Info Security Technology

Topic 4
Network Security
(Network Attack)

Types of Network Attacks

1. Denial of service
2. Man-in-the-middle
3. Replay
4. ARP Poisoning
5. DNS Poisoning

Denial of Service (DoS)

Denial-Of-Service Attack = DOS Attack is a malicious attempt by a single person or a group of people to cause the victim, site or node to deny service to it customers.

- Attempts to consume network resources so that the network or its devices cannot respond to legitimate requests
- DoS = when a single host attacks
- DDoS = when multiple hosts attack simultaneously

DOS ATTACKS

Flooding

- Attacker sends an overwhelming number of messages at your machine; great congestion
- The congestion may occur in the path before your machine
- Messages from legitimate users are crowded out
- Usually called a Denial of Service (DoS) attack, because that's the effect.
- Usually involves a large number of machines, hence Distributed Denial of Service (DDoS) attack
- Examples:
  - *TCP-SYN Flooding*: The last message of TCP's 3 way handshake never arrives from source.
  - Congesting a victim's incoming link using ICMP messages, RST packets or UDP packets.

Denial of Service (DoS)

Distributed denial of service (DDoS) attack

- A variant of the DoS
- May use hundreds or thousands of zombie computers in a botnet to flood a device with requests

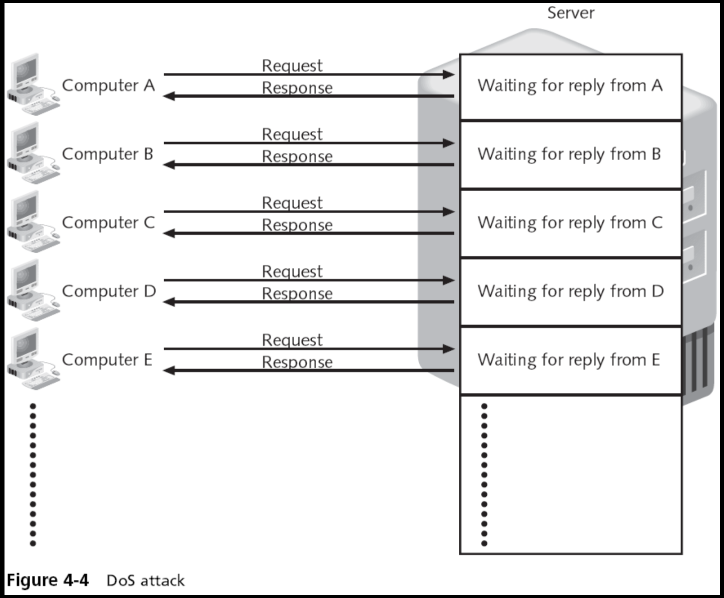
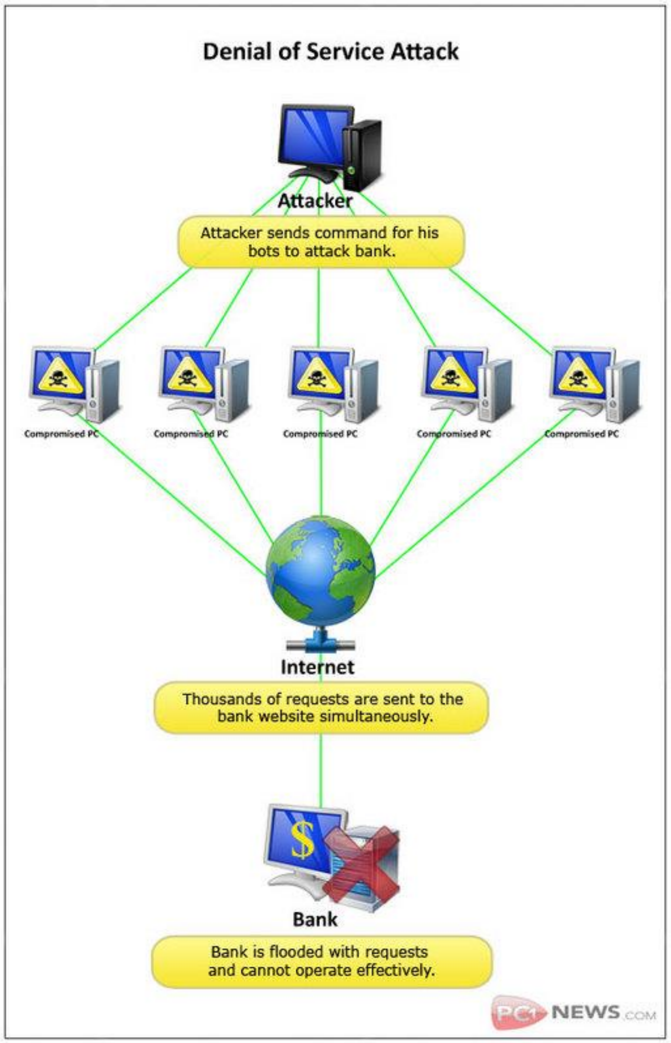


Figure 4-4 DoS attack



Denial of Service Attack
Attacker
Attacker sends command for his bots to attack bank.
Compromised PC
Compromised PC
Compromised PC
Compromised PC
Compromised PC
Internet
Thousands of requests are sent to the bank website simultaneously.
Bank
Bank is flooded with requests and cannot operate effectively.
PC1 NEWS.COM

IDEA OF "DOS ATTACKS"

- Purpose is to shut down a site, not penetrate it.
- Purpose may be vandalism, extortion or social action (including terrorism) (Sports betting sites often extorted)
- Modification of internal data, change of programs (Includes defacement of web sites)

Man-in-the-Middle

2. Man-in-the-middle attack
   - Intercepts legitimate communication and forges a fictitious response to the sender
   - Can be active or passive
     - Passive attacks attackers captures and records the data and pass on.
     - Active attacks intercept and alter the contents before they are sent on to the recipient.

