CSE 4215 (Network Security)

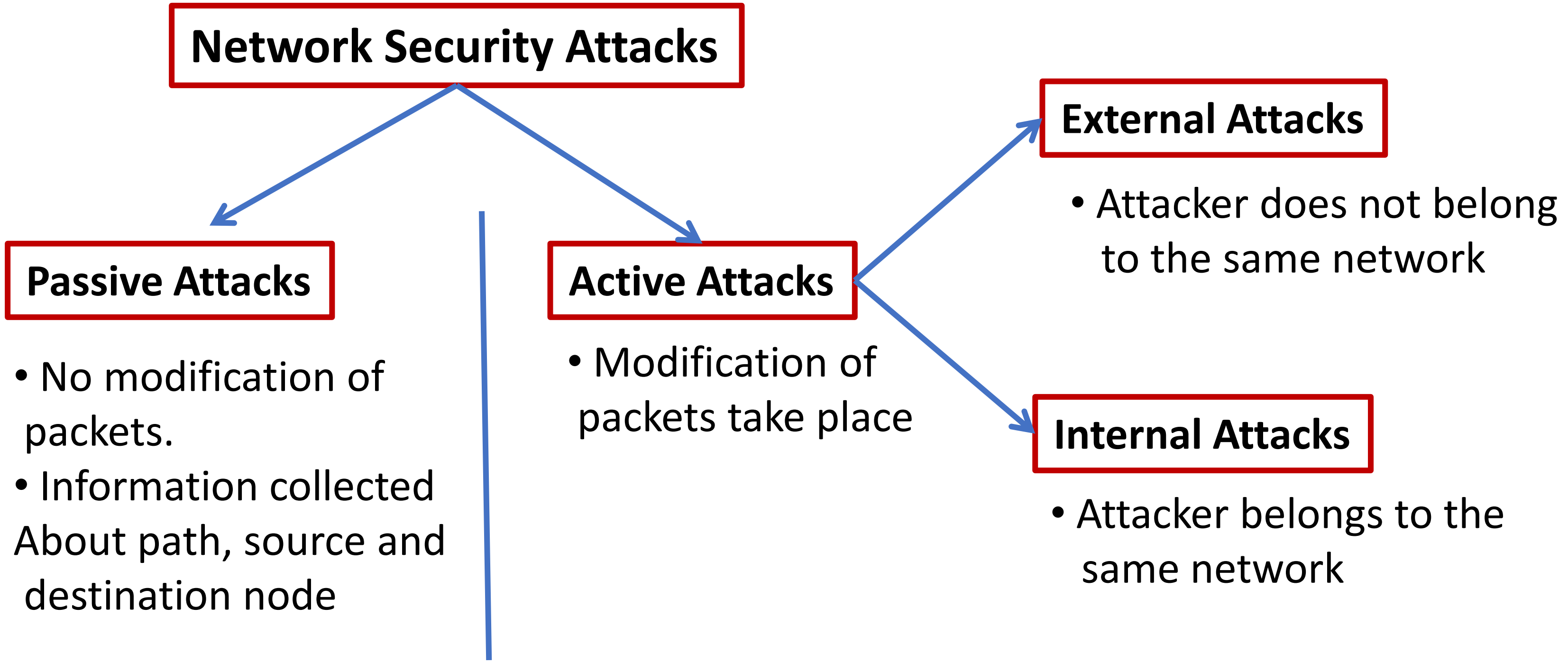
Chapter 2: Security Attacks

Md. Shahid Uz Zaman, PhD
Professor,
Department of CSE
Rajshahi University of Engineering & Technology
Email: szaman22.ruet@gmail.com

Different Attacks

- □ Denial of Service (Dos) Attack,
- □ Distributed Denial of Service (Ddos) Attack,
- □ Eavesdropping,
- □ IP Spoofing, Sybil Attack,
- □ Blackhole Attack,
- □ Grayhole Attack,
- □ Man-In-The-Middle Attack,
- □ Passwords-based Offline Attacks.

Types of Network Security Attacks



Network Security Attacks

Passive Attacks

- No modification of packets.
- Information collected About path, source and destination node

Active Attacks

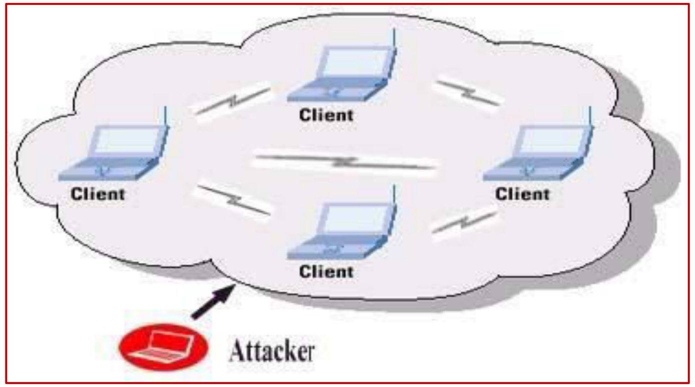
- Modification of packets take place

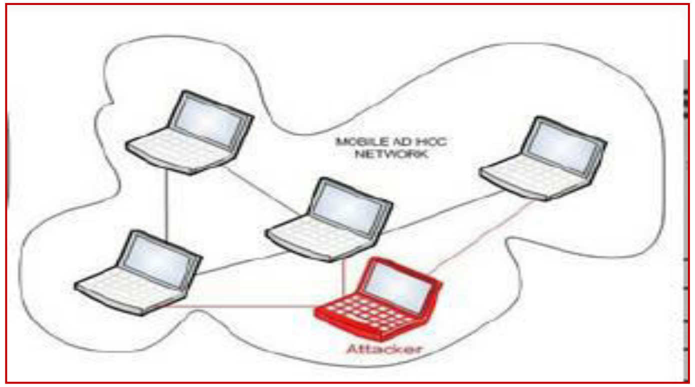
External Attacks

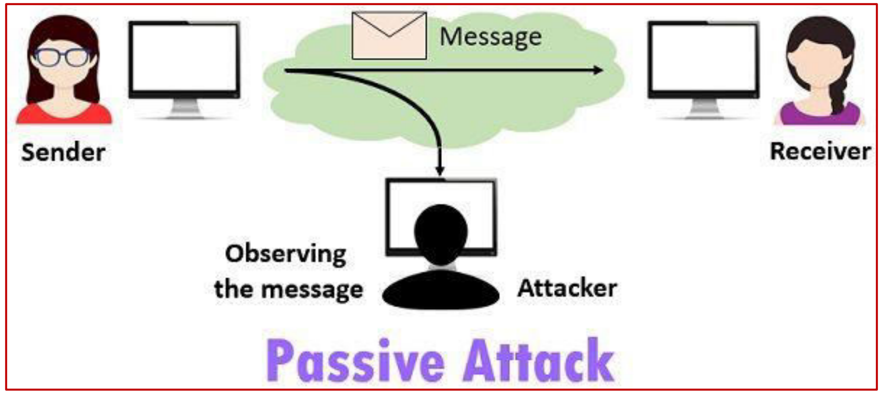
- Attacker does not belong to the same network

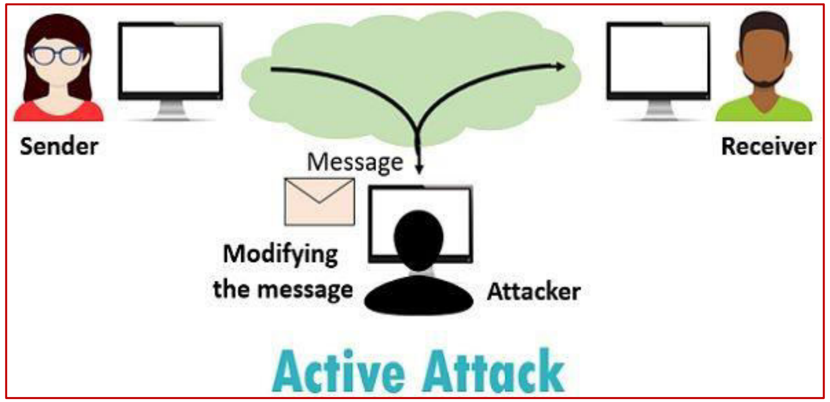
Internal Attacks

- Attacker belongs to the same network









Types of Network Security Attacks

Network Security Attacks

Passive Attacks

- Spoofing

Active Attacks

Mac Layers Attack

- Jamming

Network Layers Attack

- Wormhole
- Blackhole
- Byzantanie
- Routing

Transport Layers Attack

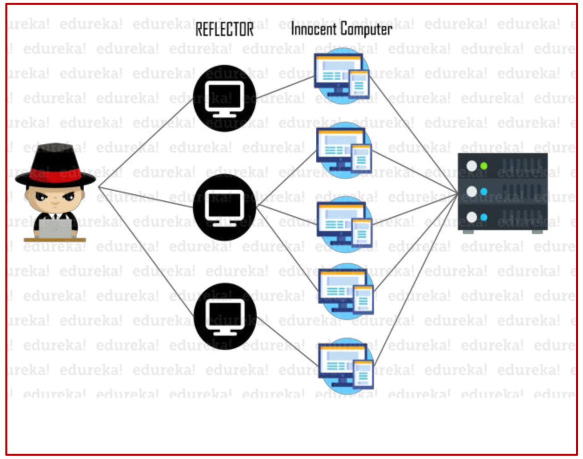
- Session Hijacking

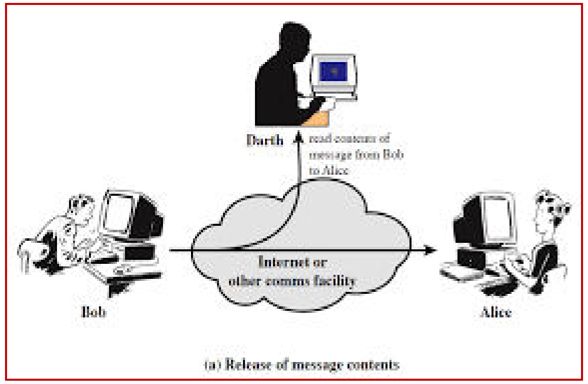
Application Layers Attack

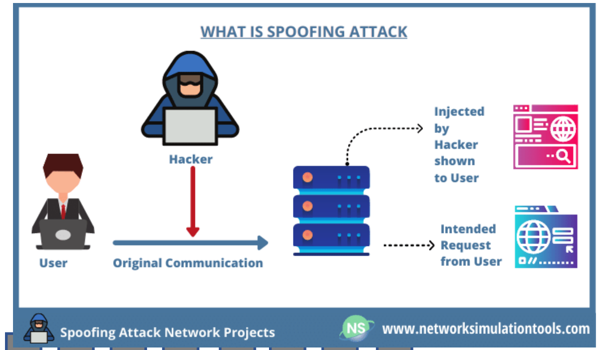
- Repudiation

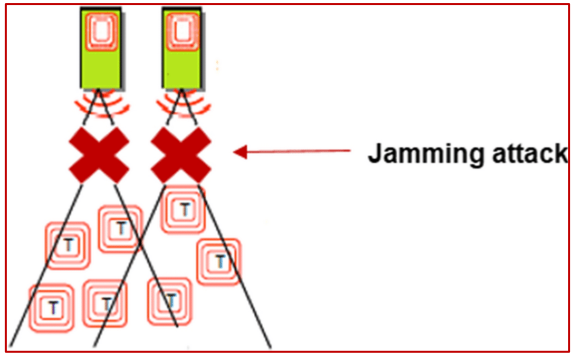
Others

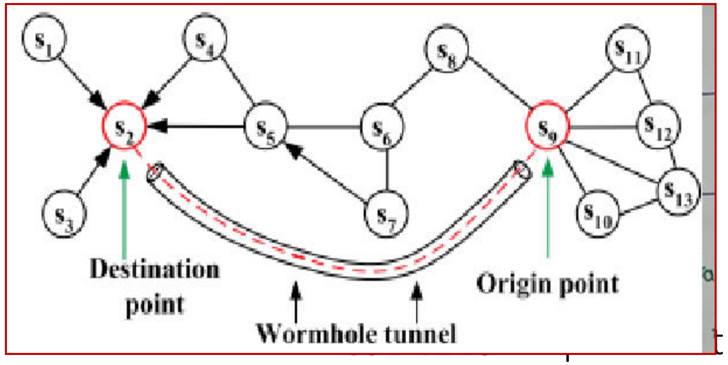
- DOS, DDOS
- Impersonation
- Manipulation of network traffic

