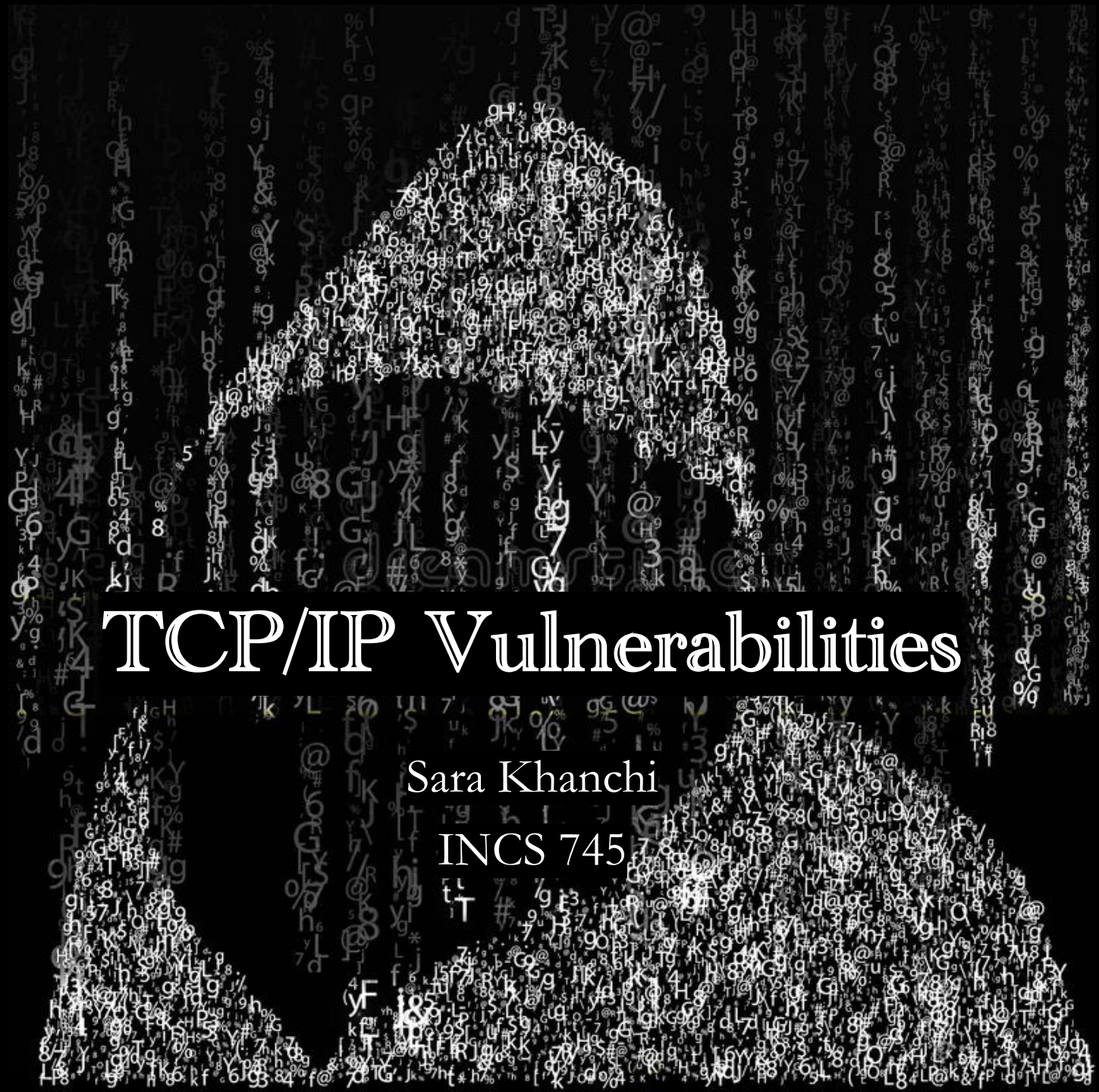

TCP/IP Vulnerabilities

Sara Khanchi

INCS 745

Vulnerabilities in TCP/IP

- During the development of TCP/IP in the 1980s Security was not a priority
- Illegitimate users take advantage of TCP/IP vulnerabilities
  - by exploiting the "three-way handshake"
- Some common vulnerabilities
  - Denial-of-service attack using flooding that regular traffic is slowed or completely interrupted
  - IP spoofing
  - Connection hijacking
  - ICMP attacks
  - TCP SYN attacks
  - RIP attacks

IP Spoofing

- Spoofing
  - A sophisticated way to authenticate one machine to another by using forged packets
  - Misrepresenting the sender of a message to cause the human recipient to behave a certain way
- Two critical issues for internetworked systems
  - Trust
  - Authentication

IP Spoofing

- Sequence Guessing
  - Hacker setups a few connections to the victim
    - Learns how quickly sequence number is incrementing
  - Attacker then sends a spoofed ACK packet with a “best guess” victim’s sequence number
  - Hacker can guess the sequence number because the number is generated using a global counter
    - And is incremented in fixed units

IP Spoofing

- Source Routing
  - Sender using **source routing** can specify return path
    - Through which the destination computer sends its reply
  - Attacker looks for an intermediate computer or router
    - That could forward packets to the target computer
  - Most newer routers and firewalls are configured to drop source-routed packets

