Network & Internet Security, vulnerabilities, attack scenarios and controls

Presented by:

Alexandros Lykesas & Fotis Papazisis
Senior undergraduate students
Dept. of Informatics & Comp. Technology
T.E.I. of Western Macedonia, Greece

TECHNOLOGICAL EDUCATIONAL INSTITUTION OF WESTERN MACEDONIA

Reviewed by:

Spyridon Nikolaou, MSc
Lecturer,
Dept. of Informatics & Comp. Technology
T.E.I. of Western Macedonia, Greece

ERASMUS INTENSIVE PROGRAMME
The Information Warfare, Cyber Warfare and Open Sources Intelligence:
An Interdisciplinary Approach
Yasar University, Izmir, 16

Contents

- General Vulnerabilities
- Firewalls
- Antiviruses
- Virtual Private Networks
- Internet Protocol (IP) level Security
- Wireless Networks
- Intrusion Detection System (IDS)
- Attack Scenarios

Definitions

Network

Internet

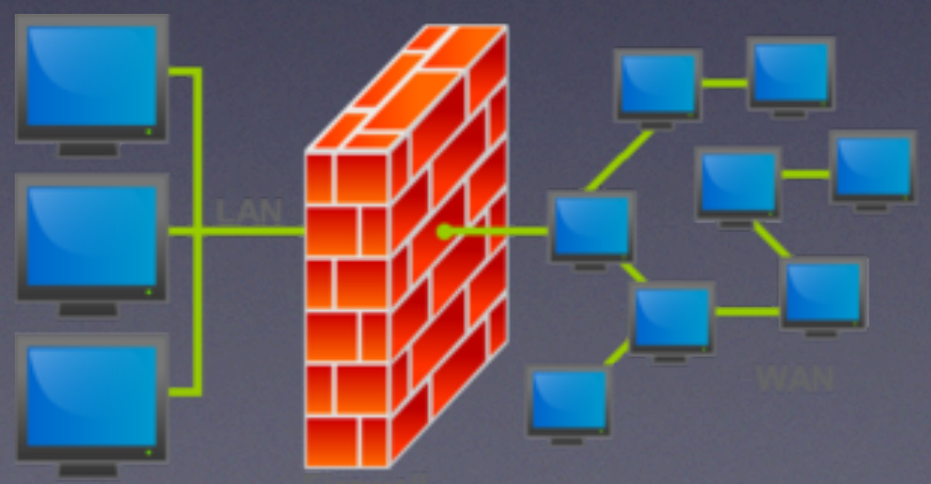
Network & Internet security

General Vulnerabilities

- Use of the same operating system
- Software bugs
- Over-Privileged Users
- Weight of numbers
- Unconfirmed code

Firewalls

- Permits or denies network transmissions based upon a set of rules.
- Internal traffic is not seen by the firewall.
- Must be strategically placed so that all traffic between the internal network and outside world passes through it.



Demilitarized Zone (DMZ)

- Connections from the internal and the external network to the DMZ are permitted, while connections from the DMZ are only permitted to the external network — hosts in the DMZ may not connect to the internal network.

Demilitarized Zone (DMZ)

- This allows the DMZ's hosts to provide services to both the internal and external network while protecting the internal network in case intruders compromise a host in the DMZ.

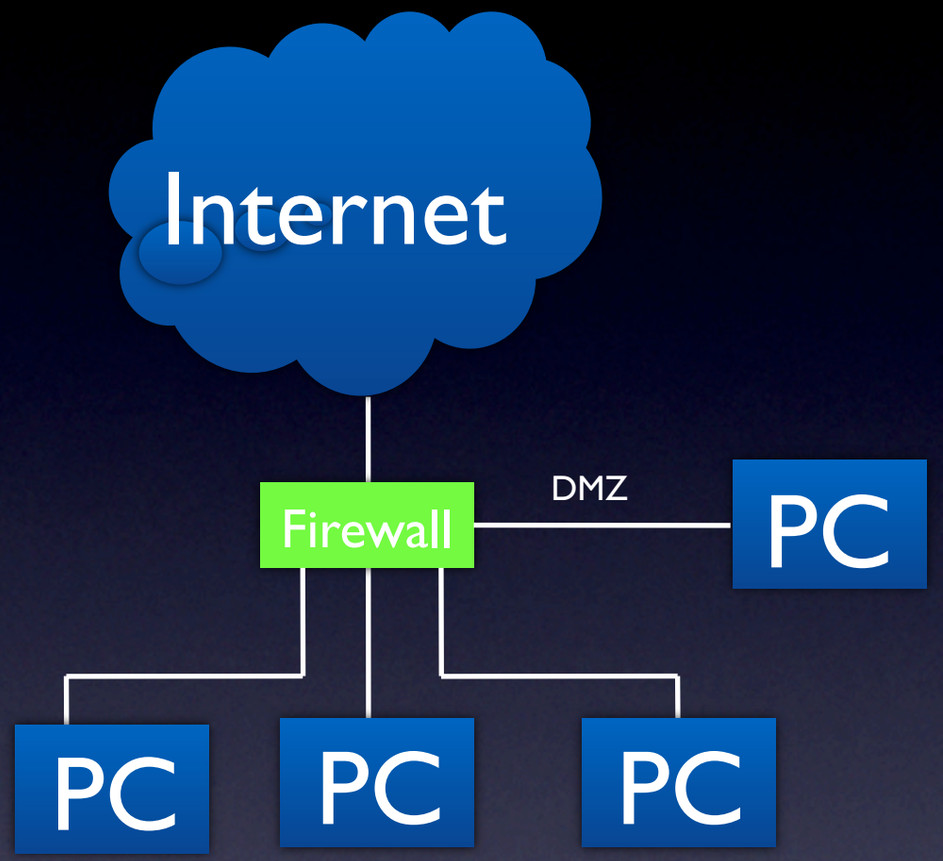
- This allows the DMZ's hosts to provide services to both the internal and external network while protecting the internal network in case intruders compromise a host in the DMZ.

Software Firewall

Software loaded on a PC that performs a firewall function. Protects ONLY that computer There are many commercially available software firewall products. After loading on a PC, it may have to be configured correctly in order to perform optimally. Many operating systems contain a built-in software firewall.