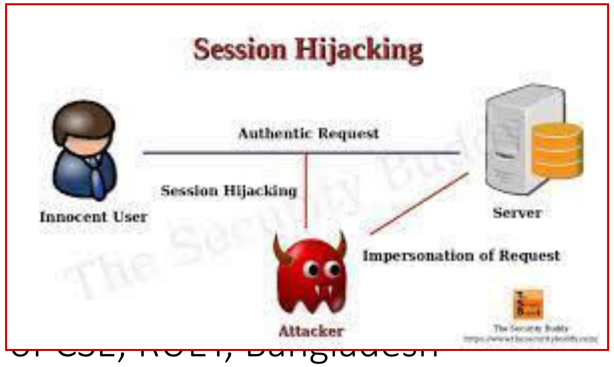



Darth
read contents of message from Bob to Alice
Internet or other comms facility
Bob
Alice
(a) Release of message contents

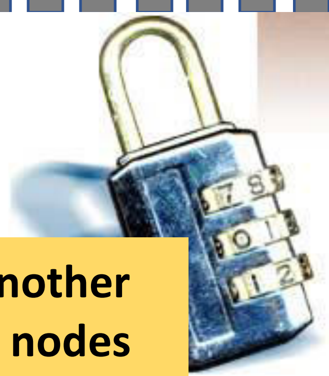

WHAT IS SPOOFING ATTACK
Hacker
User
Original Communication
Injected by Hacker shown to User
Intended Request from User
Spoofing Attack Network Projects
www.networksimulationtools.com



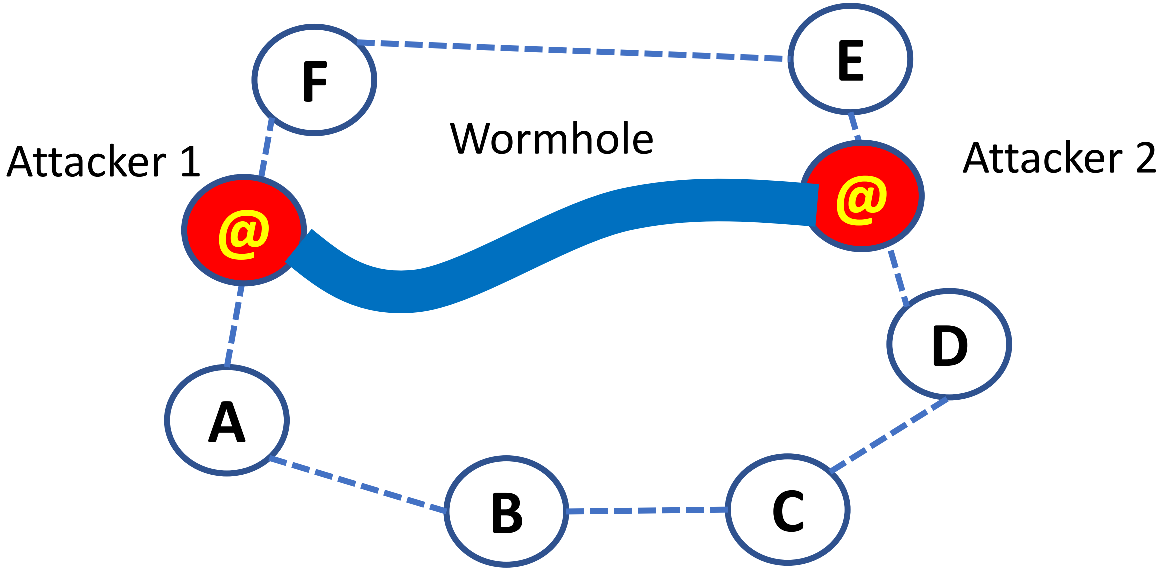




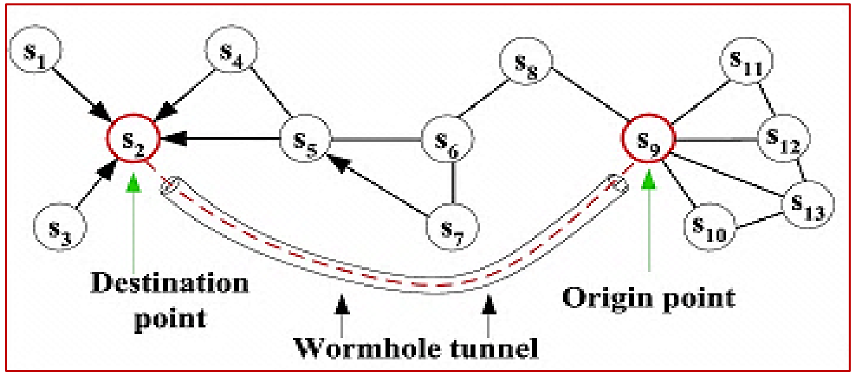
Network Security Attacks



Wormhole Attack: Attacker receives packets from one location in the network and tunnels them to another location in the network, where packets resent into the network. Example suppose a network with   six nodes connected through Wireless.



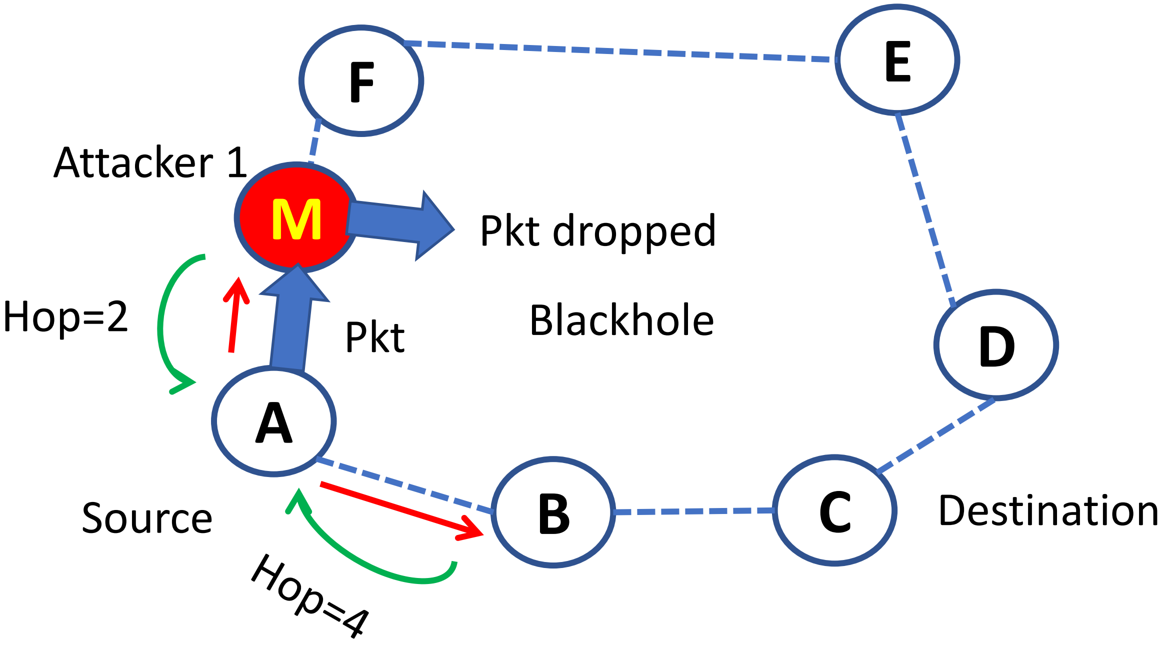
Disadvantage
- Delay in packet delivery
- Failure to find correct routes
- Attacker doesn't need to know protocol



Suppose A wants to communicate with E, then A broadcast its packets to direction of nodes F and B. The attacker receives packets and sends/resends to one another called tunneling. In the situation the packet does not reach or delayed at destination and conversation of the network getting very high. The tunnel between two malicious nodes is known as **wormhole**.

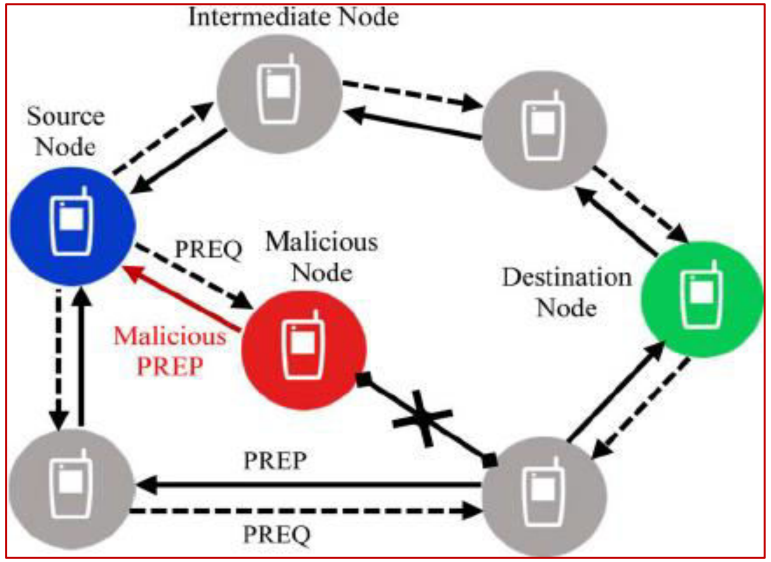
Network Security Attacks

Blackhole Attack: A malicious node falsely advertises good paths to the destination node during path finding process.