IP Spoofing

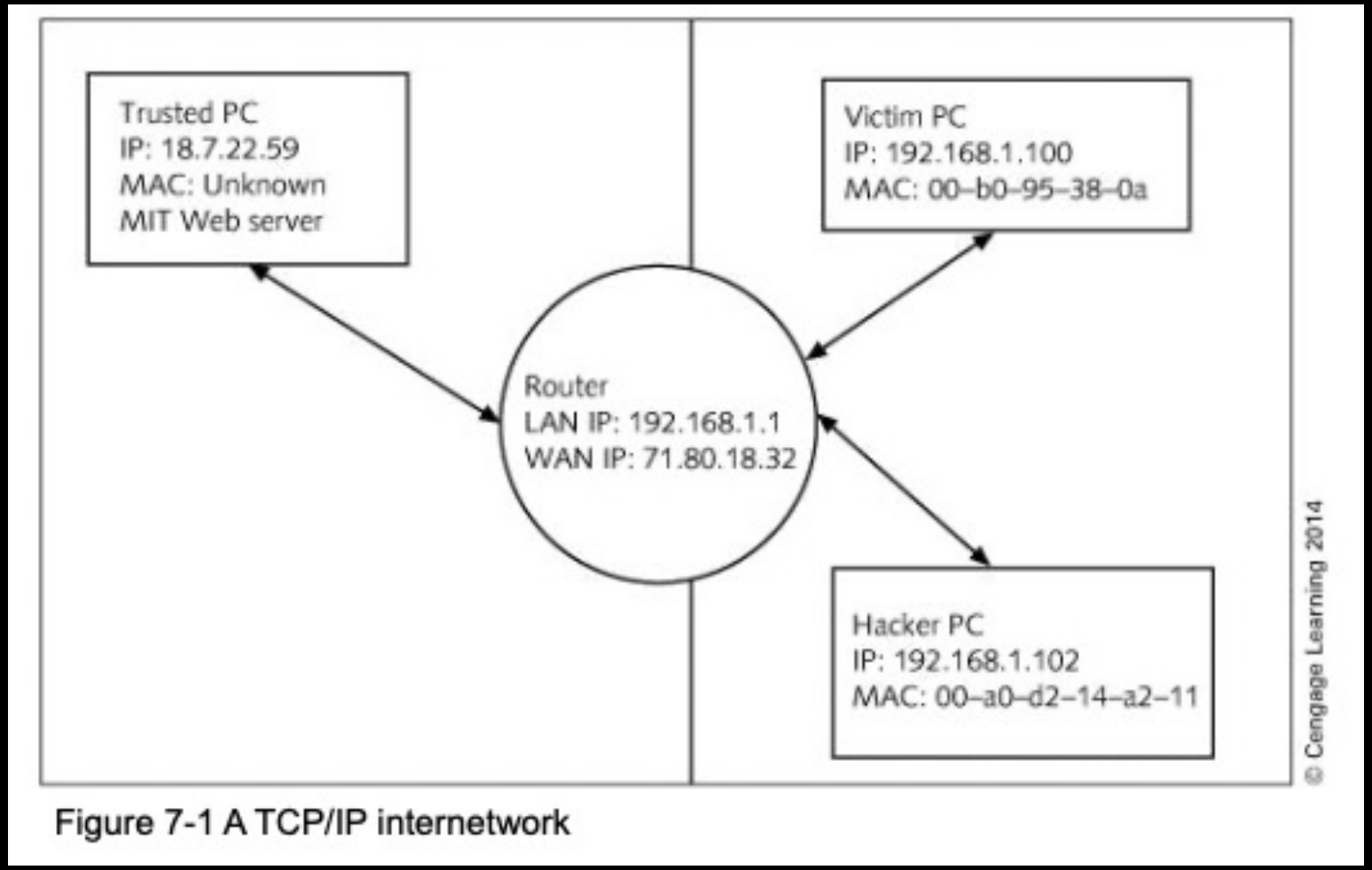

Figure 7-1 A TCP/IP internetwork

IP Spoofing

- Authentication is less critical when there is more trust
  - A computer can be authenticated by its IP address, IP host address, or MAC address
- TCP/IP has a basic flaw that allows IP spoofing
  - Trust and authentication have an inverse relationship
  - Initial authentication is based on the source address in trust relationships
  - Most fields in a TCP header can be changed (forged)

IP Spoofing

- Steps
  - Attackers send packets to the victim or target computer with a false source address
  - Victim accepts the packet and sends a response "back" to the indicated source computer
  - Attacker must guess the proper sequence numbers to send the final ACK packet
- Hacker may have a connection to victim's machine – And hold it as long as the computer remains active

The Process of an IP Spoofing Attack

- A successful attack requires more than simply forging a single header
  - Requires sustained dialogue between the machines for a minimum of three packets
- IP takes care of the transport between machines
  - But IP is unreliable
  - TCP is more reliable and has features for checking received packets
- TCP uses an indexing system to keep track of packets and put them in the right order

The Process of an IP Spoofing Attack

- To spoof a trusted machine relationship, the attacker must:
  - Identify the target pair of trusted machines
  - Anesthetize the host the attacker intends to impersonate
  - Forge the address of the host the attacker is pretending to be
  - Connect to the target as the assumed identity
  - Accurately guess the correct sequence

The Process of an IP Spoofing Attack

- You can use any network protocol analyzer to monitor your LAN
- You can anesthetize, or stun, the host that you want to impersonate
  - By performing a SYN flood (or SYN attack), Ping of Death, or some other denial-of-service attack

The Process of an IP Spoofing Attack

- Forging the address of the stunned host could be done with the same utility
  - Used to stun the trusted machine
- Big problem is guessing something close to the correct incremented victim-side sequence number
  - ISNs are not random, so the guess is not random

The Process of an IP Spoofing Attack

- Once the hacker has put the trusted machine to sleep with a SYN attack
  - Sends a SYN packet to the victim machine
- Hacker should connect to the victim machine several times on port 23 or 25
  - To get an idea of how quickly the ISN advances
- Attacker also needs to deduce the packet's round-trip time (RTT)
- When the attack is done, the trusted machine must be released and returned to normal

