Adama Science and Technology University Department of CSE

- Computer Networks and Information Security (CSE 4205)

- Chapter one lecture two

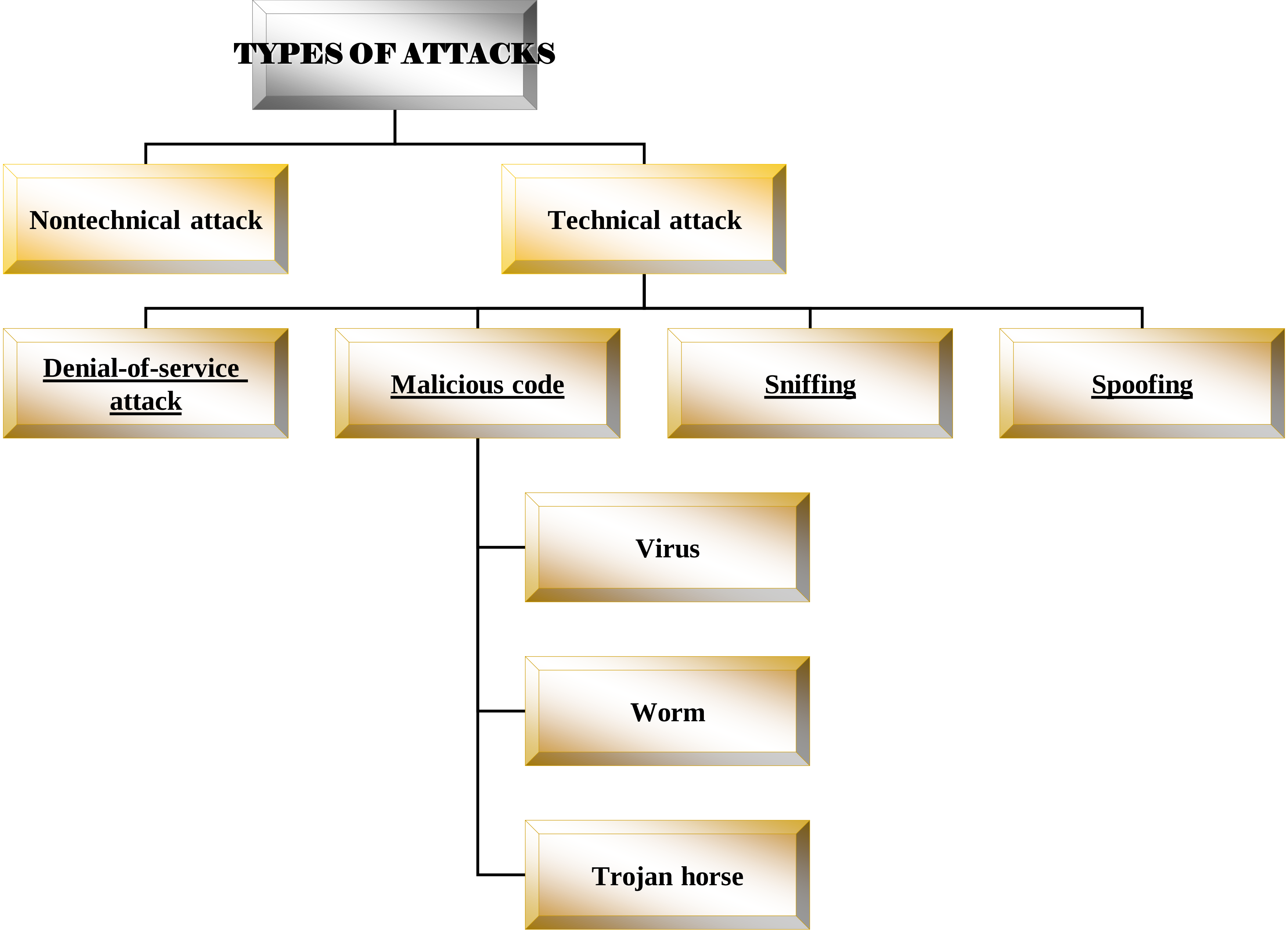
- <u>Attackers</u>

Different Attack

- DOS/DDOS
- Spoofing
- Man in the Middle
- Replay
- TCP/IP Hijacking
- Social Engineering
- Password Guessing

Security attack: Any action that compromises the security of information owned by an organization.

- **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.



TYPES OF ATTACKS

- Nontechnical attack
- Technical attack
  - Denial-of-service attack
  - Malicious code
    - Virus
    - Worm
    - Trojan horse
  - Sniffing
  - Spoofing

