موسسه آموزش عالی غیردولتی غیرانتفاعی بصیر آبیک

NETWORK AND E-COMMERCE SECURITY

Basir University, 2020-2021

By: Prof. Dr. Mohammad Hajarian

موسسه آموزش عالی غیردولتی غیرانتفاعی بصیر آبیک

- Session 2

MALWARES AND SECURITY

INTRODUCTION TO MALWARE

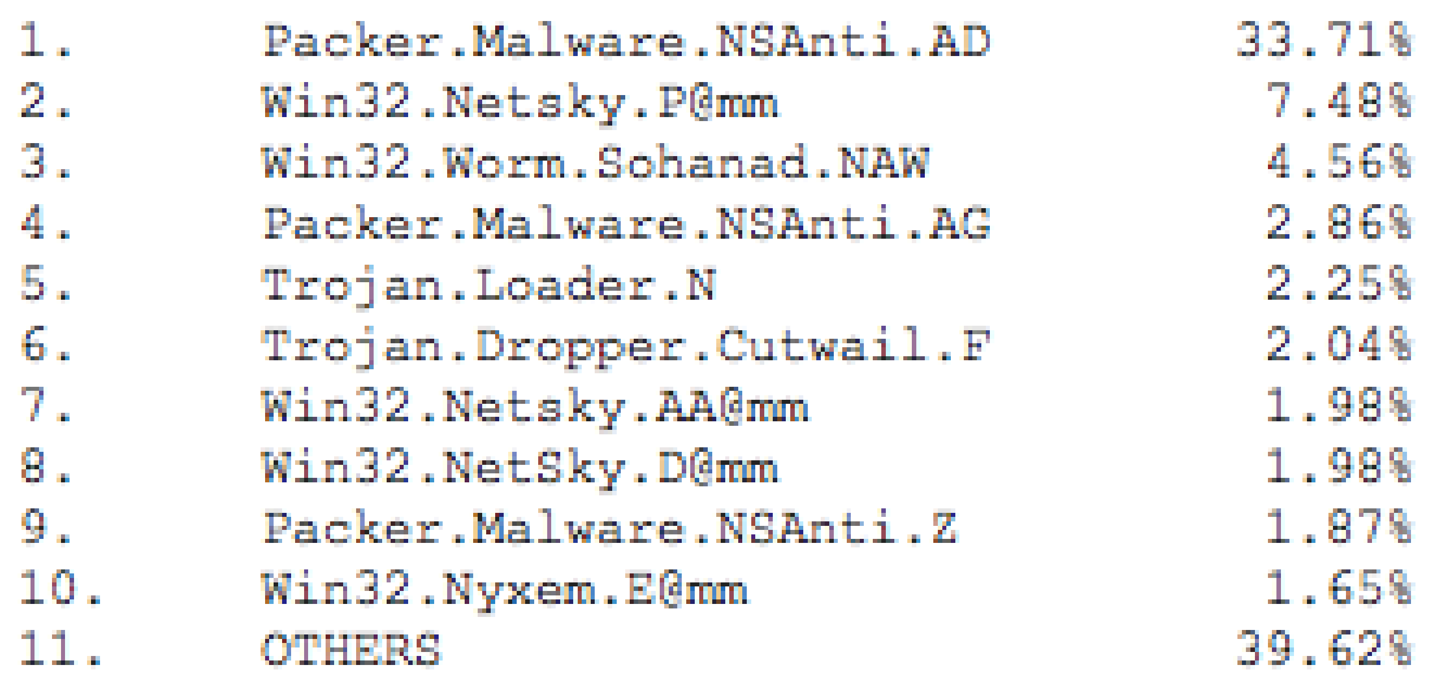
WHAT IS MALWARE

- “Malware” is short for “malicious software”
- “Malware” is the general term covering all the different types of threats to your computer safety such as viruses, spyware, worms, trojans, rootkits and so on.
- Can be loosely defined as “Malicious computer executable”
  - A bit flexible definition
  - Annoying software or program codes
- Running a code without user’s consent
  - “If you let somebody else execute code on your computer, then it is not your own computer”
- Not only virus or worm
  - Sometimes known as computer contaminant
- Should not be confused with defective software which contains harmful bugs

REASONS FOR İNCREASE

- Growing number and connectivity of computers
  - “everybody” is connected and dependant on computers
  - the number of attacks increase
  - attacks can be launched easily (automated attacks)
- Growing system complexity
  - unsafe programming languages
  - hiding code is easy
  - verification and validation is impossible
- Systems are easily extensible
  - mobile code, dynamically loadable modules
  - incremental evolution of systems

TOP 10 MALWARE



1.	Packer.Malware.NSAnti.AD	33.71%
2.	Win32.Netsky.P@mm	7.48%
3.	Win32.Worm.Sohanad.NAW	4.56%
4.	Packer.Malware.NSAnti.AG	2.86%
5.	Trojan.Loader.N	2.25%
6.	Trojan.Dropper.Cutwail.F	2.04%
7.	Win32.Netsky.AA@mm	1.98%
8.	Win32.NetSky.D@mm	1.98%
9.	Packer.Malware.NSAnti.Z	1.87%
10.	Win32.Nyxem.E@mm	1.65%
11.	OTHERS	39.62%

- According to Sophos 86% of the reported attacks is spyware

TYPES OF MALWARE

- Viruses and Worms
- Spyware and adware
- Bots, trojans and keyloggers
  - Backdoors and DoS attacks

VIRUSES AND WORMS

- Worms are the oldest one
  - First well-known worm was known as the Morris Worm
    - Used a BSD Unix flaw to propagate itself
- Viruses requires hosts
  - Word document, etc.
- Both can spread through e-mail
  - Melissa virus uses address books of the infected computers (1999)
- Because it is less beneficial to their creators, this oldest form of malware is dying out

SPYWARE AND ADWARE

- Growth of Internet helped spawn spyware
- Largely fueled by the prospect of monetary gain
- Not spreads like viruses, instead packaged with user installed software (mostly p2p programs)
- Least virulent forms causes sluggish systems, slow Web browsing, annoying pop-ups
- More dangerous spyware tracks browsing habits or sensitive information

BOTS AND TROJANS

- Bots makers infect multiple systems
  - Creates massive botnets that can be used to launch Distributed Denial of Service attacks
- Trojan is a way to secretly install a piece of malware on a system
  - It could be adware or a keylogger
  - It sneakes onto a system and delivers an unexpected and potentially devastating payload

FLAWS AND VULNERABİLİTİES

- **Homogeneity** – e.g. when all computers in a network run the same OS, if you can break that OS, you can break into any computer running it.
- **Defects** – most systems containing errors which may be exploited by malware.
- **Unconfirmed code** – code from a floppy disk, CD-ROM or USB device may be executed without the user’s agreement.
- **Over-privileged users** – some systems allow all users to modify their internal structures.
- **Over-privileged code** – most popular systems allow code executed by a user all rights of that user.

GRAYWARE

GRAYWARE

- Applications that are installed on a user’s computer to track and/or report certain information back to some external source
- Usually installed and run without the permission of the user
- Behave in a manner that is annoying or undesirable
- Designed to harm the performance of computers

GRAYWARE

- Sources can come from
  - Downloading shareware, freeware or other forms of file sharing services
  - Opening infected e-mails
  - Clicking on pop-up advertising
  - Visiting frivolous or spoofed web sites
  - Installing Trojan applications

GRAYWARE

- Not necessarily malevolent
  - Web site developers use newer techniques to customize their web sites & obtain better results
- Ultimate goal of many of them
  - Tracking the usage patterns of visitors to offer more customized search results to result in higher sales

GRAYWARE

- More of an annoyance than a security threat
  - Slower performance
  - More pop-up advertising
  - Web browser home pages being directed to other sites
- If the hackers are not counted!

GRAYWARE

- Hackers use grayware to load and run programs that
  - Collect information
  - Track usage pattern
  - Invasion of privacy
  - Track keystrokes
  - Modify system settings
  - Inflict other kinds of damage

GRAYWARE -- CATEGORİES

- Spyware
  - Included with freeware
  - Does not notify the user of its existance or ask permission to install the components
  - Designed to track & analyze a user's activity
    - Web browsing habits
    - Primarily for market purposes
  - Tracked information is sent back to the originator's Web site
  - Responsible for performance related issues

GRAYWARE -- CATEGORİES

- Adware
  - – Embedded in freeware applications that users can donwload & install at no cost
    - – By accepting the ‘End User Licence Agreement’
  - – Used to load pop-up browser windows to deliver advertisements
  - – Considered to be invasive

GRAYWARE -- CATEGORİES

- Dialers
  - – Used to control the PC’s modem
    - To make long distance calls
    - To call premium 900 numbers to create revenue for the theaf
- Gaming
  - – Installed to provide joke or nuisance games

GRAYWARE -- CATEGORİES

- Joke
  - Used to change system settings but do not damage the system
    - Changing the system cursor
    - Changing Windows' background image
- Peer-to-peer
  - Installed to perform file exchanges
  - Used to illegally swap music, movies, etc.