The Process of an IP Spoofing Attack

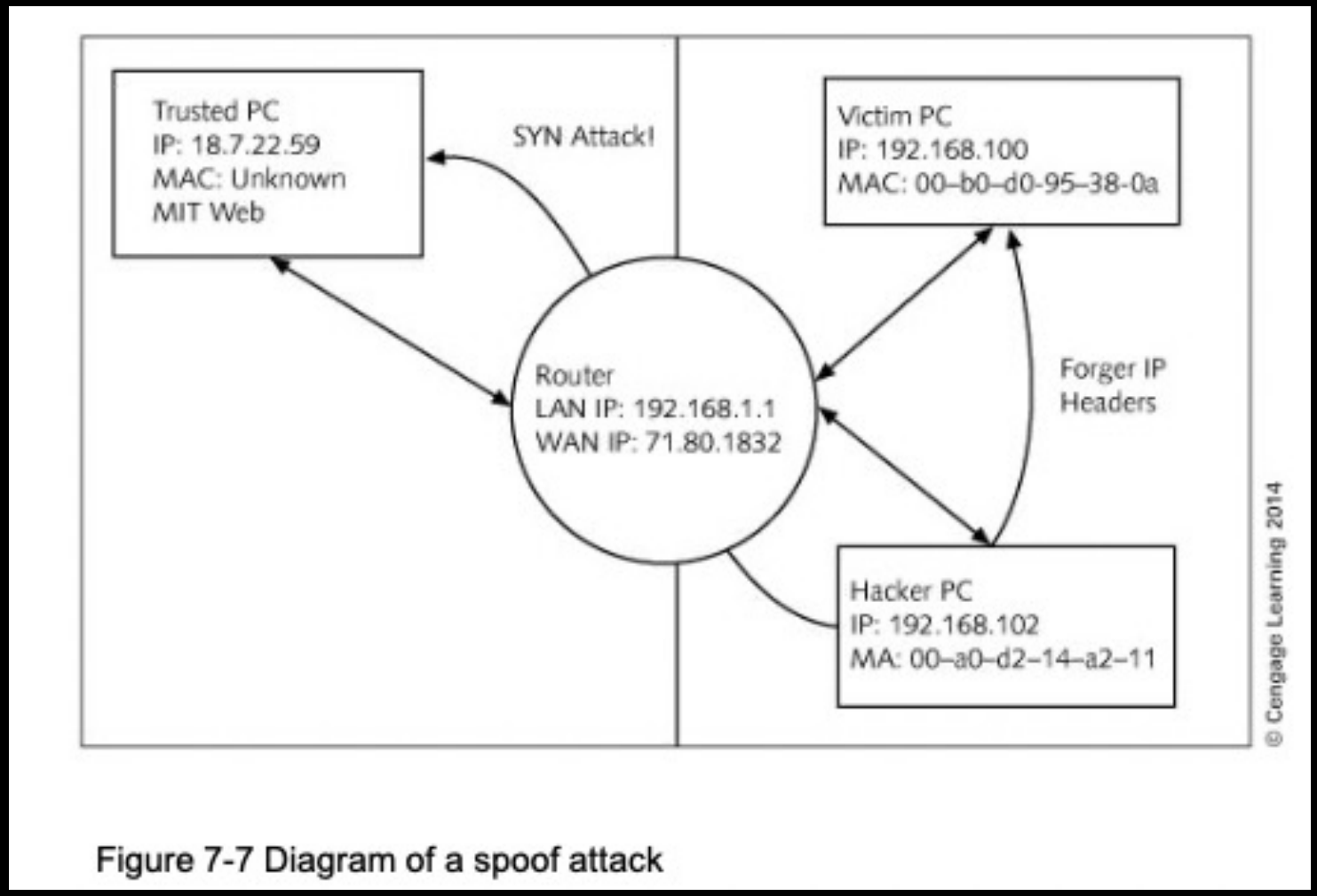

Figure 7-7 Diagram of a spoof attack

Types of Spoofing

- Main categories of spoofing include the following:
  - Blind spoofing
  - Active spoofing

  - IP spoofing
  - ARP (Address Resolution Protocol) spoofing
  - Web spoofing
  - DNS (Domain Name System) spoofing

Blind Spoofing

- Any kind of spoofing where only one side of the relationship under attack is in view
- Hacker is not aware of all network conditions
  - But uses various means to gain access to the network

Active Spoofing

- Hacker can see both parties, observe the responses from the target computer, and respond accordingly
- Hacker can perform various exploits, such as
  - Sniffing data, corrupting data, changing the contents of a packet, and even deleting some packets

IP Spoofing

- Consists of a hacker accessing a target disguised as a trusted third party
- Can be performed by hackers through either blind or active methods of spoofing

ARP Spoofing

- Modifying the Address Resolution Protocol (ARP) table for hacking purposes
- ARP table stores the IP address and the corresponding Media Access Control (MAC) address
- Router searches the ARP table for the destination computer's MAC address
- ARP spoofing attack involves detecting broadcasts, faking the IP address
  - And then responding with the MAC address of the hacker's computer

Web Spoofing

- Hacker spoofs an IP address through a Web site
- Hacker can transfer information or get information
- Hacker can spoof using a strategy
  - That ensures that all communication between the Web site and the user is directed to the hacker's computer
- Hacker may also falsely acquire a certificate used by a Web site

DNS Spoofing

- Hacker changes a Web site's IP address to the IP address of the hacker's computer
- Altering the IP address directs the user to the hacker's computer
- User is accessing the hacker's computer
  - Under the impression that he or she is accessing a different, legitimate, site

DNS Spoofing

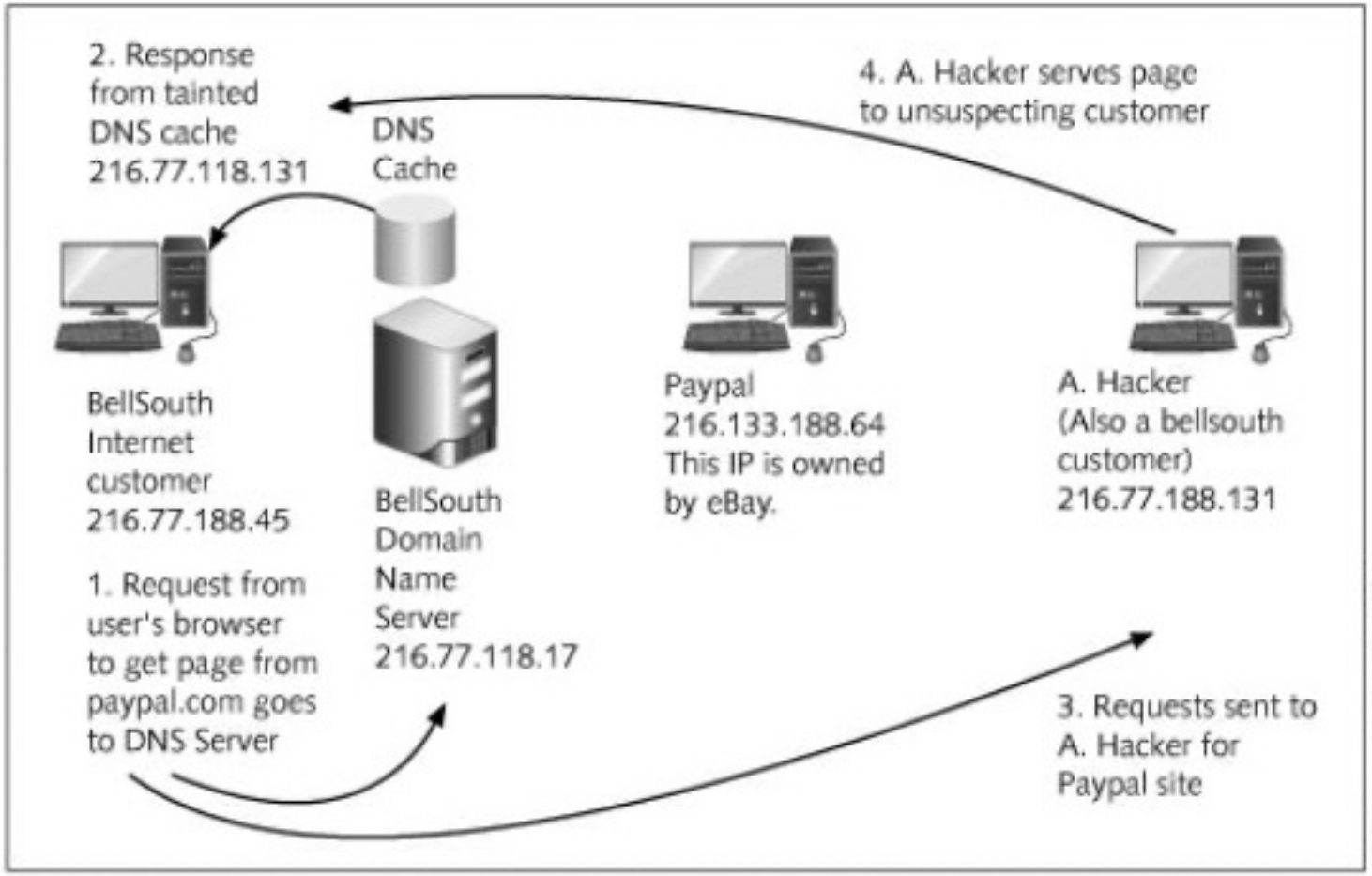

Figure 7-11 DNS spoofing

Spoofing Tools

- Apsend
- Ettercap
- Arpspoof

Prevention and Mitigation

- To avoid or defend against IP spoofing:
  - Wherever possible, avoid trust relationships that rely upon IP address only
  - On Windows systems—If you cannot remove it, change the permissions on the $systemroot$\hosts file to allow read only access
  - On Linux systems—Use TCP wrappers to allow access only from certain systems
  - Install a firewall or filtering rules
  - Use encrypted and secured protocols like IPSec
  - Use random ISNs