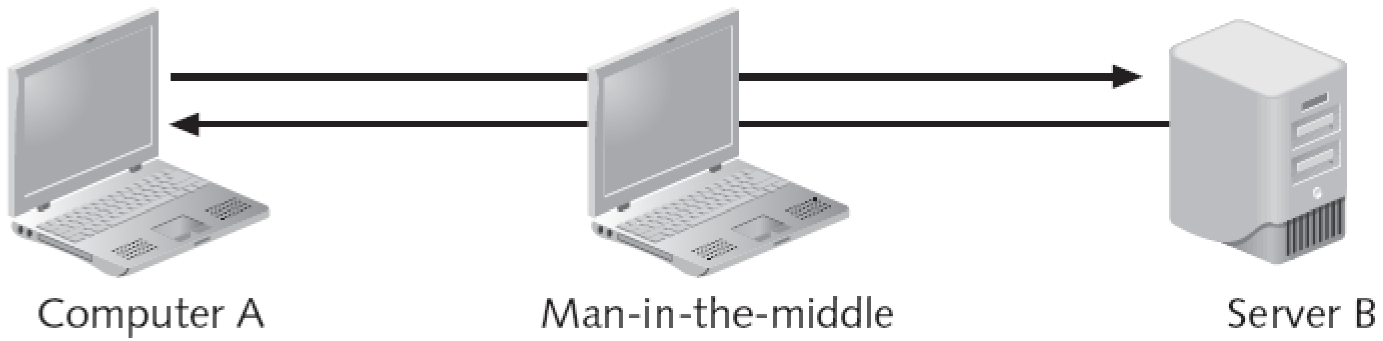
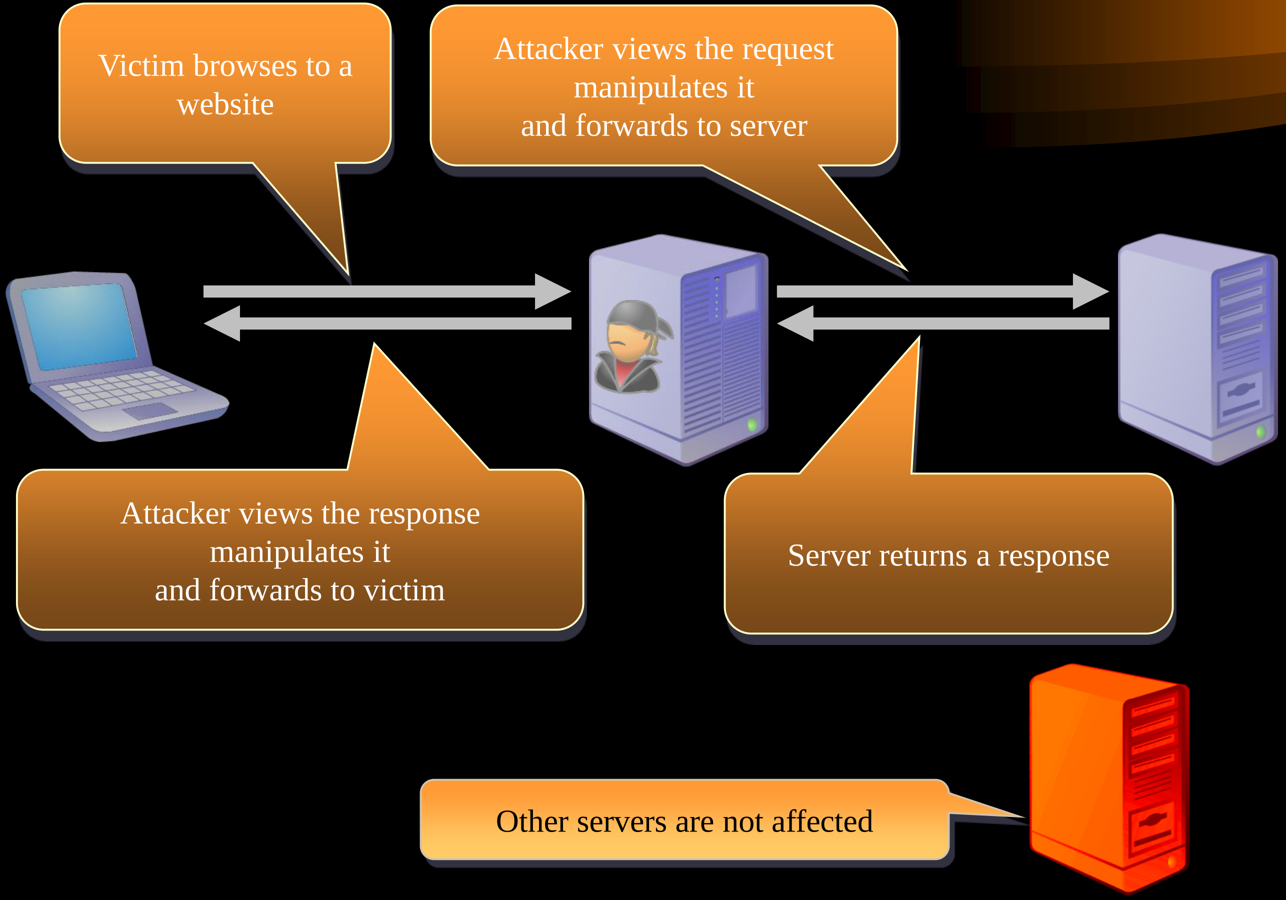