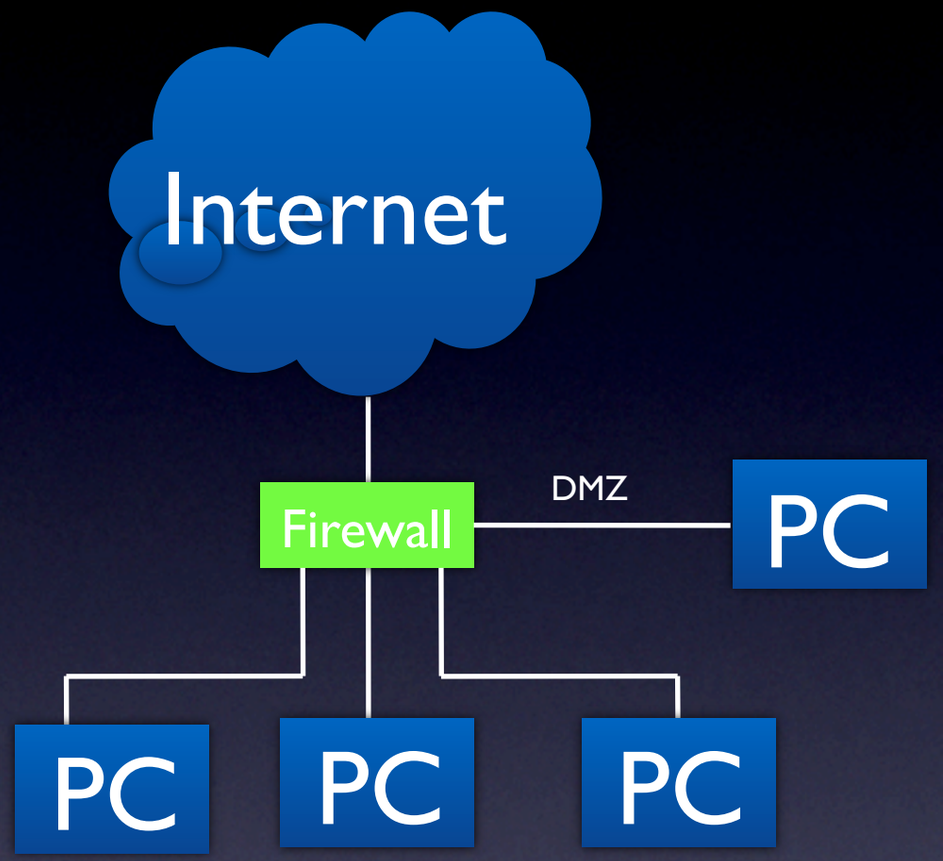
Hardware Firewall

Hardware device located between the Internet and a PC (or PCs) that performs a firewall function Protects ALL of the computers that it is behindMany have a subnet region of lesser security protection called a Demilitarized Zone (DMZ).



Hardware Firewall

May perform Network Address Translation (NAT) which provides hosts behind the firewall with addresses in the "private address range". This functionality hides true addresses of protected hosts and makes them harder to target. There are several commercially available hardware firewall products. After installation, it may have to be configured correctly in order to perform optimally.



Firewall Configuration

- Self-learning - some software firewalls will prompt the user as connection attempts occur (in-bound and out-bound) and ask for permission.
- Some require subscription to White/Black Lists.
- Many require (or can also be configured) that allowable ports and/or IP addresses
- be listed.Access Control List – ACL
- Requires a “knowledgeable” user.

Firewall Issues

- Some firewalls can also help protect against other problems such as viruses, spam, etc.
- However, just because you have a firewall, don't believe you are fully protected against malware.
- Firewalls CANNOT protect against traffic or software that does not come through it.
- Unauthorized connections (Modem, wireless, etc.)
- Malware delivered via CD, DVD, Thumbdrives, etc.

Antivirus

Prevents, detects and removes malware.

- computer viruses
- computer worms
- trojan horses
- spyware
- adware

Antivirus Strategies

- Signature-based detection involves searching for known patterns of data within executable code.

However:

- it is possible for a computer to be infected with new malware for which no signature is yet known.

Heuristics approach:

- Generic signatures can identify new viruses or variants of existing viruses by looking for known malicious code.

Antivirus Drawbacks

- Impair a computer's performance.
- Inexperienced users - prompts and decisions.
- An incorrect decision may lead to a security breach.

