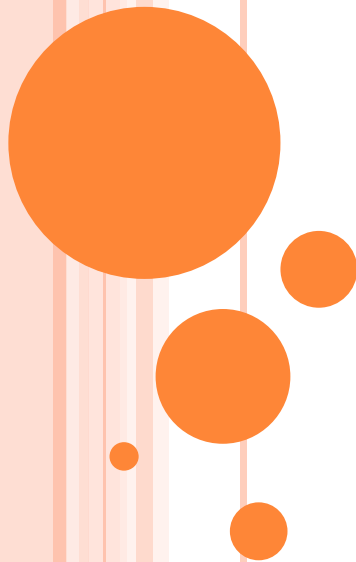


**GOVERNMENT POLYTECHNIC  
AHMEDABAD  
PROGRAM: DIPLOMA IN COMPUTER  
ENGG  
COMPUTER AND NETWORK SECURITY  
(3350704-C304)**

**UNIT\_1**

**Introduction and Security Threats**



# TEACHING AND EXAMINATION SCHEME

Teaching Scheme (In Hours)			Total Credits (L+T+P)	Examination Scheme				
				Theory Marks		Practical Marks		Total Marks
L	T	P	C	ESE	PA	ESE	PA	200
3	0	4	7	70	30	40	60	



# UNIT-1 (SYLLABUS)

<b>Unit – I</b> <b>Introduction</b> <b>and Security</b> <b>Threats:</b>	1a. List and discuss various security terms, recent trends in computer security. 1b. Describe various types of threats that exist for computers and networks.	1.1 Threats to security : Viruses and Worms, Intruders, Insiders, Criminal organizations, Terrorists, Information warfare
	1c. Describe simple steps to take minimize the possibility if an attack on a system.	1.2 Avenues of Attack, steps in attack
	1d. Define Security Basics.	1.3 Security Basics – Confidentiality, Integrity, Availability
	1e. Describe various types of computer and network attacks 1f. Identify various types of malicious software that exists.	1.4 Types of attack: Denial of service (DOS), backdoors and trapdoors, sniffing, spoofing, man in the middle, replay, TCP/IP Hacking, Phishing attacks, Distributed DOS, SQL Injection. Malware : Viruses, Logic bombs



## NEED FOR SECURITY

- Information is a strategic resource
- A significant portion of organizational budget is spent on managing information
- Have several security related objectives
  - Confidentiality (secrecy) - protect info value
  - Integrity - protect info accuracy
  - Availability - ensure info delivery



# INFORMATION SECURITY

- **Information Security** is not only about securing information from unauthorized access. Information Security is basically the practice of preventing unauthorized access , use, disclosure, disruption, modification, inspection, recording or destruction of information.
- Information can be physical or electronic one.
- like Your details or we can say your profile on social media, your data in mobile phone, your biometrics etc.



## CONT..

- ***systems security*** refers to the processes and methodologies involved with keeping information confidential, available, and assuring its integrity.
- It also refers to: Access controls, which prevent unauthorized personnel from entering or accessing a system.



# WHAT IS AN INFORMATION SECURITY THREAT?

- A threat is possible careless mistake that might be exploit a vulnerability to breach security and thus cause possible harm.
- Threats can be:
  - Natural or Human
  - Deliberate or Accidental



# VIRUS



- Virus is a piece of software that can ‘infect’ other programs by modifying them; the modification include copy of the virus program, which can then go on to infect other programs.
- Once virus executing it can perform any function , such as erasing files and programs.





# TYPES OF VIRUS

- Stealth virus-
  - Form of virus explicitly designed to hide itself from detection by antivirus software.
- Boot sector-
  - Infects master boot record or boot record and spread when booted from the disk containing virus.
- Parasitic-
  - attaches itself to executable files and replicates when infected program is executed, find other executable files to infect.
- Memory resident-
  - stay in M/M as resident system program.
  - This type of virus attaches itself to an area of the m/m and then infects every executable program that is executed.



## CONT..

- Polymorphic virus

- Mutates with every infection, making detection by the signature of the virus impossible

- Metamorphic virus

- Mutates with every infection, rewriting itself completely at each iteration changing behavior and/or appearance, increasing the difficulty of detection

```
mov eax, 5  
add eax, ebx  
call [eax]
```

Original virus instructions

```
mov eax, 5  
push ecx  
pop ecx  
add eax, ebx  
swap eax, ebx  
swap ebx, eax  
call [eax]  
nop
```

Metamorphic version of the virus



# WORMS

- worm is similar to a virus by design and is considered to be a sub-class of a virus.
- Worms spread from computer to computer, but unlike a virus, it has the capability to travel without any human action.
- A computer worm is a standalone malware computer program that replicates itself in order to spread to other computers.
- Worms almost always cause at least some harm to the network, even if only by consuming bandwidth, whereas viruses almost always corrupt or modify files on a targeted computer.



## CONT..

### Virus

- Attaches itself to OS or the programs
- Need user action to abet their propagation.
- Damages caused is mostly local to the machine
- Spread quite slowly

### Worm

- Do not Attaches itself to OS
- Self propagates across a network exploiting security in widely used services.
- It harms the network and consumes n/w bandwidth.
- Spread much more rapidly Ex. SQL Slammer worm 75,000 victims within ten minutes.



# INSIDERS

- A malicious insider threat to an organization is a current or former employee, contractor, or other business partner who has or had authorized access to an organization's network, system, or data.
- He is intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems.
- Insider attacks are among the most difficult to detect and prevent.
- Employees already have access and knowledge about the structure and content of corporate databases.



# TERRORISTS

- The terrorists use cyberspace to cause uncertainty.
- They, for their own reasons, are struggling against state authorities and governments and use all available means to achieve their own aim.
- Cyber attacks occur in two forms, one used to attack data, and others focused on control systems.
- The attacks focused on the control systems are used to disable or manipulate the physical infrastructure.



# CRIMINAL ORGANIZATION

- Organized crime is a category of transnational, national, or local groupings of highly centralized enterprises run by criminals who intend to engage in illegal activity, most commonly for money and profit.
- Some criminal organizations, such as terrorist groups, are politically motivated.