Figure 4-8 Man-in-the-middle attack

Passive Man in the Middle Attacks



Victim browses to a website

Attacker views the request manipulates it and forwards to server

Attacker views the response manipulates it and forwards to victim

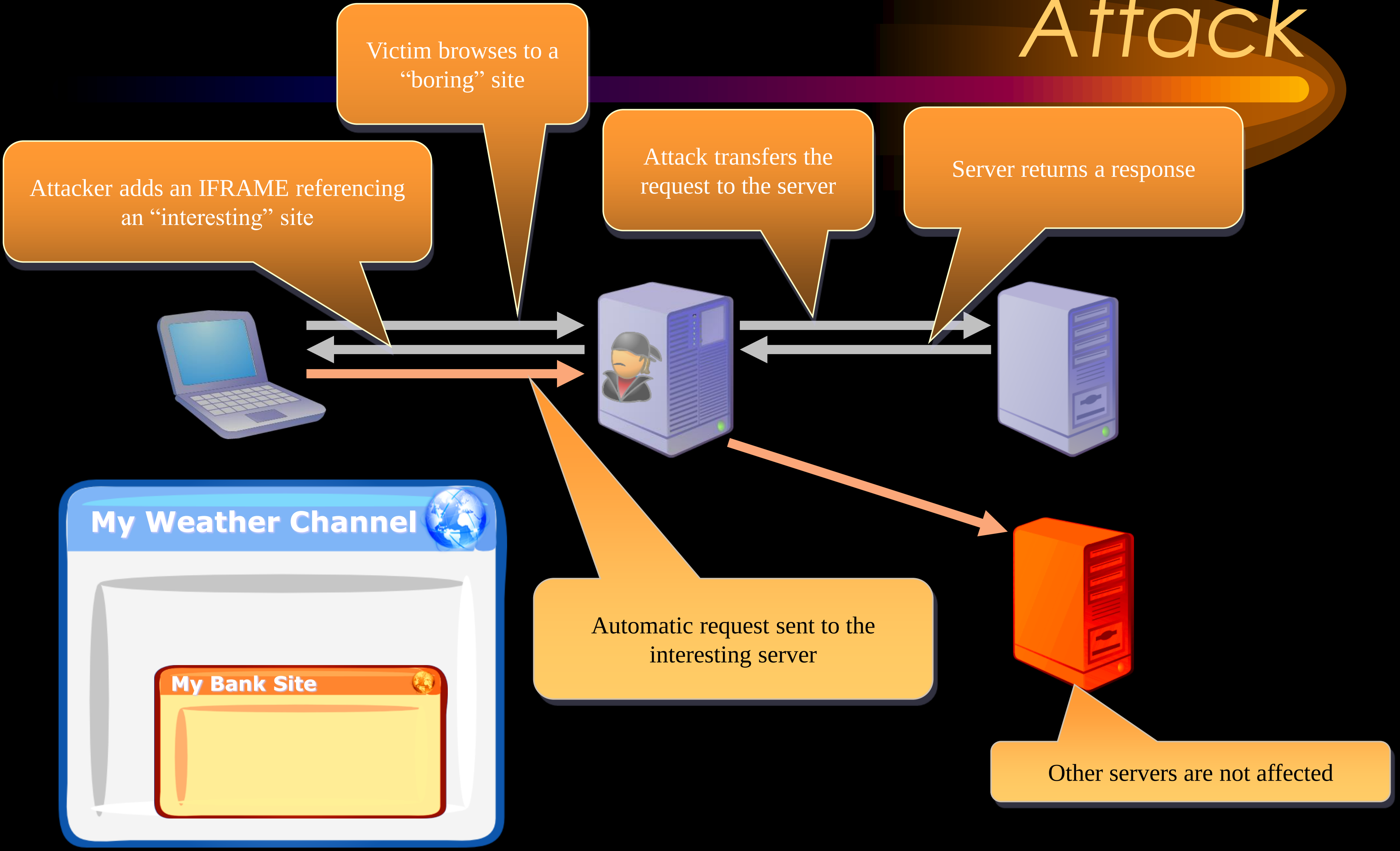
Server returns a response

Other servers are not affected

Active Man in the Middle Attack

- The attacker actively directs the victim to an “interesting” site
- The IFrame could be invisible