Disadvantage

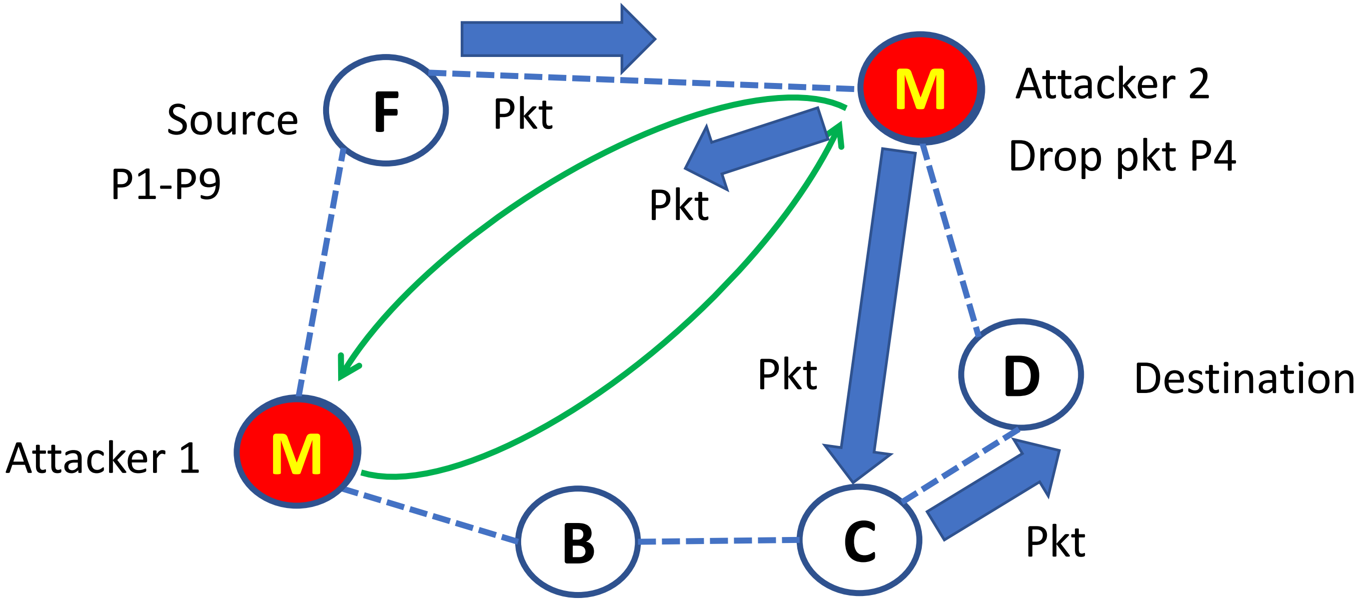
- Packets dropped by malicious node

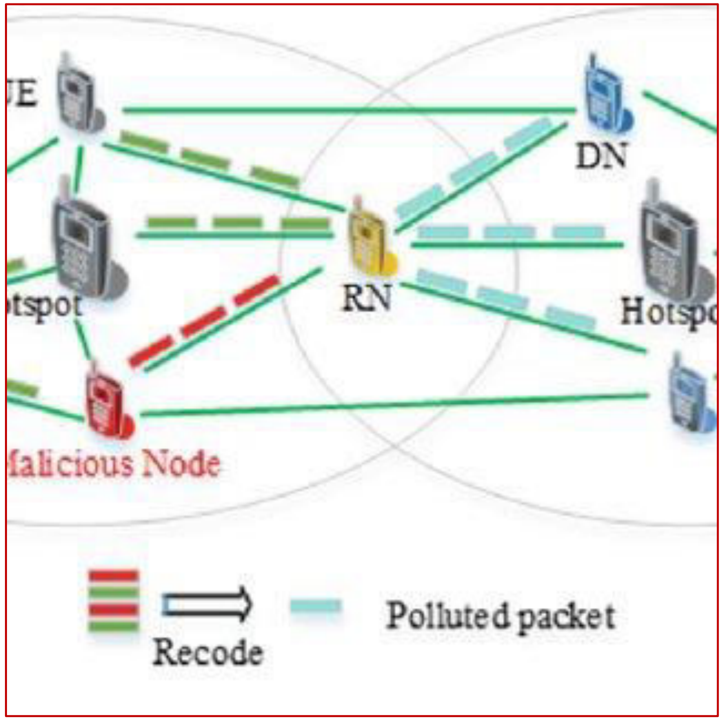


Here A wants to communicate with C, then A broadcast its packets to other nodes and these nodes replies the shortest route to destination C. Suppose A broadcast packets to B and B replies with hop count 4 Where as malicious node M replies with hop count 2. The node A choose the path of malicious node. So packets goes to M and then lost.

Network Security Attacks

Byzantine Attack: Compromised node/nodes works in collision and carries out attacks such as i) creating routing loops, ii) packets on non-optimal paths and iii) selectively dropping packets.

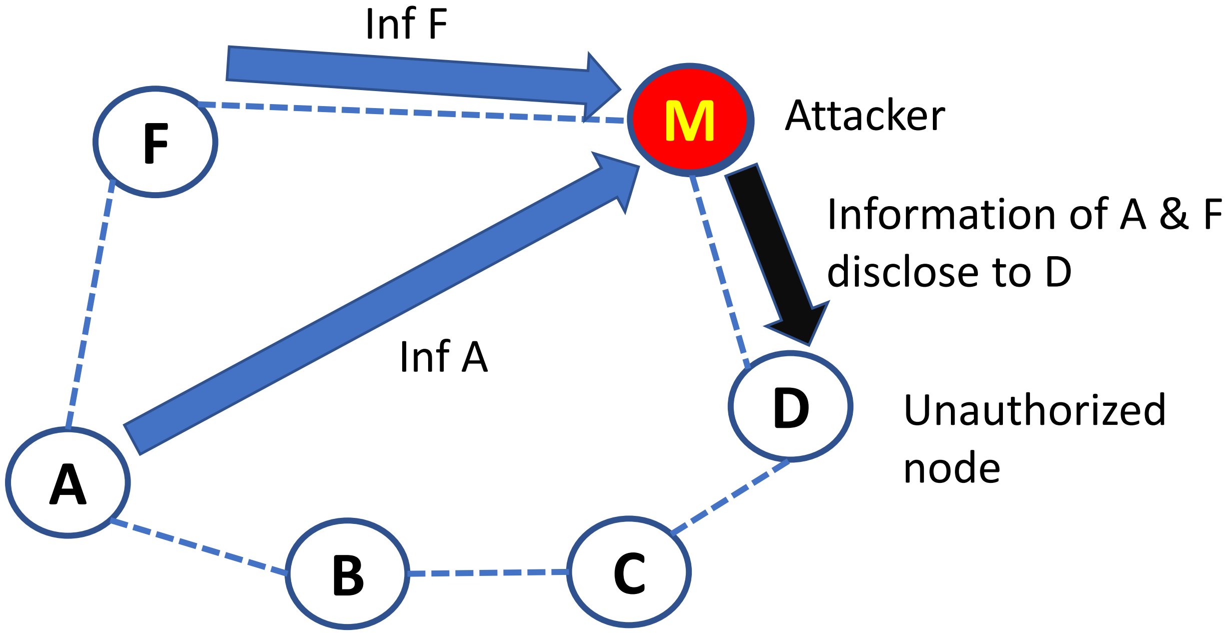




In the network here two malicious nodes creates loops enforcing delays for packets to reach the destination.
Suppose F wants to send packets to D then attacker 2 sends the packet to the non-optimal path.
If F wants to send packets P1-P9 then seclectively packet P4 is dropped by attacker 2.

Network Security Attacks

Information Disclosure Attack: Compromised node/nodes may leak confidential or important information to unauthorized nodes in the network.



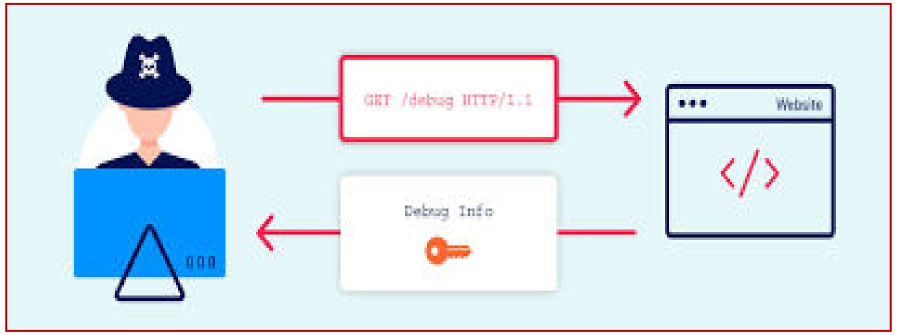
Inf F

Attacker

Information of A & F disclose to D

Inf A

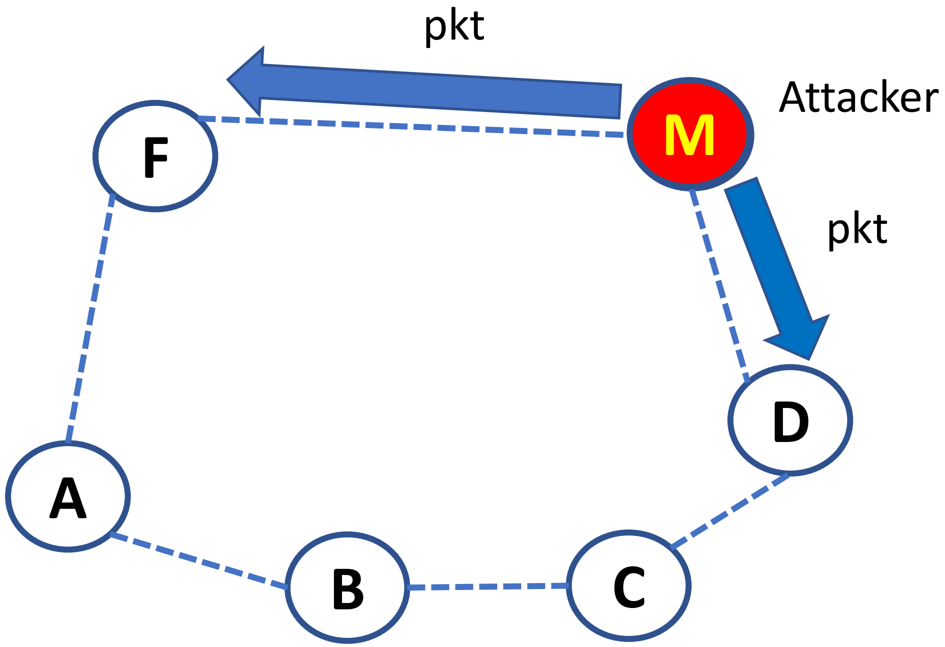
Unauthorized node

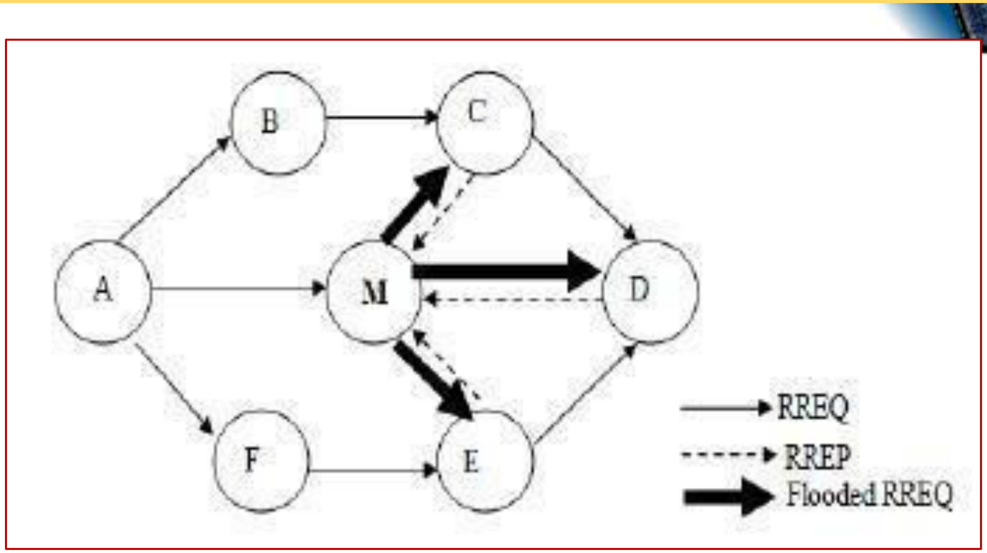


Here attacker collects information from A and F and sends it unauthorized node D

Network Security Attacks

Resource Consumption Attack: Malicious node tries to consume/waste away resources of other nodes.