## INTRUDER

- An Intruder is a person who attempts to gain unauthorized access to a system, to damage that system, or to disturb data.
- significant issue for networked systems is hostile(dislike) or unwanted access, trespass(enter without permission) being unauthorized login or by software such as a virus, worm, or Trojan horse.
- either via network or local or remote user





## TYPES OF INTRUDERS:

- Masquerader-
  - An individual who is not authorized to use the computer (outsider) –
- Misfeasor-
  - authentic user doing unauthorized actions. A legitimate user who accesses unauthorized data, programs, or resources (insider)
- Clandestine(confidential)user-
  - An individual who takeover supervisory control of the system and uses this control to to suppress audit collection



# INFORMATION WARFARE

- Information warfare is the manipulation of information trusted by a target without the target's awareness so that the target will make decisions against their interest.
- IW conducted against the information and information processing equipment used by an adversary(opponent).
- This is much more complicated subject, because *information not only may be the target of an adversary, but also may be used as a weapon.*
- *Highly structured threat.*
- *Longer period of preparation, financial backing, large group of hackers.*



# AVENUE OF ATTACK/STEPS IN ATTACK

- Two reasons for attack:
  - 1)Specifically targeted by the attacker
  - 2)Opportunistic target



## STEPS:

- Reconnaissance (also known as profiling)
- Scanning
- Researching vulnerabilities
- Perform attack



# STEPS IN ATTACK

- Step 1: Information gathering: The attacker will gather as much information about organization as possible.
- Step 2: Determination of target system: Then determine what target systems are available and active.
- Step 3: Find vulnerability & suitable tools: To perform a port scan which gives indication of which services are running on target machine.
- Step 4: Attack to the target system: Actually attacking the target system.



# SECURITY BASICS

- Confidentiality
- Integrity
- Availability

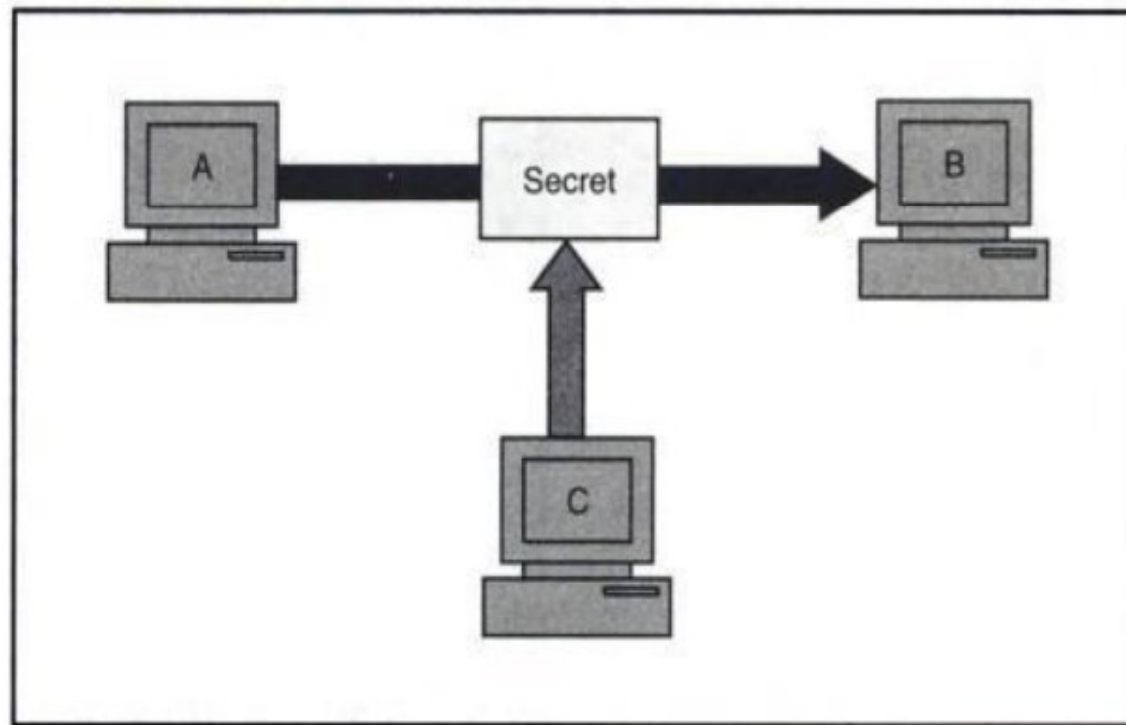


# DATA CONFIDENTIALITY

- When we talk about confidentiality of information, we are talking about protecting the information from disclosure to unauthorized parties (wrong Person).
- Information has value, especially in today's world. Bank account statements, personal information, credit card numbers, trade secrets, government documents.
- Everyone has information they wish to keep a secret. Protecting such information is a very major part of information security.



tiality of a message is shown in Fig. 1.2. Here, the user of computer A sends a message to the user of computer B. (Actually, from here onwards, we shall use the term A to mean the user A, B to mean user B etc., although we shall just show the computers of user A, B, etc.). Another user C gets access to this message, which is not desired, and therefore, defeats the purpose of confidentiality. Example of this could be a confidential email message sent by A to B, which is accessed by C without the permission or knowledge of A and B. This type of attack is called as **interception**.