Active Man in the Middle Attack



Victim browses to a “boring” site

Attacker adds an IFRAME referencing an “interesting” site

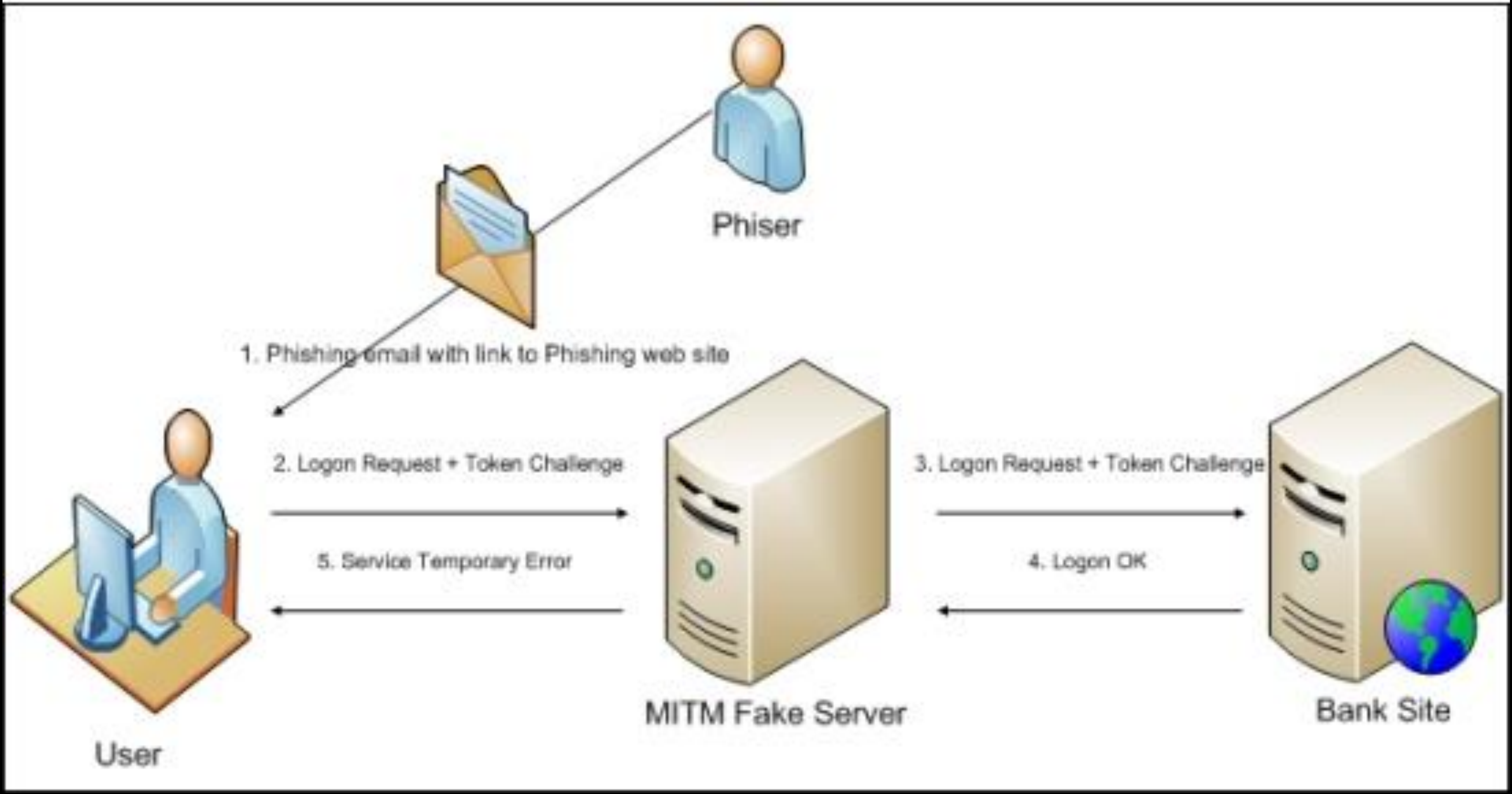
Attack transfers the request to the server

