NETWORK SECURITY

Ch. 3: Network Attacks

PTIIK
PROGRAM TEKNOLOGI INFORMASI DAN ILMU KOMPUTER

Contents

3.1 Network Vulnerabilities

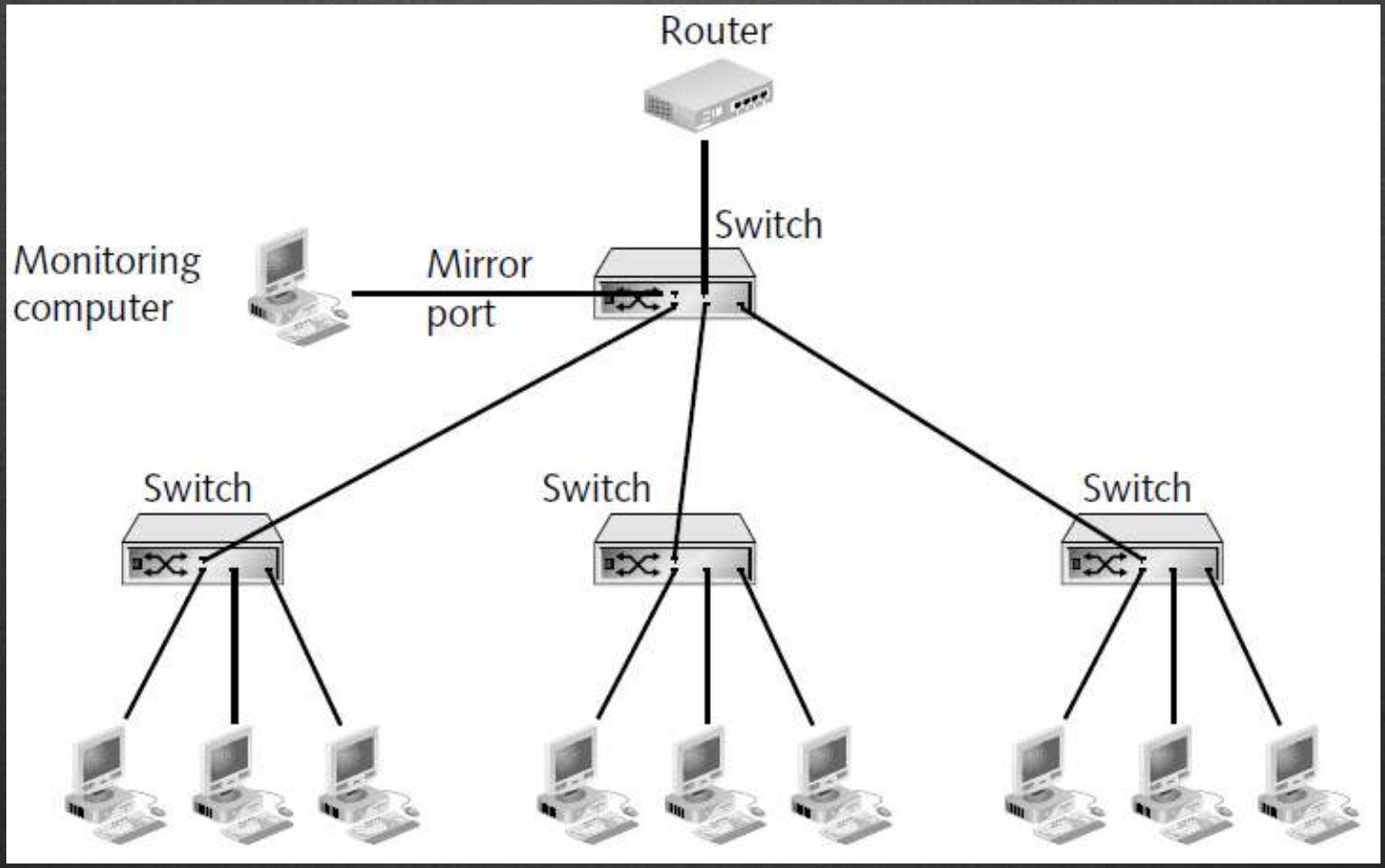
- Two broad categories of network vulnerabilities:
  - those found in *network transport media*, and
  - *network devices*.

3.1 Network Vulnerabilities

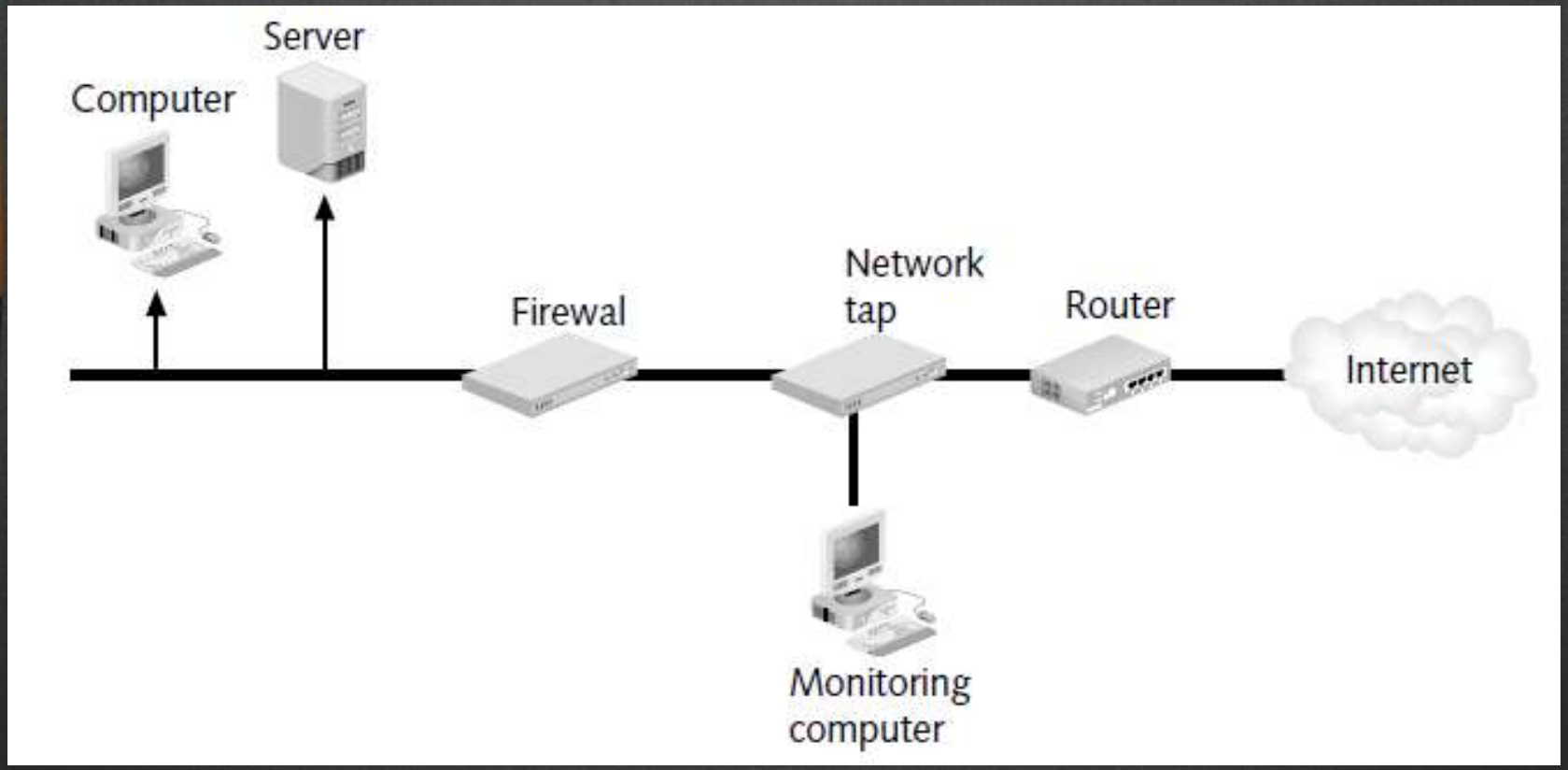
3.1.1 Media-Based Vulnerabilities

- Monitoring traffic can be done in two ways:
  - By *port mirroring* on a manageable switch, that allow traffic redirection from all or some ports to a designated port and analyze by a protocol analyzer (also called a sniffer)
  - A second method for monitoring traffic is to install a *network tap*

3.1 Network Vulnerabilities



3.1 Network Vulnerabilities



3.1 Network Vulnerabilities

- Just as network taps and protocol analyzers can be used for legitimate purposes, they also *can be used by attackers to intercept and view network traffic*.
- By default, a switch sends packets only to the intended recipient.
- However, there are several techniques that can be used to circumvent this limitation.