**Fig. 1.2** *Loss of confidentiality*

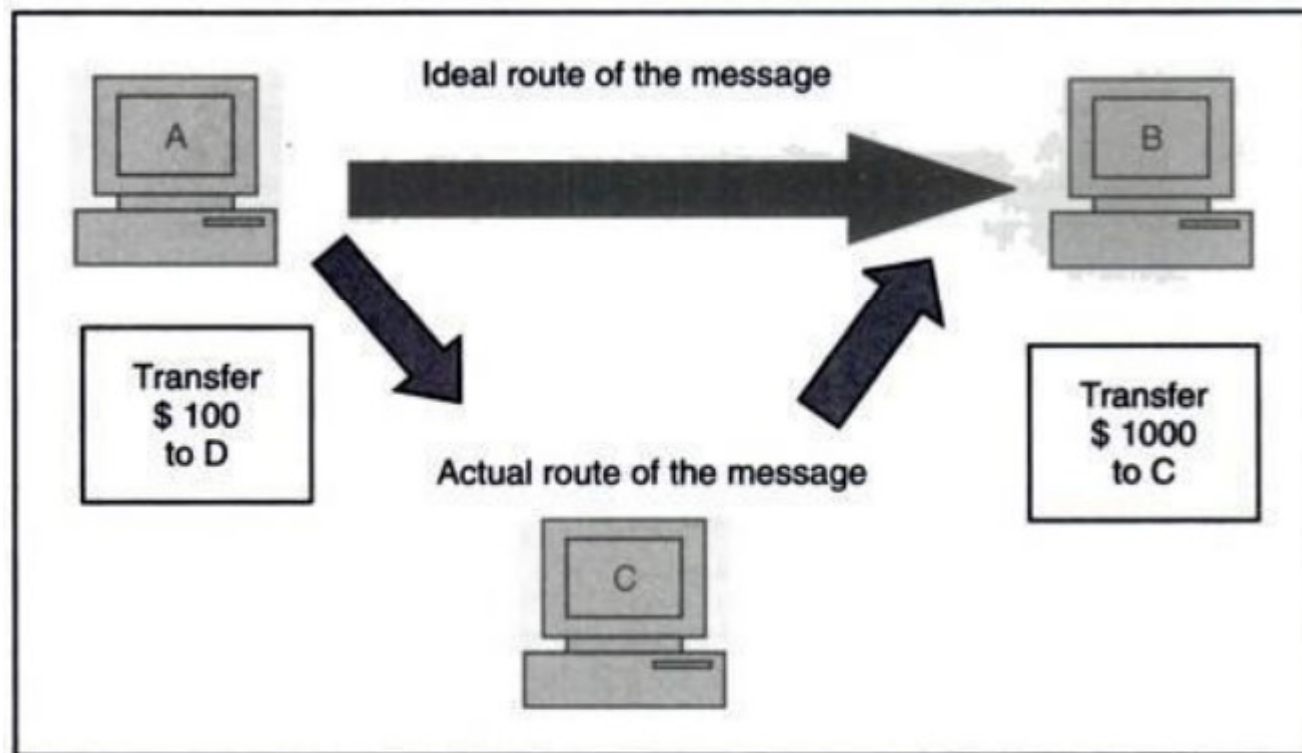


# INTEGRITY

- Integrity of information refers to protecting information from being modified by unauthorized parties.
- Information only has value if it is correct. Information that has been tampered with could prove costly.
- For example, if you were sending an online money transfer for \$100, but the information was tampered in such a way that you actually sent \$10,000, it could prove to be very costly for you.



CONT..




**Fig. 1.4** *Loss of integrity*



# CONT..

you write a cheque for \$100 to pay for the goods bought from the US. However, when you see your next account statement, you are startled to see that the cheque resulted in a payment of \$1000! This is the case for loss of message integrity. Conceptually, this is shown in Fig. 1.4. Here, user C tampers with a message originally sent by user A, which is actually destined for user B. User C somehow manages 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 also does not know about this change. This type of attack is called as **modification**.

*Note*  Modification causes loss of message integrity.



# AVAILABILITY

- Availability of information refers to ensuring that authorized parties are able to access the information when needed.
- Information only has value if the right people can access it at the right times.
- How does one ensure data availability? Backup is key. Regularly doing off-site backups can limit the damage caused by damage to hard drives or natural disasters.



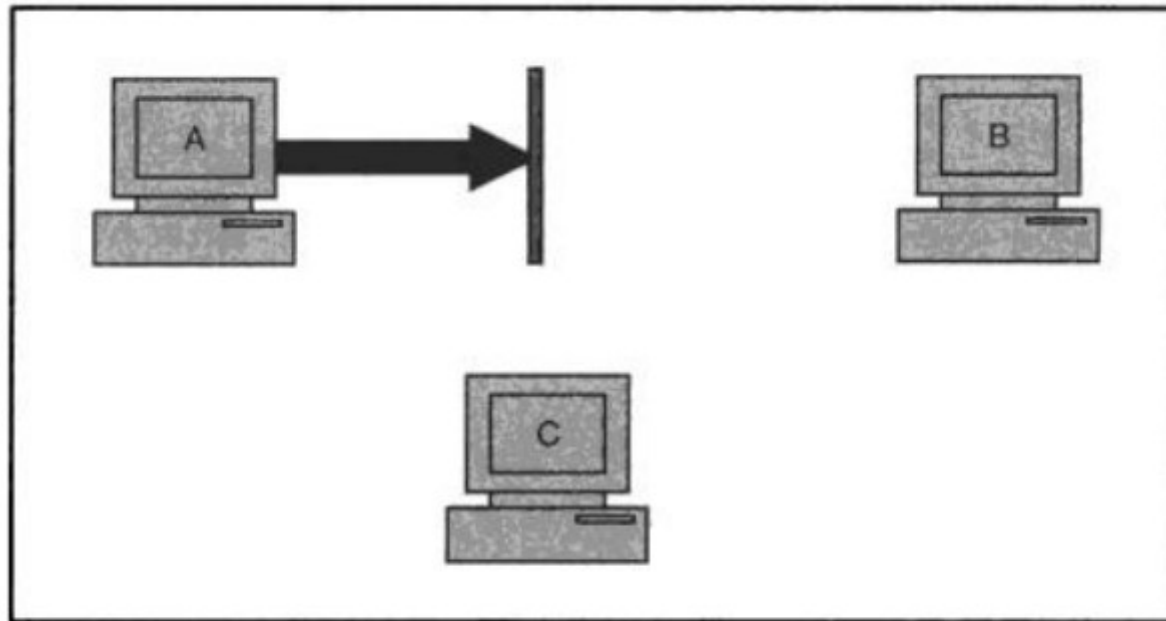
# CONT..

## **1.4.6 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 another unauthorized user C, an authorized user A may not be able to contact a server computer B, as shown in Fig. 1.5. This would defeat the principle of availability. Such an attack is called as **interruption**.



CONT...