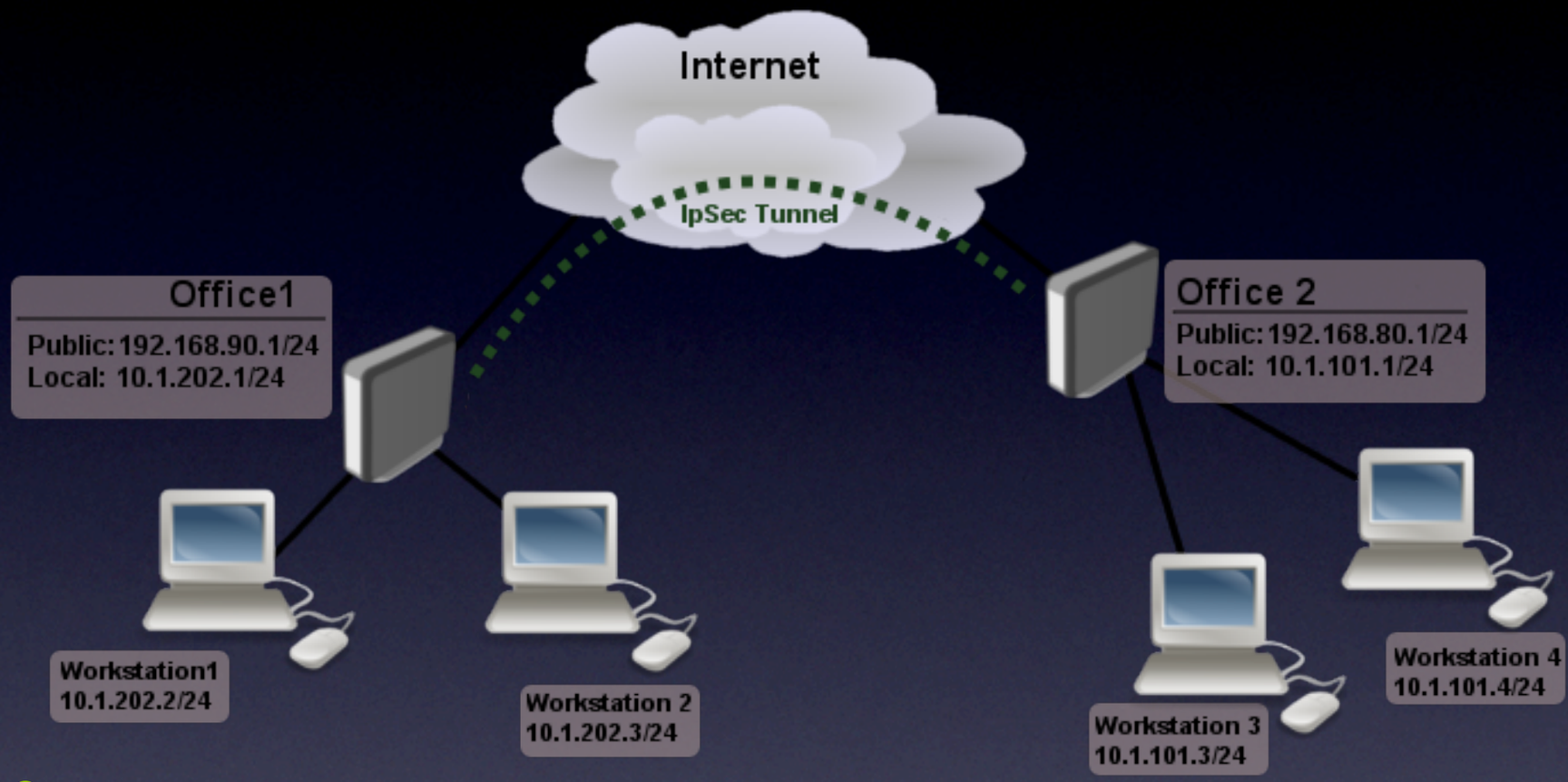
Virtual Private Networks

- Secure link between two private networks.
- The network is virtual because data are tunneled through a public network, emulating a logical point-to-point connection.

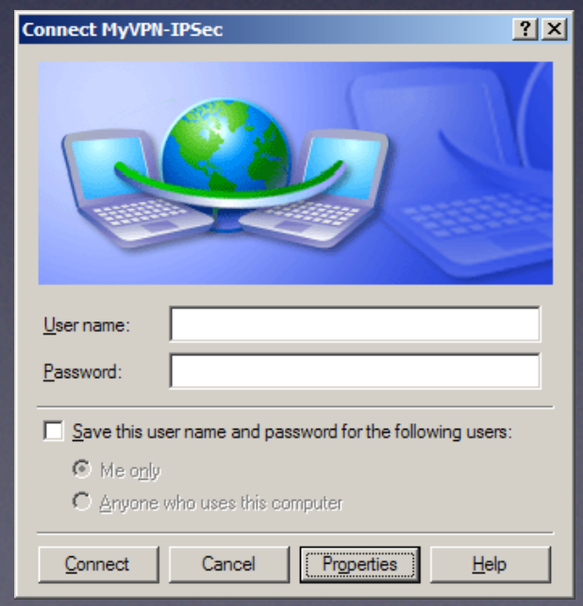
Most common VPN protocols are:

- PPTP
- L2TP
- MPLS
- IPSec

IPSecurity



- Host-to-Host Communication
- Gateway-to-Gateway Communication
- Host-to-Gateway Communication



IPSecurity

- Should achieve the following:
  - Disallow links to un-trusted sites.
  - Encrypt packets that leave the premises.
  - Authenticate packets that enter the premises.

IP Security Overview

Applications of IPSec...

- Secure branch office connectivity over the Internet: a company can build a secure private virtual network over the Internet or over a public WAN.
- Secure remote access over the Internet: An end user can gain secure access to other company’ s network over the Internet.

IP Security Overview

Applications of IPSec...

- Establsihing extranet and intranet connectivity with partners: can be used to establish secure communication with other organization.
- Enhancing electronic commerce security: use of IPsec enhances e-commerce security.