GRAYWARE -- CATEGORİES

- Key Logger
  - One of the most dangerous applications
  - Installed to capture the keystrokes
    - User & password information
    - Credit card numbers
    - E-mail, chat, instant messages, etc.
- Hijacker
  - Manipulates the Web browser or other settings to change the user's favorite or bookmarked sites, start pages or menu options
  - Some can also manipulate DNS settings

GRAYWARE -- CATEGORİES

- Plugins
  - Designed to add additional programs or features to an existing application in an attempt to control, record and send browsing preferences or other information back to an external destination
- Network Management
  - Designed to be installed to for malicious purposes
  - Used to change network settings, disrupt network security

GRAYWARE -- CATEGORİES

- Remote Administration Tools
  - Allow an external user to remotely gain access, change or monitor a computer on a network
- Browser Helper Object (BHO)
  - DLL files that are often installed as part of a software application to allow program to control the behaviour of Internet Explorer
  - Can track surfing habits

GRAYWARE -- CATEGORİES

- Toolbar
  - Installed to modify the computer's existing toolbar features
  - Can be used to monitor web habits, send information back to the developer or change the functionality of the host
- Download
  - Installed to allow other software to be downloaded & installed without the user's knowledge
  - Usually run during the startup

GRAYWARE -- SYMPTOMS

- Slower computer performance
  - Takes more CPU & memory resources
  - Can be identified from Windows Task Manager
    - Usually unkown applications to users
- Send & receive lights on modem or the network icons on the task bar are flashing even though you are not performing any online process

GRAYWARE -- SYMPTOMS

- Computer displays pop-up messages & advertisements when not connected to Internet or when not running the browser
- Change in home page
- Change in search engine settings
- Change in bookmarks
- Change in toolbars or new installed options
    - Attempt to remove those fail

GRAYWARE -- SYMPTOMS

- Increase in phone bills
- Stop in anti-virus program, anti-spyware program or any other security related program
- Receival of warnings of missing application files
  - Replacement does not work

GRAYWARE -- PROTECTİON

- User Education
  - Educating employees regarding the nature & dangers of grayware
  - Establishing policies that prohibit downloading & installing applications that are not approved
  - If the dowload & installation is allowed,‘End User License Agreement’ should be read carefully
  - Increase the security settings on the Web browser
  - Configuration of e-mail programs as not to automatically download things
    - Turn of auto-preview

GRAYWARE -- PROTECTİON

- Host-based Anti-spyware Programs
  - Client based software applications that spot, remove and block spyware
  - Functions similarly to antivirus programs
  - Difficulty: overhead of installing & maintaining client software applications on all corporate PCs
    - Resources to purchase & install software and to perform routine upgrades on each computer
  - Danger: can be disabled by the end user or by other malicious application

GRAYWARE -- PROTECTİON

- Network-based Grayware Protection
  - Through a network gateway approach
  - Install the grayware detection on a perimeter security appliance
  - Centralizes the intelligence at the ingress point
  - Lowers the overhead of installing, maintaining and keeping it up-to-date
  - Drawback
    - What happens when the user leaves the office?

TROJAN HORSE

TYPES OF TROJAN HORSE

- Remote Access
- Data Destruction
- Downloader
- Server Trojan (Proxy, FTP, IRC, Email, HTTP/HTTPS, etc.)
- Security software disabler
- Denial-of-Service attack (DoS)

DAMAGES OF TROJAN HORSE (1)

- Erasing or overwriting data on a computer
- Encrypting files in a cryptoviral extortion attack
  - Attacker encrypts the victim's files and the user must pay the malware author to receive the needed session key
- Corrupting files in a subtle way
- Upload and download files
- Copying fake links, which lead to false websites, chats, or other account based websites, showing any local account name on the computer falsely engaging in untrue context
- Allowing remote access to the victim's computer.
- Spreading other malware, such as viruses
  - called a 'dropper' or 'vector'

DAMAGES OF TROJAN HORSE (2)

- Setting up networks of zombie computers in order to launch DDoS attacks or send spam
- Spying on the user of a computer and covertly reporting data like browsing habits to other people
- Making screenshots
- Logging keystrokes to steal information such as passwords and credit card numbers
- Phishing for bank or other account details
- Installing a backdoor on a computer system
- Opening and closing CD-ROM tray Playing sounds, videos or displaying images.

DAMAGES OF TROJAN HORSE (3)

- Calling using the modem to expensive numbers, thus causing massive phone bills.
- Harvesting e-mail addresses and using them for spam
- Restarting the computer whenever the infected program is started
- Deactivating or interfering with anti-virus and firewall programs
- Deactivating or interfering with other competing forms of malware
- Randomly shutting off the computer

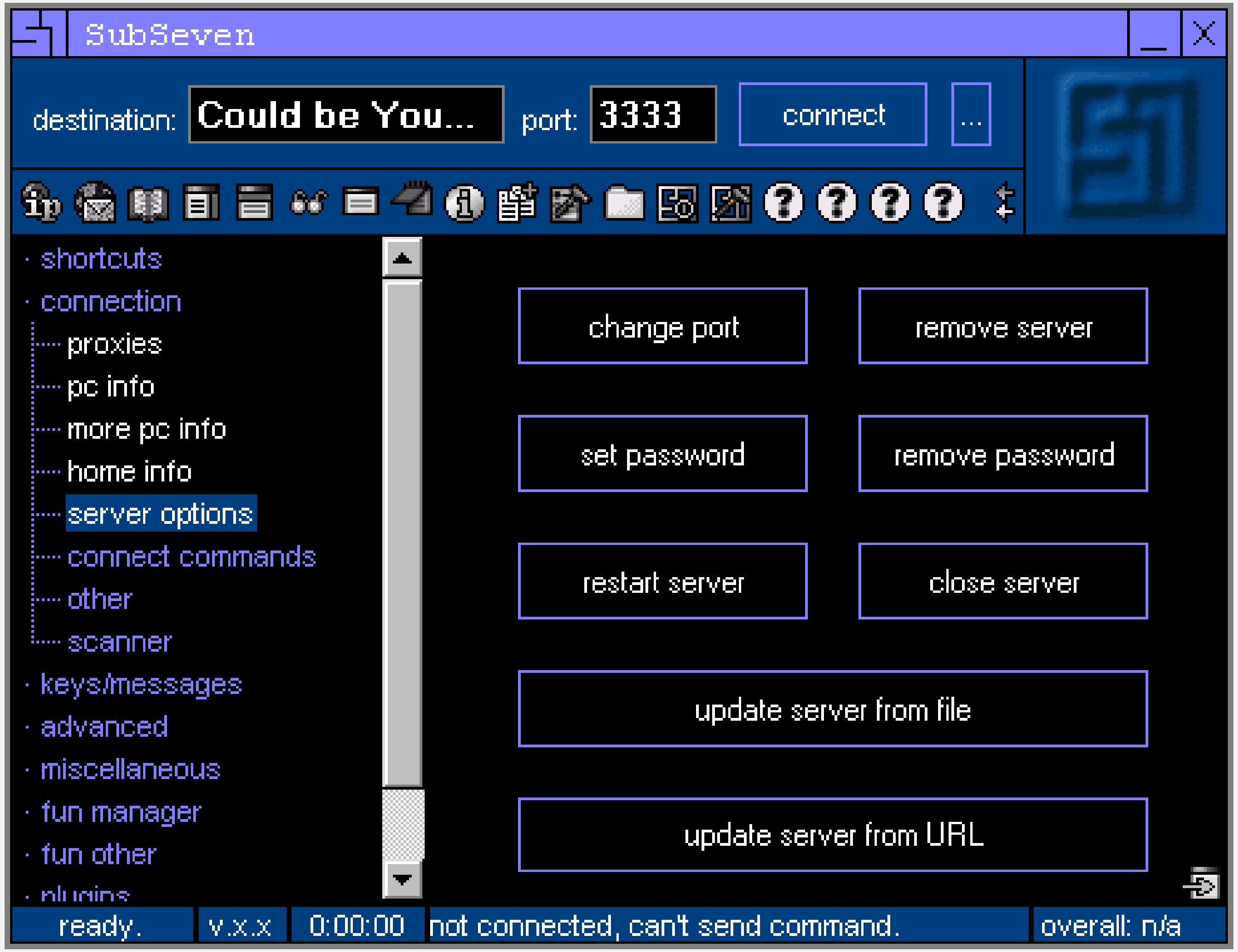
BACKDOOR (1)

- Bypassing actual authentication, securing remote access to a computer, obtaining access to plaintext
  - But remains undetected
- May be an installed program (e.g. Back Orifice) and modification to an existing program
- Threat is surfaced with development of multi-user and network based systems

BACKDOOR (2)

- Hard coded user and password combination
- Backdoors can be created by modification of source codes
  - Or modification of the compiler
- Computers infected by Sobig and Mydoom are a potential for spammers to send junk email
- Symmetric and asymmetric backdoors

LAMER 101 (BACKDOOR)