Prevention and Mitigation

- To avoid or defend against ARP poisoning:
  - Use methods to deny changes without proper authorization to the ARP table
  - Employ static ARP tables
  - Log changes to the ARP table

TCP Session Hijacking

- Hacker takes control of a TCP session between two hosts
- TCP session can be hijacked only after the hosts have authenticated successfully
  - Session cannot be initiated until the authentication process is finished.
  - A successful hijacking takes place when a hacker intervenes in a conversation, takes the role of either host or recipient, and then receives packets before the actual host.
  - Session hijacking can be accomplished by using
    - Source-routed IP packets, blind hijacking or a man-in- the-middle attack

TCP Session Hijacking

- Steps
  - An attacker desynchronizes a series of packets between the source and destination computer
  - Extra packets sent to one of the victims force the victim to choose which packet to accept
  - If the victim chooses to discard the authentic packets and interacts with the spoofed packets
    - The attacker has hijacked the connections

Session Hijacking – Hacker's Point of View

- TCP works with IP to manage data packets
- TCP tracks the packages sent to the receiver
- One popular method of session hijacking is using source-routed IP packets
- If source routing is turned off
  - The hacker can use blind hijacking
  - Guessing the responses of the two machines
- Hacker can also be inline between B and C, using a sniffing program to follow the conversation

Session Hijacking – Hacker's Point of View

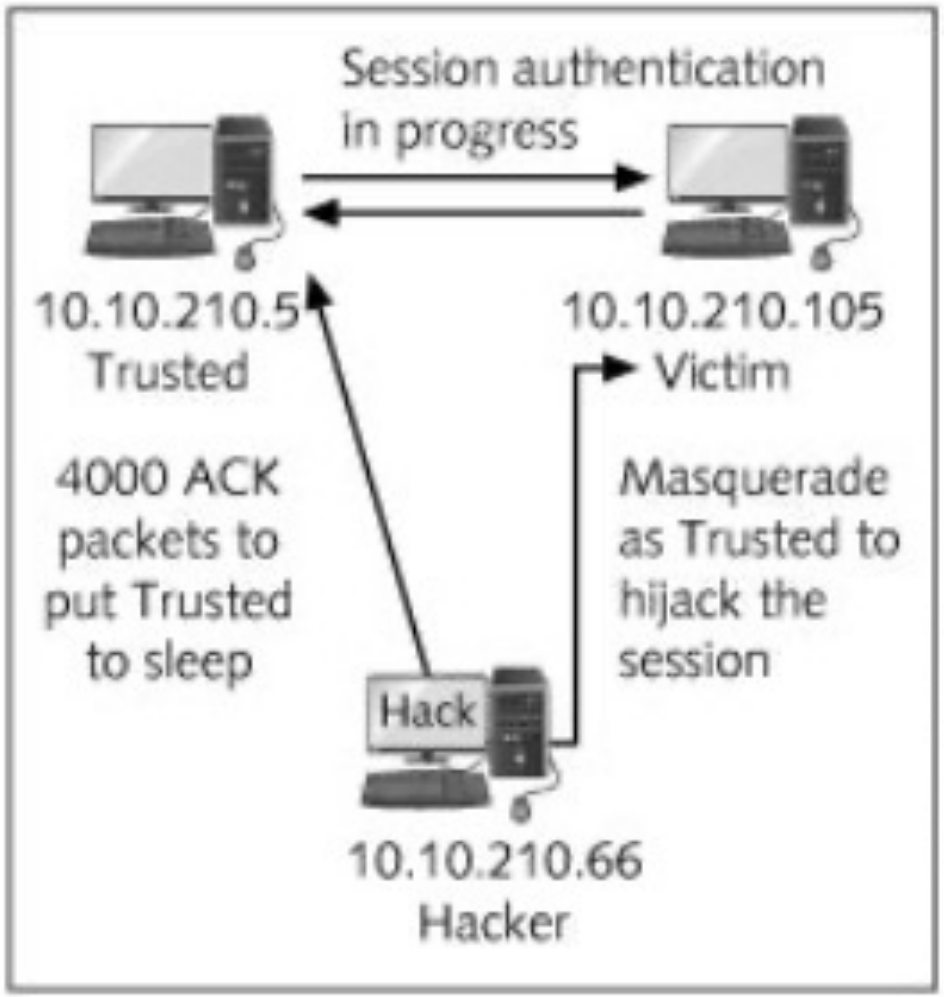

Figure 8-1 Denial-of-service (DoS) attack

Session Hijacking – Hacker's Point of View

- Hacker could find problems for two reasons:
  - Host computer that has been hijacked will continue to send the packets to the recipient
  - Recipient gives an ACK to the host computer after receiving packets from the hacker's computer