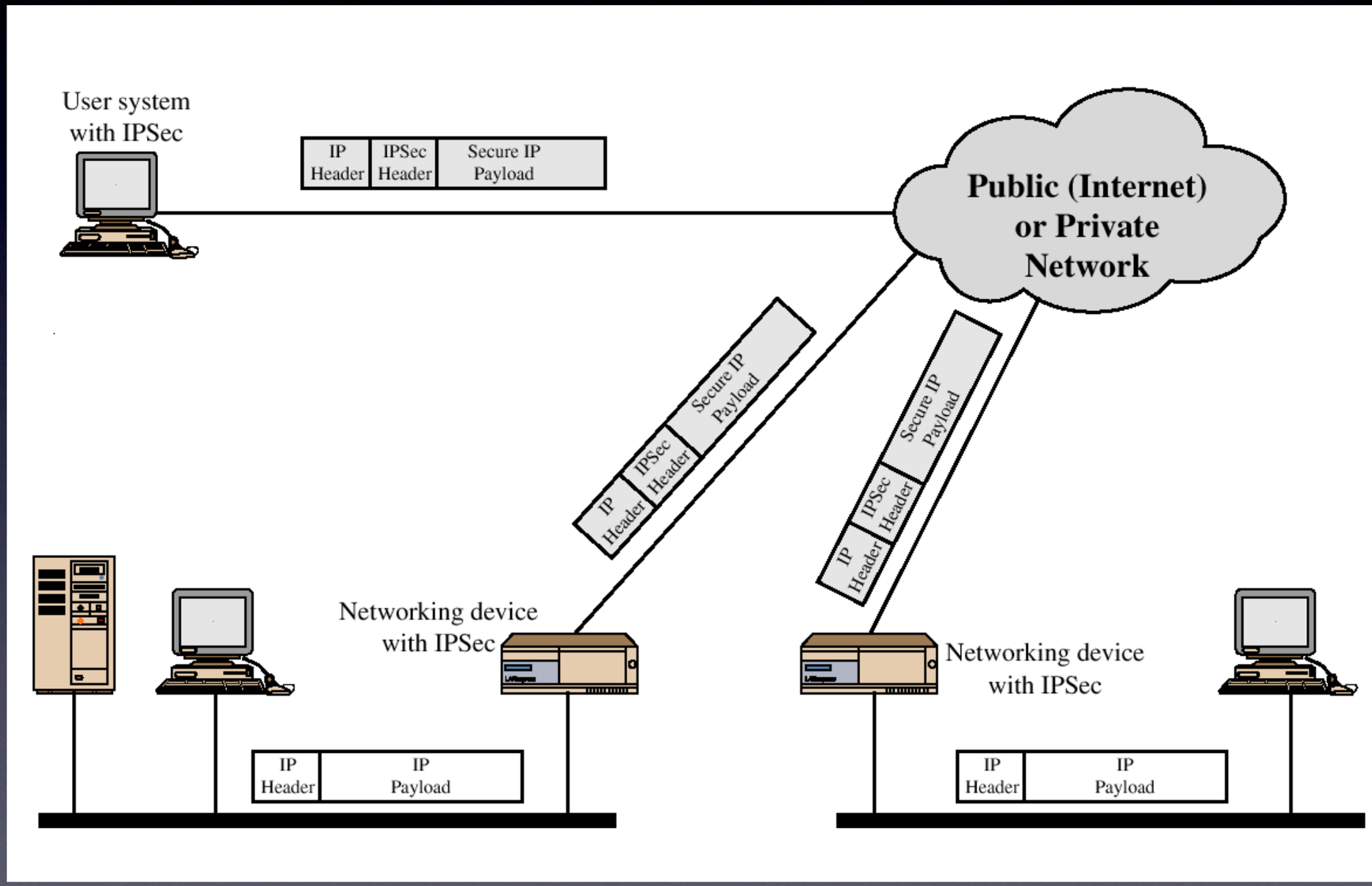
IP Security Overview

- IPSec can encrypt and authenticate all traffic at IP level.
- Distributed applications (like remote login, client-server interaction, e-mail, file transfers, web accesss etc.) can be secured.

An IP Security Overview

- Suppose an organization maintains LANs.
- At several dispersed locations.
- Within each LAN, IP traffic is not secured.
- For Site-to-Site traffic (over the Internet.
- Or a WAN, IPSec protocols are used.

IP Security Scenario



IP Security Overview

Benefits of IPSec

- Transparent to applications (below transport layer (TCP, UDP).
- No need to change software on end systems.
- IPSec can be transparent to end users.
- No need to train end users on security mechanisms.
- Provide security for individual users.

IPSec Services

IPSec uses two protocols to provide security:

- Authentication Header (AH): an authentication protocol.
- Encapsulating Security Payload (ESP): a combined encryption and authentication protocol.

IPSec Services

- Access Control
- Data integrity
- Data origin authentication
- Rejection of replayed packets
- Confidentiality (encryption)
- Limited traffic flow confidentiality

Transport vs. Tunnel Mode

AH and ESP support two modes:

- Transport and tunnel.

Transport Mode:

- Protection extends to the payload of an IP packet.
- Used for end-to-end communication between two hosts (client and server, or two workstations).

Transport vs. Tunnel Mode

Tunnel Mode:

- Provides protection to the entire IP packet.
- After AH or ESP fields are added, the entire packet plus security fields are treated as a payload of a new IP packet.
- A new IP header is attached.

Transport vs. Tunnel Mode

	Transport Mode SA	Tunnel Mode SA
AH	Authenticates IP payload and selected portions of IP header and IPv6 extension headers	Authenticates entire inner IP packet plus selected portions of outer IP header
ESP	Encrypts IP payload and any IPv6 extesion header	Encrypts inner IP packet
ESP with authentication	Encrypts IP payload and any IPv6 extesion header. Authenticates IP payload but no IP header	Encrypts inner IP packet. Authenticates inner IP packet.

Wireless Networks

WEP (Wired Equivalent Privacy)

- WEP is an old standard from 1999 which was outdated in 2003 by WPA.
- WEP is one of the least secure forms of security.
- WEP uses a 40-bit or 104-bit encryption key.
- WEP can been cracked in 2 minutes.

WPA-WPA2

WPA Enhanced security over the older WEP protocol.
WPA2 replaces the TKIP encryption protocol with CCMP (AES) to provide additional security and uses a 256 bit key.

- WPA-PSK (Pre-shared key) is designed for home and small office networks.
- WPA-802.1X is designed for enterprise networks and requires a RADIUS authentication server.

Encryption protocols

- TKIP: The RC4 stream cipher is used with a 128-bit per-packet key, meaning that it dynamically generates a new key for each packet.
- CCMP: An AES-based encryption mechanism that is stronger than TKIP. Sometimes referred to as AES instead of CCMP.

Intrusion Detection Systems IDSs

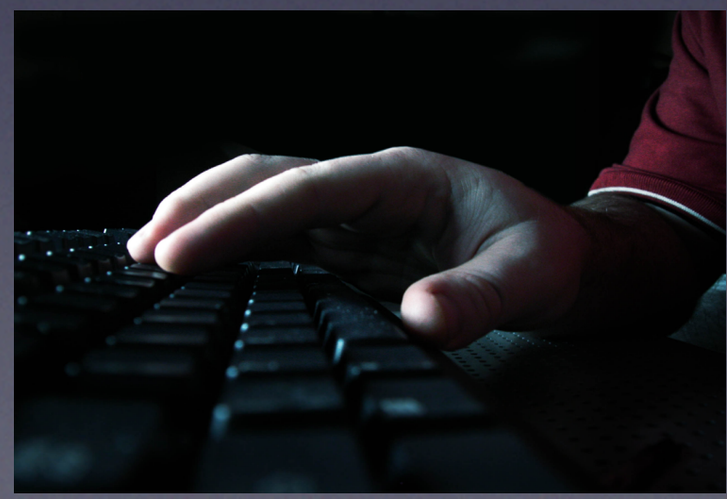
- An intrusion can generally be described as the act of entering without permission.
- Intrusion detection is the process of identifying such unauthorized action.

Intrusion and Intrusion Detection

- Intruders may be from outside the network or legitimate users of the network.
- Intrusion can be a physical, system or remote intrusion.

Different ways to intrude

- Buffer overflows
- Unexpected combinations
- Unhandled input



Intrusion Detection Systems (IDS)

- Intrusion Detection Systems look for attack signatures, which are specific patterns that usually indicate malicious or suspicious intent.

Intrusion Detection Systems (IDS)

Different ways of classifying an IDS

IDS based on

- anomaly detection
- signature based misuse
- host based
- network based

Anomaly based IDS

- This IDS models the normal usage of the network as a noise characterization.
- Anything distinct from the noise is assumed to be an intrusion activity.
- E.g flooding a host with lots of packet.
- The primary strength is its ability to recognize novel attacks.

Drawbacks of Anomaly detection IDS

- Assumes that intrusions will be accompanied by manifestations that are sufficiently unusual so as to permit detection.
- These generate many false alarms and hence compromise the effectiveness of the IDS.