Server returns a response

Automatic request sent to the interesting server

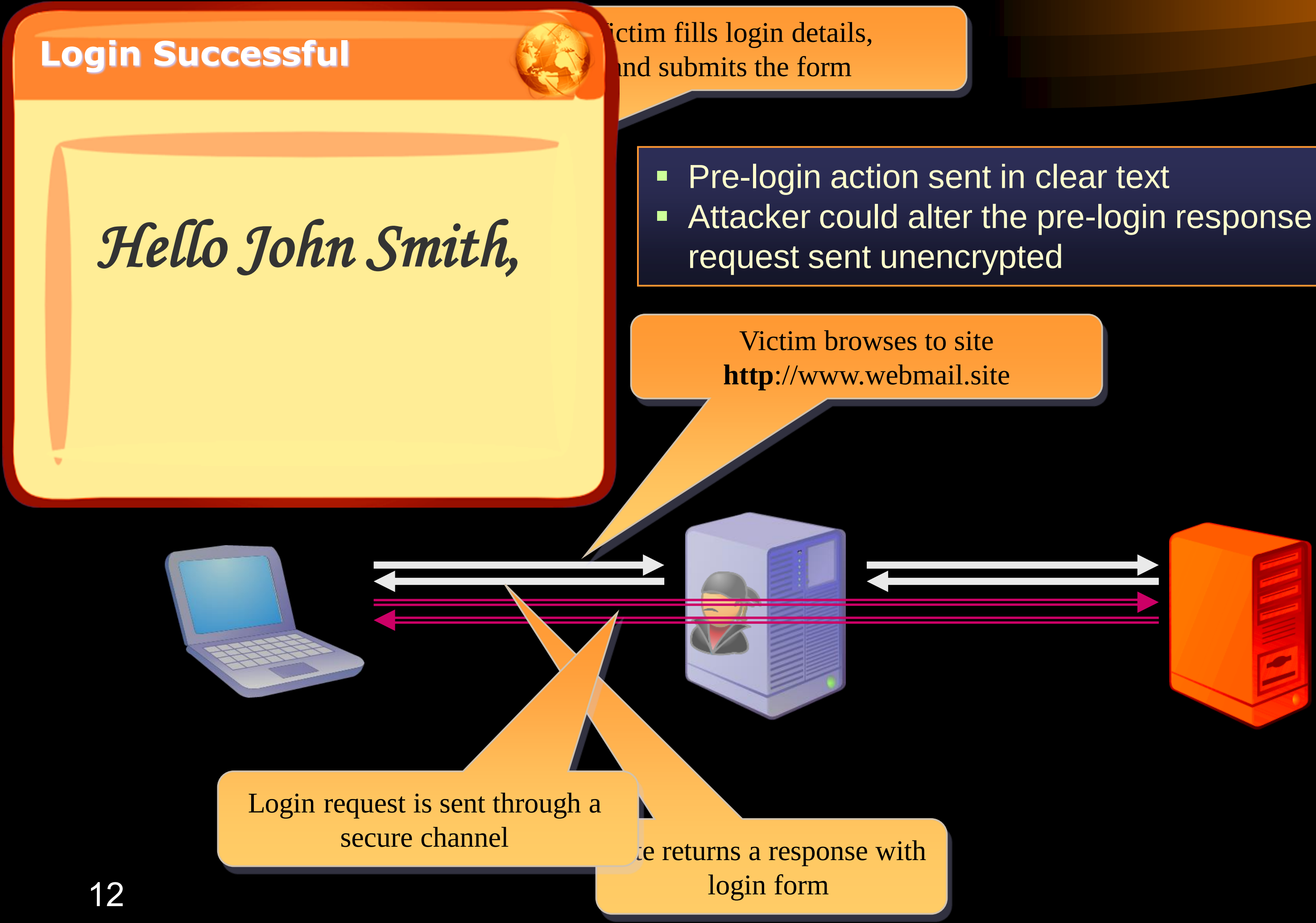
Other servers are not affected

2FA Man-in-the-Middle Attack


Phiser
1. Phishing email with link to Phishing web site
2. Logon Request + Token Challenge
5. Service Temporary Error
3. Logon Request + Token Challenge
4. Logon OK
User
MITM Fake Server
Bank Site

Secure Connections

- Pre-login action sent in clear text
- Attacker could alter the pre-login response to make the login request sent unencrypted



ictim fills login details,
nd submits the form

Victim browses to site
http://www.webmail.site

te returns a response with
login form

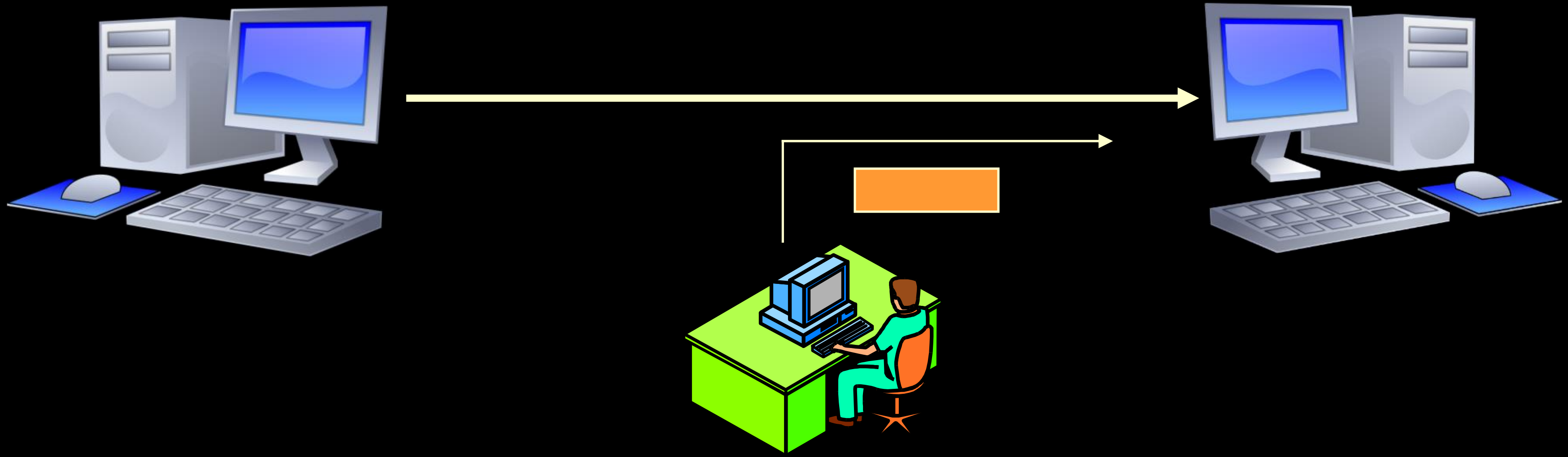
Login request is sent through a
secure channel

Replay

3. Replay attack
   - Similar to a passive man-in-the-middle attack
   - Captured data is used at a later time
   - A simple replay would involve the man-in-the-middle capturing login credentials between the computer and the server
   - A more sophisticated attack takes advantage of the communications between a device and a server
     - Administrative messages that contain specific network requests are frequently sent between a network device and a server

Replay Attack

- Why replay attacks?
  - To gain access to resources by replaying an authentication message
  - In a denial-of-service attack, to confuse the destination host