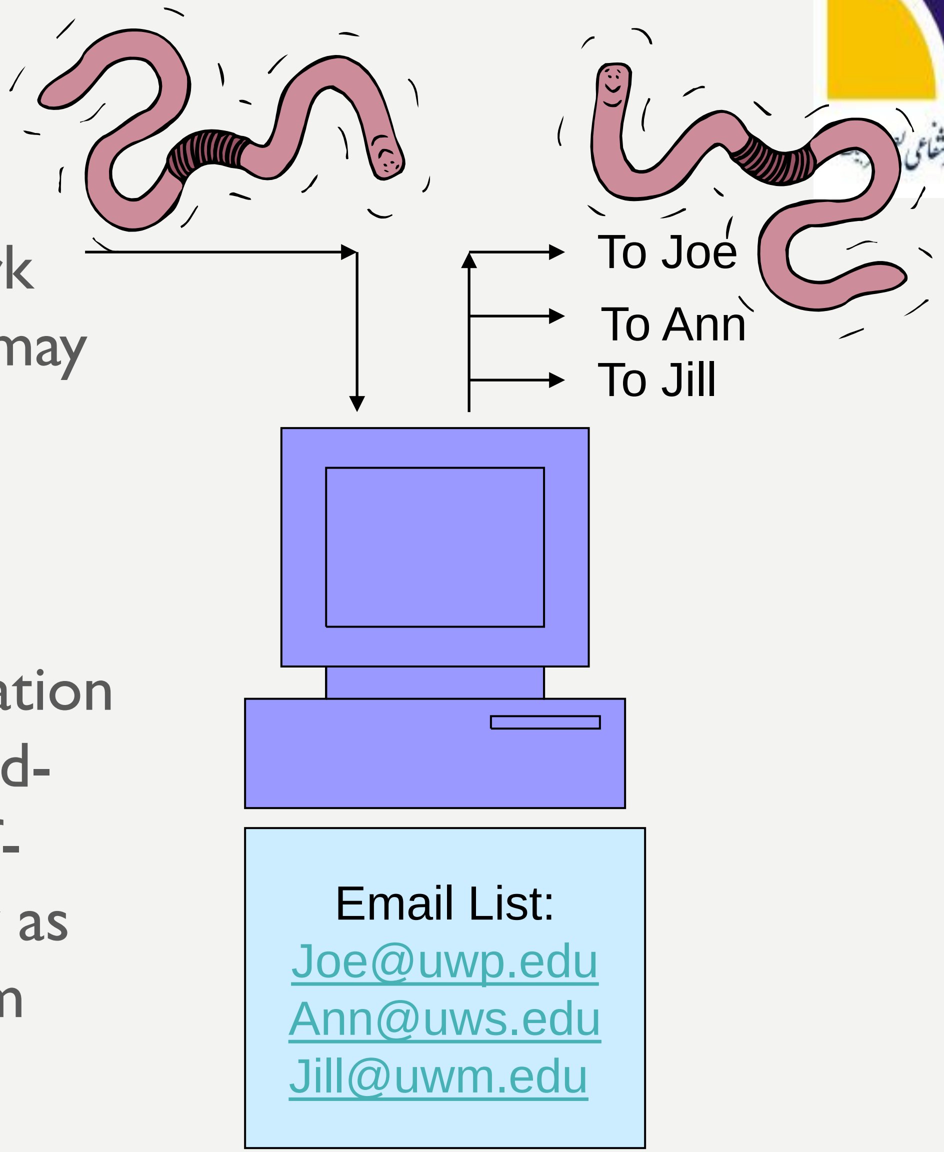
destination: Could be You... port: 3333

ready. v.x.x 0:00:00 not connected, can't send command. overall: n/a

WORMS

WORM

- **Worm**: Independent program which replicates itself and sends copies from computer to computer across network connections. Upon arrival the worm may be activated to replicate.
- Worms are a self-replicating type of malware (and a type of virus)
- viruses must be triggered by the activation of their host; whereas worms are stand-alone malicious programs that can self-replicate and propagate independently as soon as they have breached the system



Email List:
Joe@uwp.edu
Ann@uws.edu
Jill@uwm.edu

WORMS

- replicating program that propagates over net
  - using email, remote exec, remote login
- has phases like a virus:
  - dormant, propagation, triggering, execution
  - propagation phase: automatically 'scans' for other systems, connects to it, copies self to it and runs
  - fast spread phase: each infection spreads to n other nodes, exponentially
- may disguise itself as a system process

MORRIS WORM

- one of best know worms
- released by Robert Morris in 1988
- various attacks on UNIX systems
  - cracking password file to use login/password to logon to other systems
  - exploiting a bug in the finger protocol
  - exploiting a bug in sendmail to issue commands
- if succeed have remote shell access

MORRIS WORM – CONT'D

- Created by Robert Morris, convicted 1990, received $10K fine & 3 years jail, 400 hours community service
- Unintended Effect: Denial of service due to resource exhaustion: Worms created more worms (even on same machine)

Once system penetrated

- Send a bootstrap loader with 99 lines of C code to be executed on target machine
- Downloader: Fetch rest of worm, verified by password
- Stealth: encrypted itself, deleted original version, changed name periodically

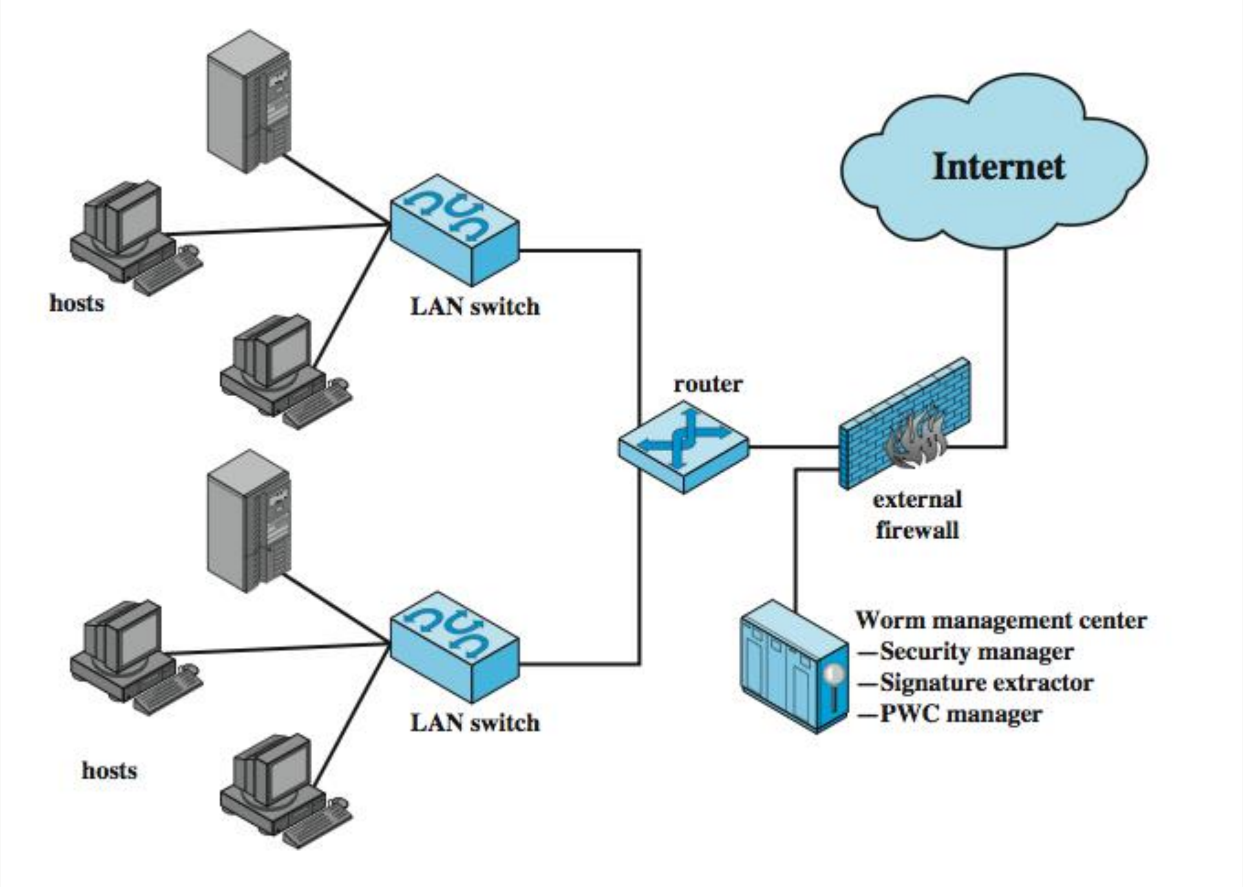
WORM TECHNOLOGY

- **Multiplatform**: Unix, Windows, …
- **Multi-exploit:** travels in multiple ways
- **Polymorphic**: generations mutate
- **Metamorphic:** self-mutating & polymorphic
- **Transport vehicles**: auto-builds bots
- **Zero-day exploit**: attacks a vulnerability before vulnerability is known