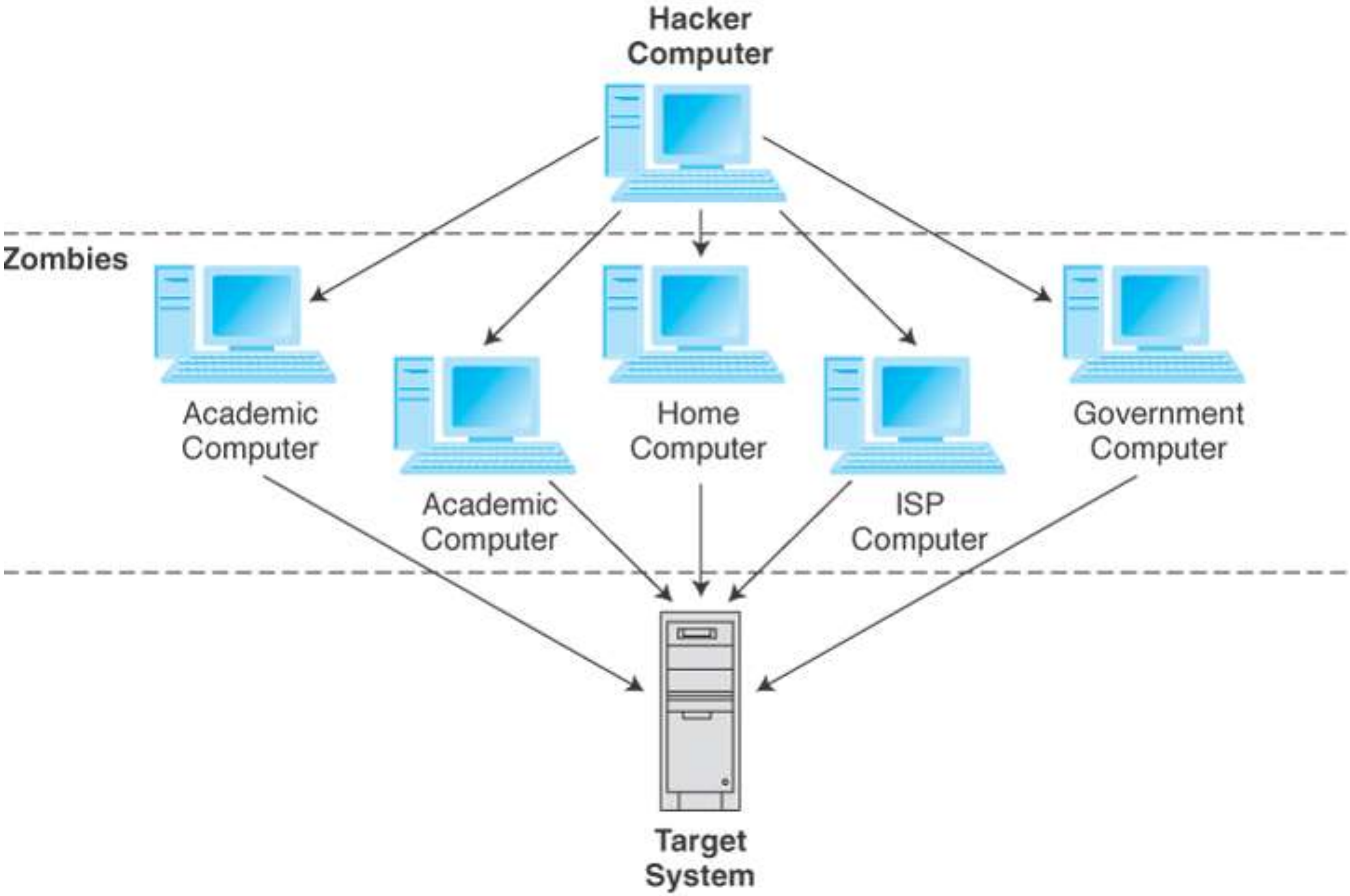
Definitions of DoS and DDoS attacks

- A DoS (Denial of Service) attack aims at preventing, for *legitimate* users, authorized access to a system resource . The attacker uses specialized software to send a flood of data packets to the target computer with the aim of overloading its resources.

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

  A denial-of-service attack in which the attacker gains illegal administrative access to as many computers on the Internet as possible and uses the multiple computers to send a flood of data packets to the target computer.

Distributed Denial-of-service (DDoS) attack



Source: Scambray, J. et al. *Hacking Exposed 2e.* New York: McGraw-Hill, 2000. Copyright © McGraw-Hill Companies, Inc.

Classification of DoS attacks

1. **Bandwidth consumption**:

Attacks will consume all available **Network bandwidth**

2. **Resource starvation**:

Attacks will consume system **resources** (mainly **CPU**, **memory**, storage space)

3. **Programming flaw**:

Failures of applications or OS components to handle exceptional conditions (i.e. unexpected data is sent to a vulnerable component).

4. **Routing and DNS attacks**:

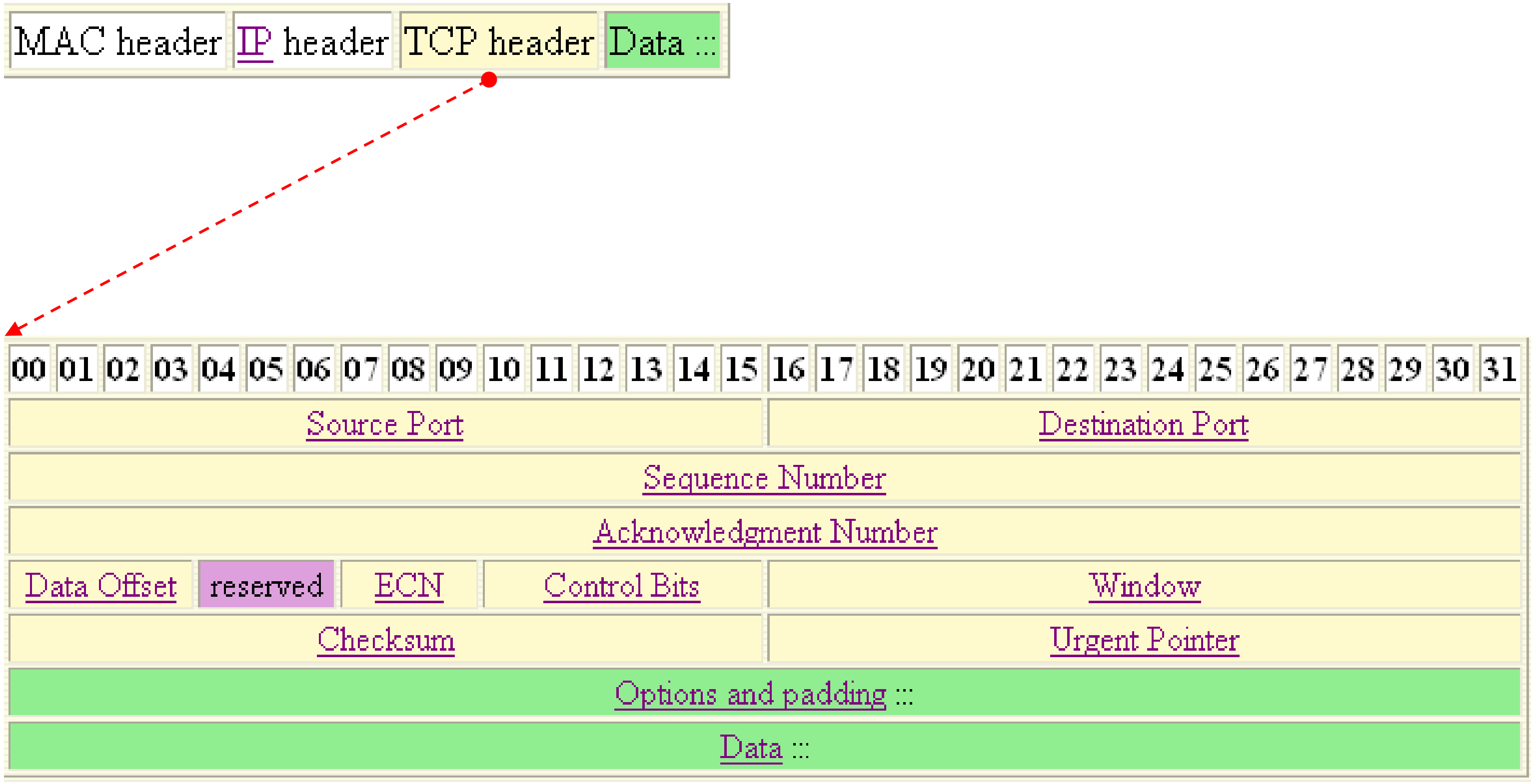
- ✓ Manipulate routing tables.
- ✓ Changing routing tables to route to attacker's net or black hole.
- ✓ Attack to DNS servers, again route to attackers or black hole.

EXAMPLES

- **Syn flood**
  - TCP three-way handshake:
    - The client requests a connection by sending a SYN (*synchronize*) message to the server.
    - The server *acknowledges* this request by sending SYN-ACK back to the client, which, Responds with an ACK, and the connection is established.
- **How it work………???**
  - Attacker sends SYN packet to victim forging non-existent IP address
  - Victim replies with Syn/Ack but neither receives Ack nor RST from non-existent IP address
  - Victim keeps potential connection in a queue in Syn_Recv state, but the queue is small and takes some time to timeout and flush the queue, e.g 75 seconds
  - If a few SYN packets are sent by the attacker every 10 seconds, the victim will never clear the queue and stops to respond.