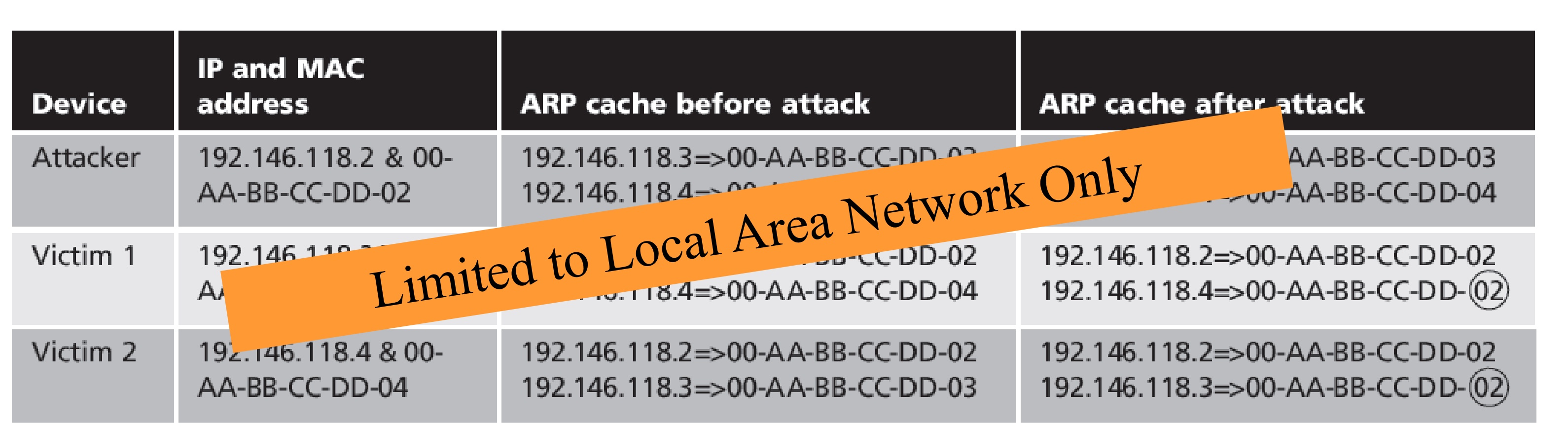


Overcoming Replay Attacks

- Random number generation.
- Integrity checks
- Put a time stamp in each message to ensure that the message is "fresh" - do not accept a message that is too old

ARP Poisoning

4. ARP poisoning attack
   - ARP (Address Resolution Protocol)
   - Used by TCP/IP on an Ethernet network to find the MAC (Media Access Control) address (manufacturer's unique identifier) of devices
   - Attacker modifies MAC address in ARP cache to point to different computer

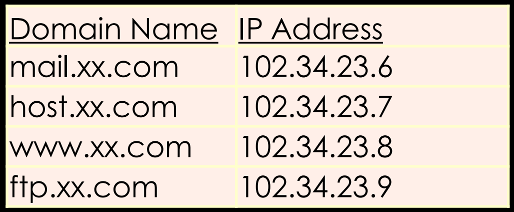


Device	IP and MAC address	ARP cache before attack	ARP cache after attack
Attacker	192.146.118.2 & 00-AA-BB-CC-DD-02	192.146.118.3=>00-AA-BB-CC-DD-0[illegible] 192.146.118.4=>[illegible]	[illegible]AA-BB-CC-DD-03 [illegible]=>00-AA-BB-CC-DD-04
Victim 1	192.146.[illegible] A[illegible]	[illegible]-CC-DD-02 [illegible].118.4=>00-AA-BB-CC-DD-04	192.146.118.2=>00-AA-BB-CC-DD-02 192.146.118.4=>00-AA-BB-CC-DD-02
Victim 2	192.146.118.4 & 00-AA-BB-CC-DD-04	192.146.118.2=>00-AA-BB-CC-DD-02 192.146.118.3=>00-AA-BB-CC-DD-03	192.146.118.2=>00-AA-BB-CC-DD-02 192.146.118.3=>00-AA-BB-CC-DD-02

Limited to Local Area Network Only

DNS Poisoning

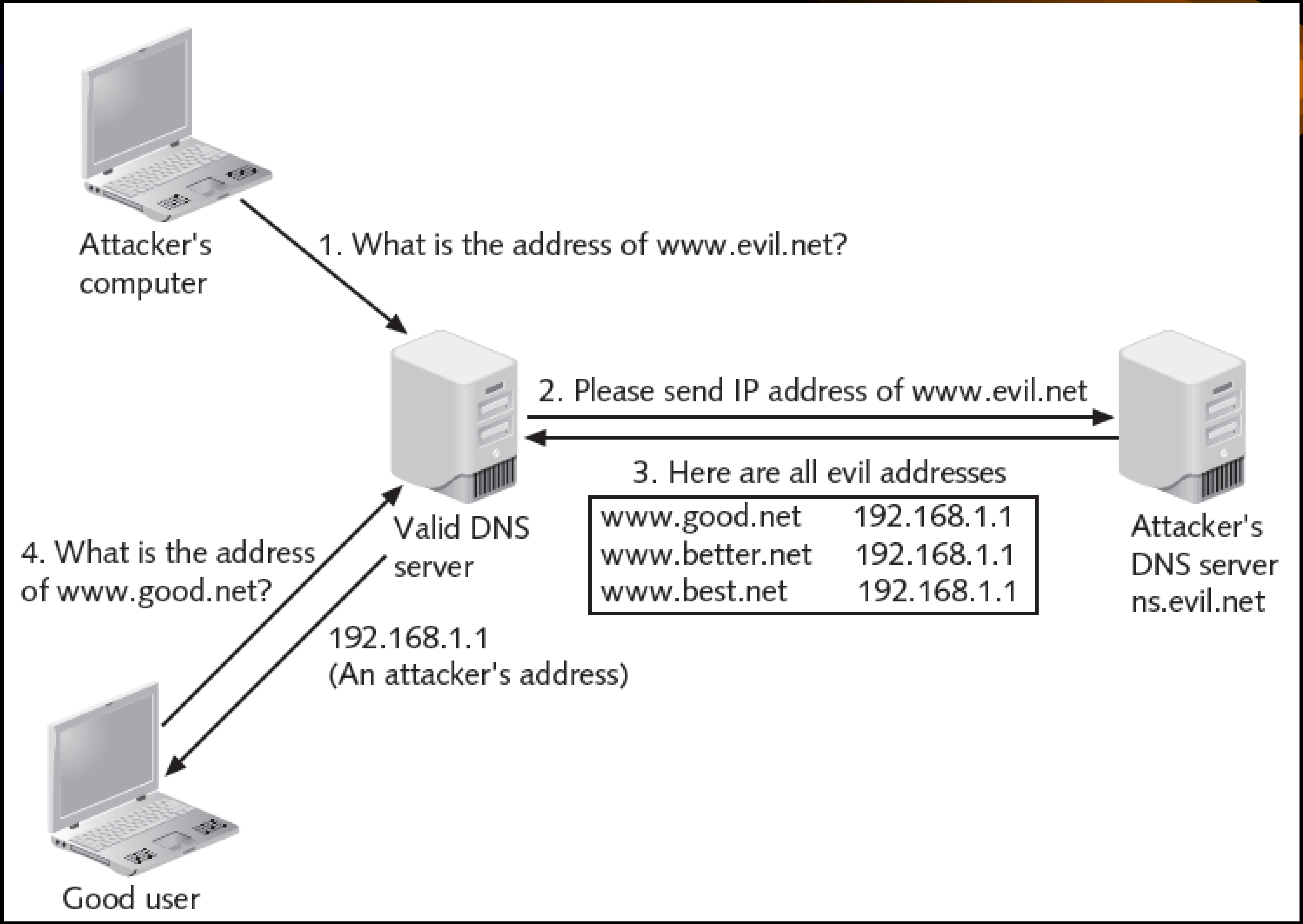
5. DNS poisoning
   - Domain Name System is current basis for name resolution to IP address
   - DNS poisoning substitutes DNS addresses to redirect computer to another device
   - Two locations for DNS poisoning
     - Local host table
     - External DNS server