WORM COUNTERMEASURES

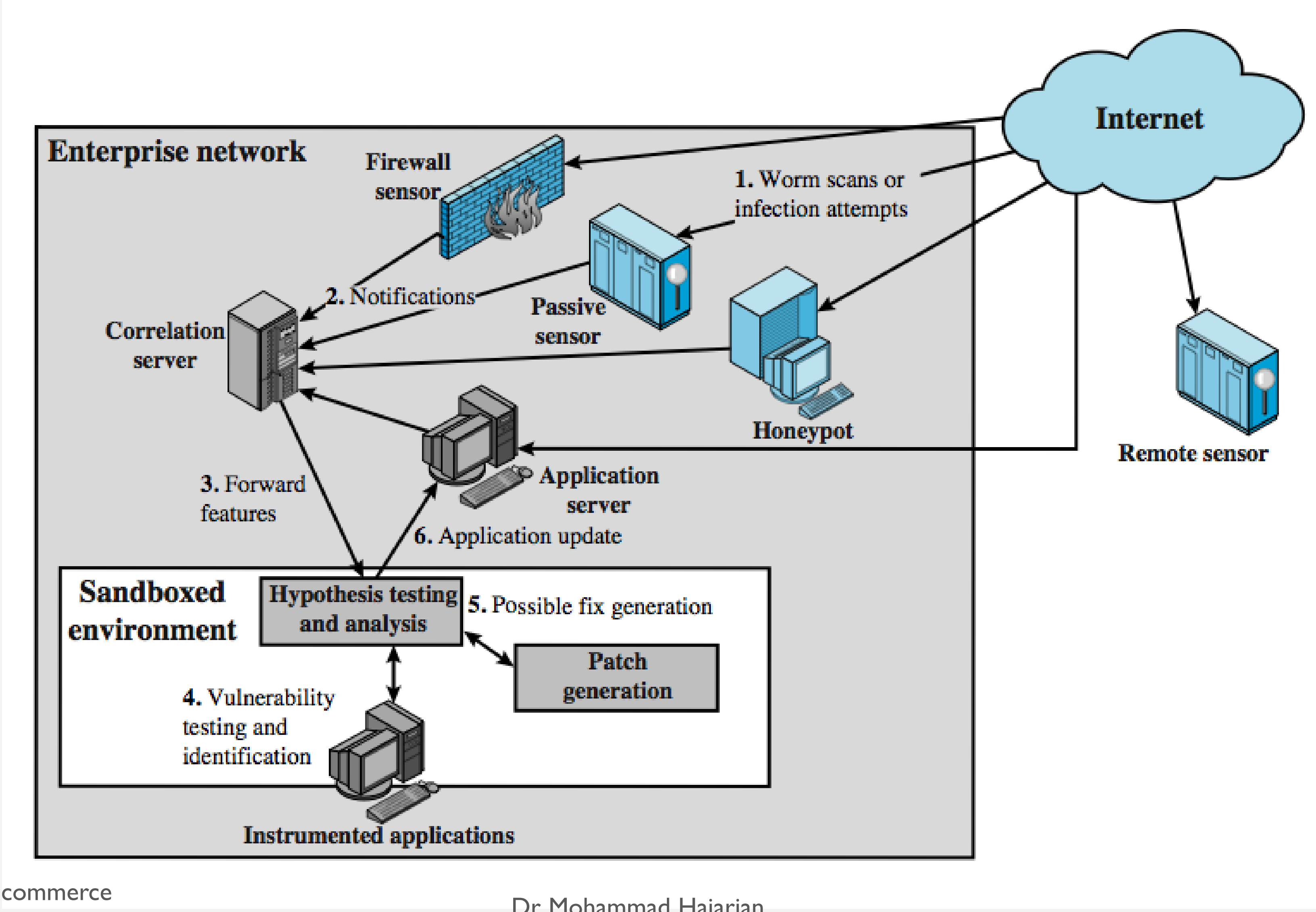
- overlaps with anti-virus techniques
- once worm on system A/V can detect
- worms also cause significant net activity
- worm defense approaches include:
  - signature-based worm scan filtering
  - filter-based worm containment
  - payload-classification-based worm containment
  - threshold random walk scan detection
  - rate limiting and rate halting
    - puts speed limit on scanning / fignerprinting actions

PROACTIVE WORM CONTAINMENT (PWC)

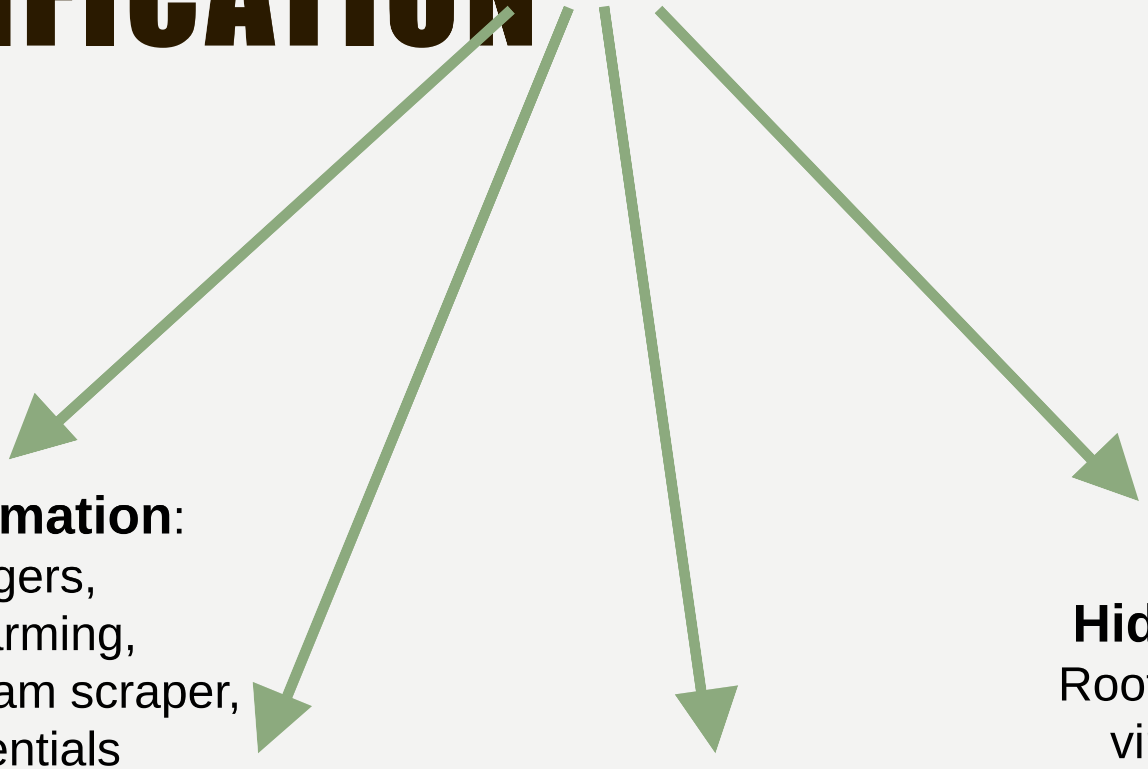


Looks for surges in the rate of frequency of outgoing connection attempts and the diversity of connections to remote hosts. When such a surge is detected, the software immediately blocks its host from further connection attempts.

NETWORK BASED WORM DEFENSE



SUMMARY: MALWARE PAYLOAD CLASSIFICATION



Theft of Information:
E.g. Keyloggers,
spyware, pharming,
Data exfiltration, ram scraper,
stolen credentials

Theft of Service
Botnet, Denial of Service
DDOS, adware, spammers,
Command & control

Corruption of System
Or Files
Virus, worm, rootkit,
ransomware

Stealth:
Hide presence:
Rootkit, backdoors,
viruses/worms

SUMMARY: MALWARE CONTROLS

Countermeasures:

- Ingress Monitor: Are traffic (flows) entering network valid?
- Egress Monitor: Is traffic exiting network valid?
- Host Scanner: Are actions on the computer suspicious?
- Malware Countermeasure: Are actions by the program suspicious?
- Distributed Intelligence: Host-based and perimeter sensors, intelligence analysis

SPAM

SPAM

- Abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages
- Remains economically viable
  - Advertisers have no operating cost beyond the management of their mailing lists
  - Difficult to hold senders accountable for their mass mailings

SPAMMİNG İN DİFFERENT MEDİA

- E-mail Spam
  - Unsolicated bulk e-mail (UBE)
  - Unsolicated commercial e-mail (UCE)
  - Practice of sending unwanted e-mail messages
  - Sent via ‘zombie networks’, networks of virus- or worm-infected PCs
  - Many modern worms install a backdoor which allows the spammer access to the computer

SPAMMİNG İN DİFFERENT MEDİA

- Instant messaging & Chat room Spam
  - Requires scriptable software & the recepients’ IM usernames
- Chat Spam
  - Can occur in any live chat environment
  - Consists of repeating the same word/sentences many times to get attention or to interfere with normal operations
- Newsgroup & Forum Spam

SPAMMİNG İN DİFFERENT MEDİA

- Mobile Phone Spam
- Online Game Messaging Spam
- Spam Targeting Search Engines
  - Spamdexing
  - Practice on the WWW of modifying HTML pages to increase the chances of them being placed high on search engine relevancy lists
- Blog, Wiki & Guestbook Spam
- Spam Targeting Video Sharing Sites

DİSTRİBUTED DENİAL OF SERVİCE ATTACK (DDOS)

DİSTRİBUTED DENİAL OF SERVİCE ATTACK (DDOS)

- DDoS attacks make computer systems inaccessible by flooding servers, networks and end-user computers
- In a DDoS attack a large number of compromised hosts are amassed
- If an attack comes from a single machine, it is referred to as a DoS

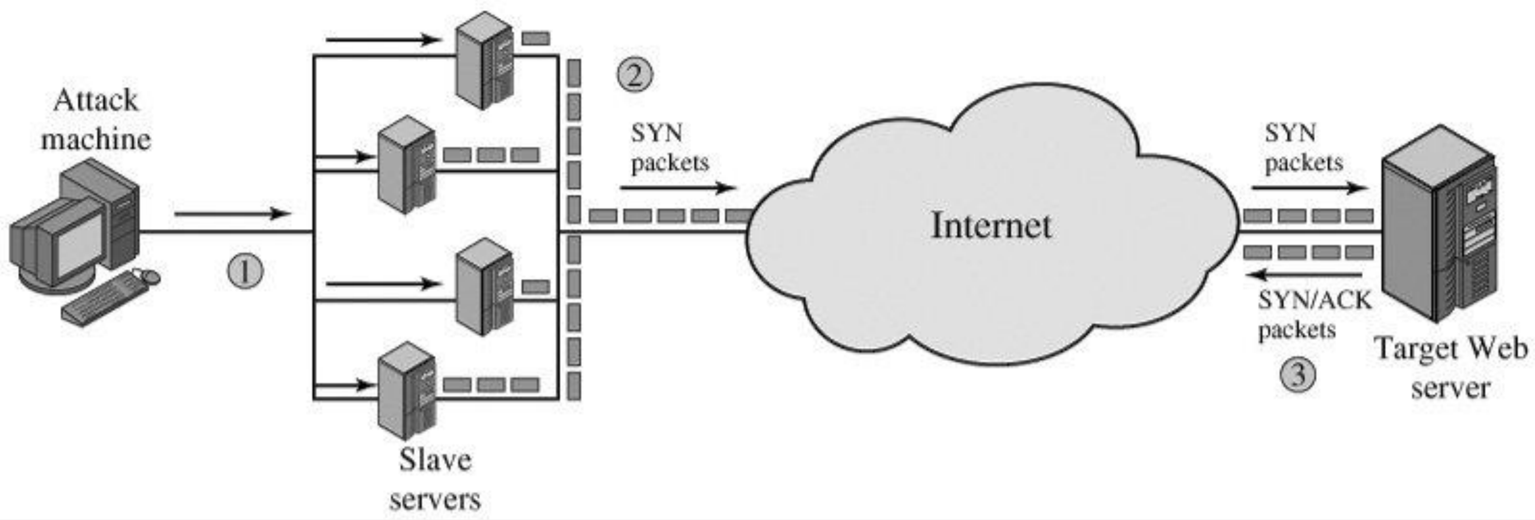
ATTACK DESCRİPTİON

- DDoS attack attempts to consume target's resources
- Consume operation is based on:
  - Internal Resource Attack
  - Consume of Data Transmission Resource