**Fig. 1.5** *Attack on availability*



### 1.4.2 Authentication

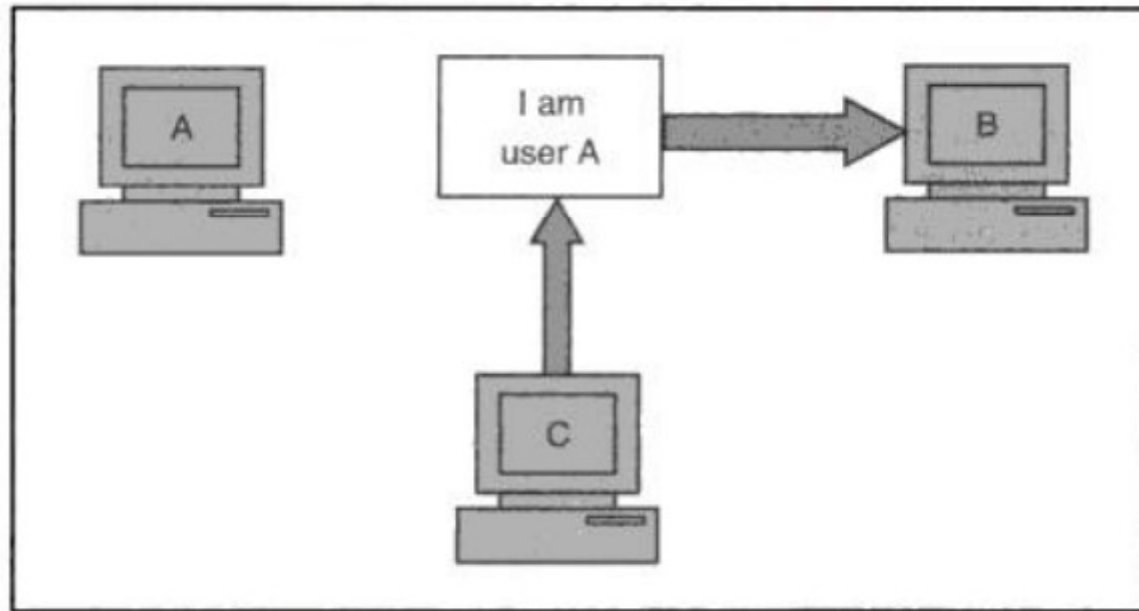
*Authentication* mechanisms help establish proof of identities. The authentication process ensures that the origin of an electronic message or document is correctly identified. For instance, suppose that user C sends an electronic document over the Internet to user B. However, the trouble is that user 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

Copyrighted material

## 6 ■ Cryptography and Network Security

A? A real life example of this could be the case of a user C, posing as user A, sending a funds transfer request (from A's account to C's account) to bank B. The bank might happily transfer the funds from A's account to C's account—after all, it would think that user A has requested for the funds transfer! This concept is shown in Fig. 1.3. This type of attack is called as **fabrication**.

CONT..



**Fig. 1.3** *Absence of authentication*






# CONT..

## 1.4.4 Non-repudiation

There are situations where a user sends a message, and later on refuses that she had sent that message. For instance, 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 repudiates, or denies,

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

**Note** 

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



### 1.4.5 Access Control

The principle of *access control* determines *who* should be able to access *what*. For instance, we should be able to specify that user A can view the records in a database, but cannot update them. However, 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 and rule management*. Role management concentrates on the user side (which user can do what), whereas rule management focuses on the resources side (which resource is accessible, and under what circumstances). Based on the decisions taken here, an access control matrix is prepared, which lists the users against a list of items they can access (e.g. it can say that user A can write to file X, but can only update files Y and Z). **An Access Control List (ACL)** is a subset of an access control matrix.



Access control specifies and controls who can access what.



## 1.4 TYPES OF ATTACK

- Denial of service (DOS),
- backdoors and trapdoors,
- sniffing,
- spoofing,
- man in the middle, replay,
- TCP/IP Hacking,
- Phishing attacks,
- Distributed DOS,
- SQL Injection
- Malware : Viruses, Logic bombs



## *DENIAL-OF-SERVICE ATTACK*

- DoS attack, denial-of-service attack, is an explicit attempt to make a computer resource unavailable by either injecting a computer virus or flooding the network with useless traffic.
- It attempts to "flood" a network, thereby preventing legitimate network traffic
- It attempts to disrupt connections between two machines, thereby preventing access to a service
- It attempts to prevent a particular individual from accessing a service
- It attempts to disrupt service to a specific system or person



# PREVENTING DENIAL OF SERVICE (SYN FLOOD)

- DoS is caused by asymmetric state allocation
  - If server opens new state for each connection attempt, attacker can initiate many connections from bogus or forged IP addresses
- Cookies allow server to remain stateless until client produces:
  - Server state (IP addresses and ports) stored in a cookie and originally sent to client
- When client responds, cookie is verified




# DoS AND DDoS

- DoS:
  - source of attack small # of nodes
  - source IP typically spoofed
- DDoS
  - From thousands of nodes
  - IP addresses often not spoofed

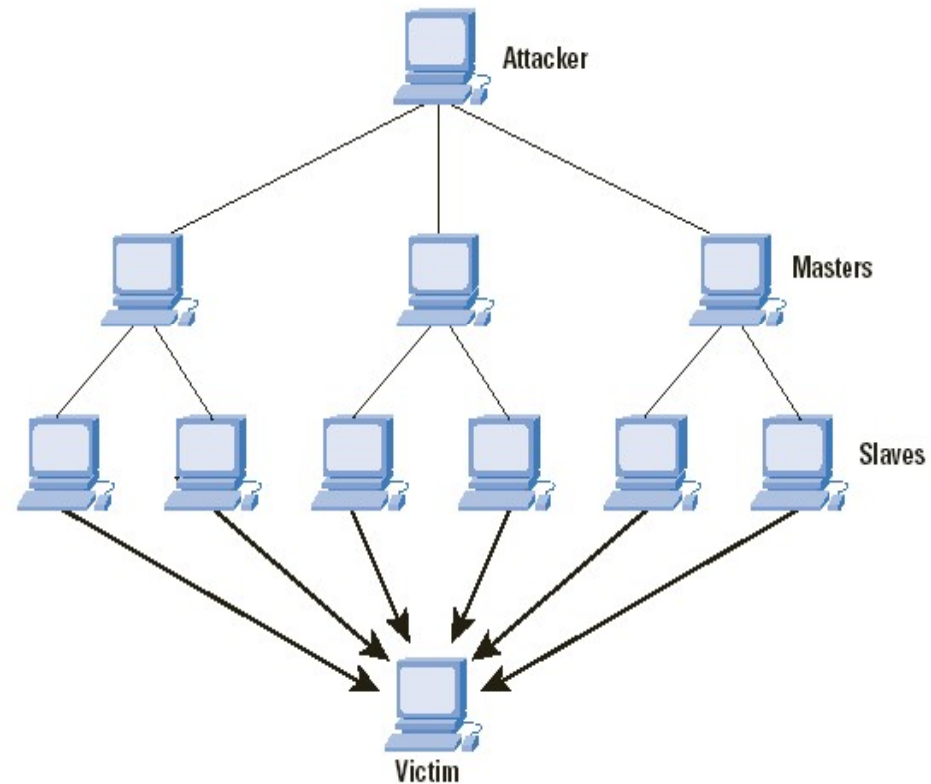


# DDoS ATTACKS

- In a typical DDoS attack, the army of the attacker consists of *master zombies* and *slave zombies*.
  - The hosts of both categories are compromised machines that have arisen during the scanning process and are infected by malicious code.
  - The attacker coordinates and orders master zombies and they, in turn, coordinate and trigger slave zombies.
  - The attacker sends an attack command to master zombies and activates all attack processes on those machines, which are in hibernation, waiting for the appropriate command to wake up and start attacking.
  - Then, master zombies, through those processes, send attack commands to slave zombies, ordering them to mount a DDoS attack against the victim.
- 

## CONTINUE...

In that way, the agent machines (slave zombies) begin to send a large volume of packets to the victim, flooding its system with useless load and exhausting its resources.