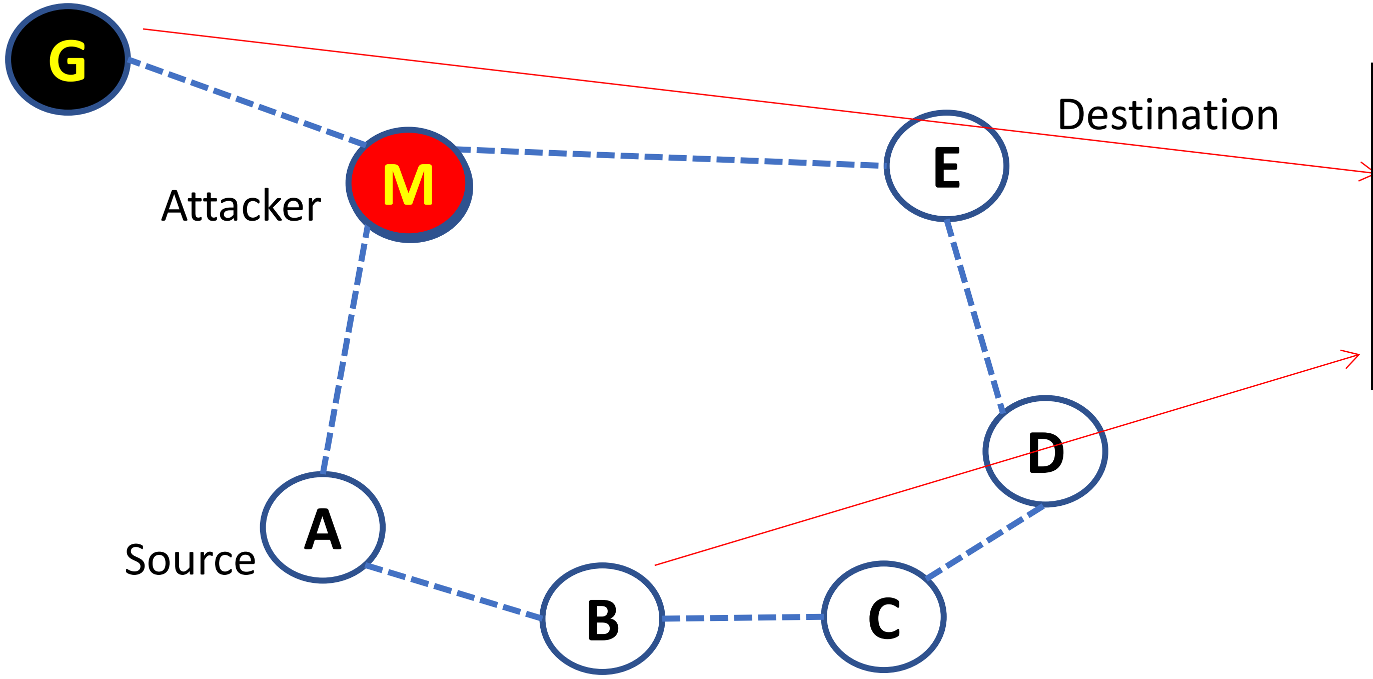




Here attacker M sends pkts to F and D and thereby consumes battery power or waste of memory space.

Network Security Attacks

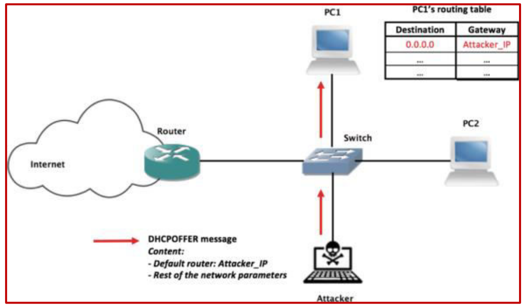
Routing Attack: Overflows the routing table with fake information



Routing Table of A

Node	Hop
G	2
H	3
B	6

fake



PC1's routing table

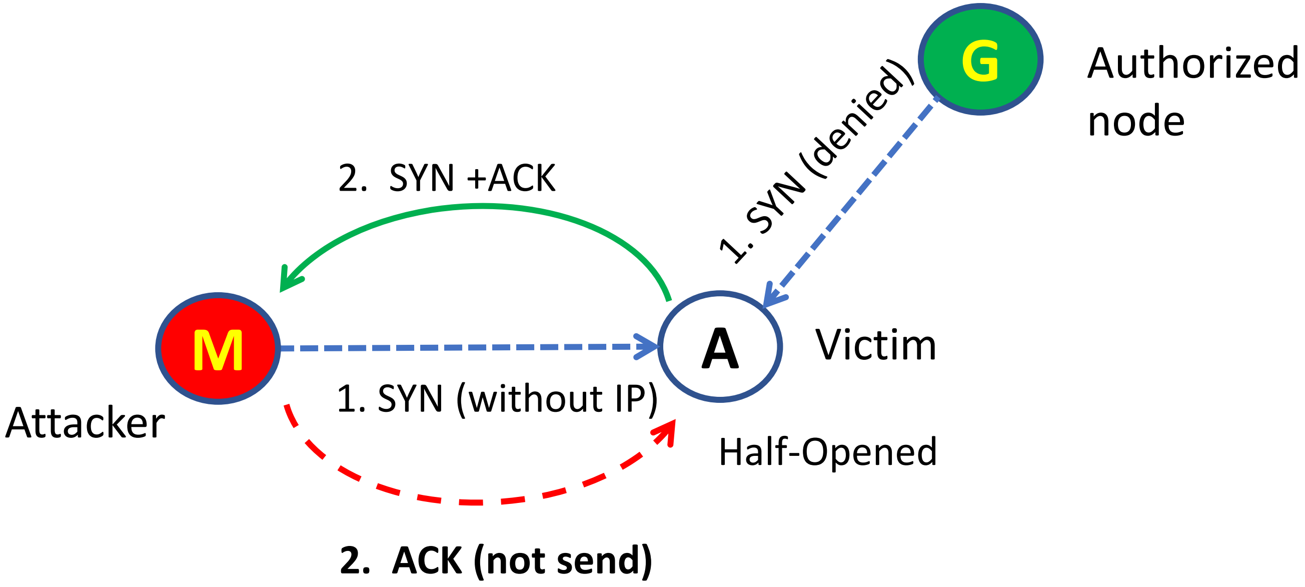
Destination	Gateway
0.0.0.0	Attacker_IP
...	...
...	...

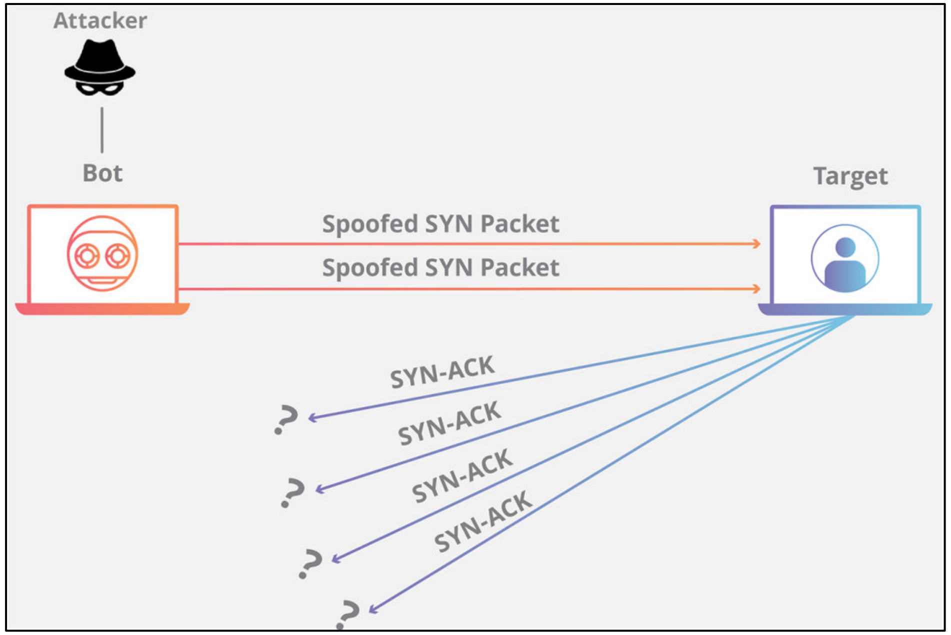
DHCPOFFER message
Content:
- Default router: Attacker_IP
- Rest of the network parameters

Suppose A wants to send pkt to E then attacker M sends the fake node information like G (not exits)
To the routing table of A makes the table overflows

Transport Layer Attacks

SYN Flooding Attack: It is a kind of DoS attack. The malicious node/attacker creates large no. of Half-opened TCP-Connection with victim node, but never completes the handshake.

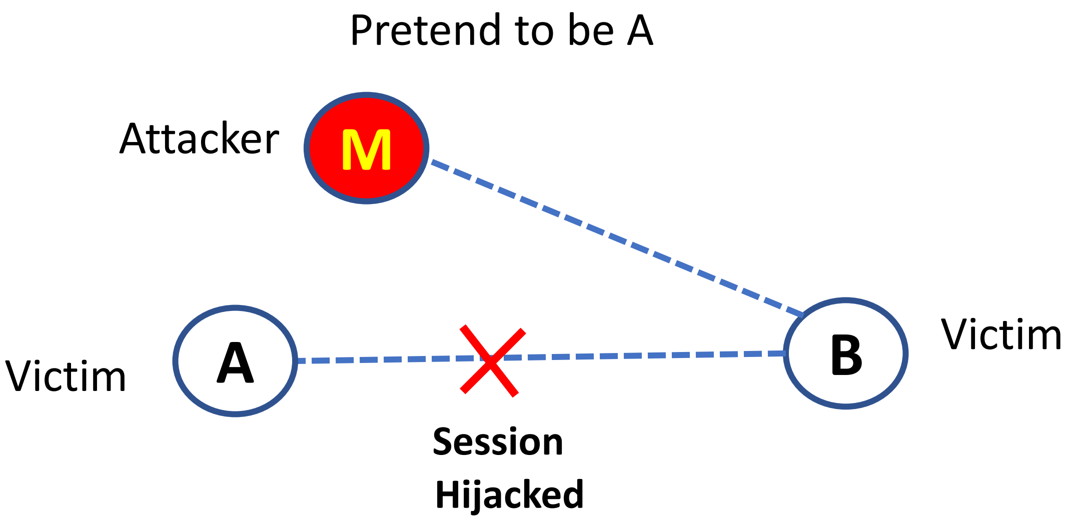


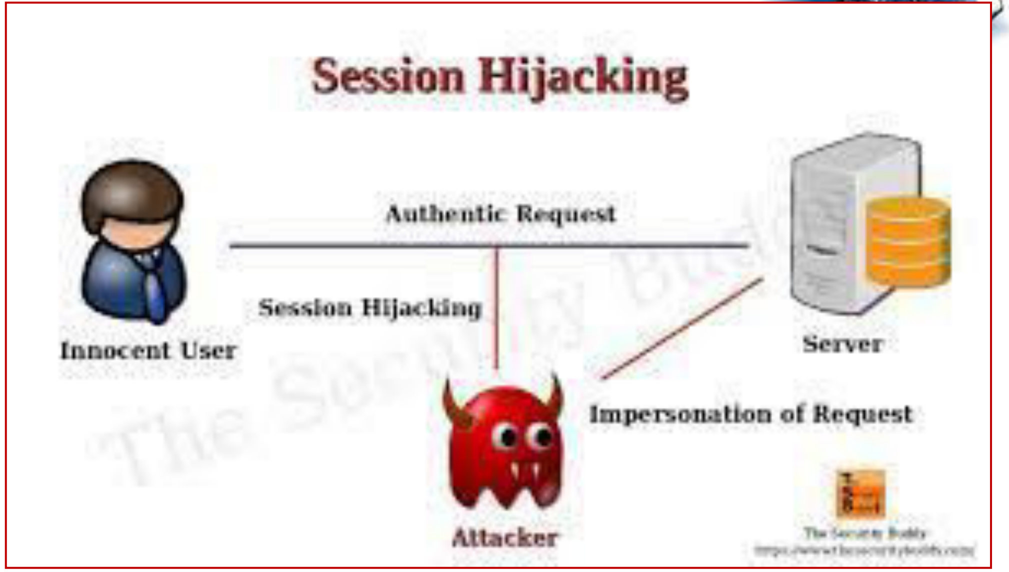


The malicious node sends SYN to victim node A. The node A sends SYN+ACK to M and keep Half-opened waiting for the ACK from M but M never sends ACK to A. There are many half-opened Processes at node A. So A stops taking from other nodes. Here valiid node G sends SYN to A but does not respond to G.