2. TCP Session Hijacking

TCP HEADER FORMAT



MAC header	IP header	TCP header	Data :::

<table>
<tr><td>00</td><td>01</td><td>02</td><td>03</td><td>04</td><td>05</td><td>06</td><td>07</td><td>08</td><td>09</td><td>10</td><td>11</td><td>12</td><td>13</td><td>14</td><td>15</td><td>16</td><td>17</td><td>18</td><td>19</td><td>20</td><td>21</td><td>22</td><td>23</td><td>24</td><td>25</td><td>26</td><td>27</td><td>28</td><td>29</td><td>30</td><td>31</td></tr>
<tr><td colspan="16">Source Port</td><td colspan="16">Destination Port</td></tr>
<tr><td colspan="32">Sequence Number</td></tr>
<tr><td colspan="32">Acknowledgment Number</td></tr>
<tr><td colspan="4">Data Offset</td><td colspan="3">reserved</td><td colspan="3">ECN</td><td colspan="6">Control Bits</td><td colspan="16">Window</td></tr>
<tr><td colspan="16">Checksum</td><td colspan="16">Urgent Pointer</td></tr>
<tr><td colspan="32">Options and padding :::</td></tr>
<tr><td colspan="32">Data :::</td></tr>
</table>

TCP SLIDING WINDOWS

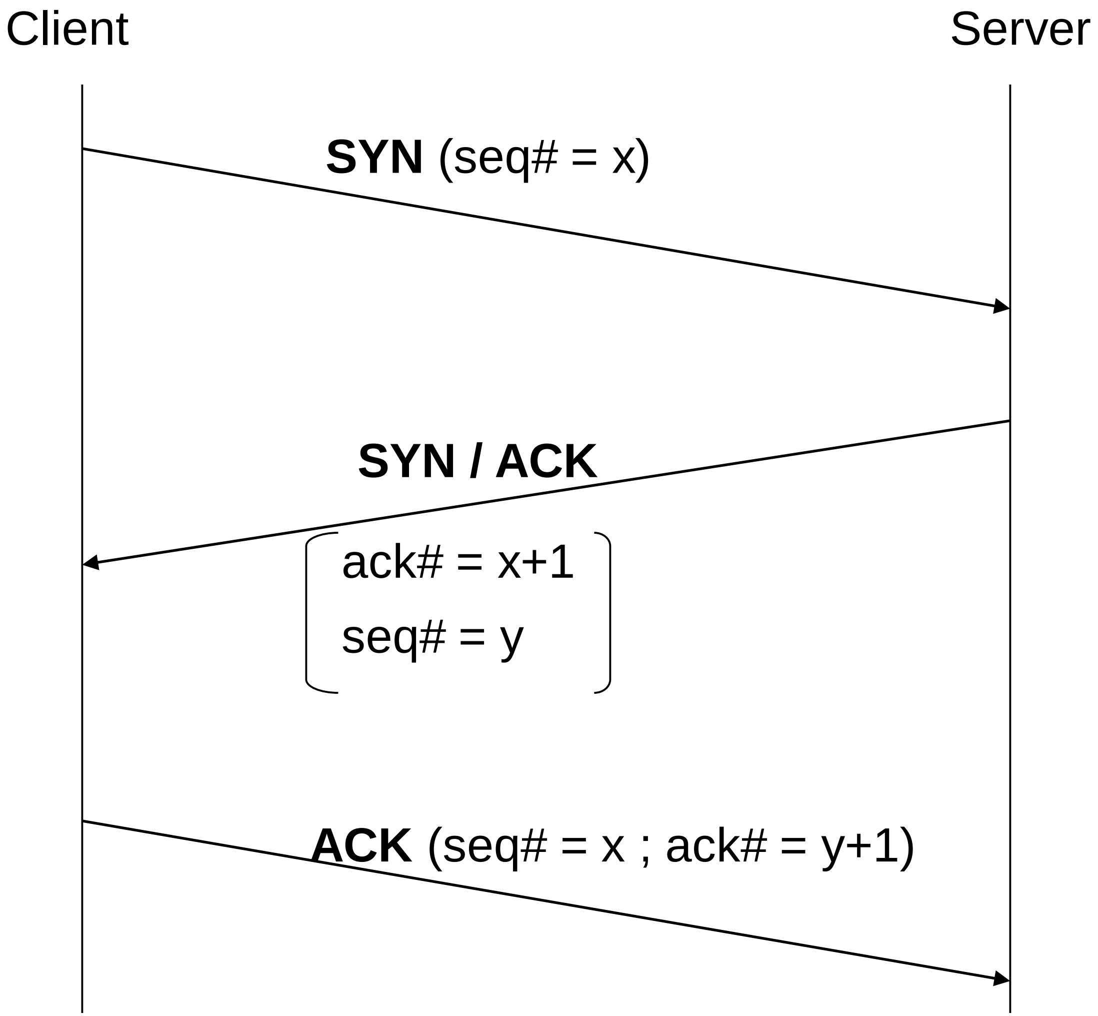
For each TCP connection each hosts keep two Sliding Windows,

- **Send sliding window**, and
- **Receive sliding window**

to make sure the correct transmission of Traffic between the send and receiver.

Each byte sent from the sender to the receiver has a unique Sequence Number associated with it.

THREE-WAY HANDSHAKING



TCP SESSION HIJACKING

TCP session hijacking is when a hacker takes over a **TCP session between two machines**.

Since most **authentication** only occurs at the start of a TCP session, this allows the hacker to gain access to a machine.

CATEGORIES OF TCP SESSION HIJACKING

Based on the anticipation of sequence numbers there are two types of TCP hijacking:

- Man-in-the-middle (**MITM**)
- Blind Hijack.

A. MAN-IN-THE-MIDDLE (**MITM**)

A hacker can also be "inline" between B and C using a sniffing[inhale] program to watch the sequence numbers and acknowledge numbers in the IP packets transmitted between B and C. And then hijack the connection. This is known as a "man-in-the-middle attack".

MAN IN THE MIDDLE ATTACK USING PACKET SNIFFERS

This technique involves using a packet sniffer to intercept the communication between client and the server. Packet sniffer comes in two categories:

- Active sniffers
- Passive sniffers.

PASSIVE SNIFFERS

Passive sniffers monitors and sniff packet from a network having same collision Domain i.e. network with a hub, as all packets are broadcasted on each port of hub.

ACTIVE SNIFFERS

One way of doing so is to change the default gateway of the client’s machine so that it will route its packets via the hijacker’s machine.

This can be done by ARP spoofing (i.e. by sending malicious ARP packets mapping its MAC address to the default gateways address so as to update the ARP cache on the client , to redirect the traffic to hijacker).

B. BLIND HIJACKING

If you are not able to sniff the packets and guess the correct sequence number expected by server, you have to implement "*Blind Session Hijacking*". You have to brute force 4 billion combinations of sequence number which will be an unreliable task.