# BACKDOORS

- This can have two different meanings.
- 1) During the development of a complicated operating system or application, programmers add backdoors or maintenance hooks. These back doors allow them to examine operations inside the code while the program is running.
  - 2) The second type of back door refers to gaining access to a network and inserting a program or utility that creates an entrance for an attacker.
  - The program may allow a certain user to log in without a password or gain administrative privileges.
  - A number of tools exist to create a back door attack such as, Back Orifice, Subseven, NetBus, and NetDevil.



# TRAPDOORS

- A trap door is a secret entry point into a program that allows someone that is aware of the trap door to gain access without going through the usual security access procedures.
- It is difficult to implement operating system controls for trap doors.

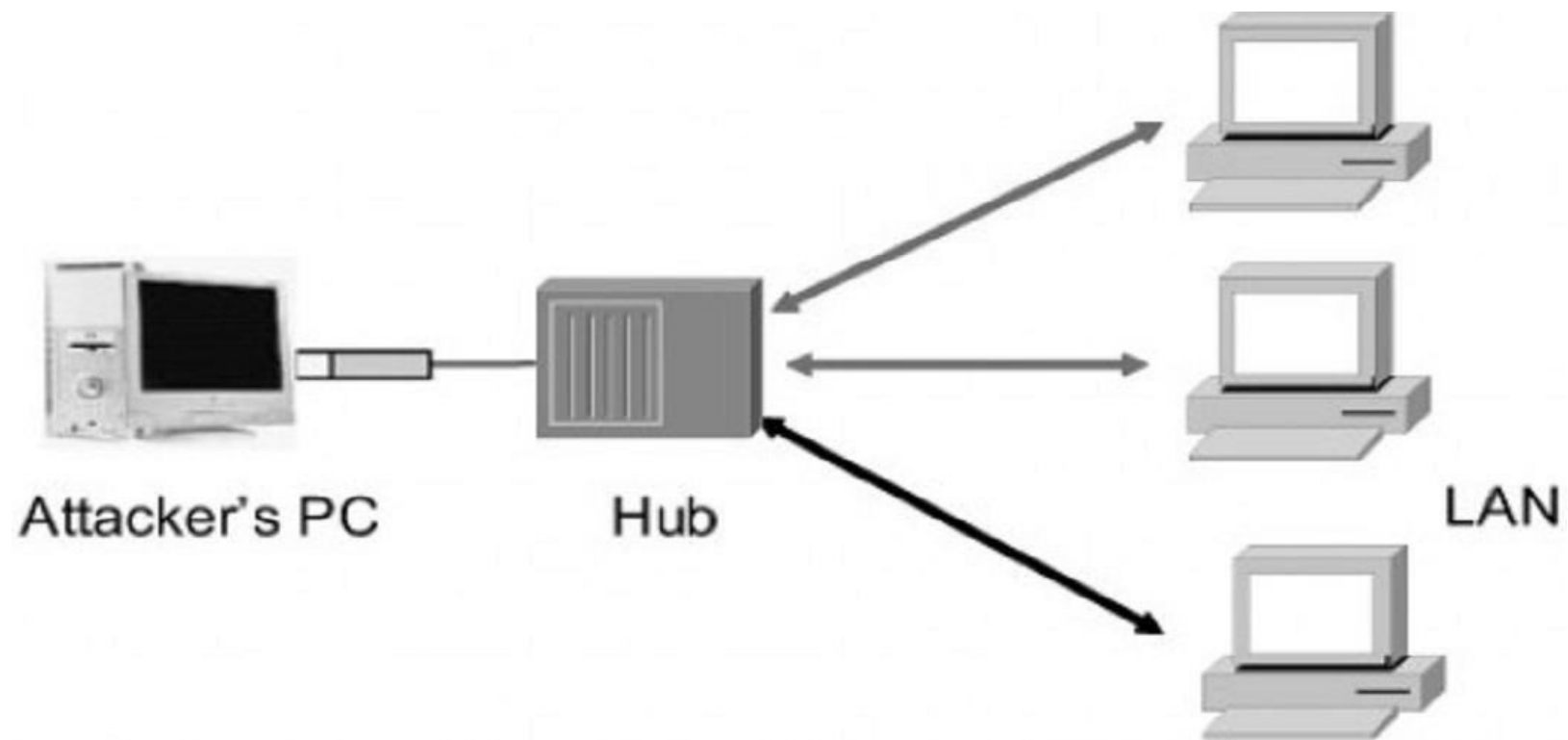


## *NETWORK SNIFFING (PACKET SNIFFING)*

- A sniffer is an application that can capture network packets.
- Sniffers are also known as network protocol analyzers.
- While protocol analyzers are really network troubleshooting tools, they are also used by hackers for hacking network.



CONT...