Transport Layer Attacks

Session Attack: The malicious node take control over a session between two nodes

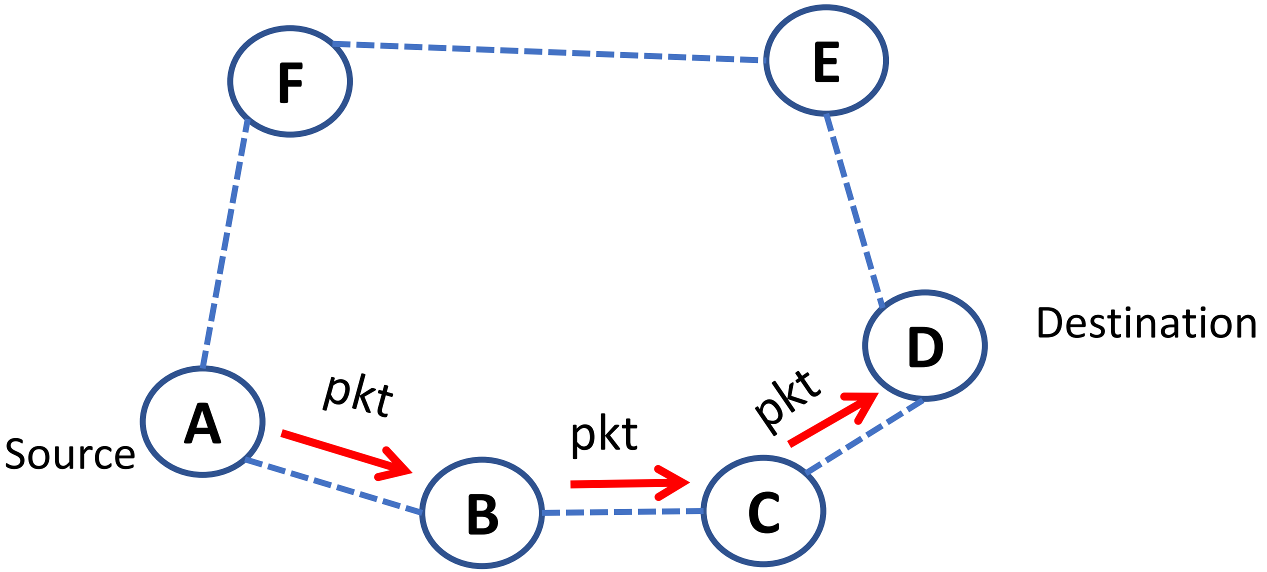


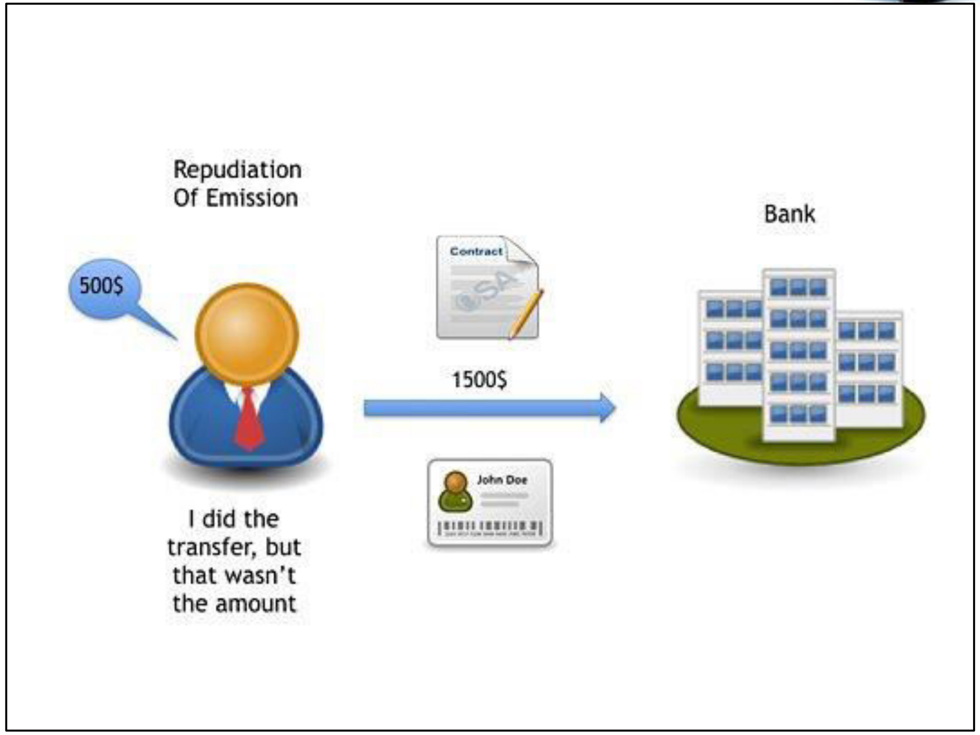


Suppose Node A & B are in valid session. A malicious node M hijacking the session and establish A session between M and B as M pretends to be A.

Application Layer Attacks

Repudiation Attack: It refers to the denial or attempted denial by a node

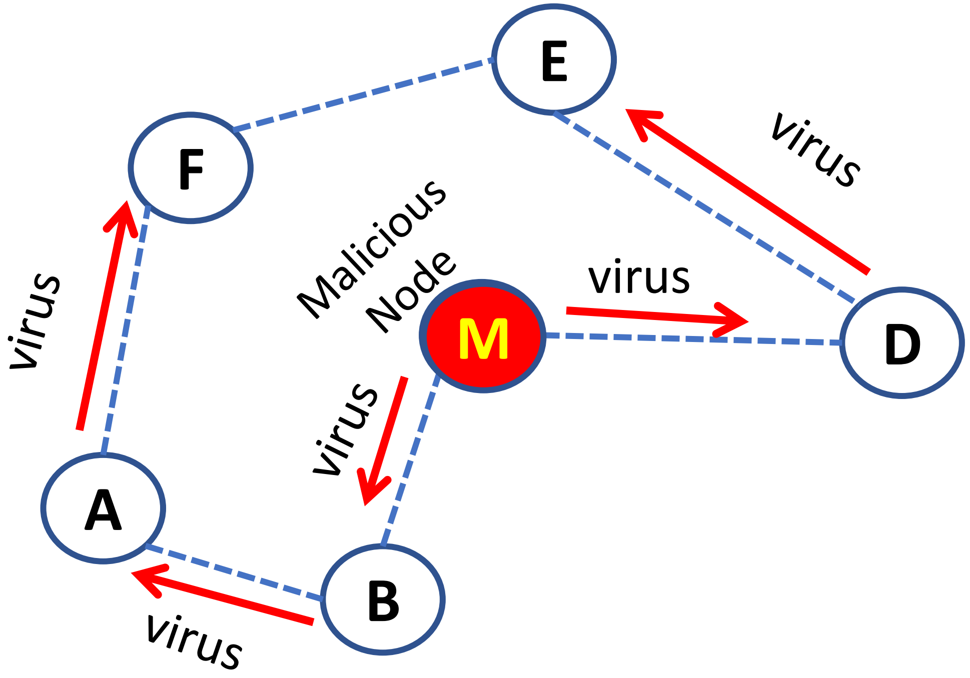




Suppose A is source and D is destination nodes. Node A sends packet to D through B and C. At D the packets are found to be malicious. But node A denies that it sent the packet.

Application Layer Attacks

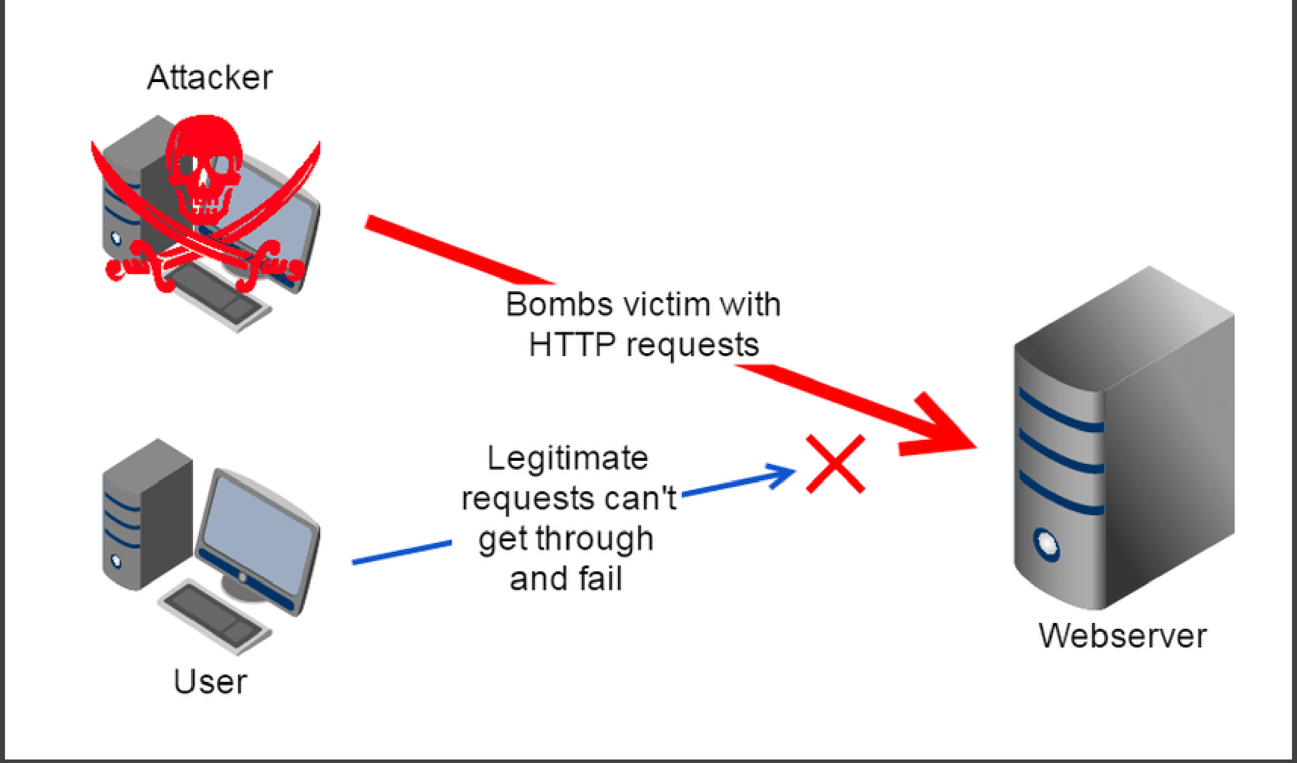
Malicious Code Attack: Malicious codes such as viruses, worms, spywares and Trojan Horses can attack both OS and user application



Suppose C is a malious node. It spreads malicious codes such as viuses through its neighbors

Security Attacks

1. **Denial of Service (DoS):** A denial of service (DoS) is an action that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources such as central processing units (CPU), memory, bandwidth, and disk space.