Signature based IDS

- This IDS possess an attacked description that can be matched to sensed attack manifestations.
- The question of what information is relevant to an IDS depends upon what it is trying to detect.
- E.g DNS, FTP etc.

Signature based IDS

- ID system is programmed to interpret a certain series of packets, or a certain piece of data contained in those packets,as an attack. For example, an IDS that watches web servers might be programmed to look for the string “phf” as an indicator of a CGI program attack.
- Most signature analysis systems are based off of simple pattern matching algorithms. In most cases, the IDS simply looks for a sub string within a stream of data carried by network packets. When it finds this sub string (for example, the ``phf'' in ``GET /cgi-bin/phf?''), it identifies those network packets as vehicles of an attack.

Drawbacks of Signature based IDS

- They are unable to detect novel attacks.
- Suffer from false alarms.
- Have to programmed again for every new pattern to be detected.

Host/Applications based IDS

- The host operating system or the application logs in the audit information.
- These audit information includes events like the use of identification and authentication mechanisms (logins etc.) , file opens and program executions, admin activities etc.
- This audit is then analyzed to detect trails of intrusion.

Drawbacks of the host based IDS

- The kind of information needed to be logged in is a matter of experience.
- Unselective logging of messages may greatly increase the audit and analysis burdens.
- Selective logging runs the risk that attack manifestations could be missed.

Strengths of the host based IDS

- Attack verification.
- System specific activity.
- Encrypted and switch environments.
- Monitoring key components.
- Near Real-Time detection and response.
- No additional hardware.

Stack based IDS

- They are integrated closely with the TCP/IP stack, allowing packets to be watched as they traverse their way up the OSI layers.
- This allows the IDS to pull the packets from the stack before the OS or the application have a chance to process the packets.

Network based IDS

- This IDS looks for attack signatures in network traffic via a promiscuous interface.
- A filter is usually applied to determine which traffic will be discarded or passed on to an attack recognition module. This helps to filter out known un-malicious traffic.

Strengths of Network based IDS

- Cost of ownership reduced
- Packet analysis
- Evidence removal
- Real time detection and response
- Operating system independence

Future of IDS

- To integrate the network and host based IDS for better detection.
- Developing IDS schemes for detecting novel attacks rather than individual instantiations.

Attack Scenarios and Countermeasures

- Information Gathering
- Sniffing or Eavesdropping
- Spoofing
- Session Hijacking (man in the middle attack)
- Denial of Service (DoS)

Information Gathering

Attackers usually start with port scanning. After that they use banner grabbing and enumeration to detect device types and to determine operating system and application versions. With this information, an attacker can attack known vulnerabilities that may not be updated with security patches.

Configure routers to restrict their responses to footprinting requests.

Configure operating systems that host network software (for example, software firewalls) to prevent footprinting by disabling unused protocols and unnecessary ports.

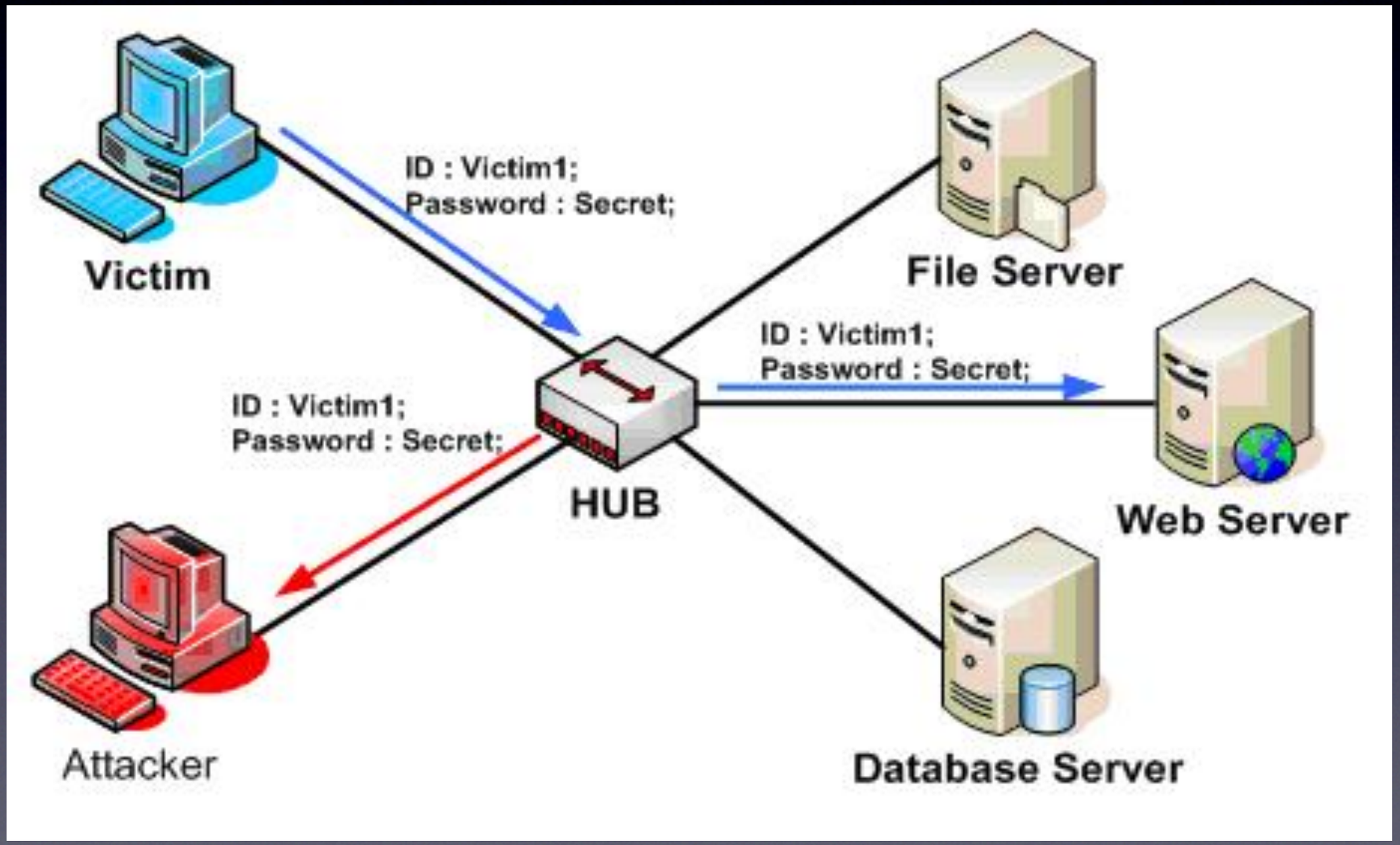
Sniffing or Eavesdropping

Sniffing or eavesdropping is a network attack consisting of capturing packets from the network transmitted by other computers and reading the data content in search of sensitive information like passwords or any kind of confidential information.