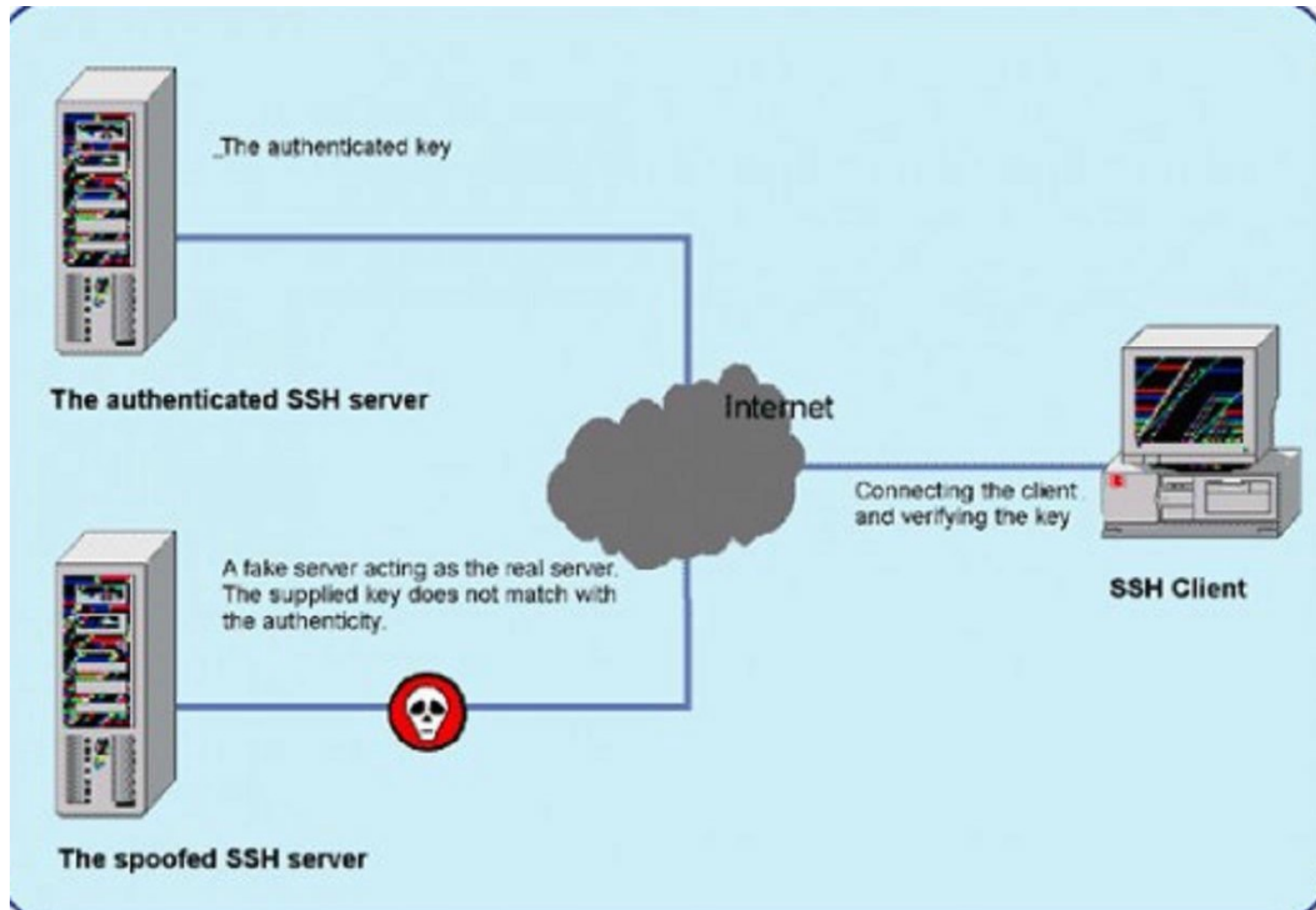


## *SPOOFING ATTACK*

- In a spoof attack, the hacker modifies the source address of the packets he or she is sending so that they appear to be coming from someone else. This may be an attempt to bypass your firewall rules.
- Any internet connected device necessarily sends IP datagram into the network. Such internet data packets carry the sender's IP address as well as data.
- If the attacker obtains control over the software running on a network device, they can then easily modify the device's protocols to place an arbitrary IP address into the data packet's source address field. This is known as **IP spoofing**.



# CONT...

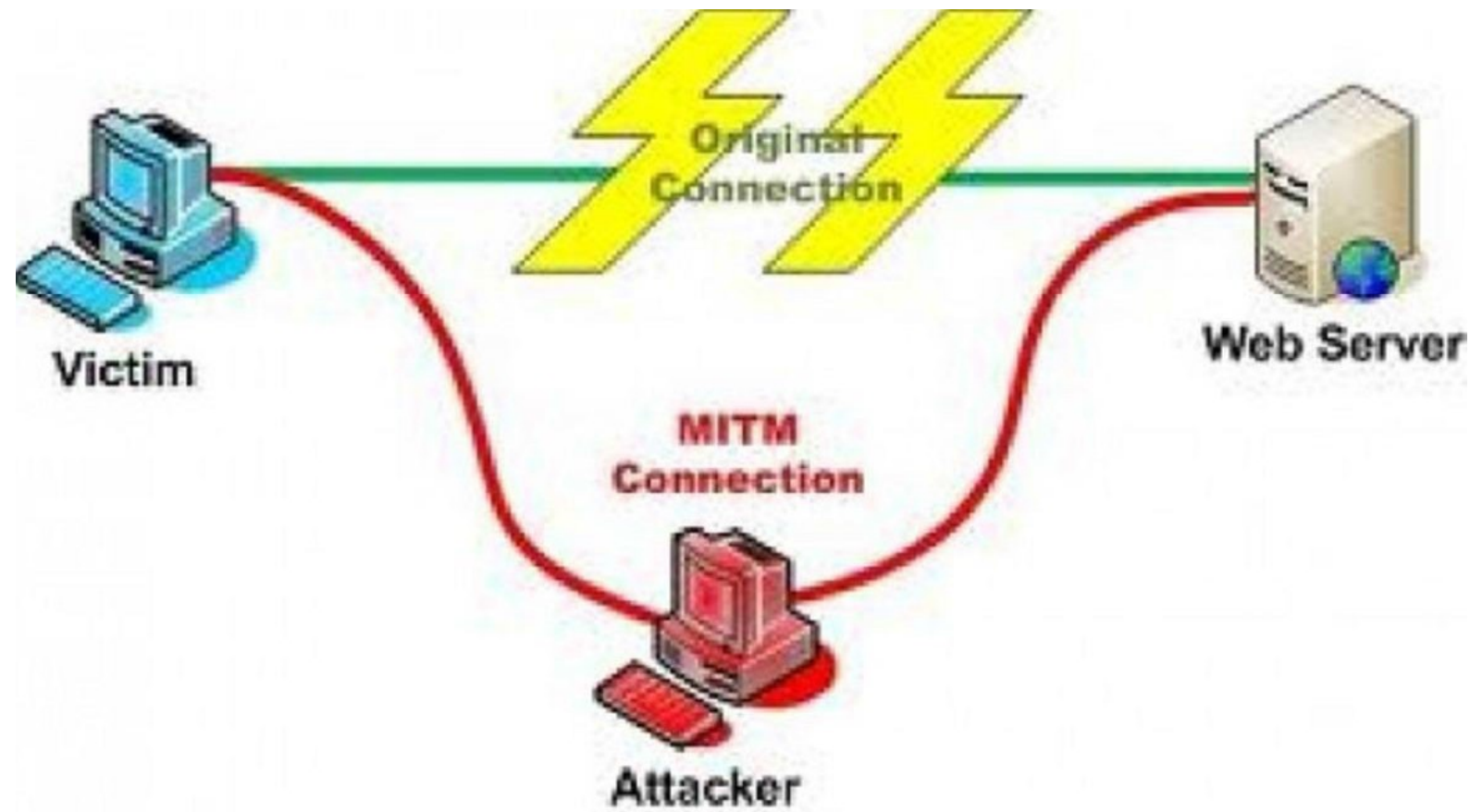


# *MAN-IN-THE-MIDDLE ATTACK*

- As the name indicates, a man-in-the-middle attack occurs when someone between you and the person with whom you are communicating is actively monitoring, capturing, and controlling your communication transparently.
- This type of attack is also an access attack, but it can be used as the starting point of a modification attack.
- This involves placing a software between a server and the user that neither the server administrators nor the user are aware of.
- This software intercepts data and then send the information to the server as if nothing is wrong.
- The server responds back to the software, thinking it's communicating with the legitimate client.
- The attacking software continues sending information to the server and so forth.