INTERNAL RESOURCE ATTACK

- Attacker takes control of multiple hosts, and instructs them to contact with target
- Slave hosts begin sending TCP/IP SYN packets with erronous return IP address information
  - SYN packets are requests to open TCP connections
- Server sends SYN/ACK response packets to these spurious IP addresses
- Data structure is consumed with “half open” connections

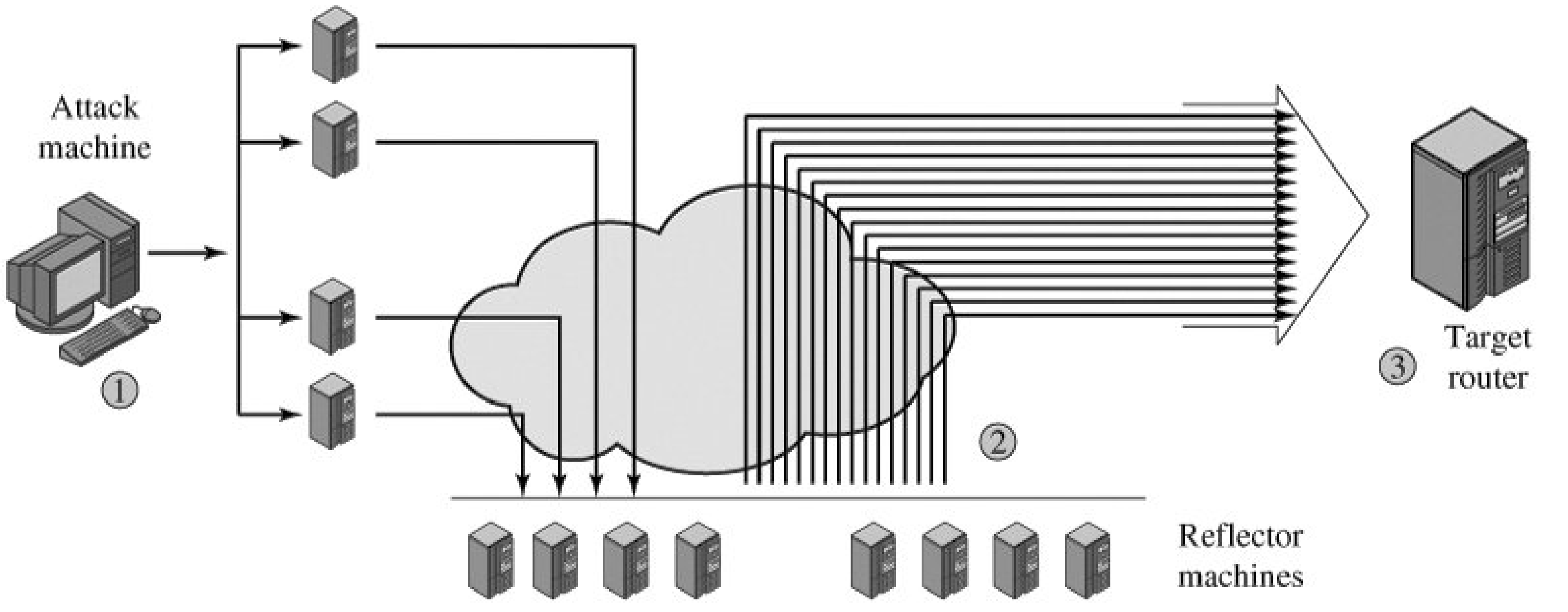
DİSTRİBUTED SYN FLOOD ATTACKS



CONSUME OF DATA TRANSMİSSİON RESOURCE

- Attacker takes control of hosts, intructs them to send ICMP ECHO packets with target's IP address, to a group of hosts
- Nodes that receive multiple requests and responds with sending echo reply packets
- Target's router is flooded, and leaves no data transmission capacity for legitimate traffic

DİSTRİBUTED ICMP ATTACK

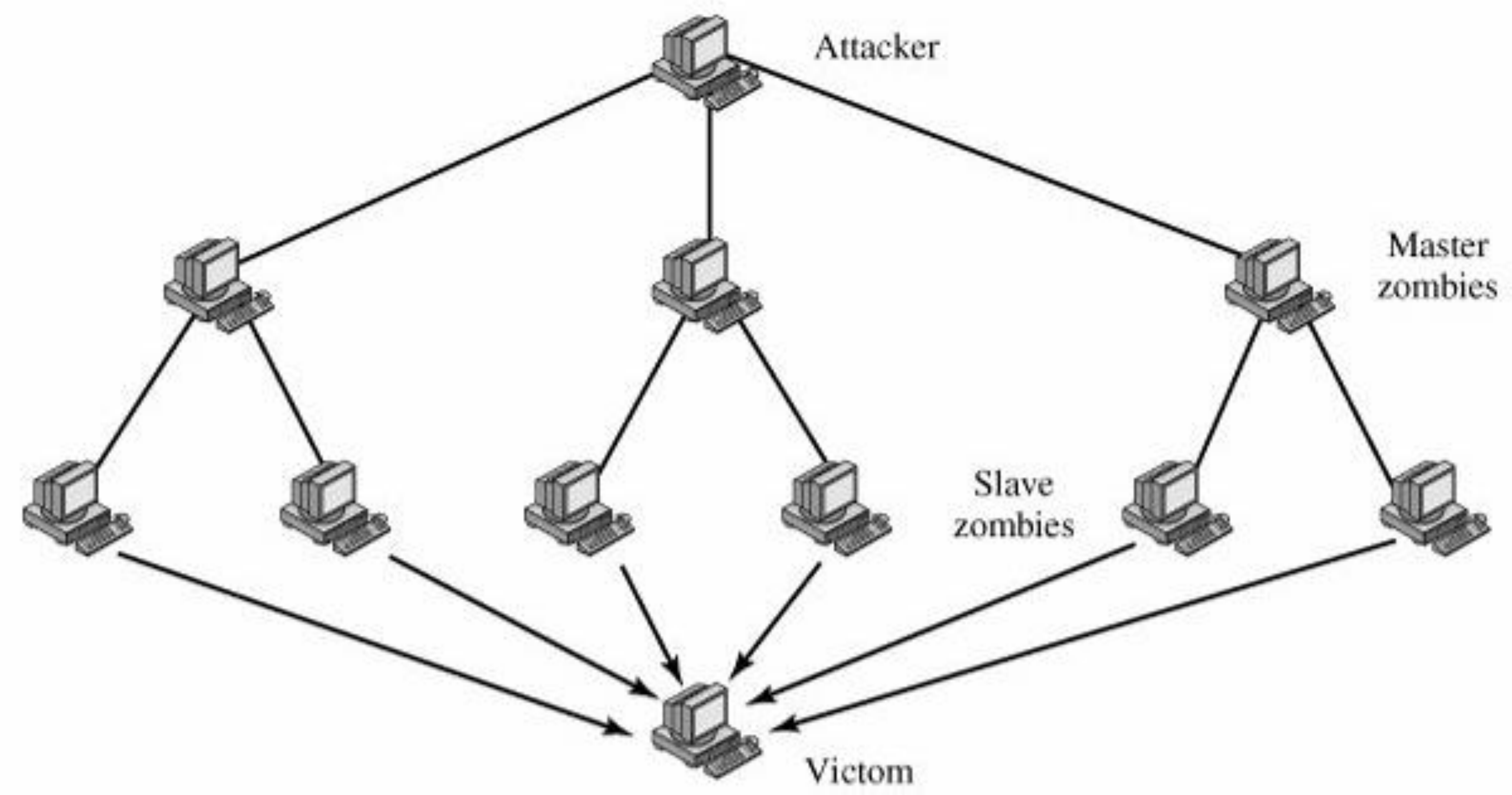


ICMP (Internet Control Message Protocol) is an error-reporting protocol network devices like routers use to generate error messages to the source IP address when network problems prevent delivery of IP packets

DİRECT DDOS ATTACK

- Attacker can implant zombie software
  - Master and slave zombies
- Attacker coordinates master zombies
  - They trigger slave zombies
- Why are two level zombies needed?
  - It makes more difficult to trace the attack back to its source