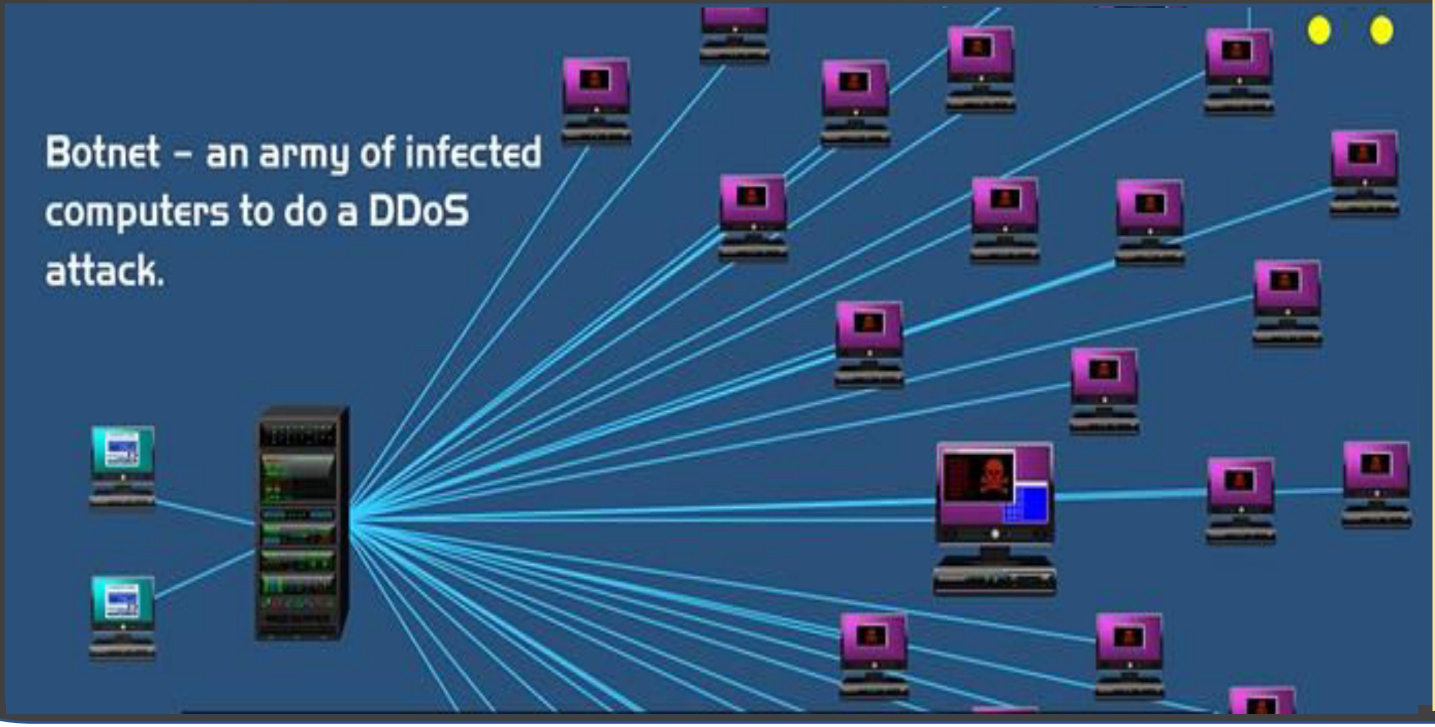

Attacker
Bombs victim with HTTP requests
Legitimate requests can't get through and fail
User
Webserver

Security Attacks

2. **Distributed Denial of Service (DDoS):** A distributed denial-of-service (DDoS) attack is a malicious attempt to disrupt the normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic.

DDoS attacks achieve effectiveness by utilizing multiple compromised computer systems as sources of attack traffic.

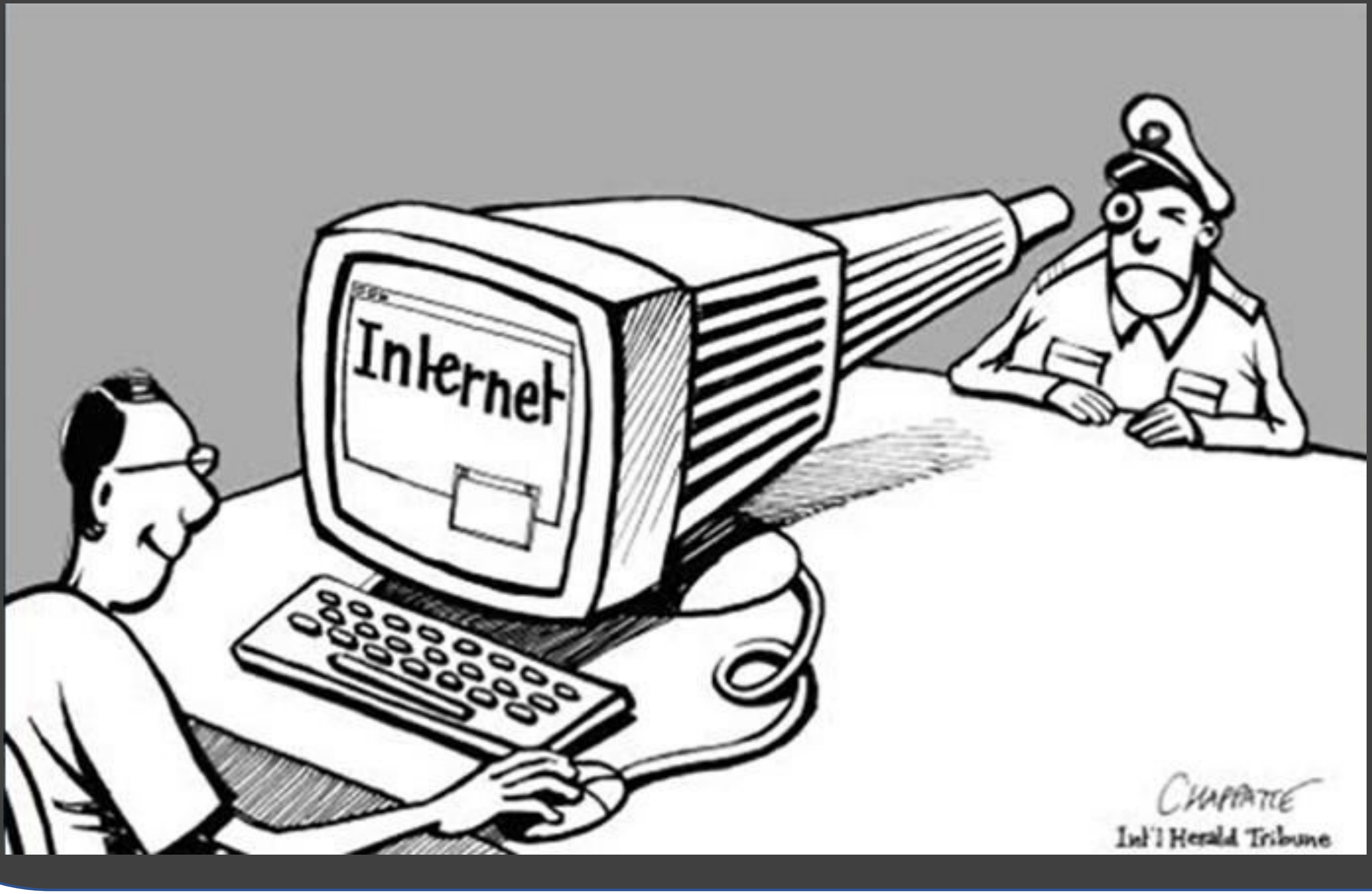
.

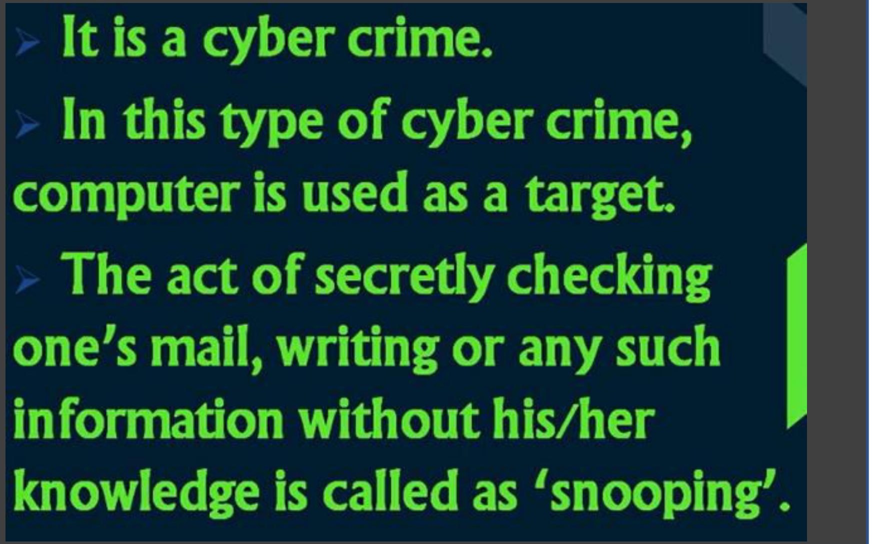


- Attacker Hack other computers Now attack originates from many Sources
- Overload CPU and Memory
- Eat up bandwidth
- Legal clients are refused to access
- Attacker sends malicios content to target computer
- Infected computers are called botnet.

Security Attacks

3. **Snooping:** Snooping attacks involve **an intruder listening to traffic between two machines on your network**. If traffic includes passing unencrypted passwords, an unauthorized individual can potentially access your network and read confidential data.

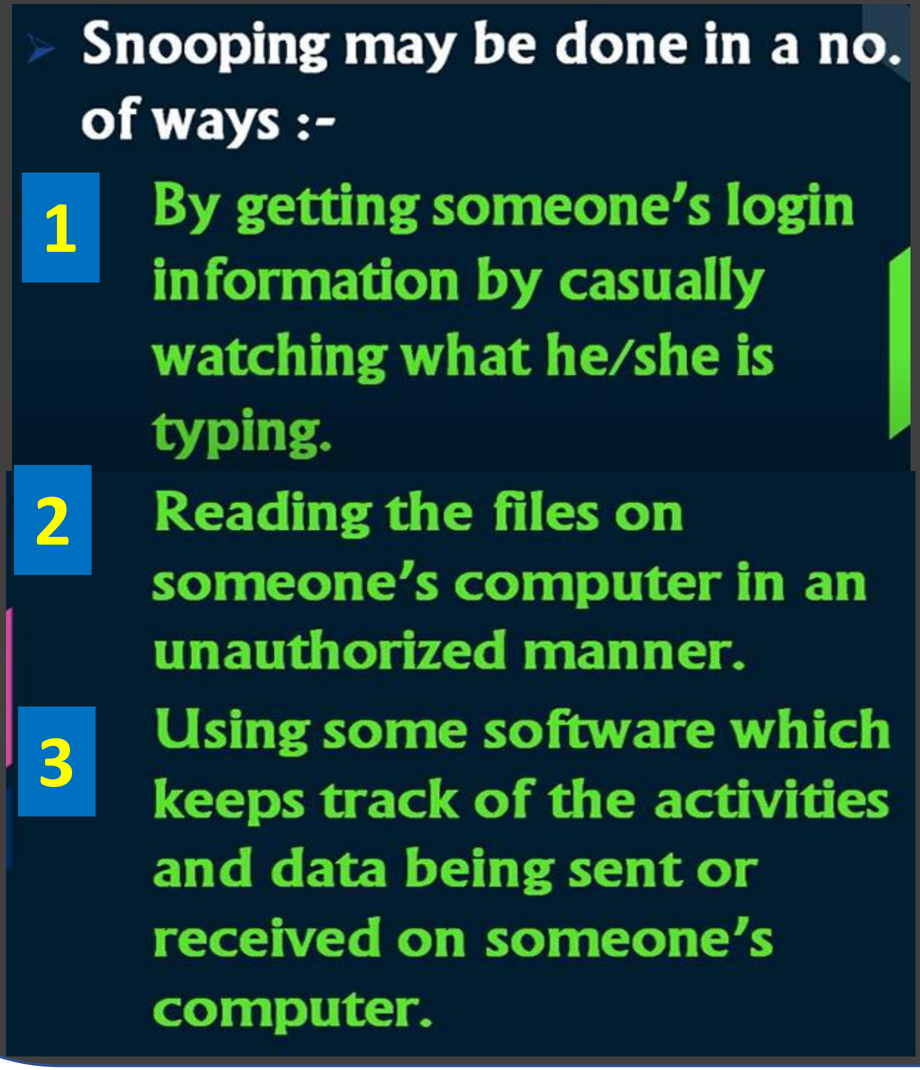




- It is a cyber crime.
- In this type of cyber crime, computer is used as a target.
- The act of secretly checking one's mail, writing or any such information without his/her knowledge is called as 'snooping'.