CONT...





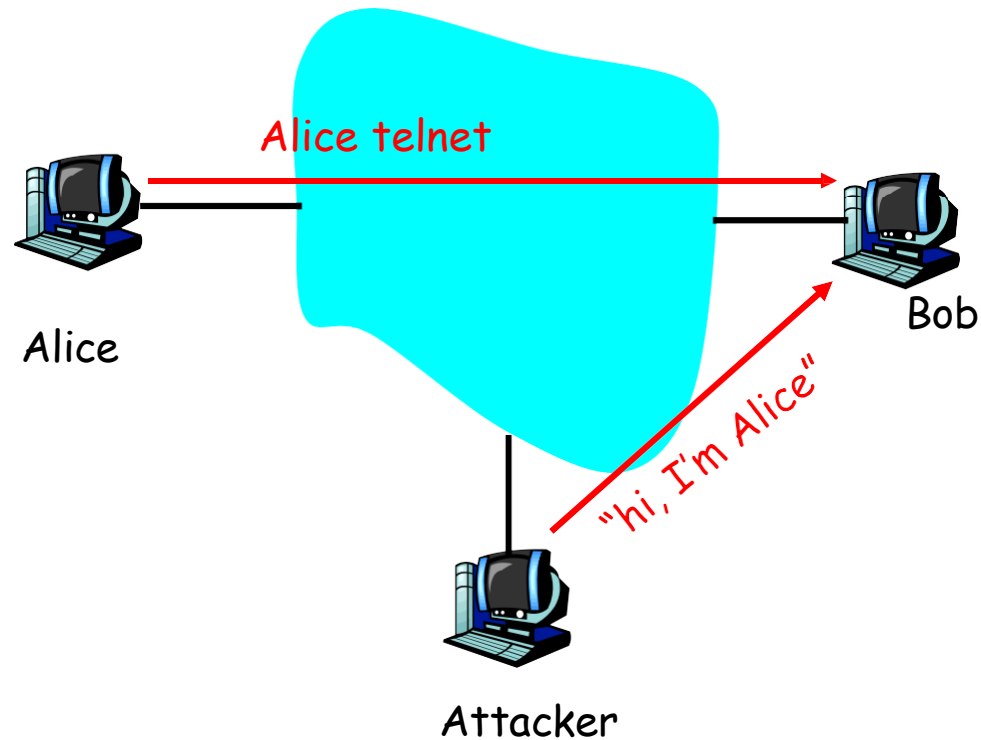
# MESSAGE REPLAY

- Message 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.



# TCP/IP HACKING

- Take control of one side of a TCP connection
- Combination of sniffing and spoofing



# SESSION HIJACKING

- Attacker is on segment where traffic passes from Alice to Bob
  - Attacker sniffs packets
  - Sees TCP packets between Bob and Alice and their sequence numbers
- Attacker jumps in, sending TCP packets to Bob; source IP address = Alice's IP address
  - Bob now obeys commands sent by attacker, thinking they were sent by Alice
- Principal defense: encryption
  - Attacker does not have keys to encrypt and insert meaningful traffic



# SESSION HIJACKING TOOLS

- Hunt
  - <http://ihackers.co/hunt-session-hijacking-tool/>
  - Provides ARP poisoning
- Netcat
  - General purpose widget
  - Very popular