3.1 Network Vulnerabilities

Technique	Explanation
Switch flooding	An attacker can overflow the switch's address table with fake media access control (MAC) addresses and make the switch act like a hub, sending packets to all devices.
MAC address impersonation	The attacker with Device X can pretend to be Device A by sending Device A's MAC address to the switch as if it were her own address.
Fake network redirect	If two computers are on different logical network segments, Device A must send its request to talk to Device B through the router. An attacker on Device X could send a fake network redirect to Device A, claiming that it should send Device B's packet to Device X.
Router advertisements	Because routers routinely send advertisements informing devices of their presence, an attacker could pretend to be a router and send false router advertisements so that all devices would send packets to the attacker's device.
Fake device redirect	An attacker can pretend to be a valid network device by sending a fake device redirect to the switch.

3.1 Network Vulnerabilities

3.1.2 Network Device Vulnerabilities

- Common network device vulnerabilities include:
  - some factors cause many network administrators to use weak passwords, or those that compromise security.
  - default accounts, is a user account on a device that is created automatically by the device instead of by an administrator.
  - a back door , an account that is secretly set up without the administrator's knowledge or permission.
  - privilege escalation, it is possible to exploit a vulnerability in the network device's software to gain access to resources.

3.2 Categories of Attacks

- There are a number of different categories of attacks that are conducted against networks.
- These categories include *denial of service*, *spoofing*, *man-in-the-middle*, and *replay attacks*.

3.2 Categories of Attacks

3.2.1 Denial of Service (DoS)

- A DoS attack attempts to consume network resources so that the network or its devices cannot respond to legitimate requests.
- DoS attacks can take several forms:
  - Overwhelm a network
  - Overwhelm a server
  - Bring down a server

3.2 Categories of Attacks

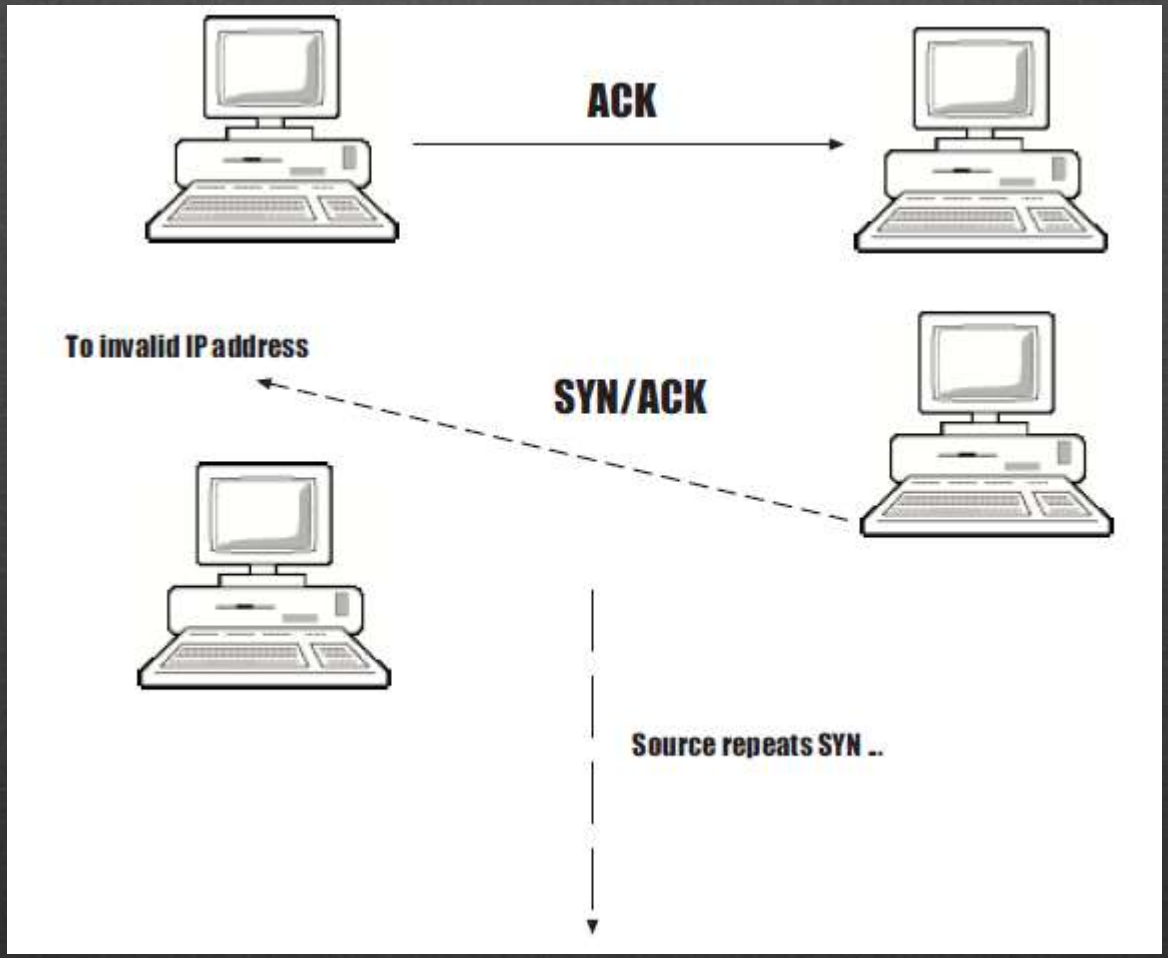
SYN Flood Attacks

- The earliest DoS attacks were launched from a single source computer.
- The attacker launches packets from his or her machine that compromise the victim.
- One of the earliest to appear was the *SYN flood attack* which takes advantage of the TCP three-way handshake.

3.2 Categories of Attacks

- The general technique of the attack is to send a flood of SYN segments to the victim with spoofed—and usually invalid—source IP addresses.
- As a result, the victim slows down and can't handle legitimate traffic in an acceptable time frame.

3.2 Categories of Attacks



3.2 Categories of Attacks

Ping of Death

- A simple way to mount a DoS attack is to flood the victim system with multiple, oversized ping requests.
- The attacker sends a ping in a packet that has too much data in its data field, creating a packet that is too long (more than 65,536 octets).
- The victim receives these oversized packets and is likely to crash, hang, or even reboot.

3.2 Categories of Attacks

Smurf

- Smurf is a DoS attack that takes advantage of ICMP and IP broadcast addresses.
- Smurf works in the following way:
  - An attacker creates an ICMP echo request packet with a spoofed return address (the IP address of the attack's victim) and a broadcast destination address.
  - The attacker then sends the packet to another target, usually a router that doesn't block ICMP echo requests to broadcast addresses.

3.2 Categories of Attacks

- The router sends the packet to all systems on its network.
- Each system that received the echo request packet responds to the victim, flooding the victim with packets that tie up its network bandwidth.
- The attacker sends the datagram to the victim.
- The victim's chargen service responds with a random string of characters, which goes to the spoofed IP address on its own network.
- The two systems continue to send characters to each other, slowing both their own processing and network traffic.