Domain Name	IP Address
mail.xx.com	102.34.23.6
host.xx.com	102.34.23.7
www.xx.com	102.34.23.8
ftp.xx.com	102.34.23.9

The Chinese government uses DNS poisoning to prevent Internet content that it considers unfavourable to reach its citizenry.

DNS Poisoning



Attacker's computer

1. What is the address of www.evil.net?

2. Please send IP address of www.evil.net

3. Here are all evil addresses

www.good.net	192.168.1.1
www.better.net	192.168.1.1
www.best.net	192.168.1.1

Valid DNS server

Attacker's DNS server ns.evil.net

4. What is the address of www.good.net?

192.168.1.1
(An attacker's address)

Good user

DNS Poisoning

- Local Host Table Poisoning
  - *Windows 95/98/Me*
    - **c:\windows\hosts**
  - *Windows NT/2000/XP Pro*
    - **c:\winnt\system32\drivers\etc\hosts**
  - *Windows XP onwards*
    - **c:\windows\system32\drivers\etc\hosts**
  - ***UNIX, Linux, Mac***
    - /etc/hosts

Crafting a Secure Network

- A common mistake in network security
  - Attempt to patch vulnerabilities in a weak network that was poorly conceived and implemented from the start
- Securing a network begins with the design of the network and includes secure network technologies

Secure Network Design: Subnetting

- Security is enhanced by subnetting a single network
  - Multiple smaller subnets isolates groups of hosts
- Network administrators can utilize network security tools
  - Makes it easier to regulate who has access in and out of a particular subnetwork
- Subnets also allow network administrators to hide the internal network layout

Secure Network Design: Subnetting

- Allows an IP address to be split anywhere
- Networks can essentially be divided into three parts: network, subnet, and host