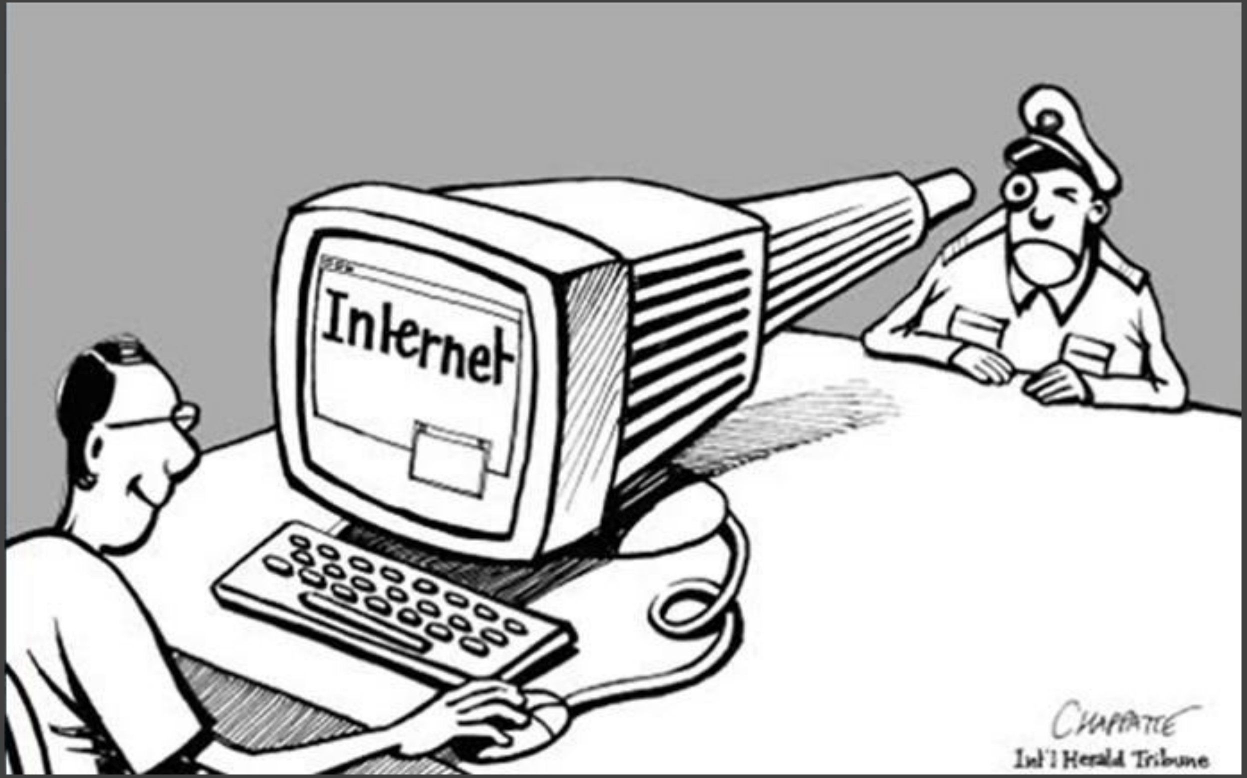
Security Attacks

3. Snooping: (continue…)



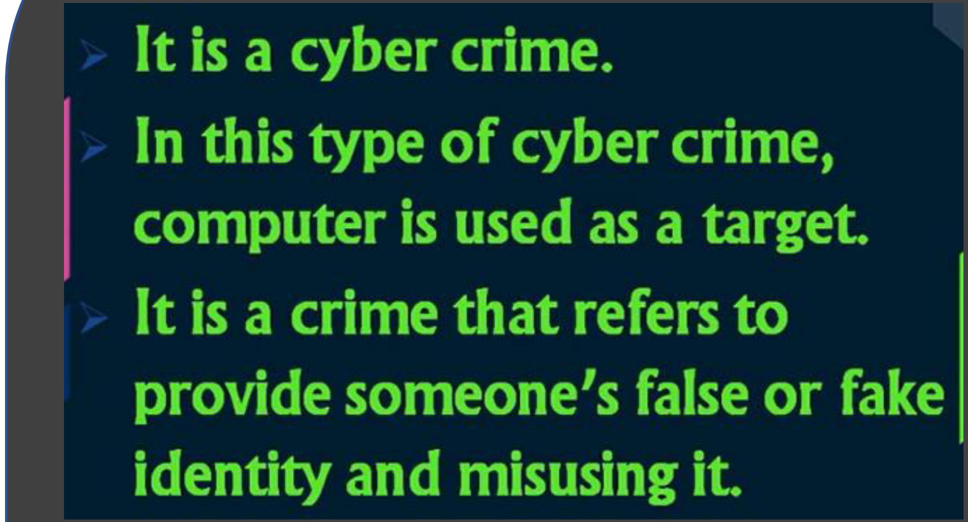
- Snooping may be done in a no. of ways :-

1. By getting someone's login information by casually watching what he/she is typing.
2. Reading the files on someone's computer in an unauthorized manner.
3. Using some software which keeps track of the activities and data being sent or received on someone's computer.

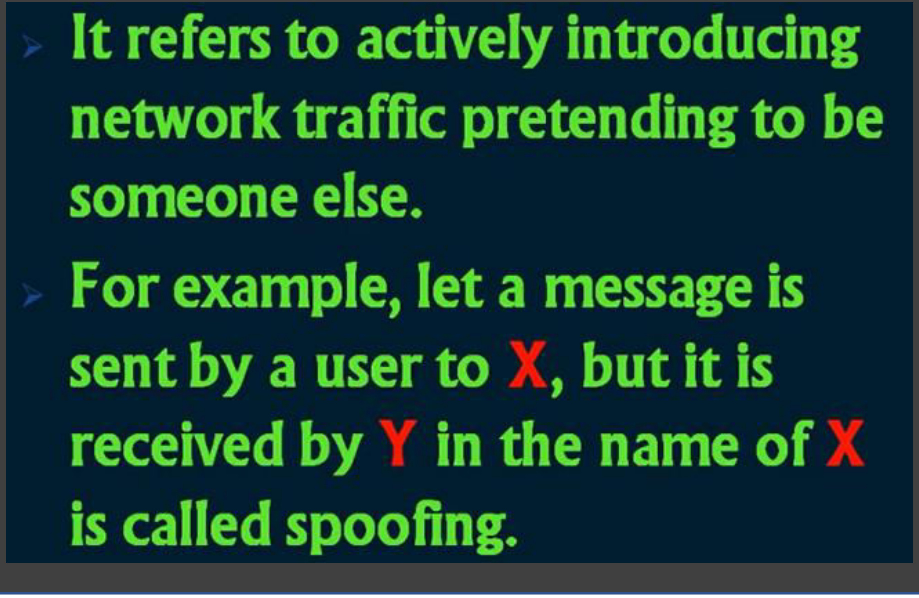


Security Attacks

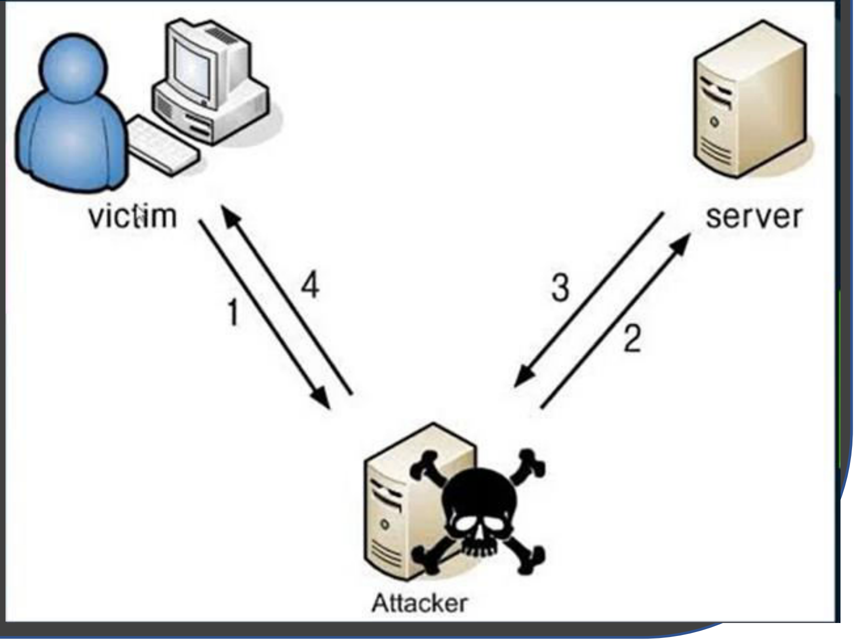
4. Spoofing:



- It is a cyber crime.
- In this type of cyber crime, computer is used as a target.
- It is a crime that refers to provide someone's false or fake identity and misusing it.



- It refers to actively introducing network traffic pretending to be someone else.
- For example, let a message is sent by a user to X, but it is received by Y in the name of X is called spoofing.



Security Attacks

4, Spoofing:(continue…)

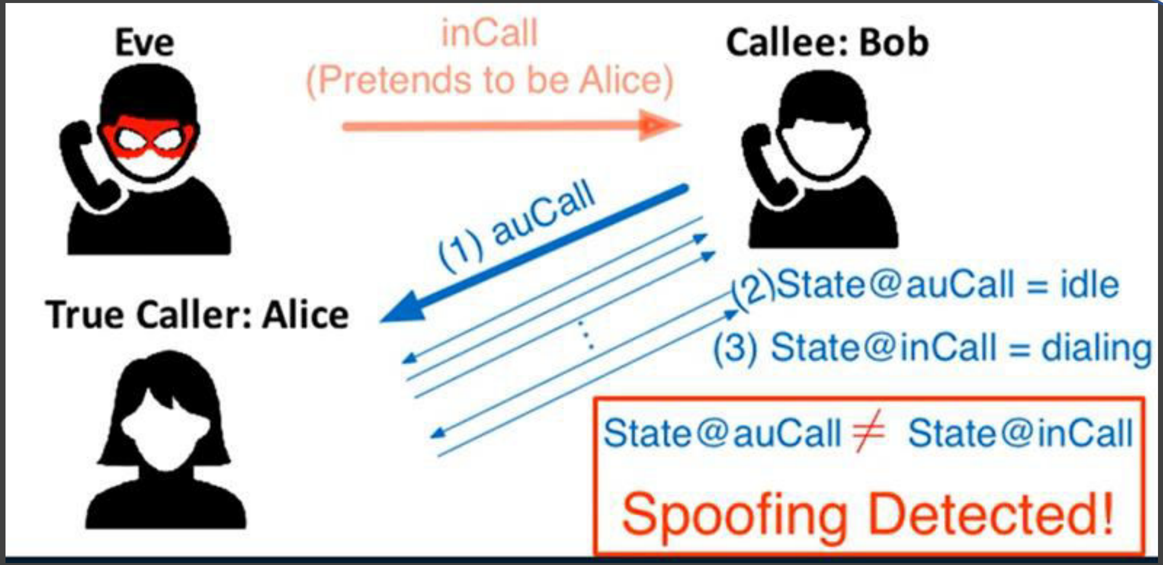
- Various types of spoofing are :-
  1. Caller ID spoofing
  2. E-mail ID spoofing
  3. IP address spoofing
  4. Protocol spoofing

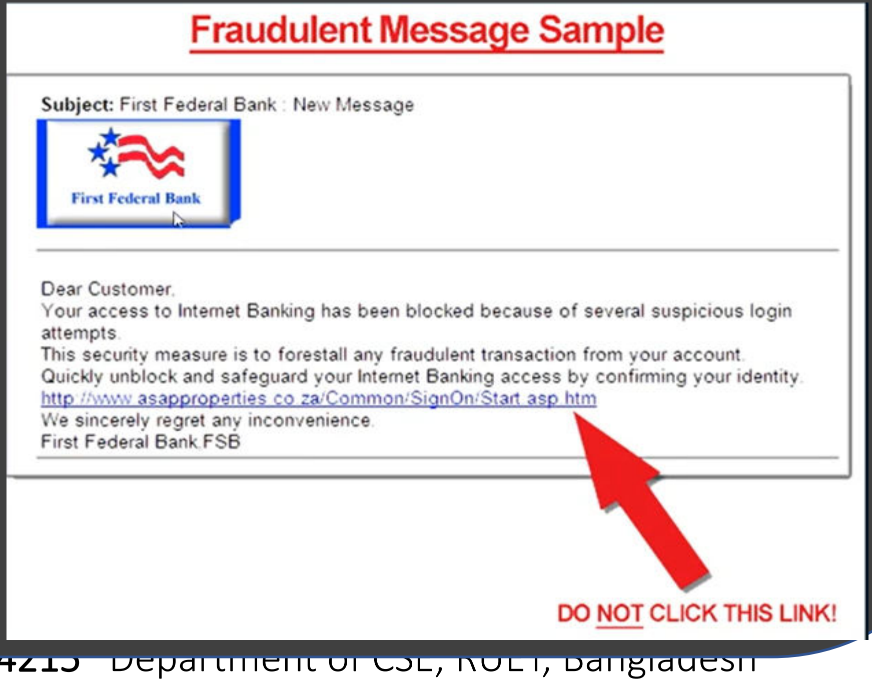
1. caller ID spoofing:-

- It is a service that allows a caller to call a user as someone else.