3.2 Categories of Attacks

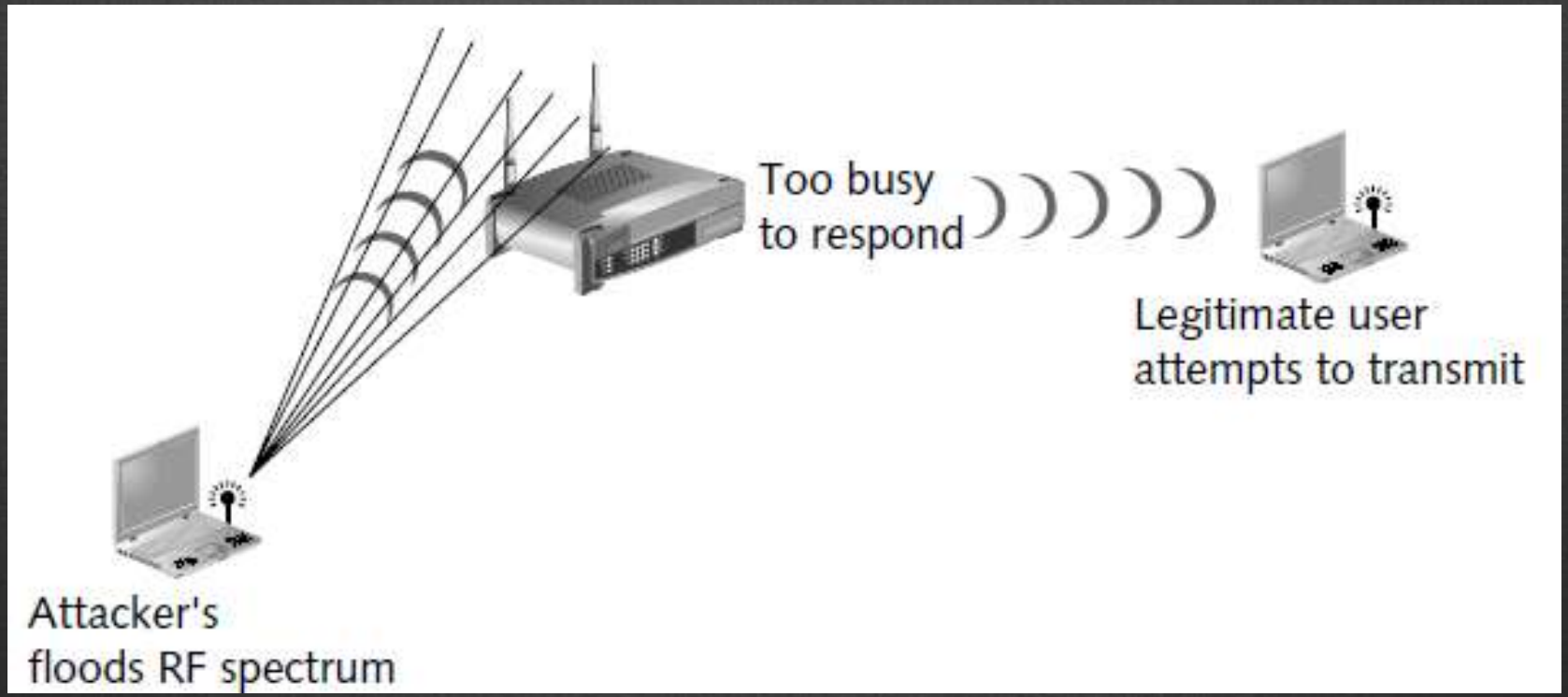
UDP Flood Attacks

- A UDP flood attack (sometimes called *pingpong*) takes advantage of the chargen (useless) service, which is used legitimately to test hosts and networks.
- An attacker mounts it in the following manner:
  - The attacker spoofs the return IP address of a UDP datagram that makes a request of the chargen service. Typically, the spoofed return address will point to a host on the victim network.
- An attacker can also mount a similar type of attack using echo requests.

3.2 Categories of Attacks

- DoS attacks can be used against wireless networks as well.
- An attacker can flood the radio frequency (RF) spectrum with enough radiomagnetic interference.
- However, these attacks generally are not widespread because sophisticated and expensive equipment is necessary

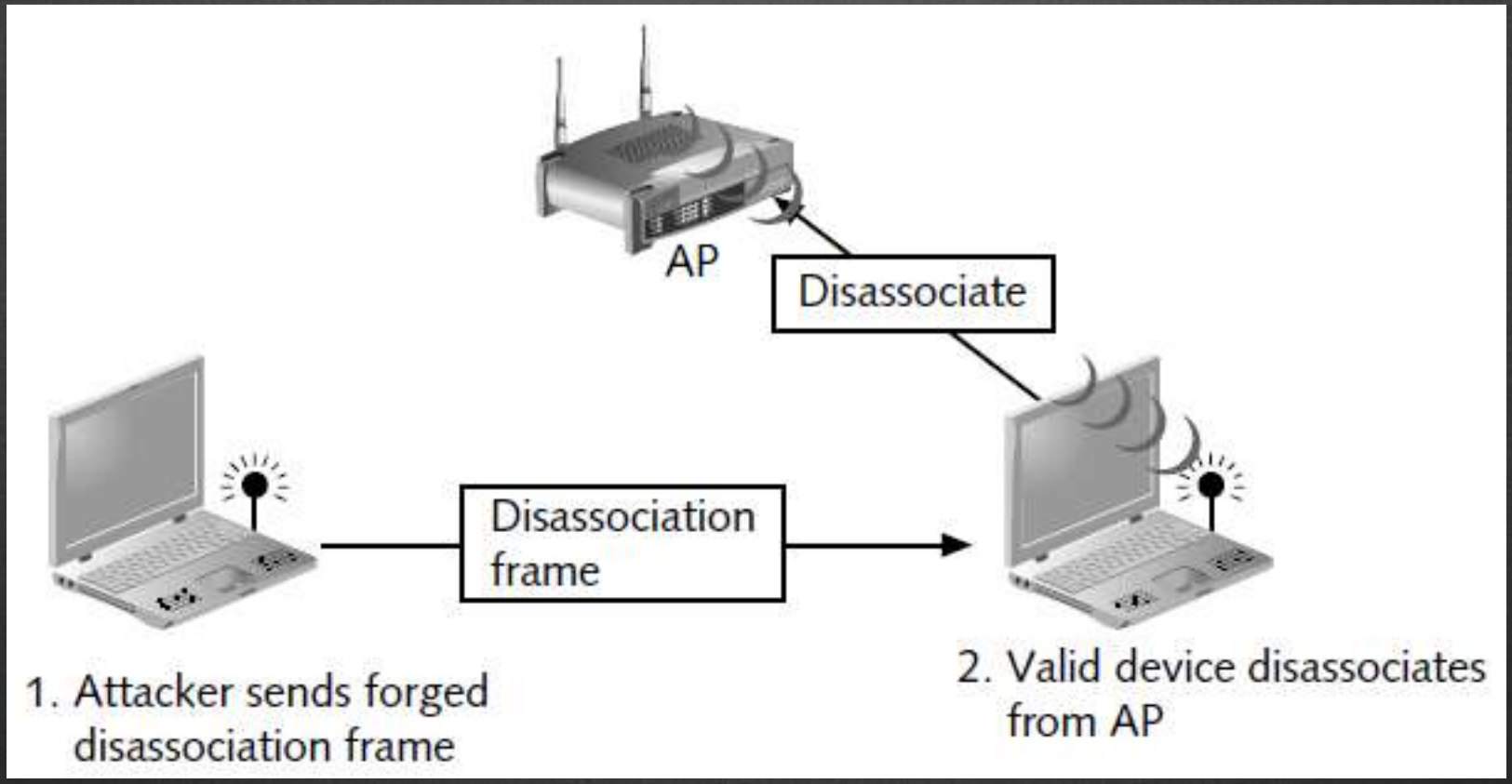
3.2 Categories of Attacks



3.2 Categories of Attacks

- Most successful wireless DoS attacks take a different approach.
- Attackers can take advantages of *CSMA/CA* and *explicit frame ACK* to perform a wireless DoS.
- Another wireless DoS attack uses disassociation frames. A disassociation frame is sent to a device to force it to temporarily disconnect from the wireless network.