3. IP SPOOFING

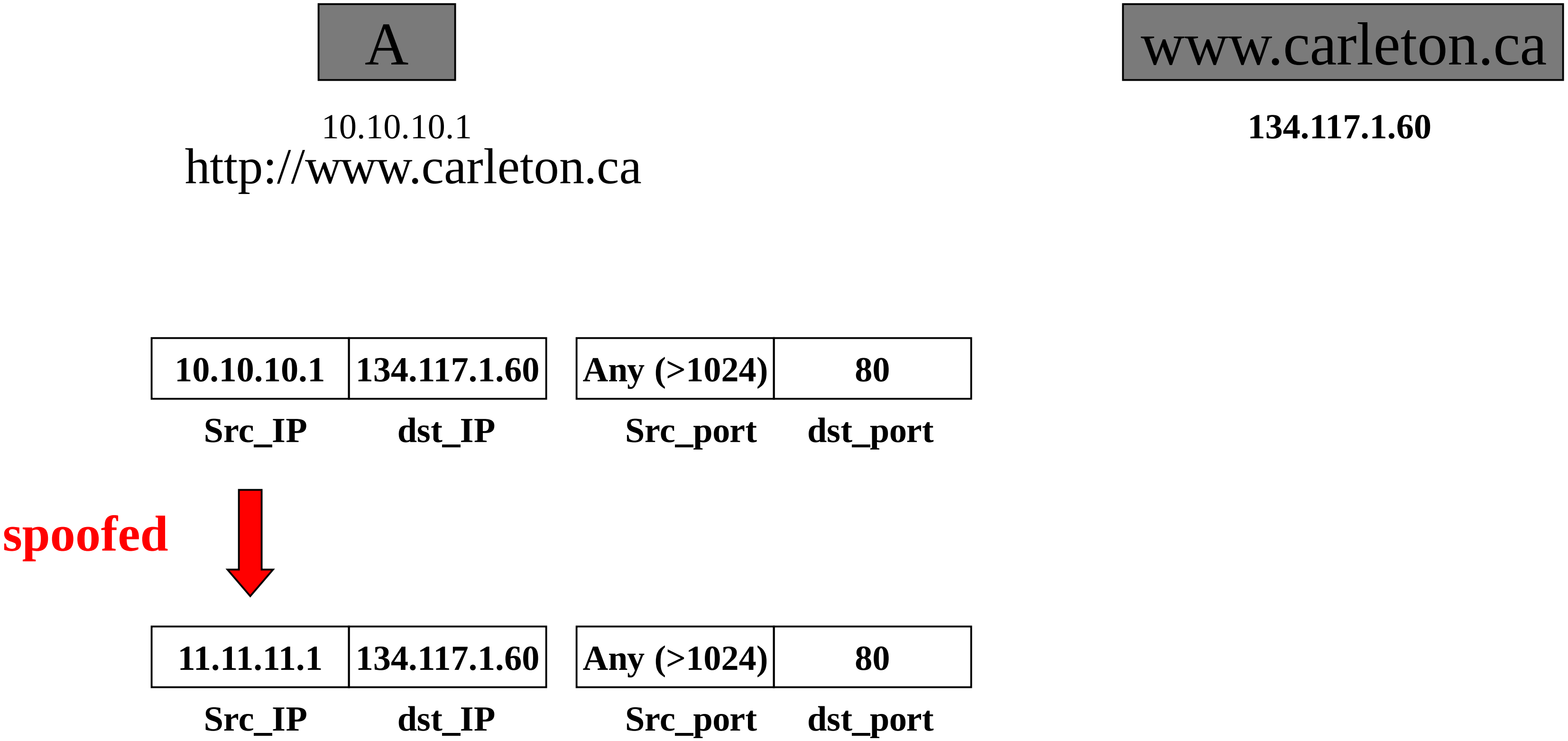
IP spoofing is a technique used to gain unauthorized access to computers, where by the attacker sends messages to a computer with a forging IP address indicating that the message is coming from a trusted host.

Attacker puts an internal, or trusted, IP address as its source. The access control device sees the IP address as trusted and lets it through.

IP SPOOFING

- IP spoofing occurs when a hacker inside or outside a Network impersonates the conversations of a trusted computer.
- Two general techniques are used during IP spoofing:
  - A hacker uses an IP address that is within the range of trusted IP addresses.
  - A hacker uses an authorized external IP address that is trusted.

Basic Concept of IP Spoofing



A

10.10.10.1

http://www.carleton.ca

www.carleton.ca

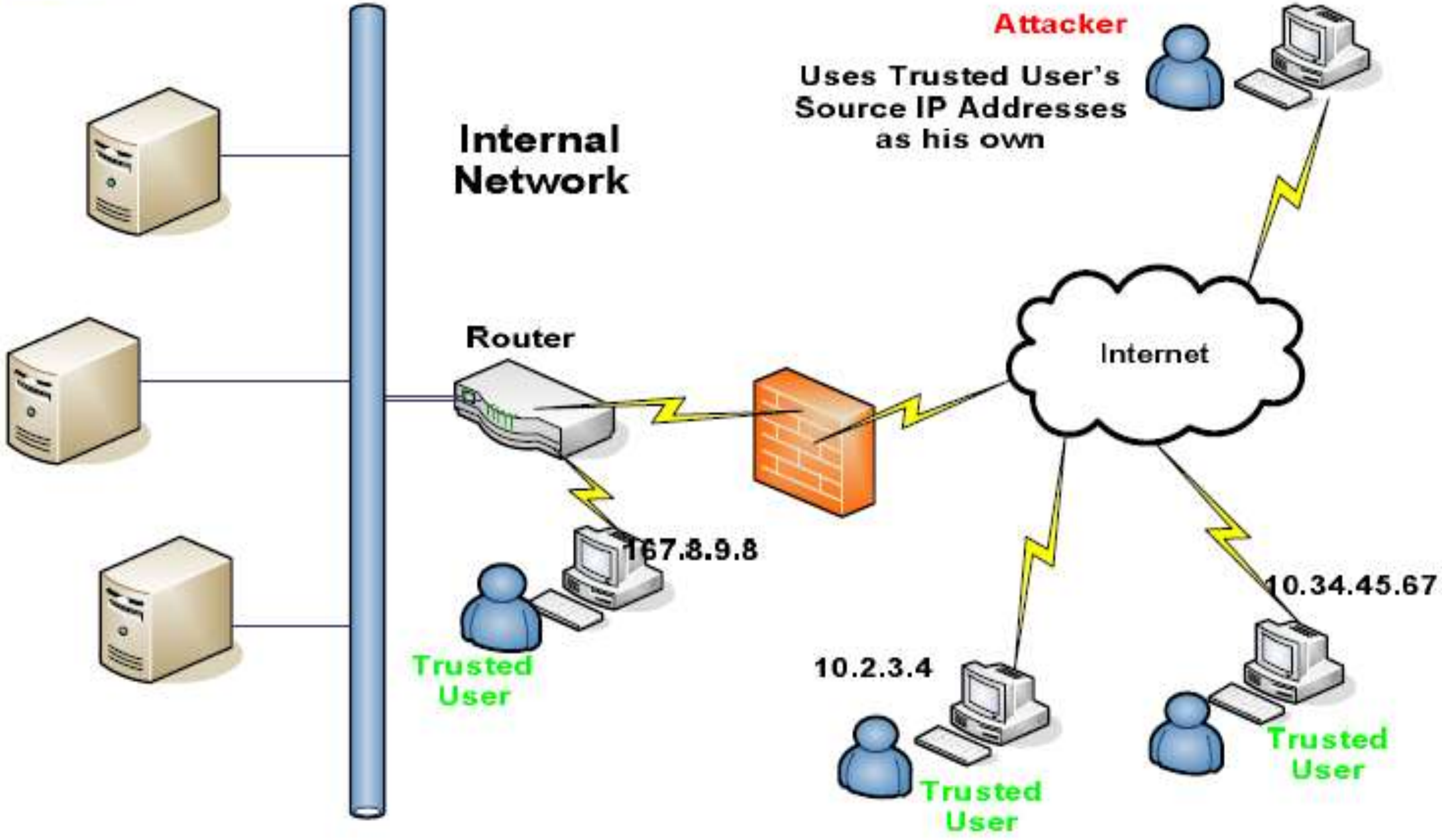
134.117.1.60

Src_IP	dst_IP	Src_port	dst_port
10.10.10.1	134.117.1.60	Any (>1024)	80

spoofed

Src_IP	dst_IP	Src_port	dst_port
11.11.11.1	134.117.1.60	Any (>1024)	80

IP SPOOFING


Attacker
Uses Trusted User's Source IP Addresses as his own
Internal Network
Router
Internet
167.8.9.8
Trusted User
10.34.45.67
10.2.3.4
Trusted User
Trusted User

SPOOFING ATTACKS:

There are a few variations on the types of attacks that using IP spoofing.