2. E-mail ID spoofing:-

- It is a practice of sending an e-mail pretending to be someone else.




Fraudulent Message Sample

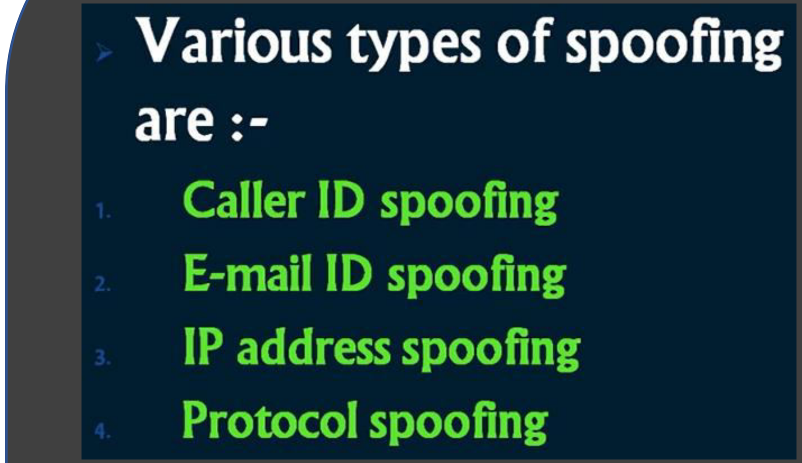
Subject: First Federal Bank : New Message

Dear Customer,
Your access to Internet Banking has been blocked because of several suspicious login attempts.
This security measure is to forestall any fraudulent transaction from your account.
Quickly unblock and safeguard your Internet Banking access by confirming your identity.
http://www.asapproperties.co.za/Common/SignOn/Start.asp.htm
We sincerely regret any inconvenience.
First Federal Bank FSB

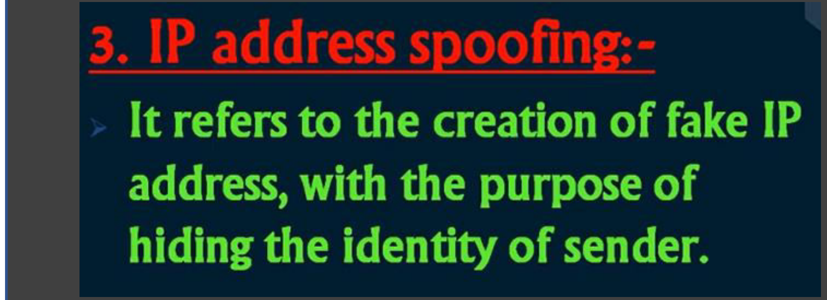
DO NOT CLICK THIS LINK!

Security Attacks

4, Spoofing:(continue…)

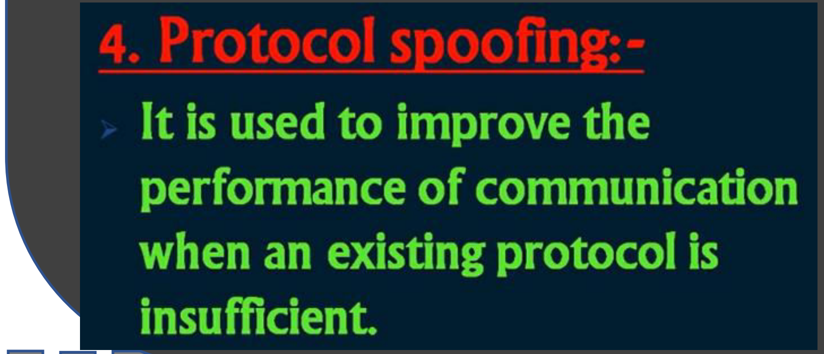


- Various types of spoofing are :-
  1. Caller ID spoofing
  2. E-mail ID spoofing
  3. IP address spoofing
  4. Protocol spoofing



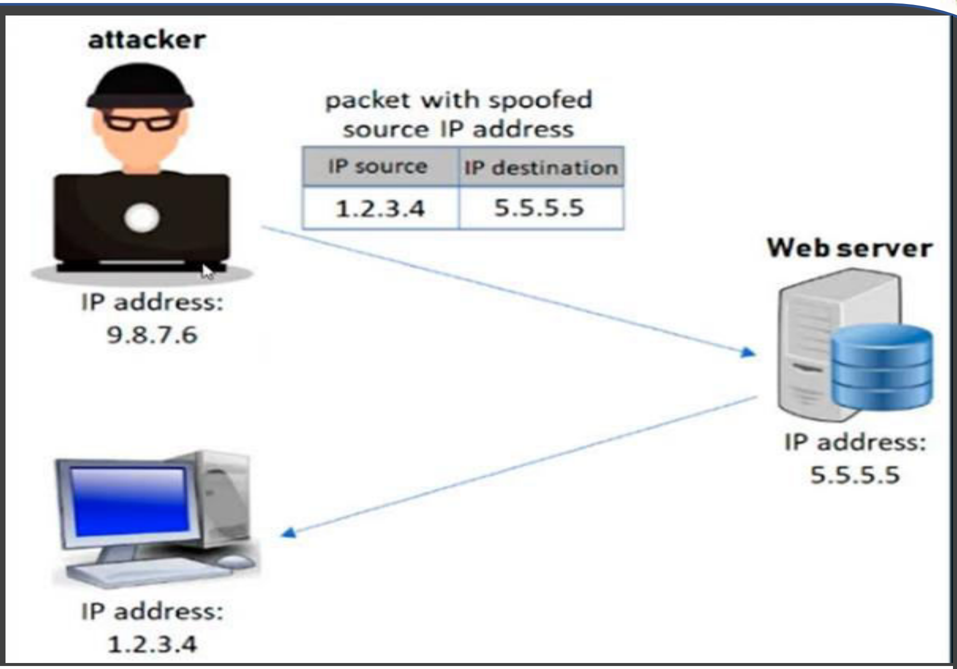
3. IP address spoofing:-

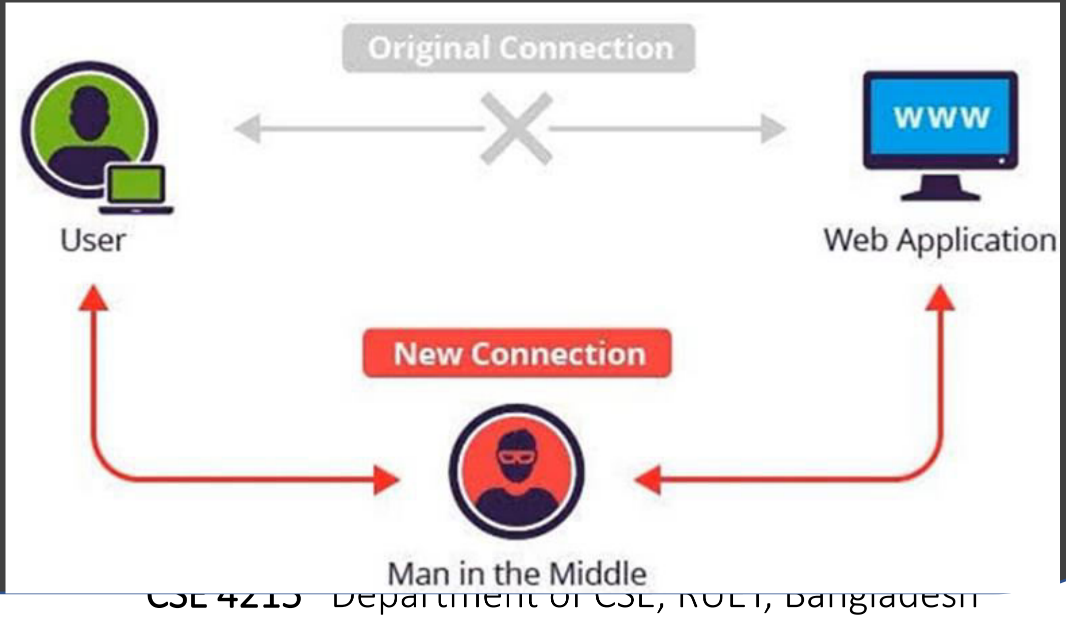
- It refers to the creation of fake IP address, with the purpose of hiding the identity of sender.



4. Protocol spoofing:-

- It is used to improve the performance of communication when an existing protocol is insufficient.





Security Attacks

5 Eavesdropping

- It is a cyber crime.
- In this type of cyber crime, computer is used as a target.

- Suppose two friends are talking to each other and a third person is secretly trying to listen to their talks. What that person is doing is called ‘eavesdropping’.

- Eavesdropping refers to unauthorized access to another person’s or organization’s data while the data is on its way on the network.

Security Attacks

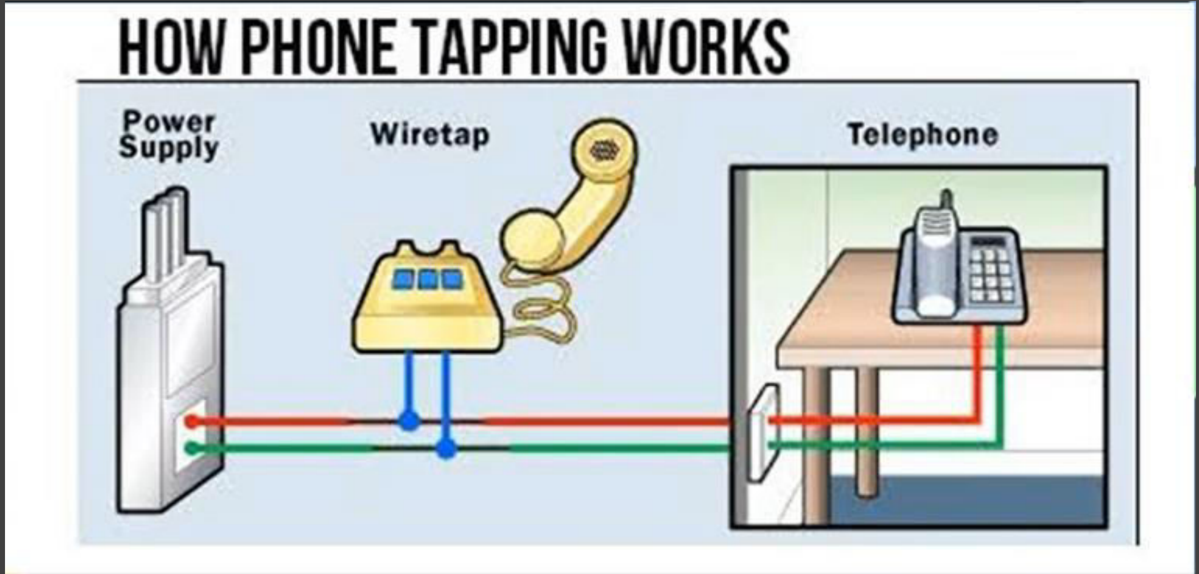
5 Eavesdropping (cont)

- This may be done in number of ways :-

I. By setting up parallel telephone lines.

II. By installing some software (spyware) in the target computer.

III. By installing some receiver which captures the data while on its way.



End of Chapter 2