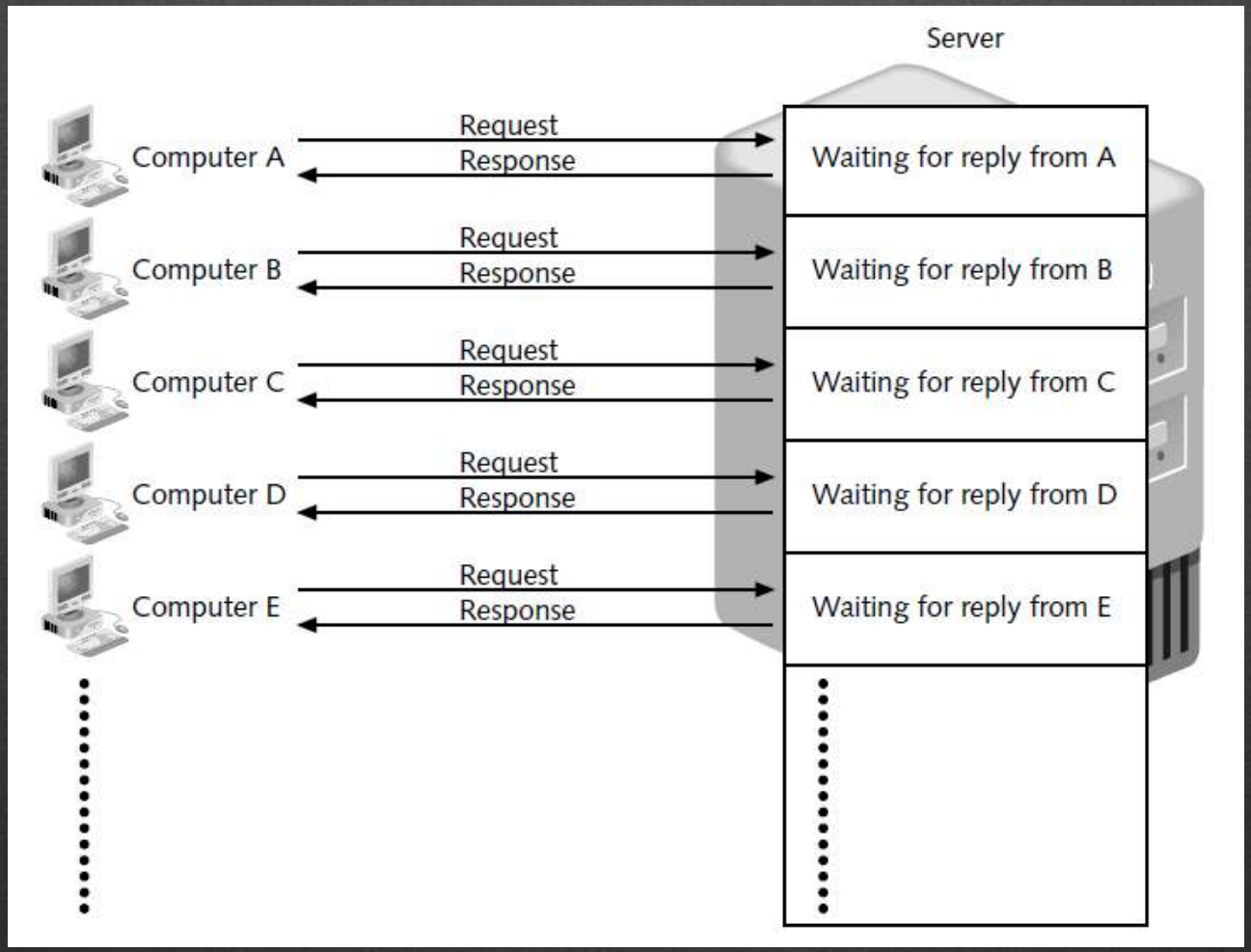
3.2 Categories of Attacks



3.2 Categories of Attacks

- A variant of the DoS is the **distributed denial of service (DDoS)** attack.
- Instead of using one computer, a DDoS may use hundreds or thousands of zombie computers in a botnet to flood a device with requests.
- This makes it virtually impossible to identify and block the source of the attack.

3.2 Categories of Attacks



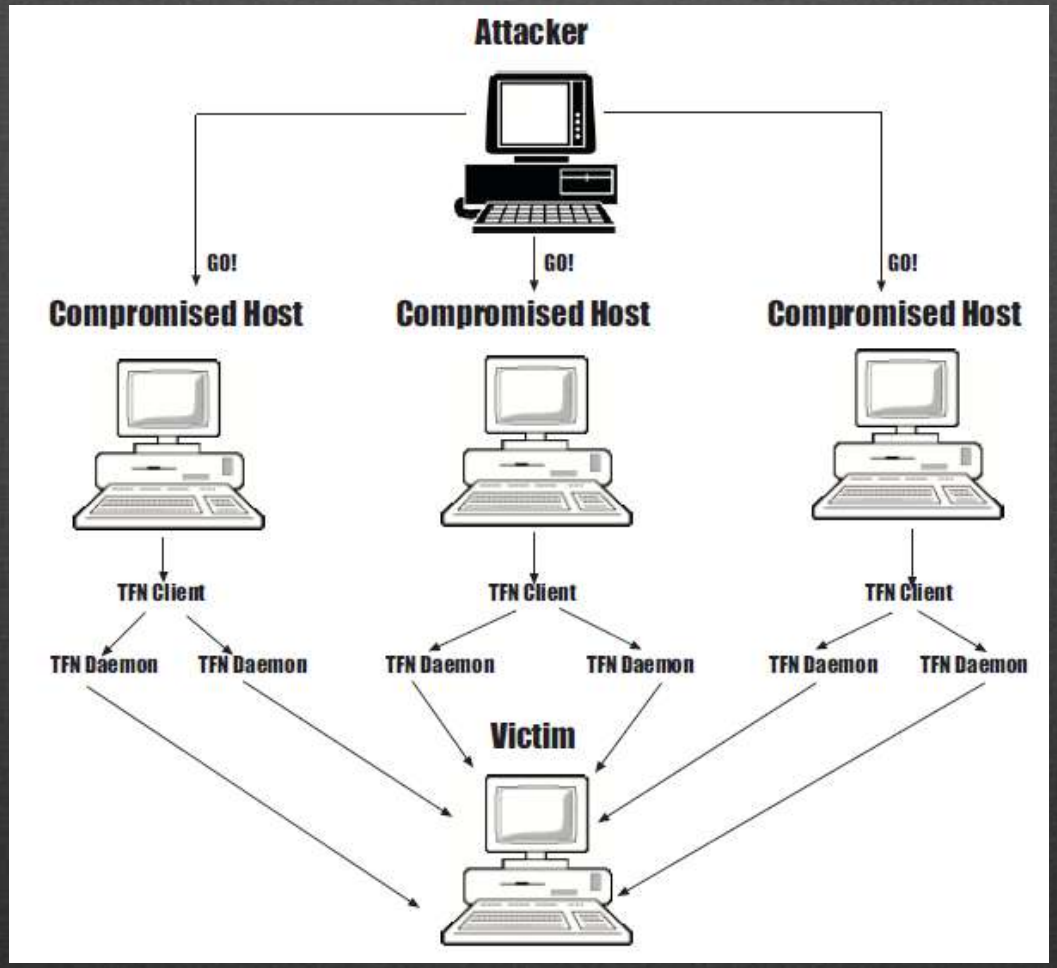
3.2 Categories of Attacks

- Attacks that were categorized in this DDoS include:
  - Tribe Flood Network,
  - Trinoo, and
  - Stacheldraht.

Tribe Flood Network

- uses client software on compromised hosts to launch attacks on a victim or victims.

3.2 Categories of Attacks



3.2 Categories of Attacks

Trinoo

- Similar to that of TFN (the attacker communicating with daemons on a compromised host).
- However, it is used to launch UDP flood attacks from multiple sources.

3.2 Categories of Attacks

Stacheldraht

- A variation of TFN and Trinoo.
- The client communicates with handlers using encrypted communication from a command line.
- Handlers are password protected.
- Stacheldraht uses both TCP and ICMP to mount attacks.