Session Hijacking – Hacker's Point of View

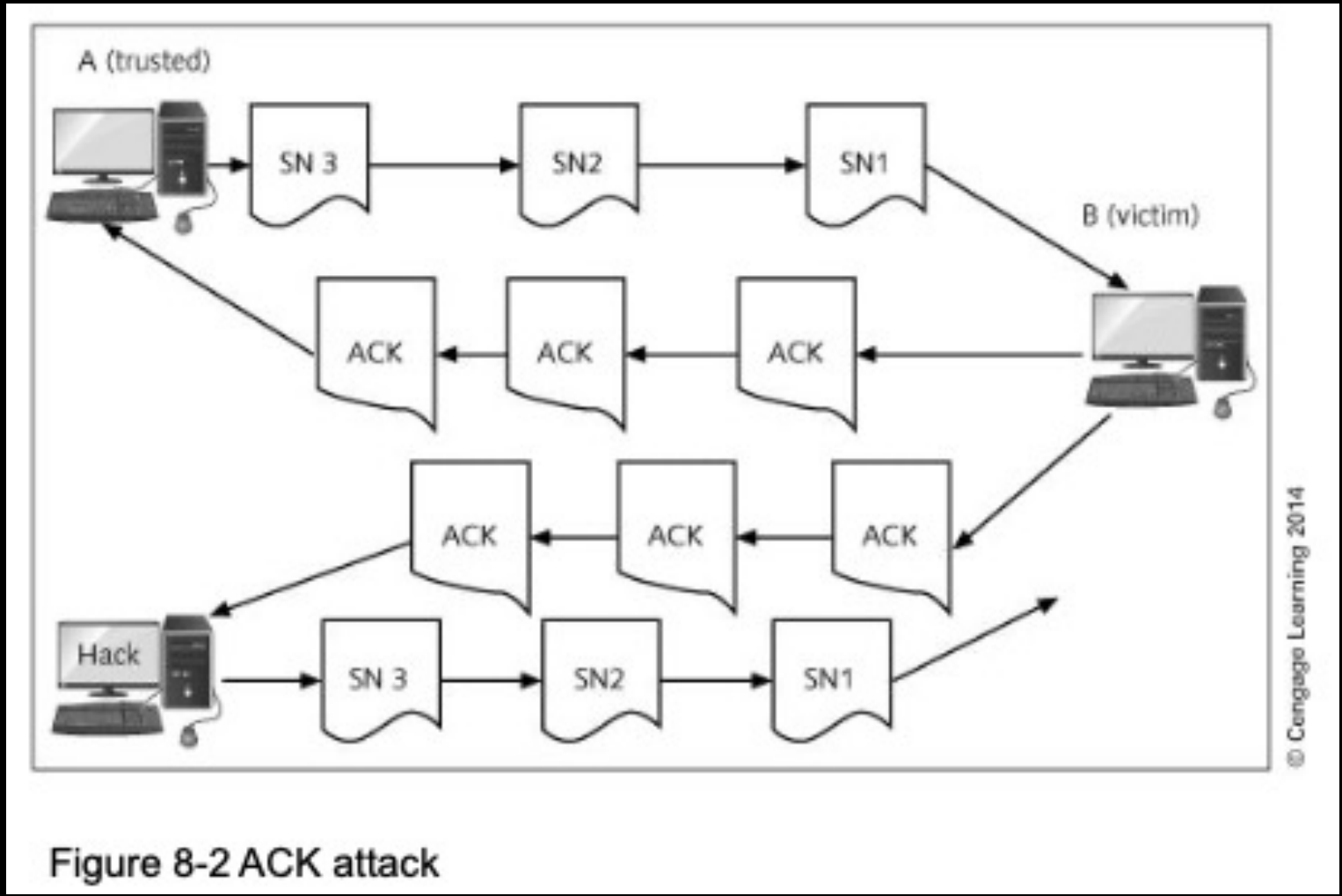

Figure 8-2 ACK attack

Session Hijacking – Hacker's Point of View

- **Continuous ACK Transfer**
  - Three ways to stop a continuous ACK transfer
    - Losing the ACK packet
    - Ending the connection
    - Resynchronizing the client and server

TCP Session Hijacking with Packet Blocking

- Packet blocking solves the ACK storm issue
  - And facilitates TCP session hijacking
- ACK storm happens because the attacker was not in a place to stop or delete packets sent by trusted computer
- Attacker must be in control of the connection itself
  - So that the session authentication takes place through the attacker's chosen channel

TCP Session Hijacking with Packet Blocking

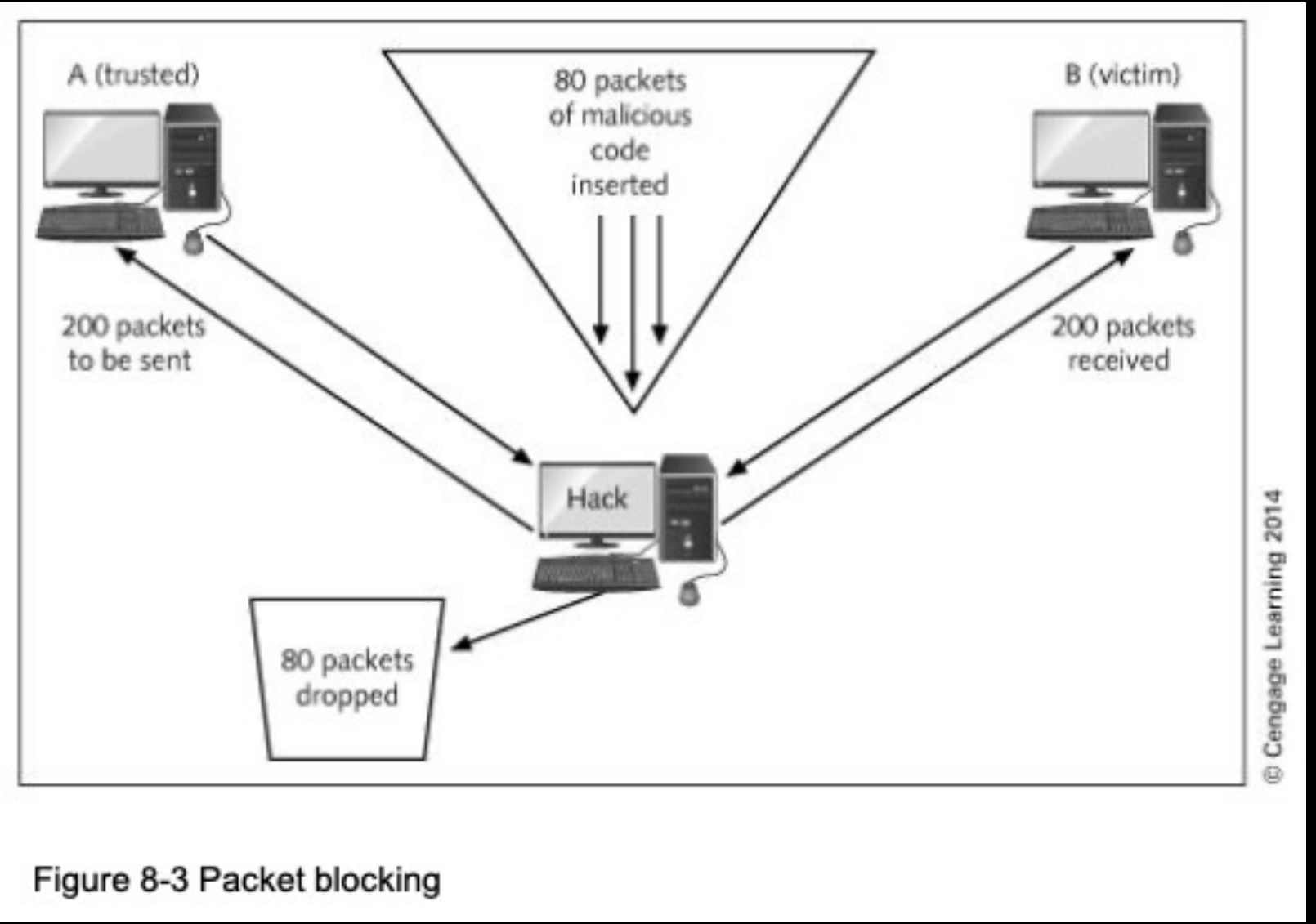

Figure 8-3 Packet blocking

TCP Session Hijacking with Packet Blocking

- Hacker can wait for the ACK packet to drop
  - Or manually synchronize the server and client records by spoofing
- If a hacker can block the packets
  - Can drop exact number of packets desired for transfer