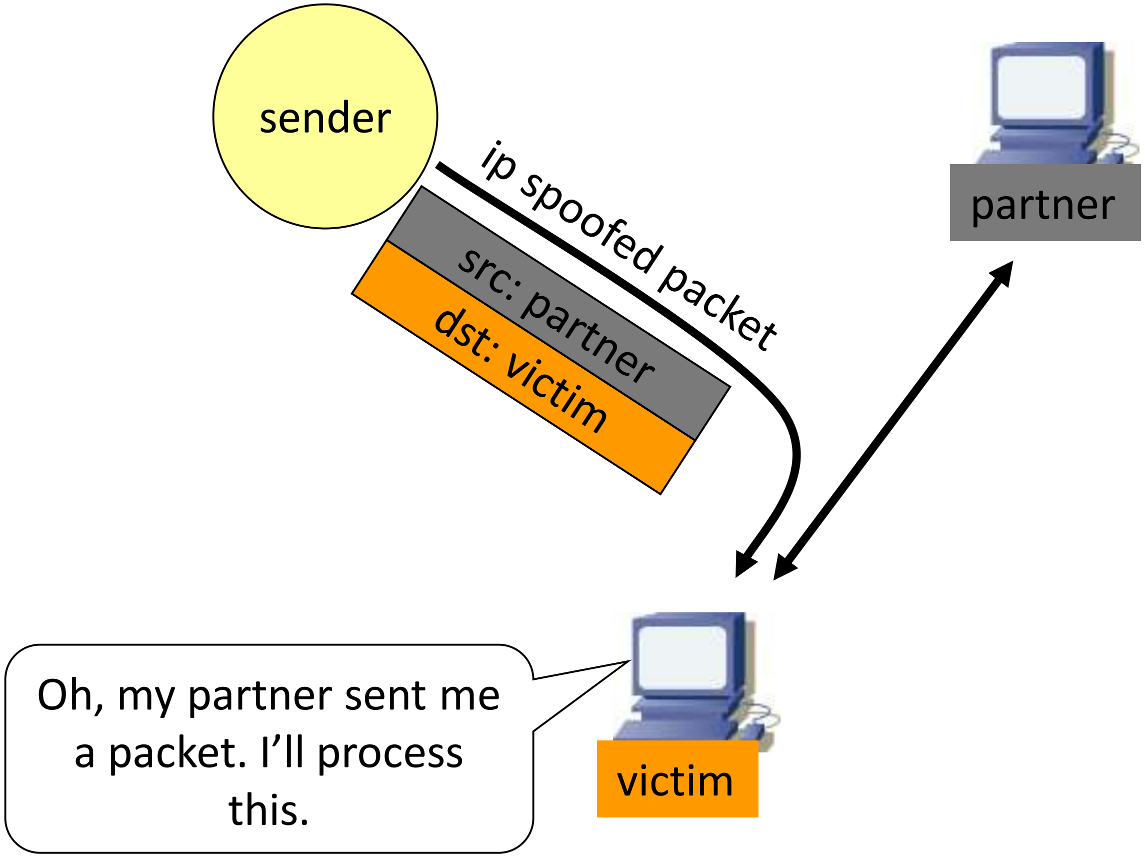
Spoofing is classified into :-

1.non-blind spoofing
This attack takes place when the attacker is on the same subnet as the target that could see sequence and acknowledgement of packets.

Using the spoofing to interfere with a connection that sends packets along your subnet.

SPOOFING ATTACKS:

Impersonation



SPOOFING ATTACKS:

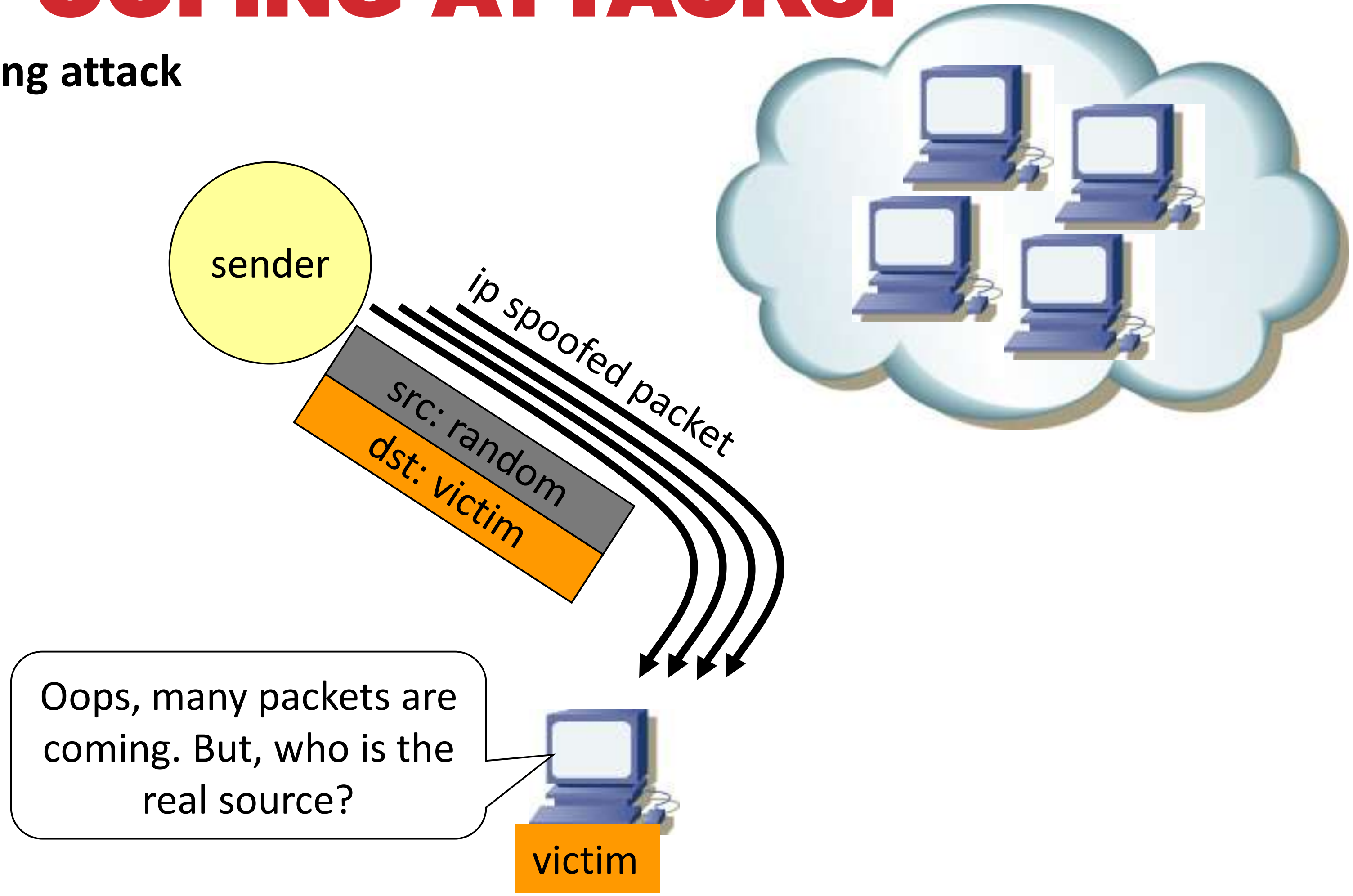
2. Blind spoofing

This attack may take place from outside where sequence and acknowledgement numbers are unreachable.

Attackers usually send several packets to the target machine in order to sample sequence numbers, which is doable in older days .