3.2 Categories of Attacks

3.2.2 Spoofing

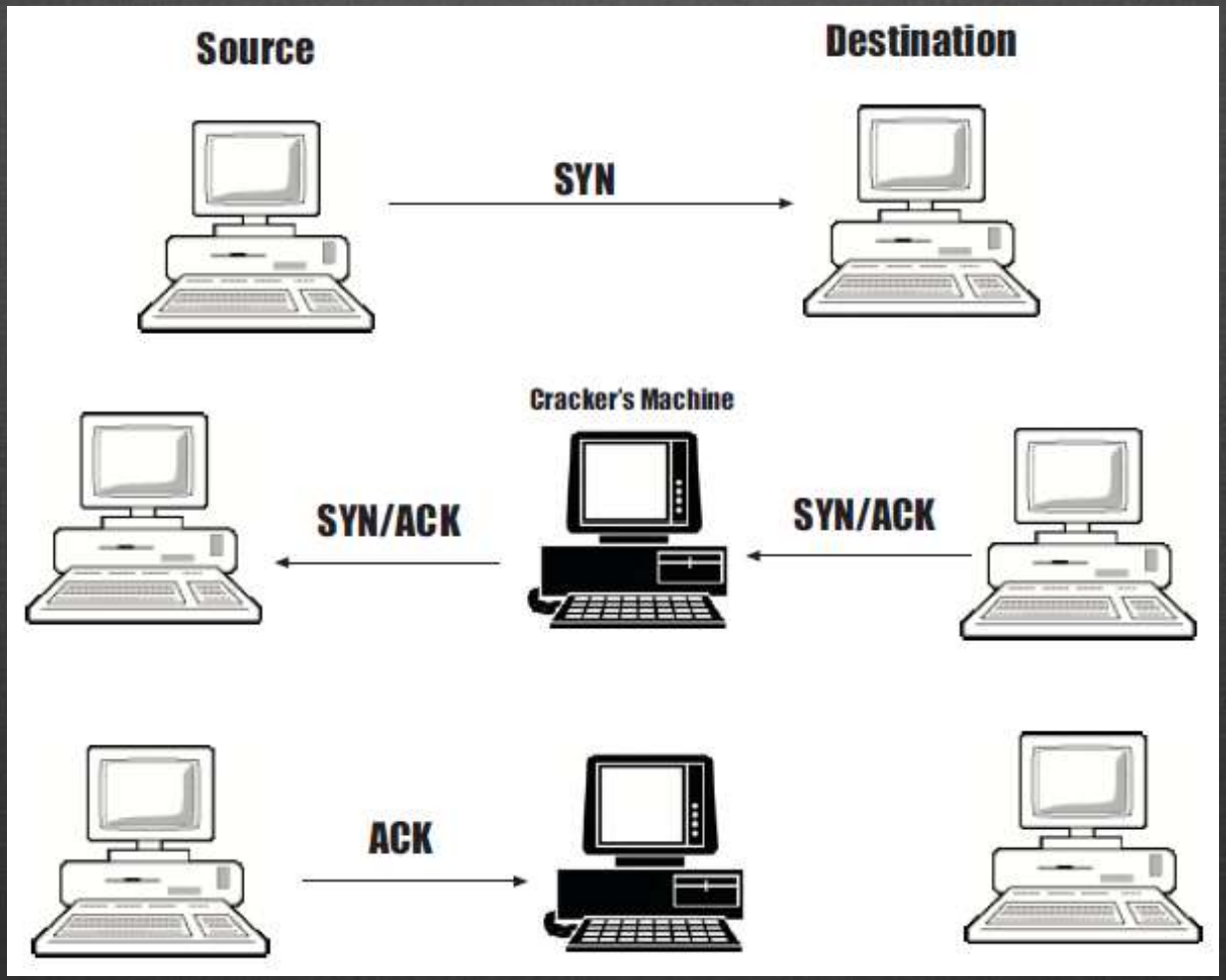
- Spoofing is impersonation; that is, it is pretending to be someone or something else by presenting false information.
- There are some type of spoofing,
  - TCP Spoofing
  - DNS Spoofing
  - IP Spoofing, and
  - Web Spoofing

3.2 Categories of Attacks

TCP Spoofing

- The goal of a cracker is to jump into the middle of the TCP exchanges, intercepting the segments and inserting his/her own segments.
- To make TCP spoofing work, the cracker needs to know the starting sequence number of the TCP segments so that the fake segment returned.

3.2 Categories of Attacks

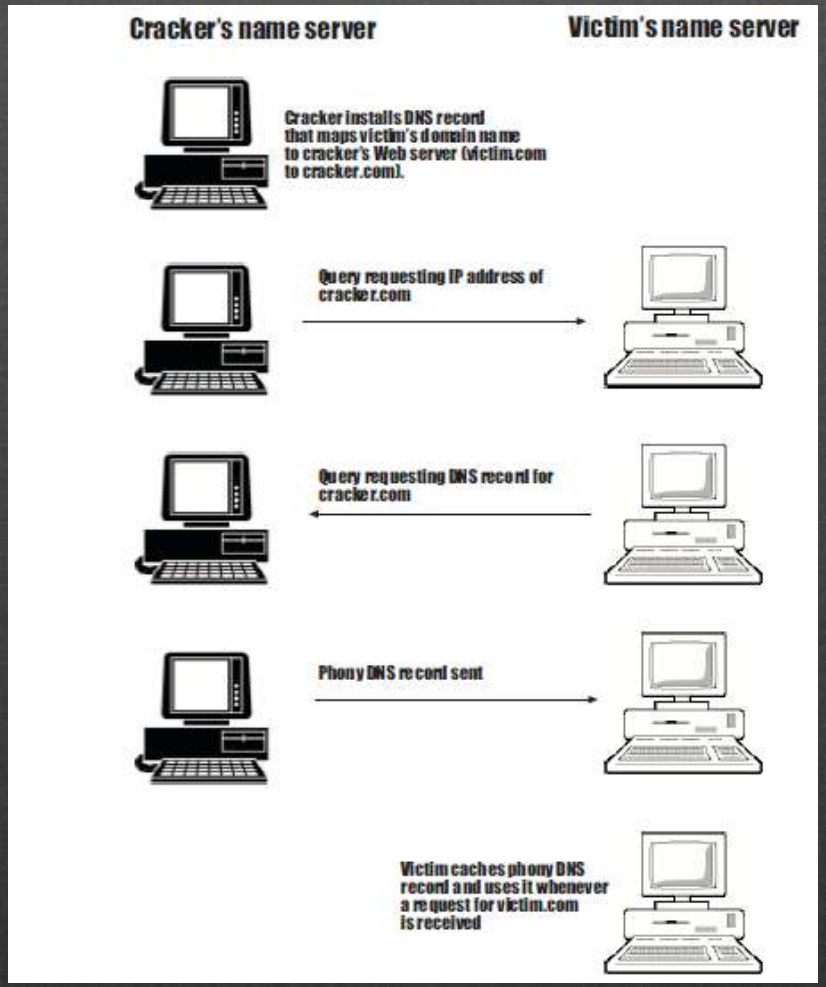


3.2 Categories of Attacks

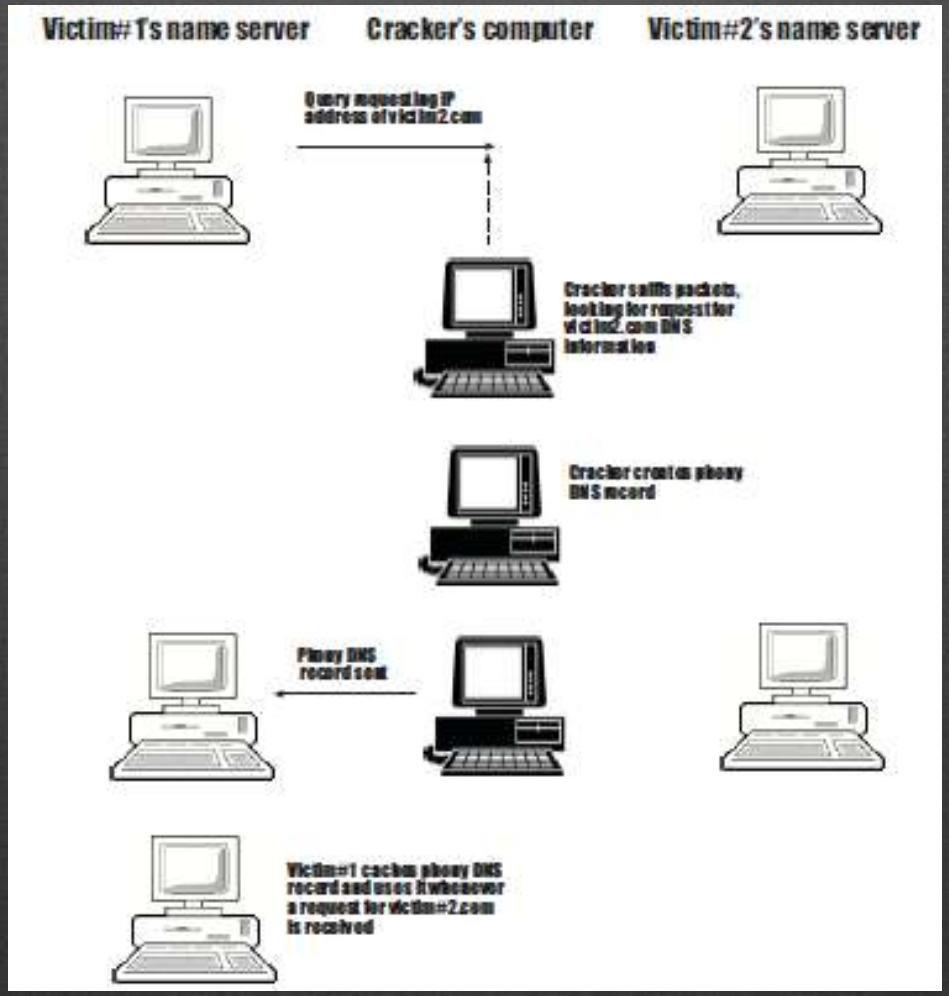
DNS Spoofing

- A method for redirecting users to a Web site other than the one to which a domain name is actually registered.
- The most common variation is *malicious cache poisoning* , which involves the modification of data in the cache of a domain name server. Any name server that specifically isn't protected against this type of attack is vulnerable.