Use strong physical security and proper segmenting of the network.

Encrypt communication fully, including authentication credentials.

Sniffing or Eavesdropping Attack Example



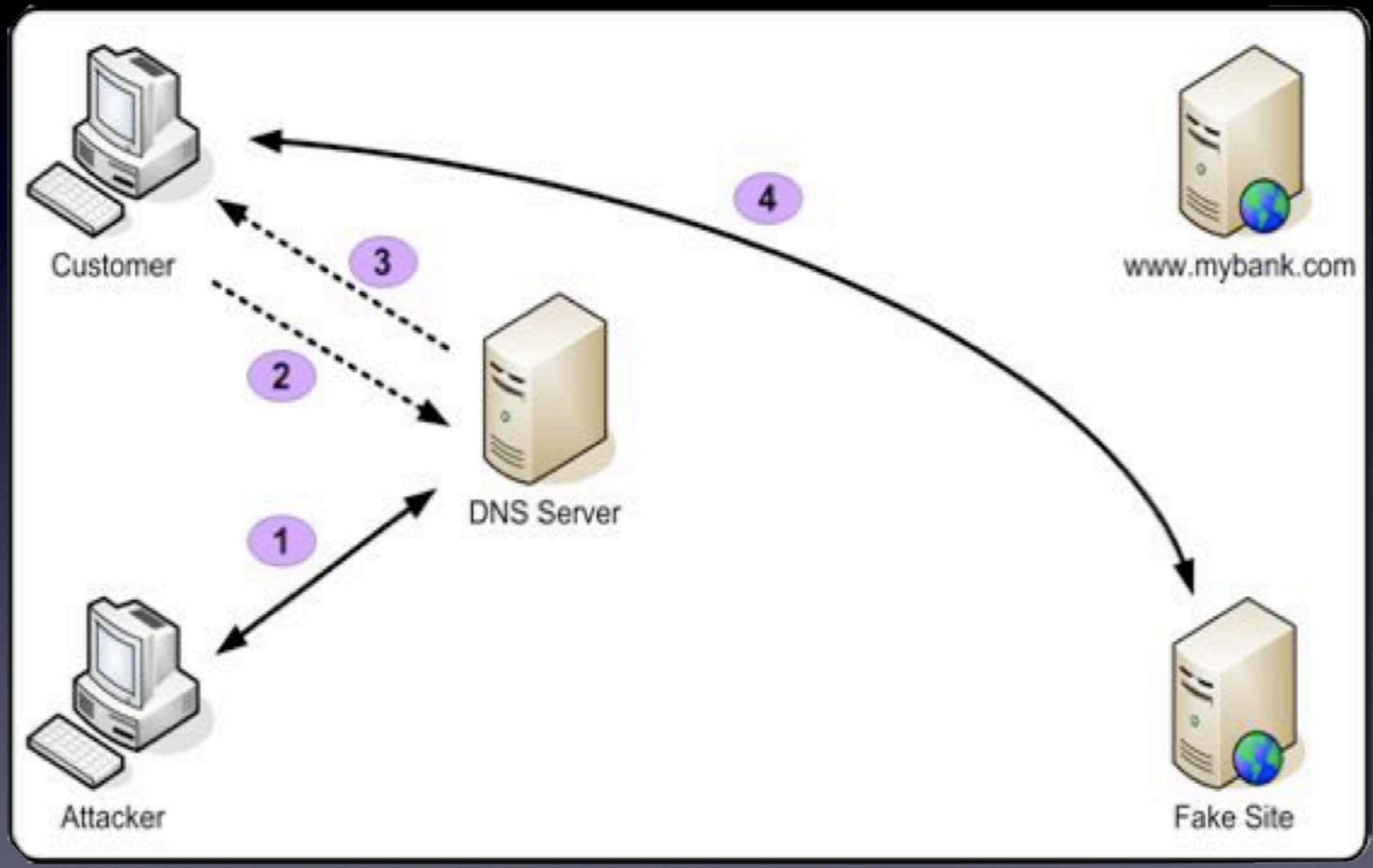
Spoofing

Is a means to hide one's true identity on the network. To create a spoofed identity, an attacker uses a fake source address that does not represent the actual address of the packet. Spoofing may be used to hide the original source of an attack.

Filter incoming packets that appear to come from an internal IP address at your perimeter.

Filter outgoing packets that appear to originate from an invalid local IP address.

Spoofing Attack Example



Session Hijacking (man in the middle attack)