SPOOFING ATTACKS:

flooding attack



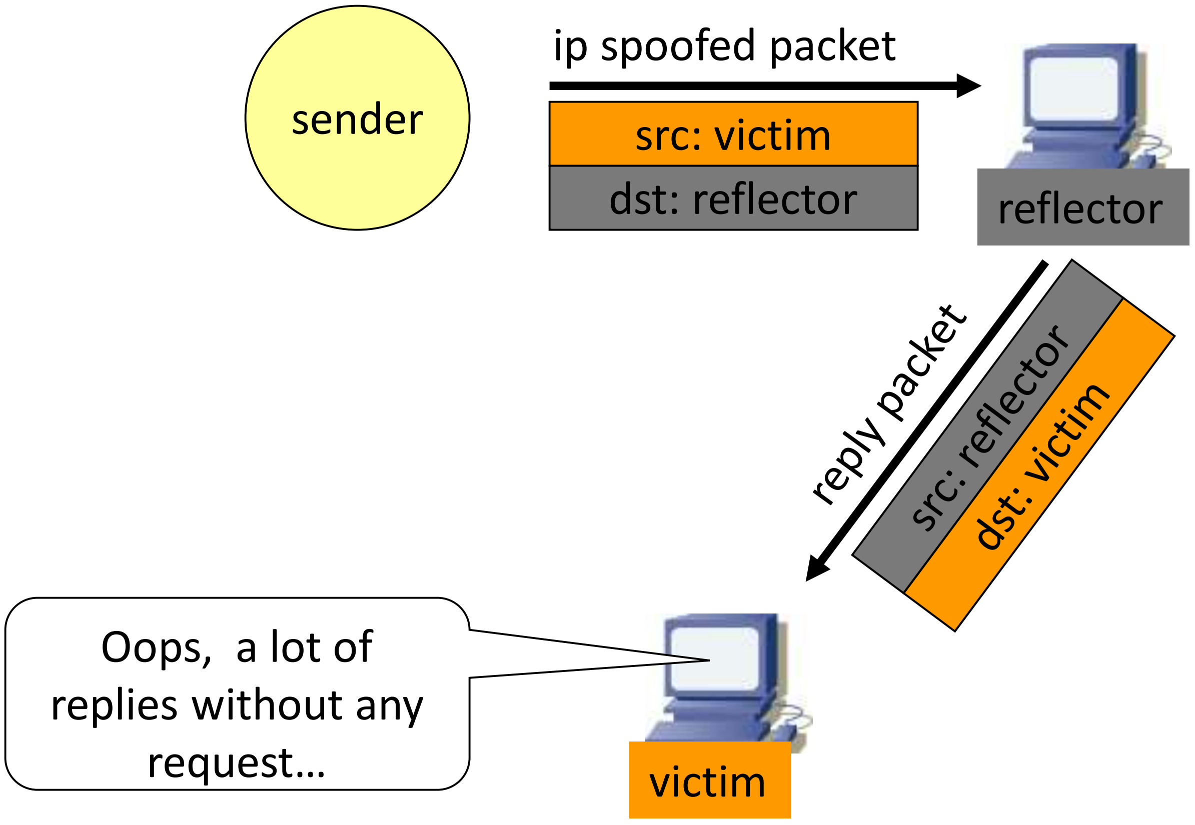
SPOOFING ATTACKS:

3.Man in the Middle Attack

This is also called connection hijacking. In this attacks, a malicious party intercepts a legitimate communication between two hosts to controls the flow of communication and to eliminate or alter the information sent by one of the original participants without their knowledge.

SPOOFING ATTACKS:

reflection



DETECTION OF IP SPOOFING:

1. If you monitor packets using network-monitoring software such as netlog, look for a packet on your external interface that has both its source and destination IP addresses in your local domain.

If you find one, you are currently under attack.

DETECTION OF IP SPOOFING:

2. Another way to detect IP spoofing is to compare the process accounting logs between systems on your internal network.

If the IP spoofing attack has succeeded on one of your systems, you may get a log entry on the victim machine showing a remote access;

On the apparent source machine, there will be no corresponding entry for initiating that remote access.

Source Address Validation :

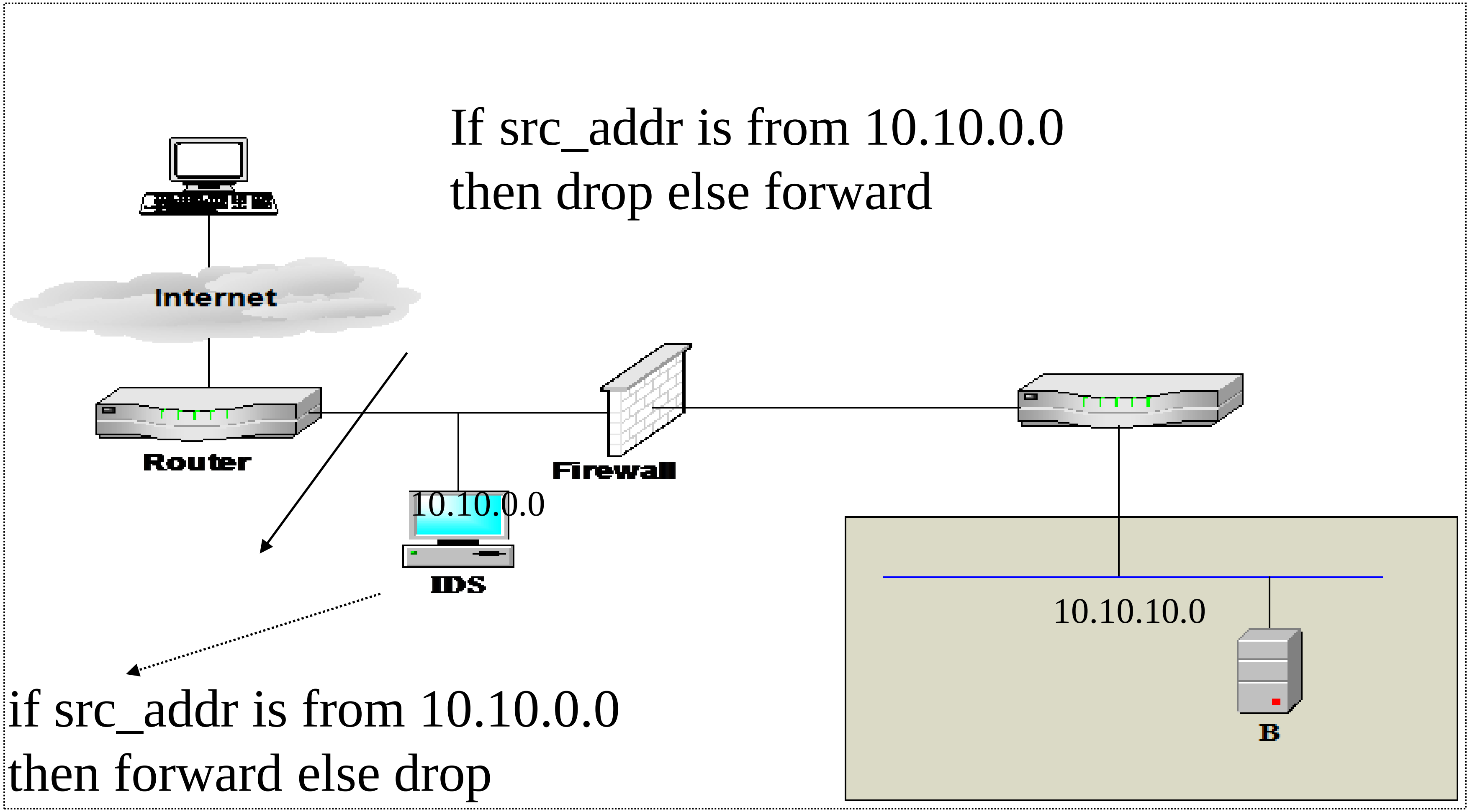
- **Check the source IP address of IP packets**
  - filter invalid source address
  - filter close to the packets origin as possible
  - filter precisely as possible
- **If no networks allow IP spoofing, we can eliminate these kinds of attacks**

PREVENTION IP SPOOFING FIREWAL

The best method of preventing the IP spoofing problem is to install a filtering router that restricts the input to your external interface (known as an input filter) by not allowing a packet through if it has a source address from your internal network.