3.2 Categories of Attacks



3.2 Categories of Attacks



3.2 Categories of Attacks

IP Spoofing

- The most common type of spoofing.
- Used primarily to spoof the source address of e-mail.
- The intent is to trick the user into thinking the e-mail comes from a trusted source.

3.2 Categories of Attacks

Web Spoofing

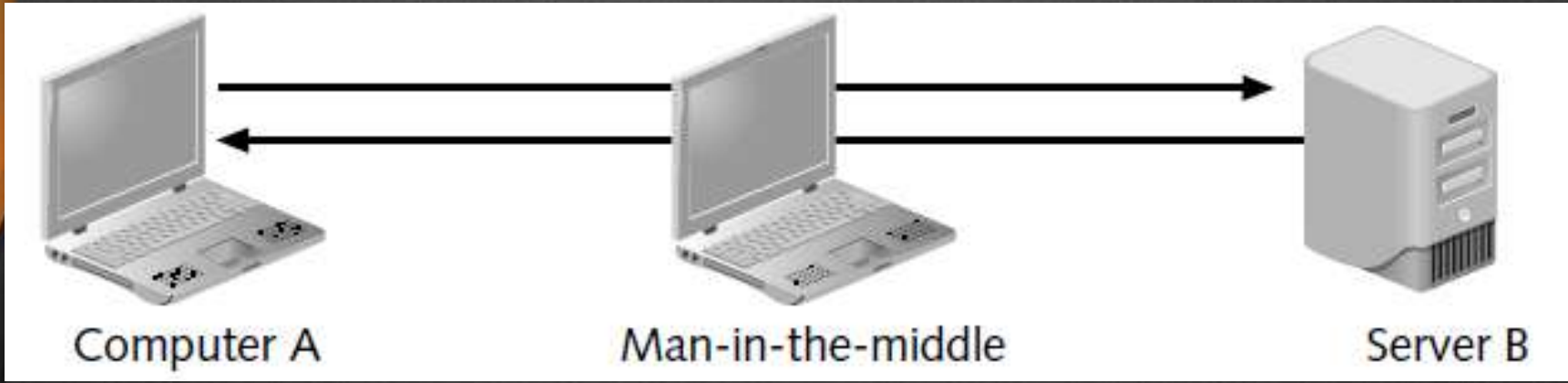
- Web spoofing involves tricking a user into thinking he or she is interacting with a trusted Web site.
- Spoofed Web sites look very much like the site they are imitating.

3.2 Categories of Attacks

3.2.3 Man-in-the-Middle

- This type of attack makes it seem that two computers are communicating with each other,
- when actually they are sending and receiving data with a computer between them, or the “man-in-the-middle.”

3.2 Categories of Attacks



3.2 Categories of Attacks

- Man-in-the-middle attacks can be active or passive.
  - In a passive attack, the attacker captures the data that is being transmitted, records it, and then sends it on to the original recipient without his presence being detected.
  - In an active attack, the contents are intercepted and altered before they are sent on to the recipient.

3.2 Categories of Attacks

3.2.4 Replay

- A replay attack is similar to a passive man-in-the-middle attack.
- Whereas a passive attack sends the transmission immediately, a replay attack makes a copy of the transmission before sending it to the recipient.
- This copy is then used at a later time (the man-in-the-middle replays it).

3.3 Methods of Net. Attacks

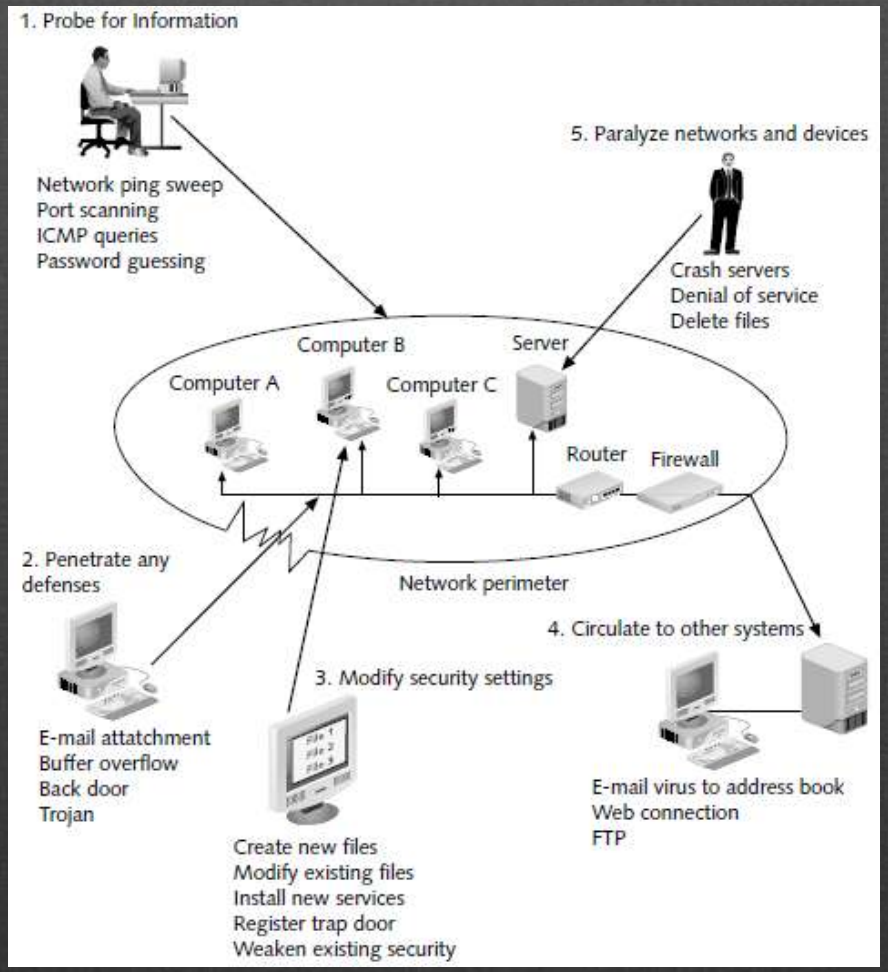
Five steps of Attack

- *Probe for information*. The first step in an attack is to probe the system for any information that can be used to attack it (*reconnaissance*).
- *Penetrate any defenses*. The next step is to launch the attack to penetrate the defenses.
- *Modify security settings*. This allows the attacker to re-enter the compromised system

3.3 Methods of Net. Attacks

- *Circulate to other systems.* The attacker then uses the compromised systems as a base to attack other networks and computers.
- *Paralyze networks and devices.* Attackers may also work to maliciously damage.

3.3 Methods of Net. Attacks



3.3 Methods of Net. Attacks

- Just as there are different categories of attacks on networks, there are several different ways to perform these attacks.
- Network attack methods can be protocol-based or wireless, as well as other methods.

3.3 Methods of Net. Attacks

3.3.1 Protocol-Based Attacks

- The most common methods of attack.
- The weakness is inherent within the protocol itself and can be harder to defend.
- Some of the most common protocol-based attacks are:
  - Antiquated Protocols,
  - DNS attacks,
  - ARP poisoning, and
  - TCP/IP hijacking.

3.3 Methods of Net. Attacks

Antiquated Protocols

- Over time, TCP/IP protocols have been updated often to address security vulnerabilities.
- Antiquated protocols, like SNMPv1 and SNMPv2, are popular targets for attackers.