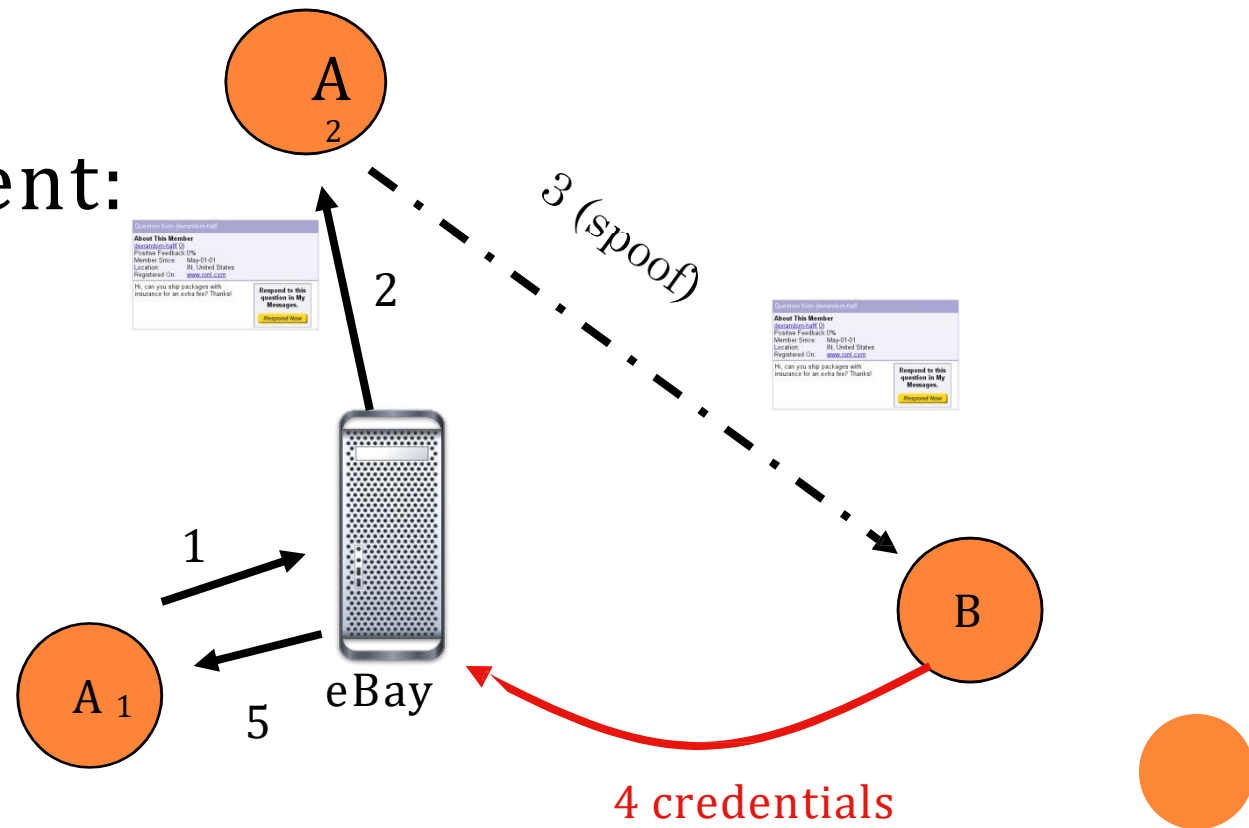
# PHISHING ATTACK

- In phishing attack the hacker creates a fake web site that looks exactly like a popular site such as the SBI bank or paypal.
- The phishing part of the attack is that the hacker then sends an e-mail message trying to trick the user into clicking a link that leads to the fake site.
- When the user attempts to log on with their account information, the hacker records the username and password and then tries that information on the real site.



# CONTINUE...

## Experiment:



# SQL INJECTION

- SQL injection is a technique where malicious users can inject SQL commands into an SQL statement, via web page input.
- Injected SQL commands can alter SQL statement and compromise the security of a web application.
- When SQL is used to display data on a web page, it is common to let web users input their own search values.
- Since SQL statements are text only, it is easy, with a little piece of computer code, to dynamically change SQL statements to provide



## CONTINUE...

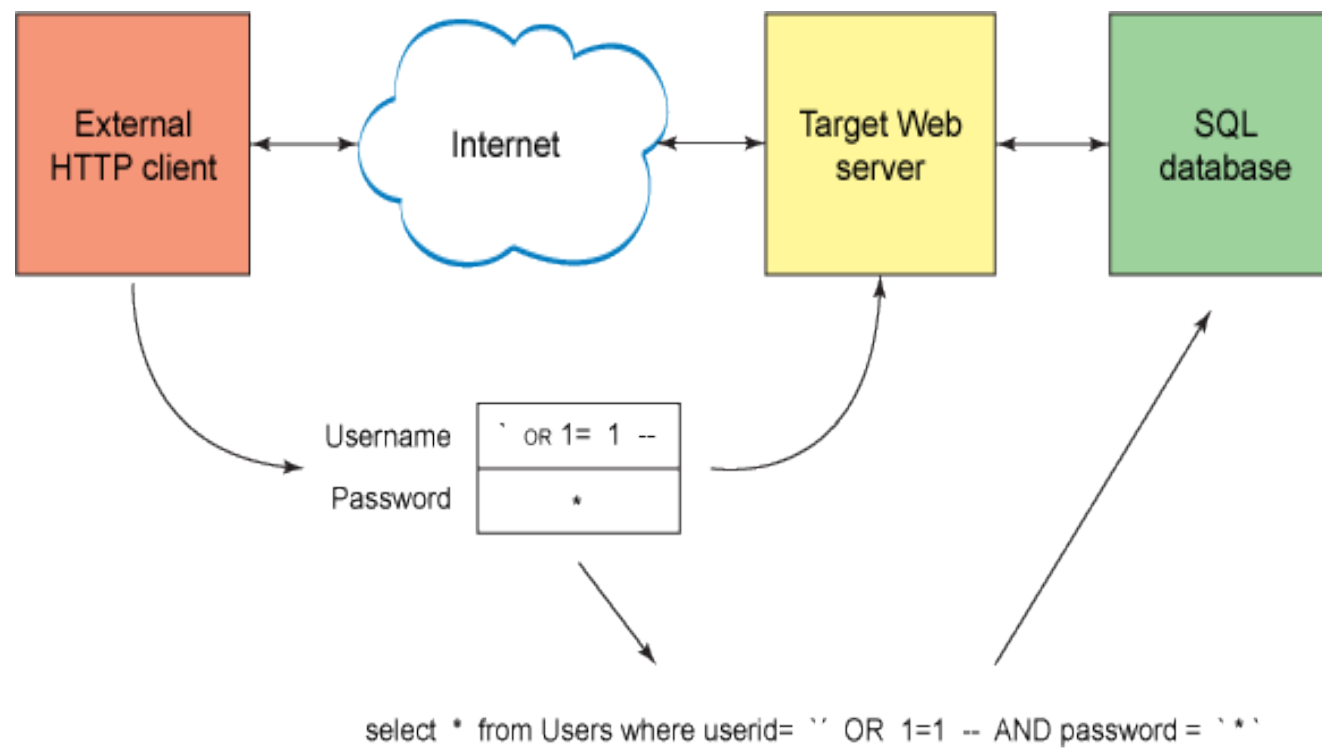
the user with selected data:

- **Server Code**
- `txtUserId = getQueryString("UserId"); txtSQL = "SELECT * FROM Users WHERE UserId = " + txtUserId;`
- The example above, creates a select statement by adding a variable (`txtUserId`) to a select string. The variable is fetched from the user input (Request) to the page.





# SIMPLE SQL INJECTION ATTACK FIGURE



# *LOGIC BOMB*

- Logic bombs are a malicious programming code that is inserted into a network system or a single computer for the purpose of deleting data or creating other malicious acts on a specified date.
- A logic bomb works similar to a time bomb because it can be set to go off at a specific date.
- A logic bomb does not distribute malicious codes until the specified date is reached.
- A logic bomb can be rather difficult to detect, however you can take security measures such as constantly monitoring the network system for any suspicious activity, using antivirus applications and other scanning programs.



# *VIRUSES*

- A VIRUS is a small program written to alter the way a computer operates, without permission or knowledge of the user.
- Two Criteria:
  - it must execute itself.
  - It must replicate itself.
- Five categories:
  - File infector viruses
  - Boot sector viruses
  - Master-boot record viruses
  - Macro viruses



## CONT...

- File infector viruses: It infects program files such as .exe, .com.
- Boot sector viruses: It infects the system area of disk like boot record on hard disk.
- Master-boot record viruses: It saves a copy of master boot record in a different location.
- Macro viruses: It infects data files like Microsoft excel, word, access, power point files.