Methods

- **Route Table Modification**
  - All computers that use TCP/IP keep a route table
  - A route table shows the way to the address sought
    - Or way to nearest source that might know the address
  - Route table has two sections
    - Active routes and active connections
  - If the route table can't locate a perfect match of the IP address
    - It searches for the closest possible match in the list of network addresses

```
wolf@l8:~$ netstat -nra
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
192.168.0.0     0.0.0.0         255.255.255.0   U         0 0          0 eth0
0.0.0.0         192.168.0.1     0.0.0.0         UG        0 0          0 eth0
wolf@l8:~$ netstat -n
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        1      0 192.168.0.102:44714     69.45.64.163:80         CLOSE_WAIT
tcp        1      0 192.168.0.102:44706     69.45.64.163:80         CLOSE_WAIT
tcp        0      0 192.168.0.102:49148     64.12.24.26:5190        ESTABLISHED
tcp        0      0 192.168.0.102:56944     207.46.4.53:1863        ESTABLISHED
tcp        1      0 192.168.0.102:49980     69.45.64.171:80         CLOSE_WAIT
tcp        0      0 192.168.0.102:58298     64.12.165.67:5190       ESTABLISHED
tcp        0      0 192.168.0.102:39341     152.2.210.65:80         ESTABLISHED
tcp        0      0 127.0.0.1:32769         127.0.0.1:57156         ESTABLISHED
tcp        0      0 127.0.0.1:49129         127.0.0.1:631           ESTABLISHED
tcp        0      0 127.0.0.1:57156         127.0.0.1:32769         ESTABLISHED
tcp        0      0 127.0.0.1:631           127.0.0.1:49129         ESTABLISHED
tcp        0      0 192.168.0.102:36909     216.155.193.170:5050    ESTABLISHED
tcp        0      0 192.168.0.102:36935     205.188.2.80:5190       ESTABLISHED
tcp        1      0 192.168.0.102:53510     208.254.57.141:80       CLOSE_WAIT
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags       Type       State         I-Node Path
unix  7      [ ]         DGRAM                    4611381  /dev/log
```

8-7

Source: Netstat

Figure 8-4 Linux route table

Methods

- **Route Table Modification**
  - After the match is found, the IP address of Computer A sends the packets to the IP address
  - If the route table cannot find a match, it refers the request to the network gateway
  - Active connections section shows the network addresses of the computers
    - That are connected with the host computer