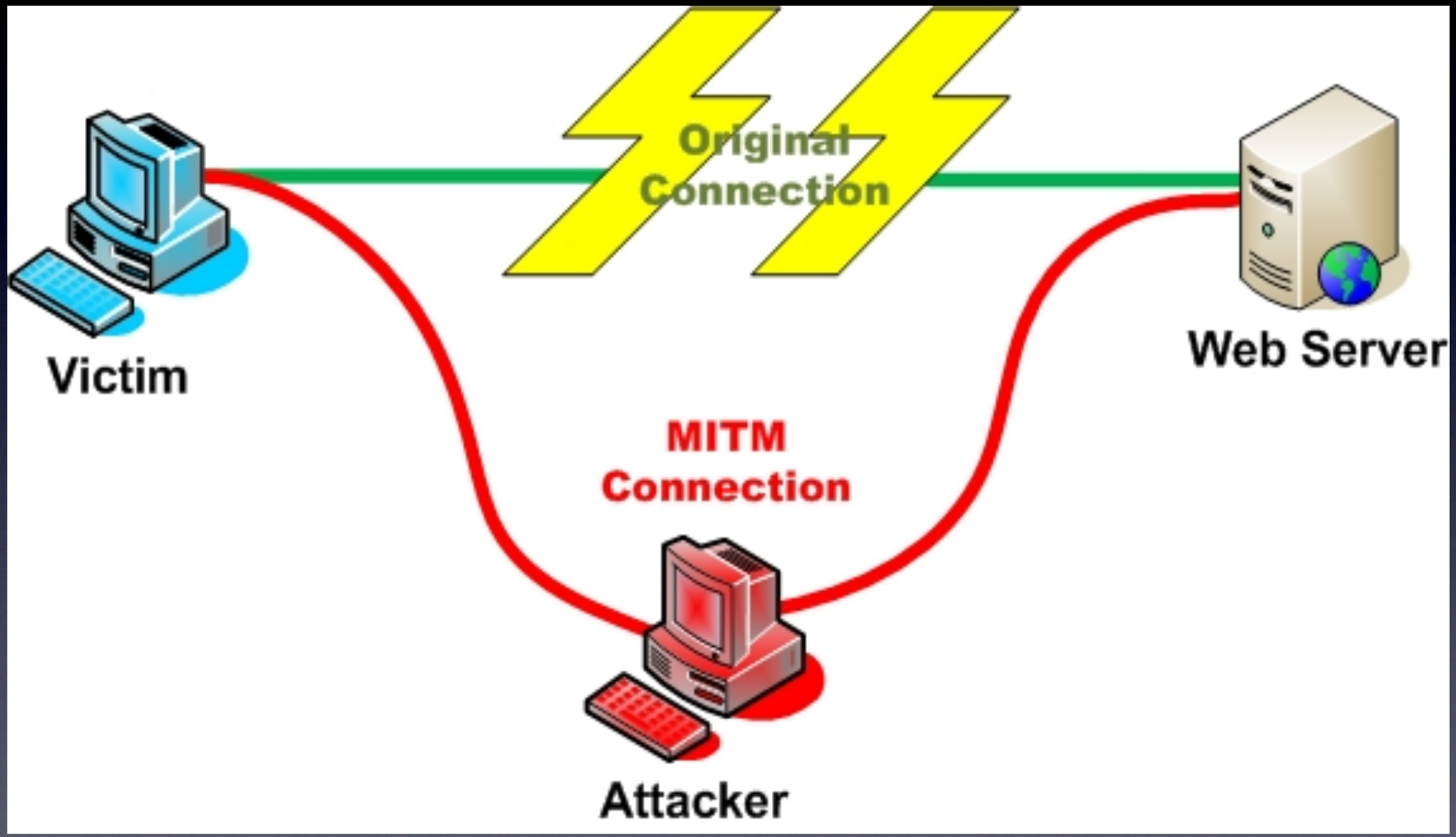
It deceives a server or a client into accepting the upstream host as the actual legitimate host. Instead the upstream host is an attacker's host that is manipulating the network so the attacker's host appears to be the desired destination.

Use encrypted session negotiation.

Use encrypted communication channels.

Stay informed of platform patches to fix TCP/IP vulnerabilities, such as predictable packet sequences.