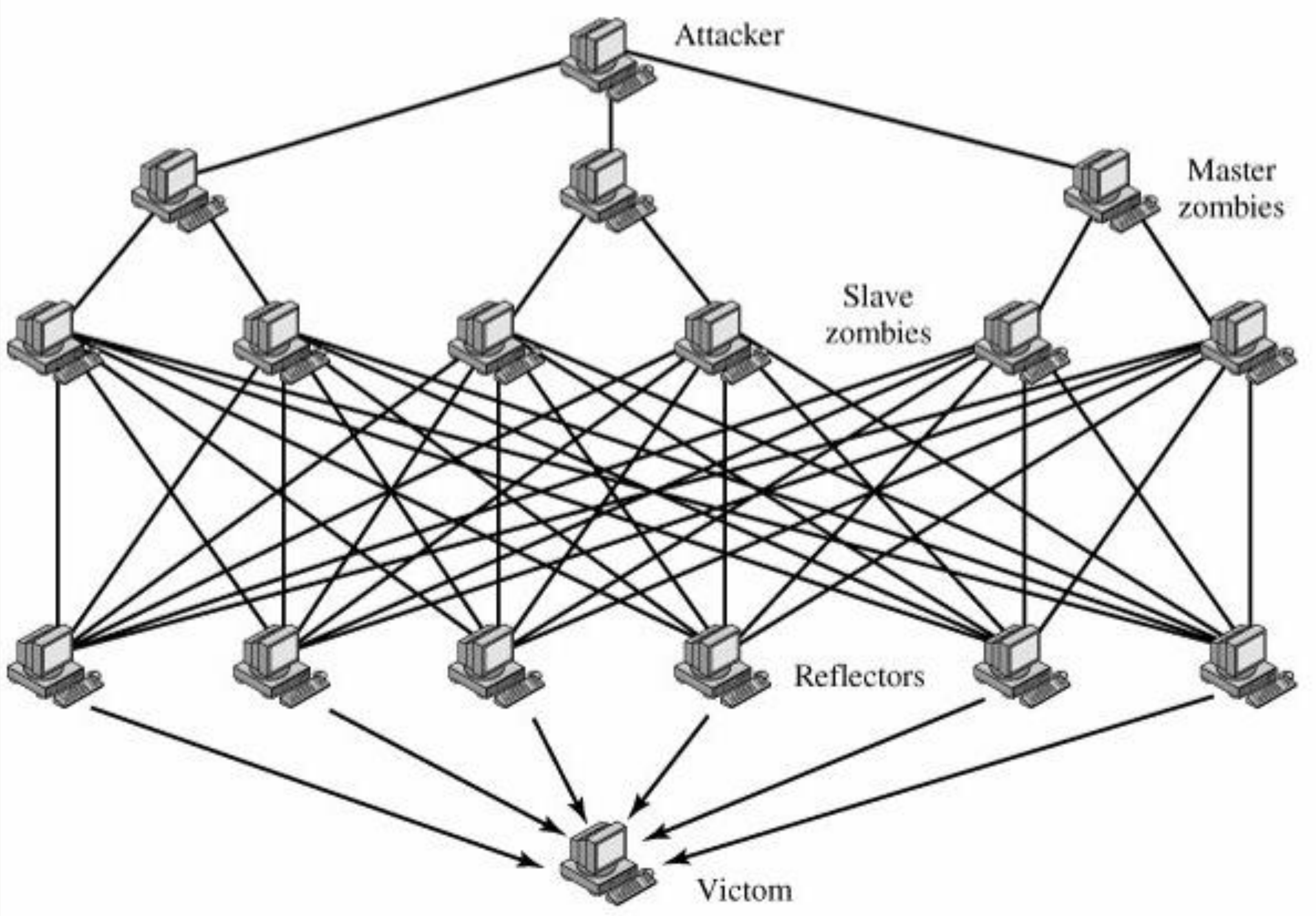
DİRECT DDOS ATTACK



REFLECTOR DDOS ATTACK

- This time slaves send packets to reflectors (uninfected machines)
- Source address of these packets are spoofed IP address of the target
- Reflectors response with packets directed to the target machine
- A reflector DDoS can easily involve more machines
- Hard to detect the source because attack comes from uninfected machines

REFLECTOR DDOS ATTACK



HOW TO FİND VİCTİMS?

- Random
  - This may cause generalized disruption
- Hit-list
  - It results very short scanning period
- Topological
- Local subnet

DDOS COUNTERMEASURES

- Attack prevention and preemption
  - Enforcing policies for resource consumption
- Attack detection and filtering
  - Looking for suspicious patterns of behaviour
- Attack source traceback and identification
  - Does not yield results fast enough

MALWARE TO PROFIT

MALWARE TO PROFİT

- During 1980s and 1990s
  - Created as a form of vandalism or prank
- Recently
  - Written with a financial or profit motive
  - Choice of the author to monetize control over infected systems
    - Turn the control into a source of revenue
- Since 2003
  - Some redirect search engine results to paid advertisements

MALWARE TO PROFİT

- Another way
  - Directly use the infected computers to do work for the creator
  - Infected computers are used as proxies to send out spam messages or to targat anti-spam organizations with distributed DoS attacks
  - Advantage: anonymity

MALWARE TO PROFİT

- In order to coordinate the activity of many infected computers
  - Use of coordinating systems – botnets
- Botnets are also used to push ungraded malware to the infected systems
- Other than those
  - Stealing credit card number
  - Stealing passwords of the online games
  - Taking the control of the modem

VIRUS COUNTERMEASURES

VİRUS COUNTERMEASURES

- Antivirus approaches
- Advanced antivirus techniques

ANTİVİRUS APPROACHES

- The best way is prevention
- Detection
- Identification
- Removal

GENERATİONS OF ANTİVİRUS SOFTWARE

- First generation
  - Simple scanners, requires virus signature, examines proram length
- Second generation
  - Heuristic scanners, looks for fragments of virus codes, decrypts the virus
  - Computes checksum
- Third generation
  - Examines virus actions, not structure
- Fourth generation
  - Conducts a combination of mentioned techniques
  - Includes access control capability

ADVANCED ANTİVİRUS TECHNİQUES

- Generic Decryption
- Digital Immune Sytem
- Behaviour-Blocking Software

GENERİC DECRYPTİON

- CPU emulator
- Virus signature scanner
- Emulation control module

DİGİTAL IMMUNE SYSTEM

- Monitoring program in client machine discovers suspicious programs, signatures or behaviours, forwards program to administrative machine
- Administrative machine encrypts and sends it to central analysis machine
- Central analysis machine uses emulation technique identifies the virus and produces a prescription
- Prescription is sent back

BEHAVİOUR-BLOCKİNG SOFTWARE

- It is integrated with OS
- Monitors suspicios behaviours such as file operations, disk operations, system settings, scripts in e-mails

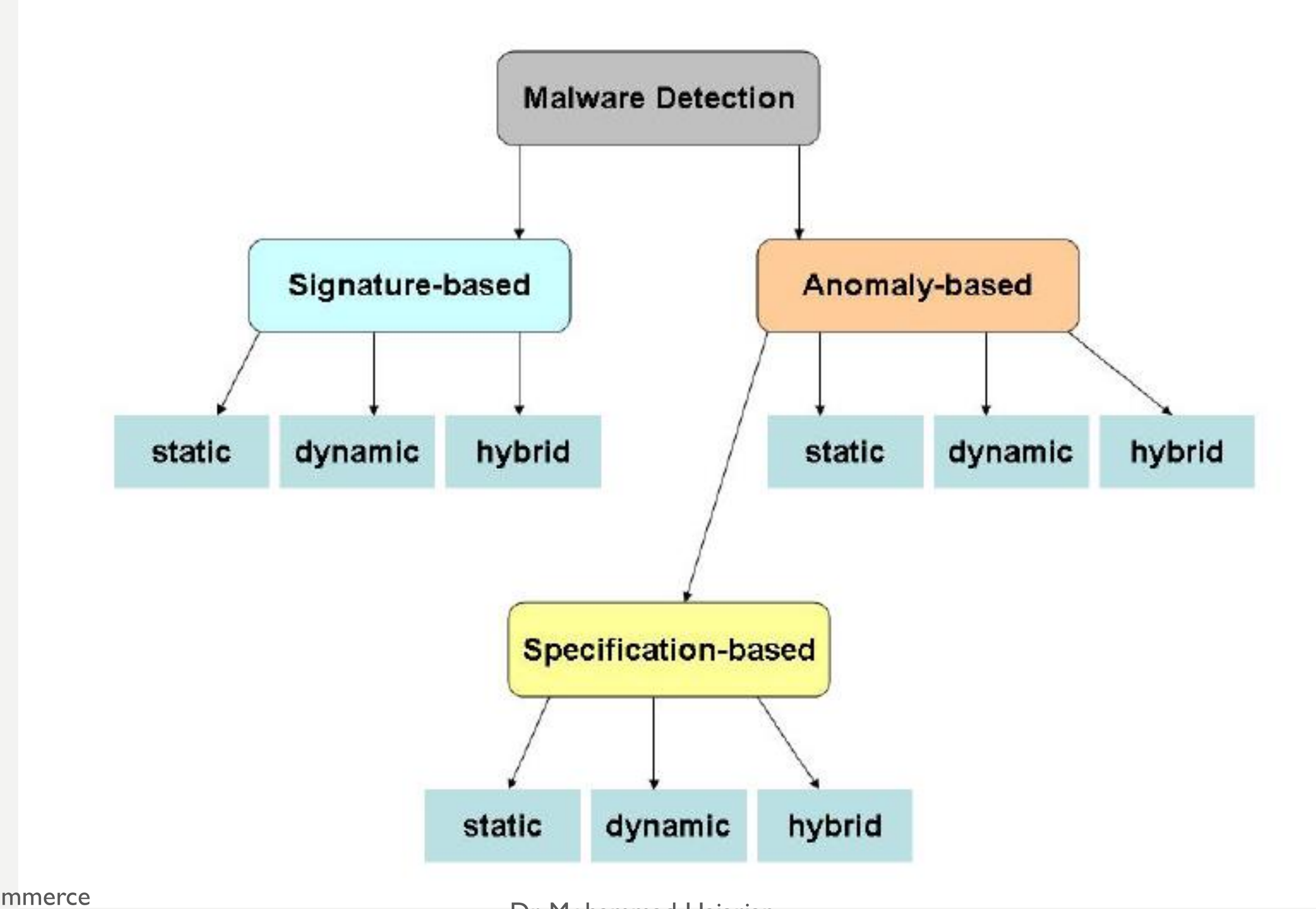
موسسه آموزش عالی غیردولتی غیرانتفاعی بصیر آبیک