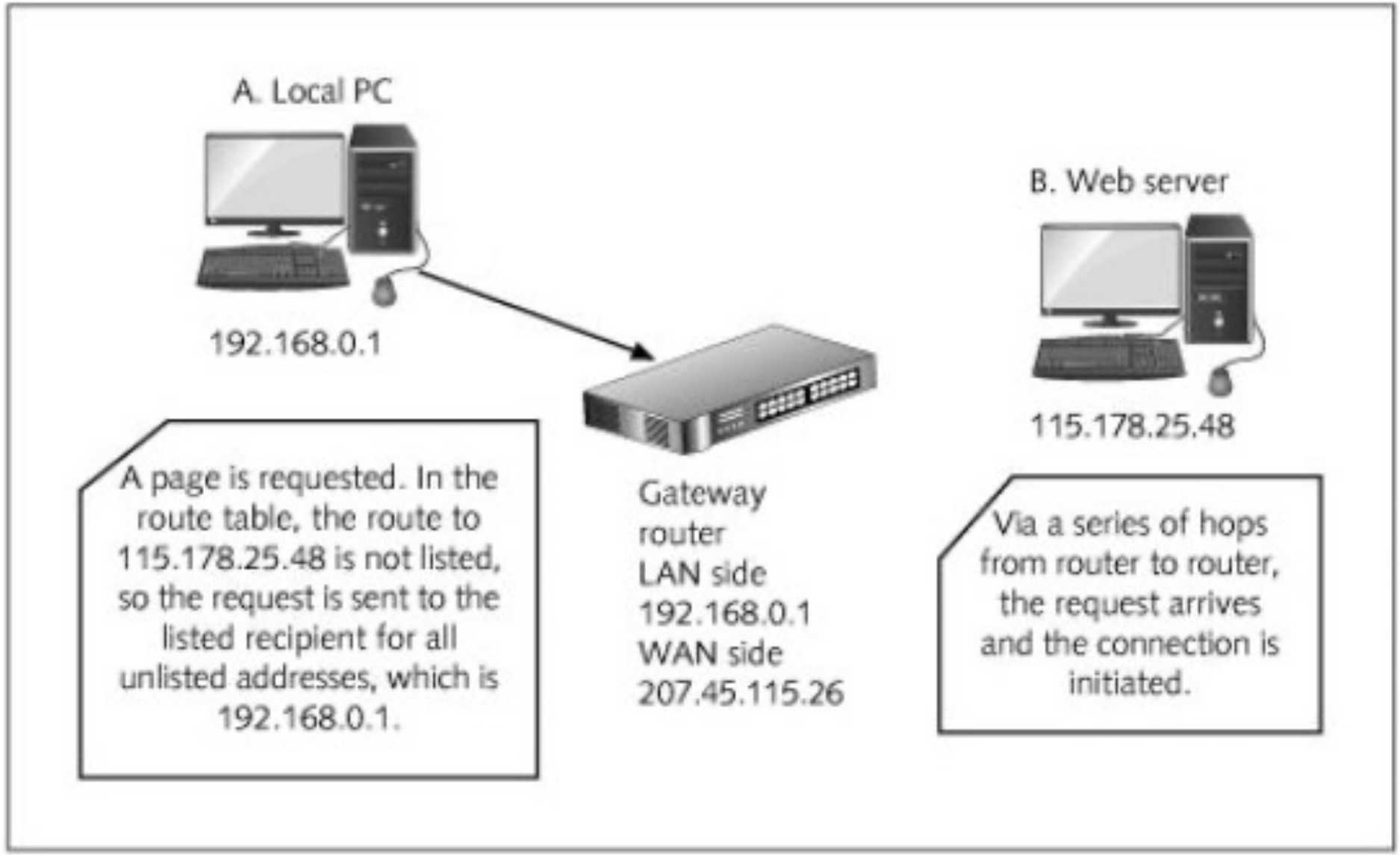

Figure 8-5 Route table in action

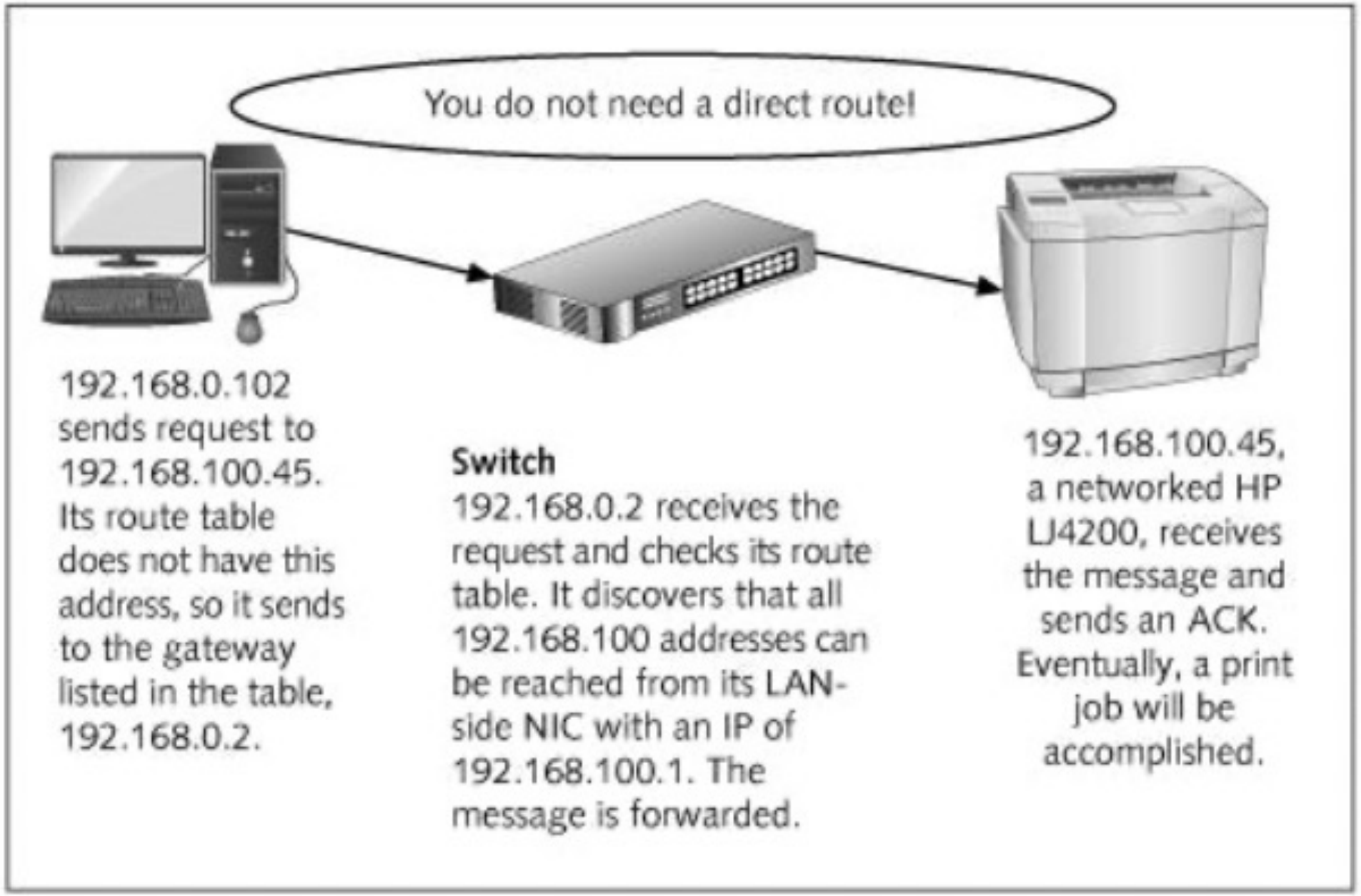

Figure 8-6 Route discovery

Methods

- **Route Table Modification**
  - Hacker changes the route table
  - Host computer assumes that the best possible path for the transfer of data packets is through the hacker's computer

Methods

- **Route Table Modification**
  - Hackers can modify a route table using two methods
    - Erase all necessary records from the route table
      - And then provide the hacker's own IP address as the default gateway address
    - Change the corresponding route in the route table of the gateway router