Man In The Middle Attack

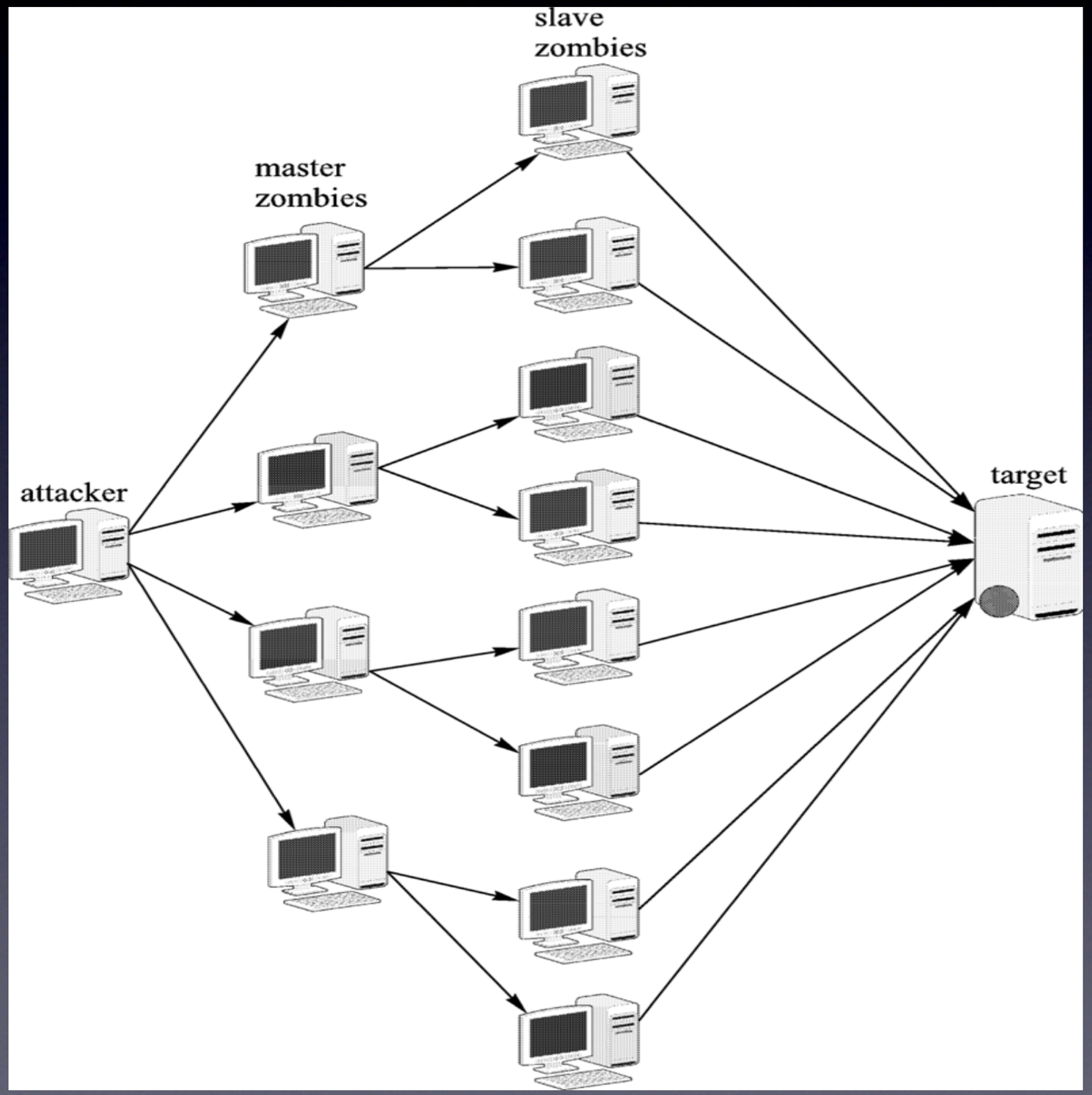


Denial of Service (DoS) Attack

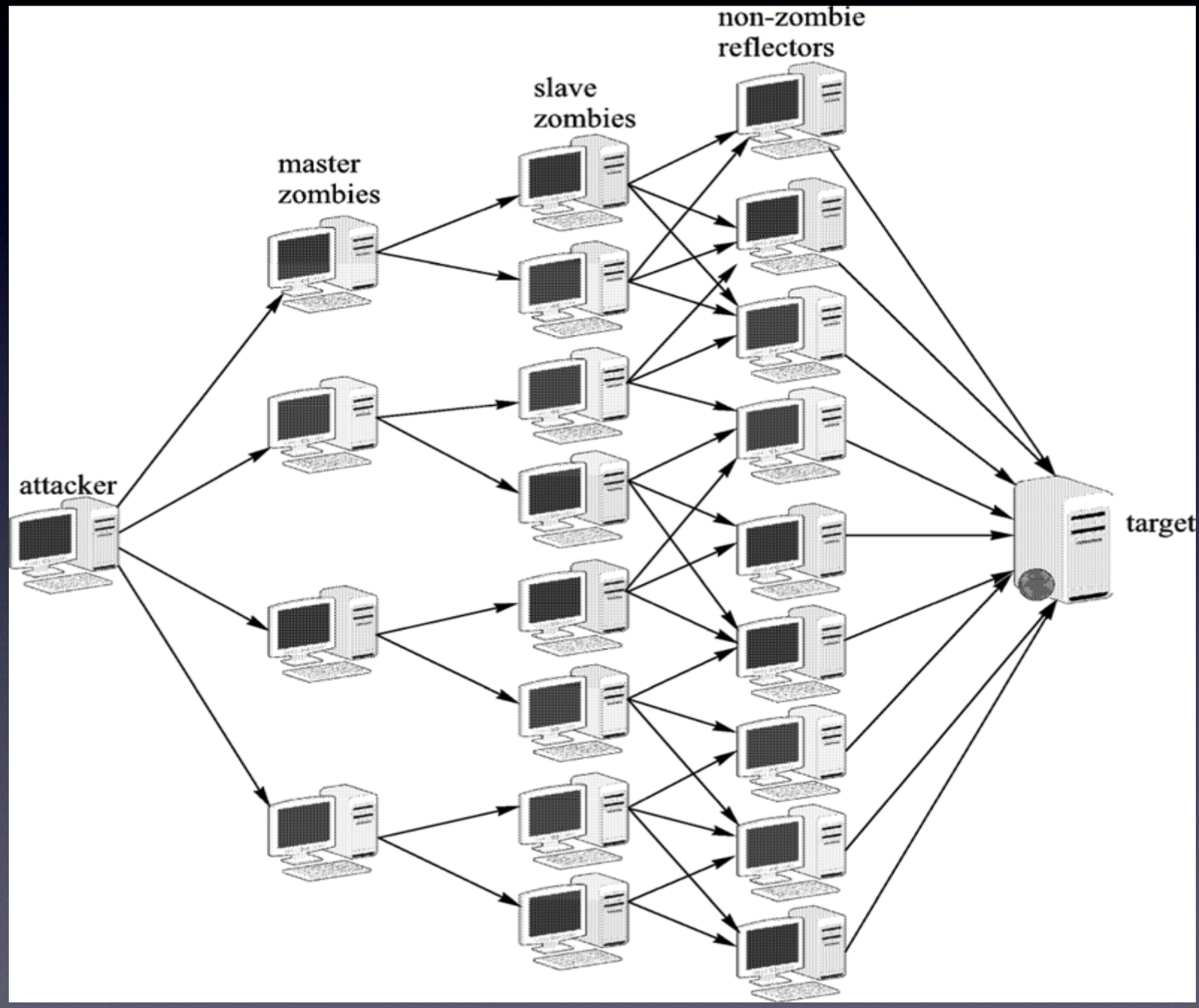
- Denial of service denies legitimate users access to a server or services.

- The aim of the attack is to send more requests to a server than it can handle.

Example of master slave DDoS attack



Example of master-slave-reflector DDoS attack



DDos Attacks Countermeasures

- Apply the latest service packs.
- Harden the TCP/IP stack by applying the appropriate registry settings to increase the size of the TCP connection queue, decrease the connection establishment period, and empty dynamic backlog mechanisms to ensure that the connection is never exhausted.
- Use a network Intrusion Detection System (IDS) because these can automatically detect and respond to SYN attacks.

DDos Attacks Countermeasures

- Backup system
- Monitoring system
- System log
- Close all unnecessary ports to deny IP scans
- Automatically disconnect when not in use
- Detect and remove zombieware

CONCLUSIONS

Attackers (Hackers) will always try to find new ways to harm our systems, but on the other side, there is continuous struggle from Network and Internet security personnel to stop them.

Users should be more careful when using network devices connected and exchanging information over the internet and should be aware about possible threats and attacks.

References

- Douligeris C., Serpanos D., Network Security, Wiley – Interscience, USA, 2007, pp 33-81
- Wang Jie, Computer Network Security: Theory and Practice, Higher Education Press, Beijing and Springer-Verlag GmbH Berlin Heielberg, 2009, Pages 277-316
- Network Management & Security http://www.javvin.com/etraffic/network-vulnerabilities.html,
- Wireless Networking Security - Windows http://technet.microsoft.com/en-us/library/bb457019.aspx

References

- Beginners Guides: Firewall Setup and Configuration http://www.pcstats.com/articleview.cfm?articleID=1618
- James H. Yu & Tom K. Le, "Internet and Network Security", Journal of Industrial technology, Volume 17, January 2001, http://atmae.org/jit/Articles/yu101800.pdf
- Esoft, "Network Security", White Paper - Modern Network Security: The Migration to Deep Packet Inspection, http://www.esoft.com/content/pdf/dpi-migration-whitepaper.pdf
- Meier J.D., Mackman A., Dunner M., Vasireddy S., Escamilla R., Murukan A., *Microsoft Corporation, "Improving Web Application Security: Threats and Countermeasures"*, http://msdn.microsoft.com/en-us/library/ff648641.aspx

Thank you

Any questions?