MALWARE DETECTION

MALWARE DETECTOR

- Attemps to protect the system by detecting malicious behaviour
- May or may not reside on the same system it is trying to protect
- Performs its protection through the manifested malware detection techniques
- Take two inputs:
  - Its knowledge of malicious behaviour
  - Program under inspection

MALWARE DETECTİON TECHNİQUES



MALWARE DETECTİON TECHNİQUES

- Anomaly-based
  - Uses its knowledge of what constitutes normal behaviour to decide the maliciousness of a program
  - Specification-based detection: leverage a rule set of what is valid behaviour
- Signature-based
  - Uses its characterization of what is known to be malicious to decide the maliciousness of a program

MALWARE DETECTİON TECHNİQUES

- Specific approach is determined by how the technique gathers information to detect malware
- Static analysis
  - Before the program under inspection executes
    - i.e. Sequence of bytes
- Dynamic analysis
  - During or after program execution
    - i.e. Systems seen on the runtime stack

SECURITY

ELEMENTS OF PERIMETER DEFENSE (FORTIFIED BOUNDARY)

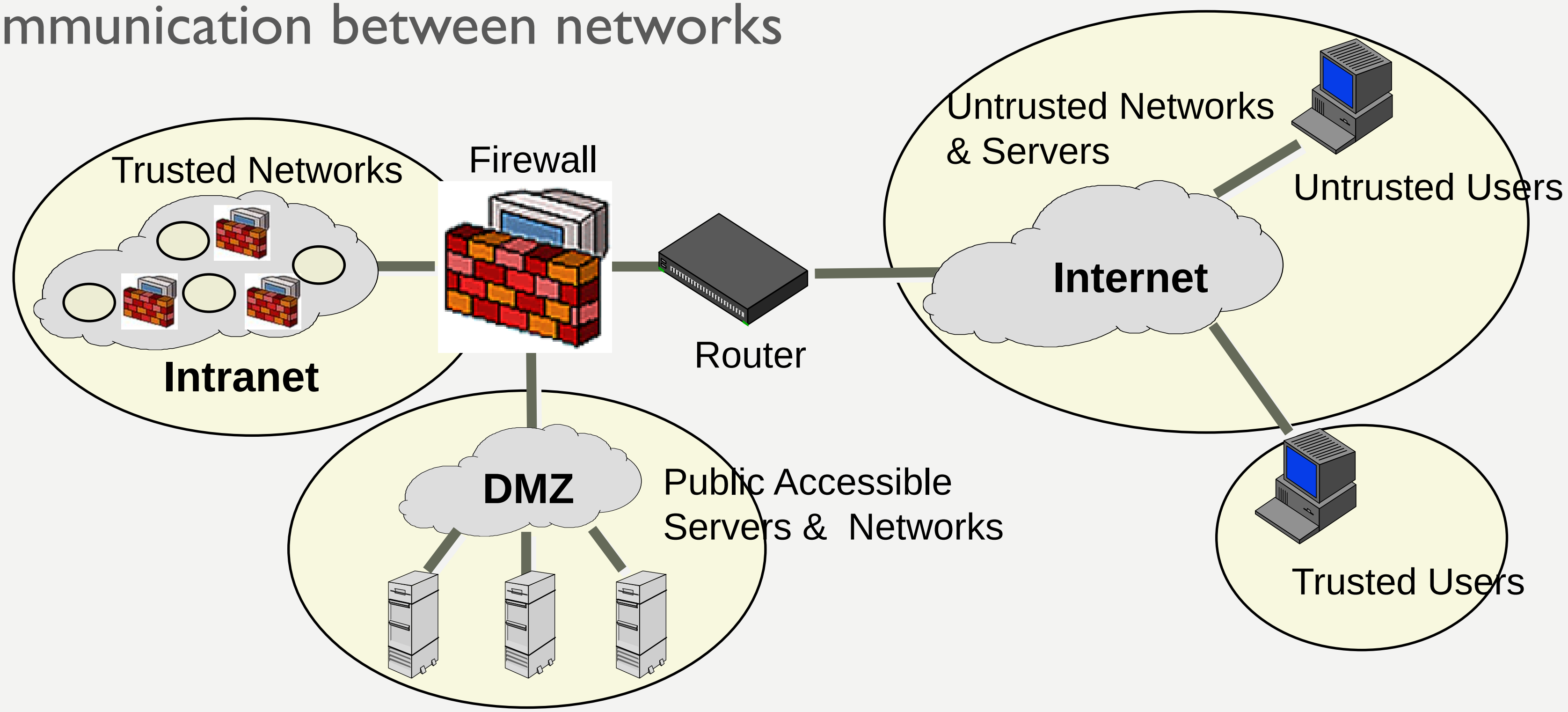
- Border Routers:
  - the last router you control before an untrusted network (such as Internet)
- Firewalls:
  - a chokepoint device that decide what traffic is to be allowed or denied
  - static packet filters, stateful firewalls, proxies
- Intrusion detection system
  - an alarm system that detects malicious events and alerts
  - network-based (NIDS) and host-based (HIDS)

PERIMETER (FORTIFIED BOUNDARY)

- Intrusion Prevention Systems
  - provide automatic defense without administrators' involvements
- Virtual Private Networks
  - protected network session formed across an unprotected channel such as Internet
    - hosts connected through VPN are part of borders
- De-militarized zones (DMZ)
  - small network providing public services (not protected by firewall)

WHAT IS A FIREWALL?

- Device that provides secure connectivity between networks (internal/external; varying levels of trust)
- Used to implement and enforce a security policy for communication between networks



USAGE OF FIREWALL

- Controlling inbound communications
  - Prevent vulnerable programs from being exploited

- Controlling outbound communications is generally harder

COMMON ACCEPTABLE OUTBOUND CONNECTIONS

- SMTP to any address from SMTP mail gateway(s);
- DNS to any address from an internal DNS server to resolve external host names;
- HTTP and HTTPS from an internal proxy server for users to browse web sites;
- NTP to specific time server adds from internal time server(s);
- Any ports required by AV, spam filtering, web filtering or patch management software to appropriate vendor address(es) to pull down updates; and
- Anything else where the business case is documented and signed off by appropriate management.

ROUTING FILTERING

- A router can ensure that source IP address of a packet belongs to the network it is coming from
  - known as network ingress filtering [RFC 2827]
- Example
  - No outbound traffic bears a source IP address not assigned to your network.
  - No outbound traffic bears a private (non-routable) IP address.
  - No inbound traffic bears a source IP address assigned to your network.
  - No inbound traffic bears a private (non-routable) IP address.

DEFENSE IN DEPTH

- Perimeter
  - static packet filter
  - stateful firewall
  - proxy firewall
  - IDS and IPS
  - VPN device
- Internal network
  - Ingress and egress filtering
  - Internal firewalls
  - IDS sensors

DEFENSE IN DEPTH

- Individual Hosts
  - host-centric firewalls
  - anti-virus software
  - configuration management
  - audit
- The human factor

- Why defense in depth, or perimeter defense is not enough?

WHY PERIMETER DEFENSE NOT ENOUGH?

- Wireless access points and/or modem connection.
- Network ports accessible to attacker who have physical access
- Laptops of employees and/or consultants that are also connected to other networks
- Compromised end hosts through allowed network communications, e.g., drive-by downloads, malicious email attachments, weak passwords

TYPES OF FIREWALLS

- Network-based vs. host-based (Personal)
- Hardware vs. Software
- Network layer vs. application layer

Stateless firewalls protect based on static information such as source and destination and packets based on the full context of a given network connection,

stateless firewalls filter packets based on the individual packets themselves

STATELESS PACKET FILTERS

- Inspecting the "packets"
- Use rules to determine
  - Whether to allow a packet through, drop it, or reject it.
  - use only info in packet (no state kept)
    - source IP, destination IP, source port number, destination port number, TCP or UDP

- Example:
  - no inbound connection to low port
  - outgoing web/mail traffic must go through proxies

MORE ABOUT NETWORKING: PORT NUMBERING

- TCP connection
  - Server port uses number less than 1024
  - Client port uses number between 1024 and 16383
- Permanent assignment
  - Ports <1024 assigned permanently
    - 20,21 for FTP 23 for Telnet
    - 25 for server SMTP 80 for HTTP
- Variable use
  - Ports >1024 must be available for client to make connection

STATEFUL FIREWALL

- Why need stateful: a stateless firewall doesn’t know whether a packet belong to an accesptable connection

- Packet decision made in the context of a connection
- If packet is a new connection, check against security policy
- If packet is part of an existing connection, match it up in the state table & update table
  - can be viewed as packet filtering with rules dynamically updated

PROXY FIREWALLS (APPLICATION LAYER FIREWALLS)

- Relay for connections
- Client ↔ Proxy ↔ Server
- Understands specific applications
  - Limited proxies available
  - Proxy ‘impersonates’ both sides of connection
- Resource intensive
  - process per connection
- HTTP proxies may cache web pages

PERSONAL FIREWALLS

- Running on one PC, controlling network access
  - Windows firewall, iptables (Linux), ZoneAlarm, etc.
- Typically determines network access based on application programs
- Typically block most incoming traffic, harder to define policies for outgoing traffic
- Can be bypassed/disabled if host is compromised

SYSTEM INTRUSION DETECTION AND PREVENTION

DEFINITION

- Intrusion Detection
  - Intrusion detection is a technique of detecting unauthorized access to a computer system or a computer network.
  - An intrusion into a system is an attempt by an outsider to the system to illegally gain access to the system.
  - Intrusion prevention, on the other hand, is the art of preventing an unauthorized access of a system’s resources.
  - The two processes are related in a sense that while intrusion detection passively detects system intrusions, intrusion prevention actively filters network traffic to prevent intrusion attempts.

