***Man in the middle attacks***

A man in the middle attack involves attackers intercepting traffic, either between your network and external sites or within your network. If communication protocols are not secured or attackers find a way to circumvent that security, they can steal data that is being transmitted, obtain user credentials and hijack their sessions.

***Code and SQL injection attacks***

Many websites accept user inputs and fail to validate and sanitize those inputs. Attackers can then fill out a form or make an API call, passing malicious code instead of the expected data values. The code is executed on the server and allows attackers to compromise it.

# Some Other Types of Attacks

***Privilege escalation***

Once attackers penetrate your network, they can use privilege escalation to expand their reach. Horizontal privilege escalation involves attackers gaining access to additional, adjacent systems, and vertical escalation means attackers gain a higher level of privileges for the same systems.

# Some Other Types of Attacks

***Insider threats***

A network is especially vulnerable to malicious insiders, who already have privileged access to organizational systems. Insider threats can be difficult to detect and protect against, because insiders do not need to penetrate the network in order to do harm. New technologies like User and Even Behavioral Analytics (UEBA) can help identify suspicious or anomalous behavior by internal users, which can help identify insider attacks.

# Thank You