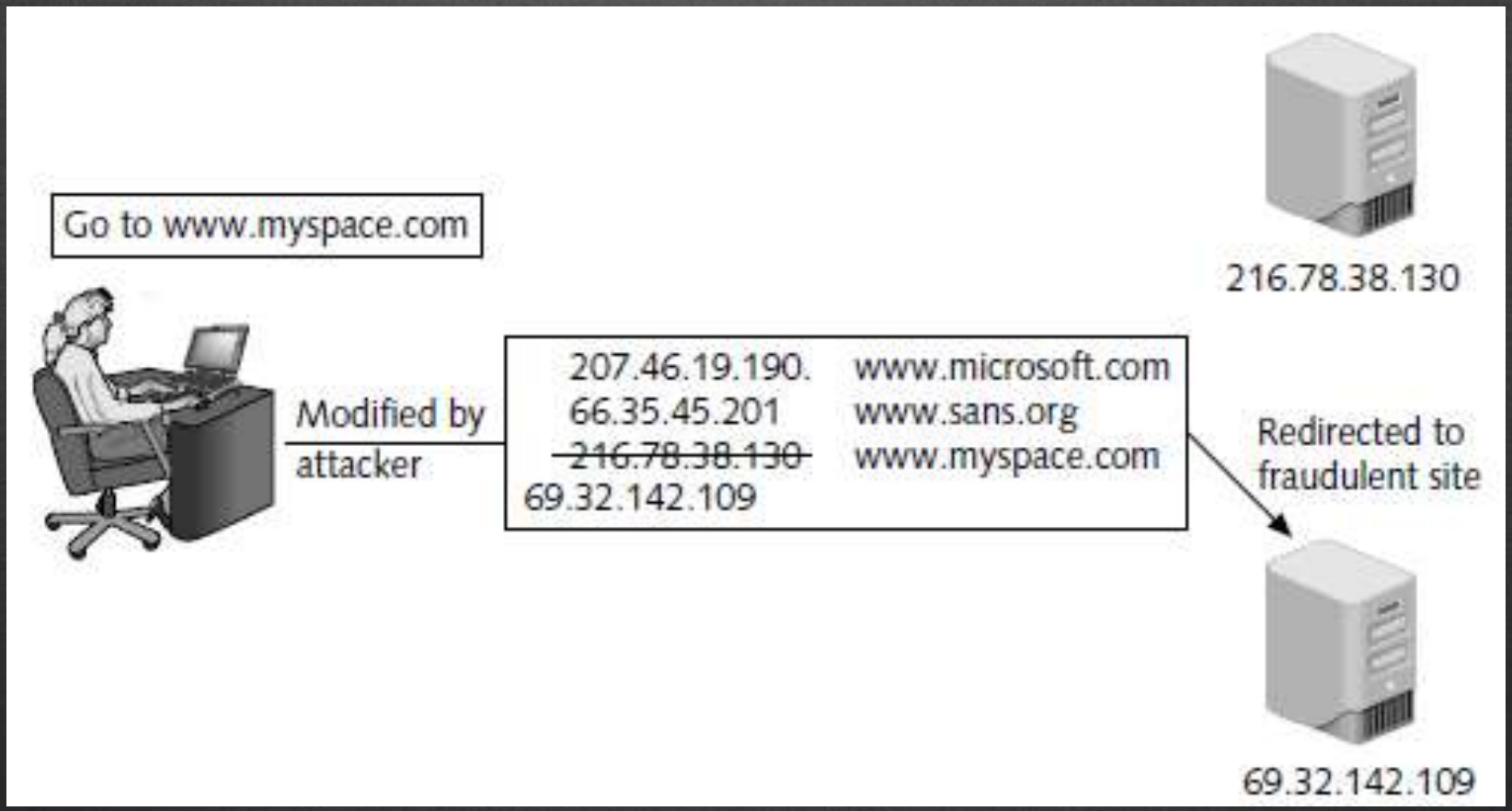
3.3 Methods of Net. Attacks

DNS Attacks

- The DNS is frequently the focus of attacks. These attacks include DNS poisoning and DNS transfers.

- *DNS Poisoning*. One type of DNS attack is to substitute a fraudulent IP address so that when a user enters a symbolic name, she is directed to the fraudulent computer site.

3.3 Methods of Net. Attacks



3.3 Methods of Net. Attacks

- Substituting a fraudulent IP address can be done in one of two different locations.
  - First, TCP/IP still uses host tables stored on the local computer. Attackers can target a local host's file to create new entries that will redirect users to their fraudulent site.
  - Another approach to substituting a fraudulent IP address is to target the external DNS server and is called **DNS poisoning** (also called **DNS spoofing**).

3.3 Methods of Net. Attacks

- *DNS Transfers* A second attack using DNS is almost the reverse of DNS poisoning.
- An attacker asks the valid DNS server for a zone transfer.
- With this information it would be possible for the attacker to map the entire internal network.

3.3 Methods of Net. Attacks

ARP Poisoning

- Similar to DNS poisoning, an attacker could alter the MAC address in the ARP cache so that the corresponding IP address would point to a different computer.
- Attackers would :
  - Send a malicious ARP reply to the router (1) and victims (2) associating his MAC and begin to send or forward any network traffic it receives (3).

3.3 Methods of Net. Attacks

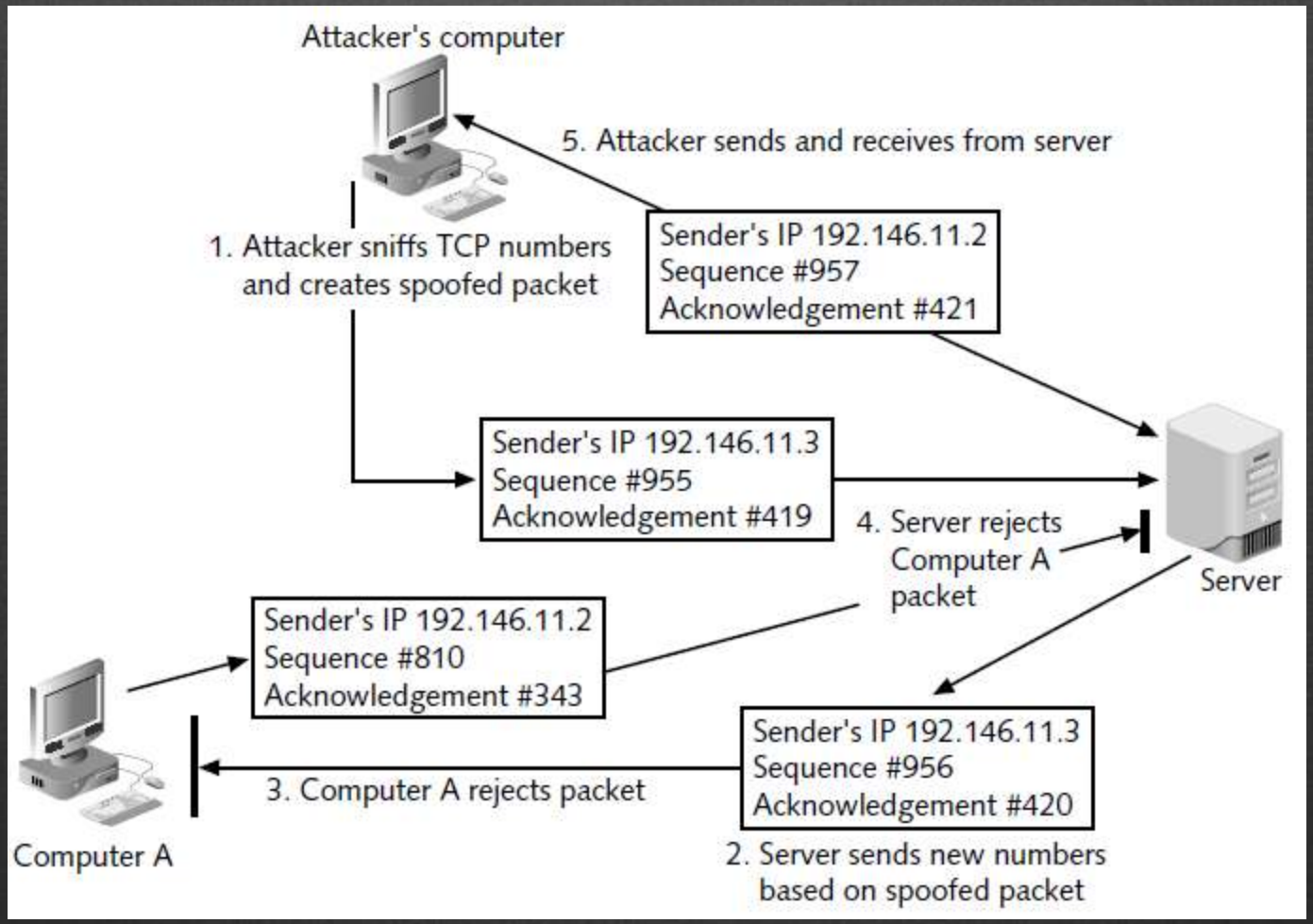
Result	Description
Steal data	An attacker could substitute his own MAC address and steal data intended for another device.
MAC flooding	Substituting the MAC address of the switch, an attacker could flood the switch with packets and force it to revert to a hub in order to use a protocol analyzer to view all traffic.
Prevent Internet access	An attacker could substitute an invalid MAC address for the network gateway so that no users could access external networks.
Man-in-the-middle	A man-in-the-middle device could be set to receive all communications by substituting that MAC address.