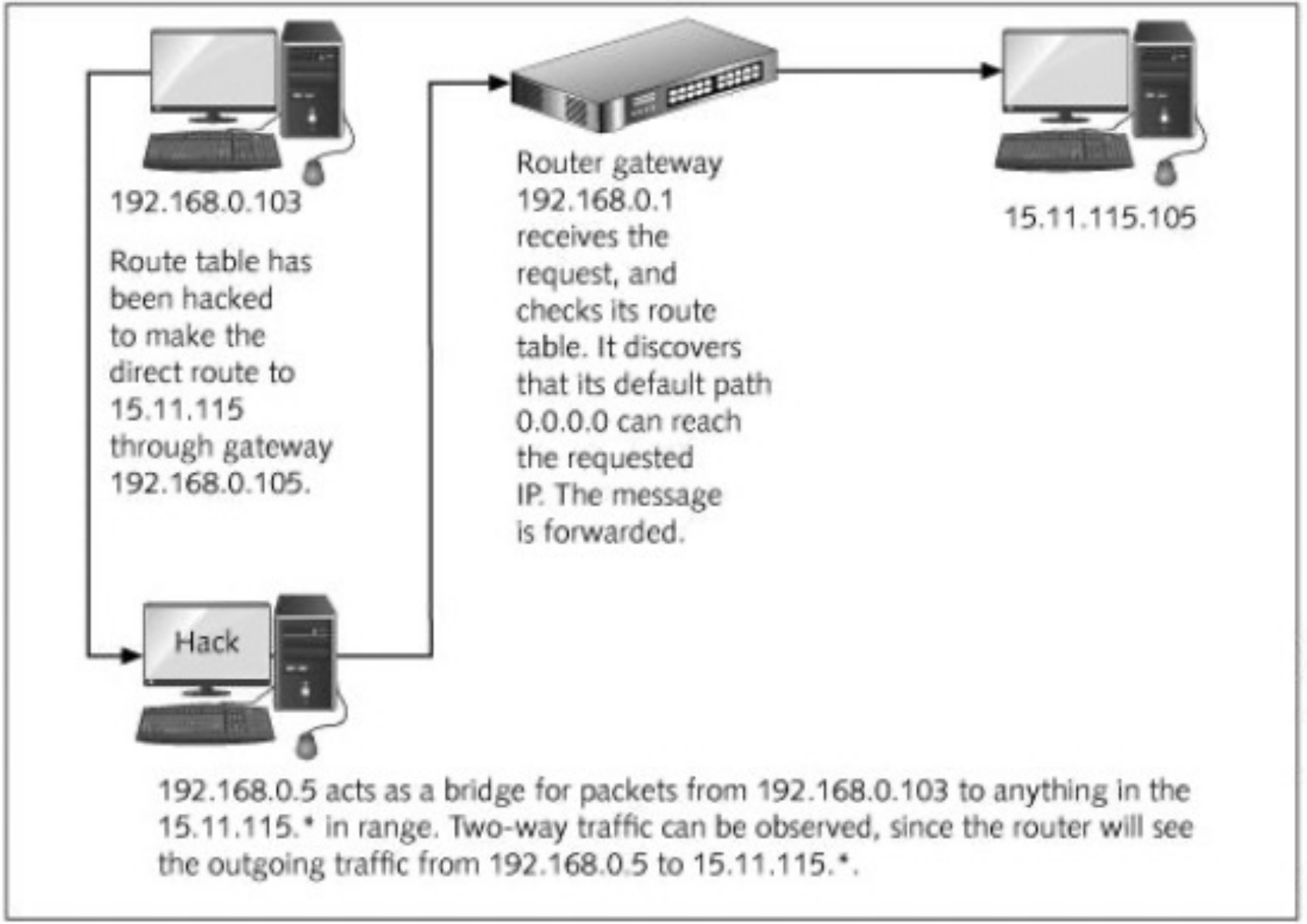

Figure 8-7 Route table modification hack

UDP Hijacking

- **User Datagram Protocol (UDP)**
  - Connectionless protocol that runs on top of IP networks
- UDP/IP provides very few error recovery services
  - Offers direct way to send and receive datagrams over an IP network
  - Used primarily for broadcasting messages
- More vulnerable to hijacking
  - Hacker needs only to sniff the network for a UDP request for a Web site and drop a spoofed UDP packet in before the Web server responds

Prevention and Mitigation

- Two methods to prevent session hijacking
  - Encryption
  - Storm watching

Encryption

- Hacker needs to be authenticated on the network to be able to successfully hijack a session
- If the data transfer is encrypted
  - It is far too complicated and time consuming to get authenticated
- Standard protocols like POP3, Telnet, IMAP, and SMTP are excellent targets
  - Because they transfer data as plaintext

Storm Watching

- Refers to setting an IDS rule to watch for abnormal increases in network traffic
  - And to alert the security officer when they occur
- An unexpected increase in traffic could be evidence of an ACK storm
- Packet size can be cached for a short period
  - Two packets with the same header information but different sizes could be evidence of a hijacking in progress

Storm Watching

- Three ways of stopping a continuous ACK transfer:
  - Losing an ACK packet,
  - Ending the TCP connection,
  - Resynchronizing the client and server
- Packet blocking places the hacker in the actual flow of packets, solving the problem of the ACK transmission storm
- TCP session hijacking with packet blocking can be performed in two ways:
  - Modify route table
  - Initiate an ARP attack

ARP Attacks

- An ARP table stores the IP address and corresponding MAC address.
- When the host computer does not have the MAC address, it transmits a broadcast message on the network called an ARP request in order to identify the destination computer's MAC address.
- Attackers can interrupt the response from the destination computer and change its MAC address to the MAC address of the attacker's computer
- All the packets that are sent to the destination computer will instead be sent to the attacker's computer

ICMP Attacks

- Packets are used to send fraudulent or deceptive connection information among computers
- ICMP is used to test for connectivity using utilities such as the *ping command*
- Denial-of-service (DoS) attacks can be formulated by using ICMP packets
  - Destination Unreachable and Time to Live Exceeded
- Attackers transmitting spoofed packets can successfully reset existing connections

TCP SYN Attacks

- Exploits host implementation of three-way handshake
- When Host B receives the SYN request from A, it must keep track of the partially opened connection
  - In a queue for at least 75 seconds
- Most systems are limited and can keep track of only a small number of connections
- An attacker can overflow the listed queue by sending more SYN requests than the queue can handle
  - SYN flooding

RIP Attacks

- Take advantage of RIP (Routing Information Protocol)
- RIP
  - Essential component in a TCP/IP network
  - Distribution of routing information within networks
- RIP packet is often used without verification
  - Attacks on RIP change the destination of data
- Once the router is modified, it transmits all of the packets to the hacker computer

Securing TCP/IP

- Data in packets is not encrypted or authenticated
- Packet sniffer can observe contents of the packets
- Attackers can send spoofed packets from any computer
- Must employ many methods simultaneously to achieve success in this area

Securing TCP/IP

- Methods to decrease vulnerabilities in TCP/IP
  - Modify default timer values
  - Increase the number of simultaneous connections that a computer can handle
  - Reduce the time limit used to listen for replies to the SYN/ACK in the three-way handshake
  - Change method used to generate sequence numbers
  - Firewall rules that block spoofed packets

Securing TCP/IP

- Methods to decrease vulnerabilities in TCP/IP
  - Avoid using the source address authentication
  - If an operator allows outside connections from trusted hosts, enable encryption sessions at the router
  - Packets can be encrypted or sent via encrypted VPN

IP Security Architecture (IPSec)

- **IP Security Architecture (IPSec)**
  - Collection of Internet Engineering Task Force (IETF) standards
  - Defines an architecture at the Internet Protocol (IP) layer that protects IP traffic
    - By using various security services

IP Security Architecture (IPSec)

Table 5-4 Some IPSec protocols

RFC Number	Name	Description
2401	Security Architecture for the Internet Protocol	The main IPSec document, describing the architecture and general operation of the technology, and showing how the different components fit together
2402	IP Authentication Header	Defines the IPSec Authentication Header (AH) protocol used for ensuring data integrity and origin verification
2403	The Use of HMAC-MD5-96 within ESP and AH	Describes a particular encryption algorithm for use by AH and ESP called Message Digest 5 (MD5)
2404	The Use of HMAC-SHA-1-96 within ESP and AH	Describes a particular encryption algorithm for use by AH and ESP called Secure Hash Algorithm 1 (SHA-1)

IP Security Architecture (IPSec)

Table 5-4 Some IPSec protocols (continued)

RFC Number	Name	Description
2406	IP Encapsulating Security Payload (ESP)	Describes the IPSec Encapsulation Security Payload (ESP) protocol that provides data encryption for confidentiality
2408	Internet Security Association and Key Management Protocol (ISAKMP)	Defines methods for exchanging keys and negotiating security associations
2409	The Internet Key Exchange (IKE)	Describes the Internet Key Exchange (IKE) protocol used to negotiate security associations and exchange keys between devices for secure communications; based on ISAKMP and OAKLEY
2412	The OAKLEY Key Determination Protocol	Describes a generic protocol for key exchange

IP Security Architecture (IPSec)

- IPSec provides:
  - Encryption of user data for privacy
  - Authentication of the integrity of a message
  - Protection against certain types of security attacks, such as replay attacks
  - Ability for devices to negotiate security algorithms and keys required for secure authenticated connections
  - Two security modes, tunnel and transport, to meet different network needs

Summary

- Spoofing
  - IP
  - ARP
  - DNS
  - Web
- TCP session hijacking
- UDP hijacking
- ARP attack
- ICMP attack
- TCP SYN attack
- RIP attack
- Securing TCP/IP
- IPSec

References

- [Textbook 3] Chapter 5