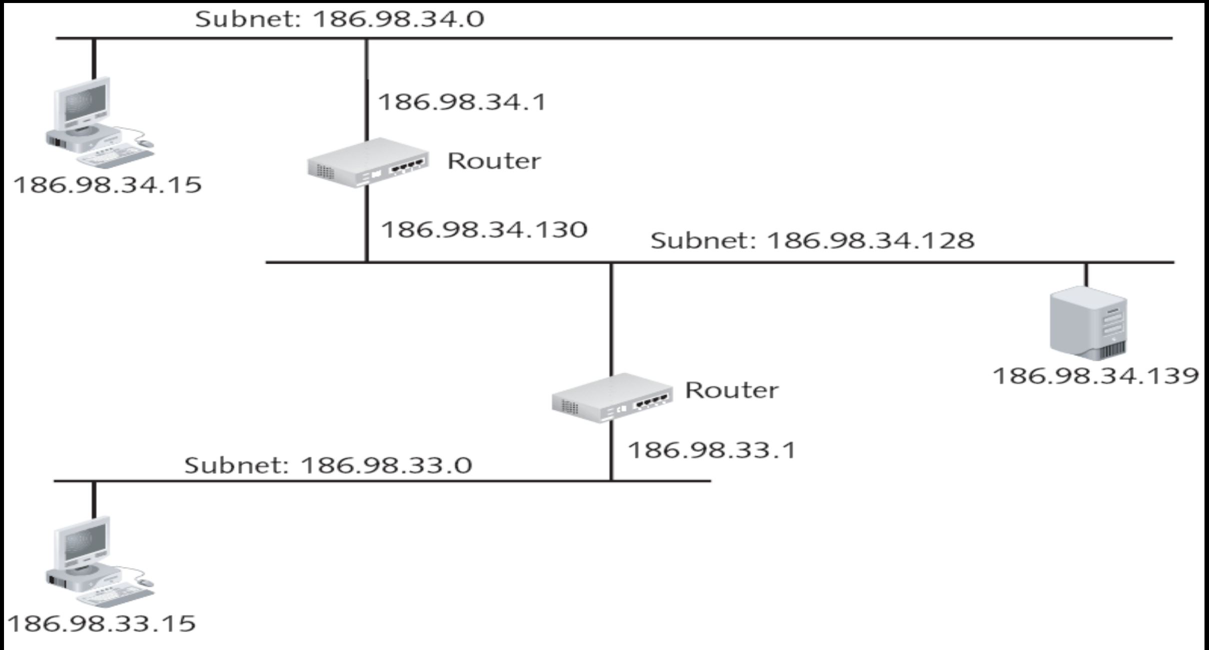


Figure 5-1 Subnets

Secure Network Design: Virtual LAN

- Allows scattered users to be logically grouped together even though they may be attached to different switches
- Can reduce network traffic and provide a degree of security similar to subnetting:
  - VLANs can be isolated so that sensitive data is transmitted only to members of the VLAN
- A VLAN is heavily dependent upon the switch for correctly directing packets
  - Attacks on the switch that attempt to exploit vulnerabilities such as weak passwords or default accounts are common

Secure Network Design: Virtual LAN

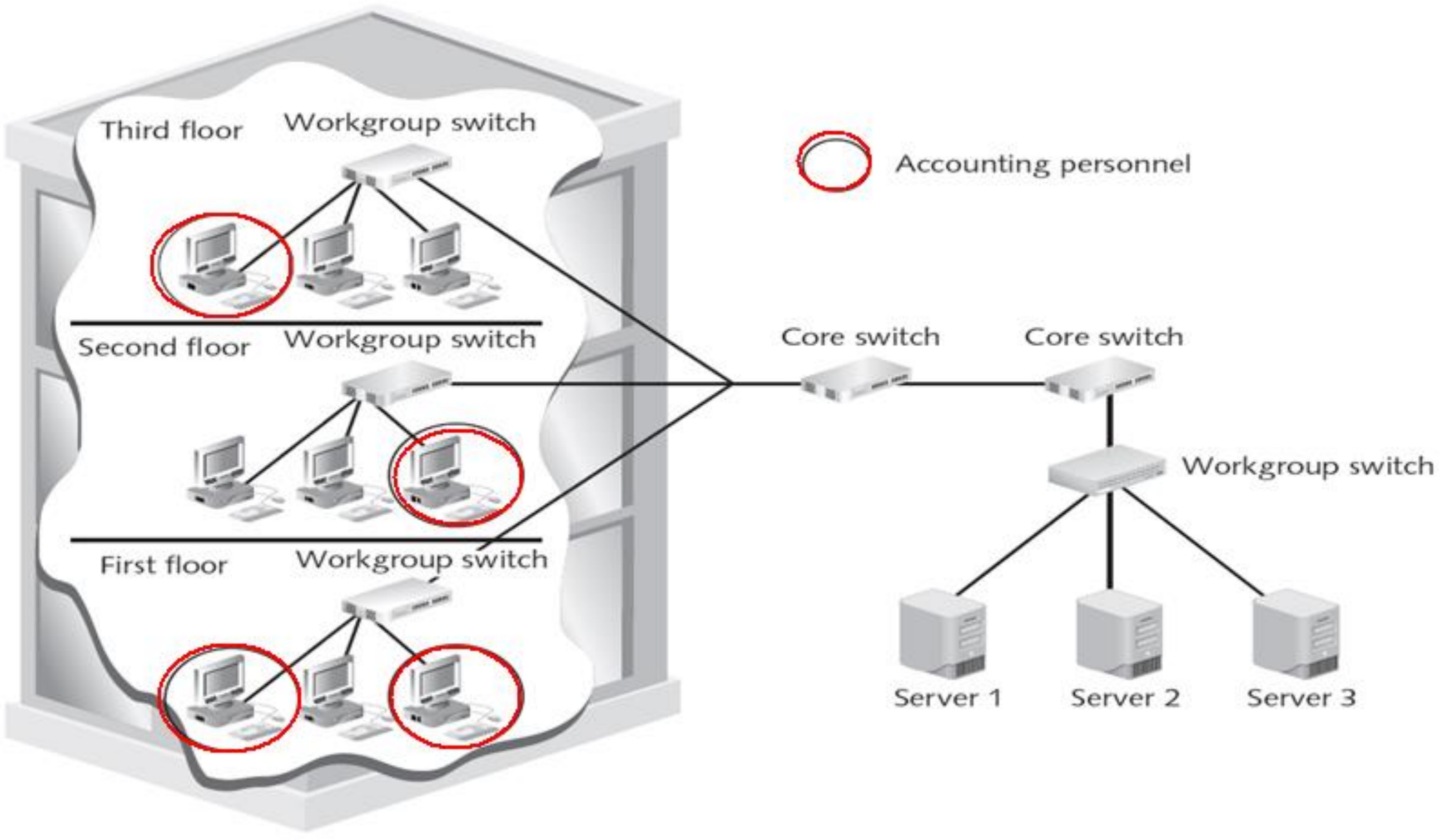


Figure 5-3 Scattered accounting personnel

Class assignment

Network Firewall Comparison

- Use the Internet to identify two (2) network firewalls, and create a chart that compares their features.
- Note if they are rule-based or application-aware, perform stateless or stateful packet filtering, what additional features they include (IDS, content filtering, etc.), their costs, etc.
- Which would you recommend?
- Why?