3.3 Methods of Net. Attacks

TCP/IP Hijacking

- In order to identify TCP packets, the TCP header consists of two 32-bit fields that are used as packet counters.
- In a TCP/IP hijacking attack, the attacker creates fictitious ("spoofed") TCP packets to take advantage of the weaknesses.

3.3 Methods of Net. Attacks



3.3 Methods of Net. Attacks

3.3.2 Wireless Attacks

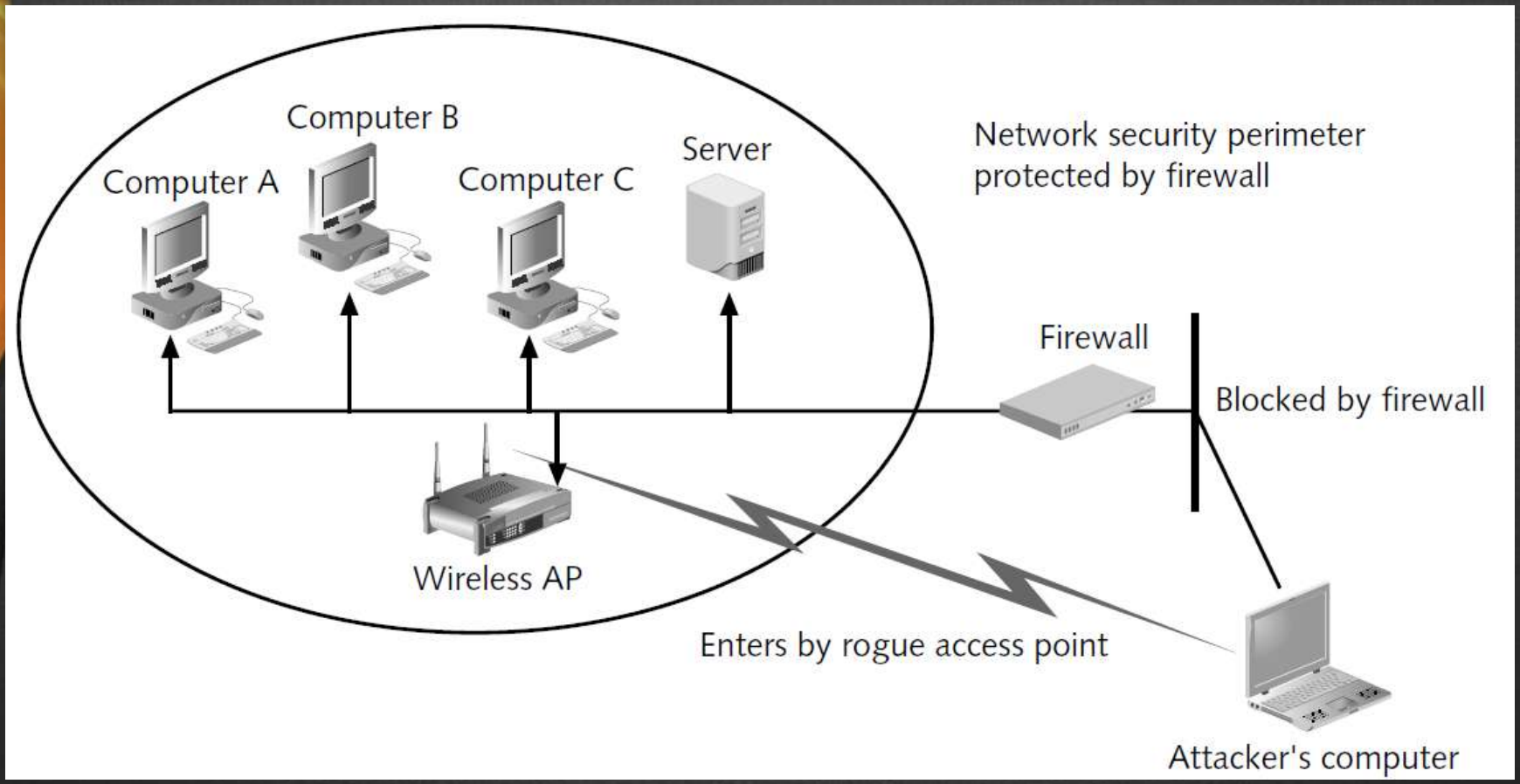
- As wireless networks have become commonplace, new attacks have been created to target these networks.
- These attacks include :
  - rogue access points,
  - war driving,
  - bluesnarfing, and
  - blue jacking.

3.3 Methods of Net. Attacks

Rogue Access Points

- Improperly configured (rogue) AP provided open access to an attacker who also picks up the wireless signal.
- This attacker can then circumvent the security protections of the company's network and launch attacks on all users.

3.3 Methods of Net. Attacks



3.3 Methods of Net. Attacks

War Driving

- At regular intervals (normally every 100 microseconds) a wireless AP sends a beacon frame to announce its presence and to provide the necessary information for devices that want to join the network.
- There is no means to limit who receives the signal, unapproved wireless devices can likewise pick up the beaconing RF transmission.

3.3 Methods of Net. Attacks

- War driving technically involves using an automobile to search for wireless signals over a large area.

- Wireless location mapping (or War Driving, informal) is the formal expression for this passive wireless discovery, or the process of finding a WLAN signal and recording information about it.

3.3 Methods of Net. Attacks

Bluesnarfing

- Bluetooth is the name given to a wireless technology that uses short-range RF transmissions.
- It provides for rapid “on the fly” and ad hoc connections between devices.
- Standardized as IEEE 802.15.1, with one of their network topologies is known as a piconet.

3.3 Methods of Net. Attacks

- Due to the ad hoc nature of Bluetooth piconets and scatternets, attacks on wireless Bluetooth technology have appeared.
- Bluesnarfing is the unauthorized access of information from a wireless device through a Bluetooth connection, often between phones, desktops, laptops, and personal digital assistants.

3.3 Methods of Net. Attacks

- Bluesnarfing allows an attacker to access e-mails, calendars, contact lists, and cell phone pictures and videos by simply connecting to that Bluetooth device without the owner's knowledge or permission.

3.3 Methods of Net. Attacks

- Blue jacking is sending unsolicited messages from Bluetooth to Bluetooth-enabled devices.
- Bluejacking is usually considered less harmful than bluesnarfing because no data is stolen.

3.3 Methods of Net. Attacks

3.3.3 Other Attacks and Frauds

- Other types of attacks and frauds that are sometimes found today are
  - Null sessions and
  - Domain Name Kiting.

3.3 Methods of Net. Attacks

Null Sessions

- Null sessions are unauthenticated connections to a Microsoft Windows 2000 or Windows NT computer that do not require a username or a password.
- Using a command as simple as

  C:\>net use \\192.168.###.###\IPC$ "" /u:

  could allow an attacker to connect to open a channel

3.3 Methods of Net. Attacks

Domain Name Kiting

- "Check kiting" is a type of fraud that involves the unlawful use of checking accounts to gain additional time before the fraud is detected.
- Domain Name Kiting is a variation on the kiting concept of taking advantage of additional time.