In addition, you should filter outgoing packets that have a source address different from your internal network in order to prevent a source IP spoofing attack originating from your site.

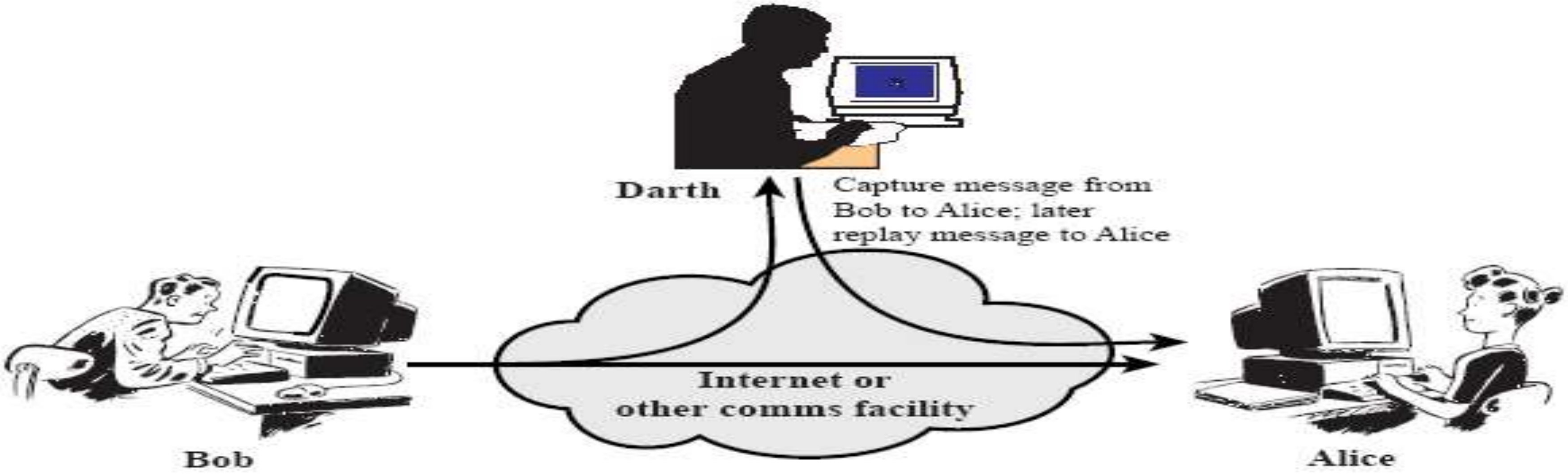
FILTERING



If src_addr is from 10.10.0.0
then drop else forward

if src_addr is from 10.10.0.0
then forward else drop

4. **Replay:** involves the re-use of captured data at a later time than originally intended in order to repeat some action of benefit to the attacker: for example, the capture and replay of an instruction to transfer funds from a bank account into one under the control of an attacker. This could be foiled by confirmation of the freshness of a message.


Darth
Capture message from Bob to Alice; later replay message to Alice
Internet or other comms facility
Bob
Alice

(b) Replay

5. WHAT IS SOCIAL ENGINEERING?

Social engineering is a Collection of techniques used to manipulate people into performing actions or divulging confidential information.

Social engineering is emerging as one of the biggest challenges, as there is no technical defense against the exploitation of human weaknesses.

- Easier than technical hacking Hard to detect and track.

GOALS OF A SOCIAL ENGINEER

Someone who tries to gain unauthorized access to your computer systems.

The mind of a Social Engineer make the victim want to give them the information they need.

It affects all kinds of systems.

RELATED CONCEPTS

Phishing

- Deceiving a user into using a fake web site

Identity theft

- pretend to be someone else, e.g., calling support while on a trip (with no way to authenticate the call)

Trojans - Deceiving a user into running a malicious program

SOCIAL ENGINEERING THREATS AND DEFENSES

Online

Telephone

Waste management

Personal approaches

- **Online threat**
    - Obtaining private information
    - Download Malware
    - Download Hackers software
- **Telephone Threat**
    - Request information.
    - Gain access to “free” telephone usage.
    - Gain access to communications network.
- ***Waste Management Threats***
    - Huge amount of information in the trash
    - Most of it does not seem to be a threat
    - **Company Confidential**. Shared all company confidential waste documents before disposal in any bin.
    - **Private**. Shared all private waste documents before disposal in any bin.

PERSONAL APPROACHES

The simplest and cheapest way for a hacker to get information is for them to ask for it directly.

- **Persuasion**. The most common forms of persuasion include flattery or name dropping.
- **Intimidation**. This approach may involve the impersonation of an authority figure to coerce/force a target to comply with a request.
- **Ingratiation**. This approach is usually a more long term ploy, in which a subordinate or peer coworker builds a relationship to gain trust and, eventually, information from a target.

ASSIGNMENT ONE

Write the defense of social engineering problem

6. Password Guessing

Passwords are the most widely used means of authentication

Humans have a tendency to choose relatively short and simple passwords

Thus, passwords bring along with them, the threat of dictionary attacks

Dictionary attacks

Dictionary attack means guessing the password and somehow check whether it is valid or not

If the rate of guessing and validating is reasonably high, the attacker stands a good chance of breaking the password

Two types: offline and online

Offline dictionary attacks

The attacker somehow gets access to some data which allow him to test passwords without any interaction with the server

Online dictionary attacks

For each password validation, interaction with the server is required

By attempting a login, it is always possible to test for password validity and hence, these attacks cannot be totally prevented

Common countermeasures like account locking and delayed response are not satisfactory

How are passwords broken – GUESSING AND CRACKING.

Guessing – **Find or guess a user’s identifier**

Create a list of possible passwords

Try each one

On success you are in, else keep trying

Hampered by unsuccessful login timeout – If (n) attempts are unsuccessful, lock the system for (m) minutes – n & m variable.

Most cracking is done off-line to avoid the timeout problem.

Major steps: **Find user ids**

Get encrypted or hashed passwords or password files

Create a list of trial passwords

Encrypt or hash the trial passwords

See if there is a match

Attacks: **Dictionary attacks (build a dictionary of passwords).**

Brute force (try all possible passwords).

Hybrid attacks (modified dictionary attack using altered dictionary words (party becomes).

This really is still guessing – these systems don’t break encryption!

PASSWORD CRACKING – HOW DO WE GET THE PASSWORDS?

If administrator – Dump the hashes to a file

▪If not administrator – Sniff the passwords off the network

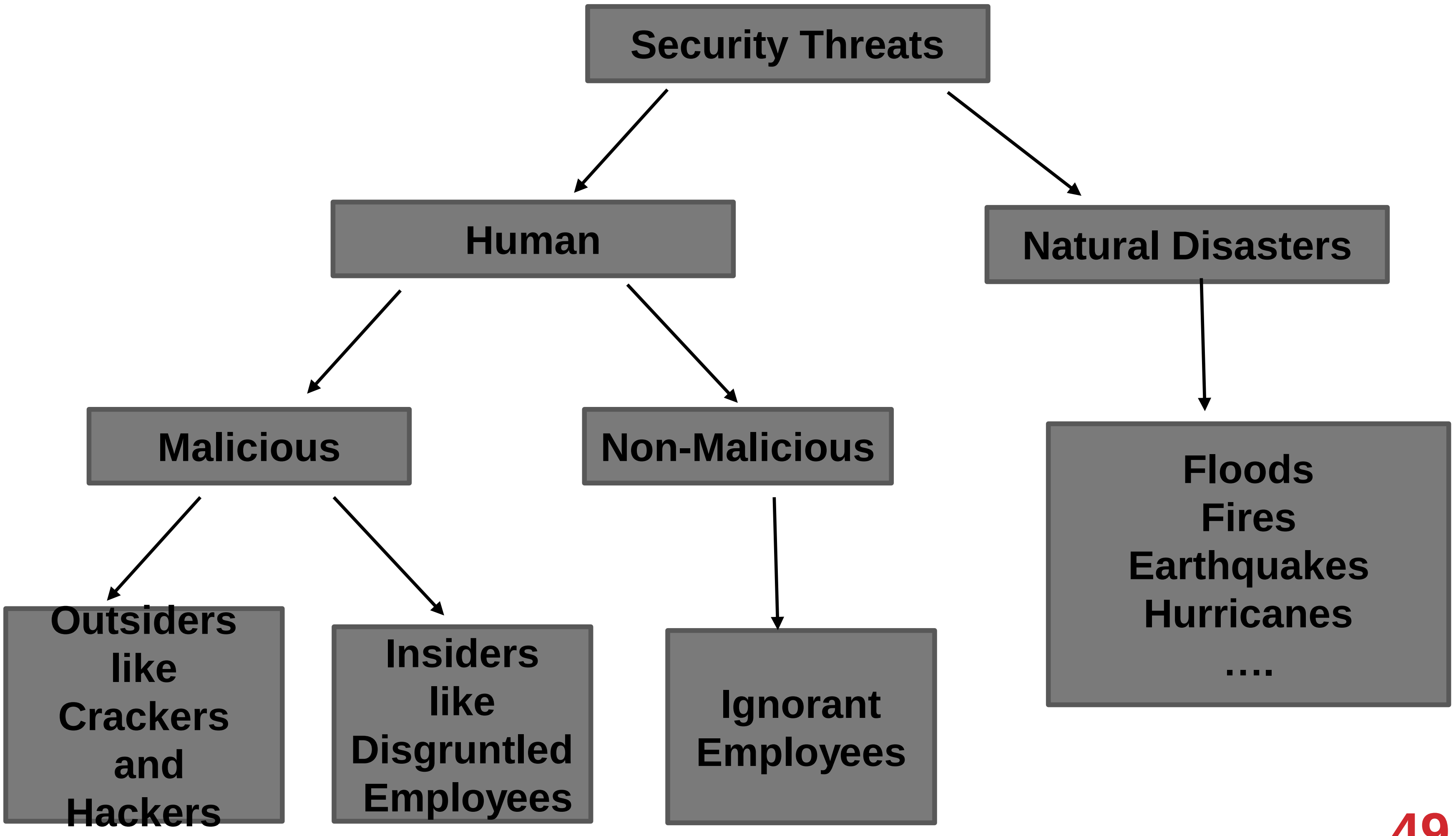
- Get administrator privilege
- Boot another OS and read the file
- Copy from backup
- Copy from emergency repair disk

Reminder to physically protect the system and all media.

Also to install patches that allow intrusions that result in root
or

administrator access.

SECURITY THREATS



Security Threats

Human

Natural Disasters

Malicious

Non-Malicious

Floods
Fires
Earthquakes
Hurricanes
….

Outsiders like Crackers and Hackers

Insiders like Disgruntled Employees

Ignorant Employees

CONTD.

1. **Natural Disaster:- Nobody can stop nature from taking its course.**

- Earthquakes, hurricane, floods, lightning, and fire can cause severe damage to computer systems.
- Information can be lost, downtime or loss of productivity can occur, and damage to hardware can disrupt other essential services.
- Few safeguards can be implemented against natural disasters.
  - The best approach is to have **disaster recovery plans and contingency plans** in place.
- Other threats such as **riot, wars, and terrorist attacks** could be included here.
- Although they are human-caused threats, they are classified as disastrous.

CONTD.

2. **Human Threats:-** ***Malicious*** **threats consist of inside attacks by disgruntled or malicious employees and outside attacks by non-employees just looking to harm and disrupt an organization.**

- Insiders are the most dangerous attackers, because they know many of the codes and security measures that are already in place .
- Insiders can plant viruses, Trojan horses, or worms, and they can browse through the file system.
- By browsing through a system, an insider can learn confidential information.
- Insiders can affect availability by overloading the system's processing or storage capacity, or by causing the system to crash.
- Disgruntled employees can create both **mischief** and **sabotage** on a computer system.

COMMON EXAMPLES OF COMPUTER-RELATED EMPLOYEE SABOTAGE INCLUDE:

i. Changing/Deleting Data

ii. Destroying data or programs with logic bombs

iii. Crashing systems

iv. Holding data hostage

v. Destroying hardware or facilities

vi. Entering data incorrectly.

- **Outsiders like hackers and crackers are also some of the security human threats.**

A. Hackers are people who either break in to systems for which they have no authorization or intentionally overstep their bounds on systems for which they don't have legitimate access.

- ➢ Hacker usually is a programmer who constantly seeks further knowledge, freely share what they have discovered, and never intentionally damage data.

CONTD.

B. **Crackers are people who breaks into or otherwise violates system integrity with malicious intent.**

- They destroy vital data or cause problems for their targets.
- Common methods for gaining access to a system include password cracking, exploiting known security weaknesses, network spoofing, and social engineering.
- Malicious attackers normally will have a specific goal, objective, or motive for an attack on a system:
  - Denial of Service
  - Stealing Information or hardware (Resources).

WAYS TO GAIN ACCESS OR DENY SERVICES

- **Malicious attackers can gain access or deny services in numerous ways. Here are some of them:-**

1. **Viruses:- Attackers can develop harmful codes, called viruses, and plant them into systems.**

   - Viruses can also be spread via e-mail and disks.

2. **Trojan horses:- are malicious programs or software code hidden inside what looks like a normal program.**

   - When a user runs the normal program, the hidden code runs as well.
   - It can then start deleting files and causing other damage to the computer.
   - Trojan horses are normally spread by e-mail attachments.
   - Trojan horses are a threat to both the **integrity** and **confidentiality** of information in the system.

CONTD.

3. **Worms:- are programs that copy themselves from one system to another over a network, without the assistance of a human being.**

   - ➢ Worms usually propagate themselves by transferring from computer to computer via e-mail.

4. **Password cracking:- is a technique attackers use to surreptitiously gain system access through another user's account.**

   - ➢ This is possible because users often select weak passwords.
   - ➢ The two major problems with passwords is:

     i. when they are easy to guess based on knowledge of the user (for example, wife's maiden name) and

     ii. when they are susceptible to dictionary attacks (that is, using a dictionary as the source of guesses).

Next slide