INTRUSION

- Intrusion
  - An *intrusion* is a deliberate unauthorized attempt, successful or not, to break into, access, manipulate, or misuse some valuable property and where the misuse may result into or render the property unreliable or unusable.
  - The person who intrudes is an *intruder*.

TYPES OF INTRUSIONS

- There are six types of intrusions:
  - Attempted break-ins, which are detected by atypical behavior profiles or violations of security constraints. An intrusion detection system for this type is called anomaly-based IDS.
  - Masquerade attacks, which are detected by atypical behavior profiles or violations of security constraints. These intrusions are also detected using anomaly-based IDS.
  - Penetrations of the security control system, which are detected by monitoring for specific patterns of activity.
  - Leakage, which is detected by atypical use of system resources.
  - Denial of service, which is detected by atypical use of system resources.
  - Malicious use, which is detected by atypical behavior profiles, violations of security constraints, or use of special privileges.

INTRUSION DETECTION SYSTEMS (IDSS)

- An *intrusion detection system (IDS)* is a system used to detect unauthorized intrusions into computer systems and networks. Intrusion detection as a technology is not new, it has been used for generations to defend valuable resources.
- These are three models of intrusion detection mechanisms: *anomaly-based* detection, *signature-based* detection, and *hybrid* detection.

- Anomaly Detection –
  - Anomaly based systems are “learning” systems in a sense that they work by continuously creating “norms” of activities. These norms are then later used to detect anomalies that might indicate an intrusion.
  - Anomaly detection compares observed activity against expected normal usage profiles “leaned”. The profiles may be developed for users, groups of users, applications, or system resource usage.

- Misuse Detection -
  - The misuse detection concept assumes that each intrusive activity is representable by a unique pattern or a *signature* so that slight variations of the same activity produce a new signature and therefore can also be detected.
  - Misuse detection systems, are therefore, commonly known as *signature systems*. They work by looking for a specific signature on a system. Identification engines perform well by monitoring these patterns of known misuse of system resources.
- Hybrid Detection -
  - Because of the difficulties with both the anomaly-based and signature-based detections, a hybrid model is being developed. Much research is now focusing on this hybrid model.

TYPES OF INTRUSION DETECTION SYSTEMS

- Intrusion detection systems are classified based on their monitoring scope. There are: network-based intrusion detection and host-based detections.
- Network-Based Intrusion Detection Systems (NIDSs)
  - NIDSs have the whole network as the monitoring scope. They monitor the traffic on the network to detect intrusions. They are responsible for detecting anomalous, inappropriate, or other data that may be considered unauthorized and harmful occurring on a network. There are striking differences between NIDS and firewalls.

- Host-Based Intrusion Detection Systems (HIDS)
  - Recent studies have shown that the problem of organization information misuse is not confirned only to the “bad” outsiders but the problem is more rampart within organizations. To tackle this problem, security experts have turned to inspection of systems within an organization network. This local inspection of systems is called *host-based intrusion detection systems* (HIDS).
  - Host-based intrusion detection is the technique of detecting malicious activities on a single computer.
  - A host-based intrusion detection system, is therefore, deployed on a single target computer and it uses software that monitors operating system specific logs including system, event, and security logs on Windows systems and syslog in Unix environments to monitor sudden changes in these logs.
  - When a change is detected in any of these files, the HIDS compares the new log entry with its configured attack signatures to see if there is a match. If a match is detected then this signals the presence of an illegitimate activity.

- The Hybrid Intrusion Detection System
  - Both NIDS and HIDS are each patrolling its own area of the network for unwanted and illegal network traffic. They, however, complement each other. Both bring to the security of the network their own strengths and weaknesses that nicely complement and augment the security of the network.
  - Hybrids are new and need a great deal of support to gain on their two cousins. However, their success will depend to a great extent on how well the interface receives and distributes the incidents and integrates the reporting structure between the different types of sensors in the HIDS and NIDS spheres. Also the interface should be able to smartly and intelligently gather and report data from the network or systems being monitored.

THE CHANGING NATURE OF IDS TOOLS

- Recent studies have shown that the majority of system intrusion actually come from insiders. So newer IDS tools are focusing on this issue and are being built to counter systems intrusion, new attack patterns are being developed to take this human behavior unpredictability into account.
- To keep abreast of all these changes, ID systems are changing constantly.
- The primary focus of ID systems has been on a network as a unit where they collect network packet data by watching network packet traffic and then analyzing it based on network protocol patterns "norms," "normal" network traffic signatures, and network traffic anomalies built in the rule base. But since networks are getting larger, traffic heavier, and local networks more splintered, it is becoming more and more difficult for the ID system to "see" all traffic on a switched network such as an Ethernet. This is leading to new designs of IDS.

OTHER TYPES OF INTRUSION DETECTION SYSTEMS

- Although NIDS and HIDS and their hybrids are the most widely used tools in network intrusion detection, there are others that are less used but more targeting and, therefore, more specialized.
- Because many of these tools are so specialized, many are still not considered as being intrusion detection systems but rather intrusion detection add-ons or tools.

- System Integrity Verifiers (SIVs)
  - SIVs monitor critical files in a system, such as system files, to find whether an intruder has changed them. They can also detect other system components' data; for example, they detect when a normal user somehow acquires root/administrator level privileges. In addition, they also monitor system registries in order to find well known signatures.
- Log File Monitors (LFM)
  - LFMs first create a record of log files generated by network services. Then they monitor this record, just like NIDS, looking for system trends, tendencies, and patterns in the log files that would suggest an intruder is attacking.

- Honeypots
  - A *honeypot* is a system designed to look like something that an intruder can hack. They are built for many purposes but the overriding one is to deceive attackers and learn about their tools and methods.
  - Honeypots are also add-on/tools that are not strictly sniffer-based intrusion detection systems like HIDS and NIDS. However, they are good deception systems that protect the network in much the same way as HIDS and NIDS.
  - Since the goal for a honeypot is to deceive intruders and learn from them without compromising the security of the network, then it is important to find a strategic place for the honeypot. In the DMZ for those networks with DMZs or behind the network firewall if the private network does not have a DMZ.

RESPONSE TO SYSTEM INTRUSION

- A good intrusion detection system alert should produce a corresponding response.
- A good response must consist of pre-planned defensive measures that include an incident response team and ways to collect IDS logs for future use and for evidence when needed.

- Incident Response Team
  - An *incident response team* (IRT) is a primary and centralized group of dedicated people charged with the responsibility of being the first contact team whenever an incidence occurs. An IRT must have the following responsibilities:
    - keeping up-to-date with the latest threats and incidents,
    - being the main point of contact for incident reporting,
    - notifying others whenever an incident occurs,
    - assessing the damage and impact of every incident,
    - finding out how to avoid exploitation of the same vulnerability, and
    - recovering from the incident.

- IDS Logs as Evidence
  - IDS logs can be kept as a way to protect the organization in case of legal proceedings. If sensors to monitor the internal network are to be deployed, verify that there is a published policy explicitly stating that use of the network is consent to monitoring.

CHALLENGES TO INTRUSION DETECTION SYSTEMS

- There is an exciting future and challenges for IDS as the marriage between it and artificial intelligence takes hold
- Although there are also IDS challenges in many areas including in the deployment of IDSes in switched environments.
- Deploying IDS in Switched Environments
  - Network-based IDS sensors must be deployed in areas where they can "see" network traffic packets. However, in switched networks this is not possible because by their very nature, sensors in switched networks are shielded from most of the network traffic. Sensors are allowed to "see" traffic only from specified components of the network.
  - One way to handle this situation has traditionally been to attach a network sensor to a mirror port on the switch. But port mirroring, in addition to putting an overhead on the port, gets unworkable when there is an increase in traffic on that port because overloading one port with traffic from other ports may cause the port to bulk and miss some traffic.

- Other issues still limiting IDS technology are:
  - False alarms. Though the tools have come a long way, and are slowly gaining acceptance as they gain widespread use, they still produce a significant number of both false positives and negatives,
  - The technology is not yet ready to handle a large-scale attack. Because of its very nature it has to literally scan every packet, every contact point, and every traffic pattern in the network. For larger networks and in a large-scale attack, it is not possible that the technology can be relied on to keep working with acceptable quality and grace.
  - Unless there is a breakthrough today, the technology in its current state cannot handle very fast and large quantities of traffic efficiently.
  - Probably the biggest challenge is the IDS's perceived and sometimes exaggerated capabilities. The technology, while good, is not the cure of all computer network ills that it is pumped up to be. It is just like any other good security tool.

IMPLEMENTING AN INTRUSION DETECTION SYSTEM

- An effective IDS does not stand alone. It must be supported by a number of other systems. Among the things to consider, in addition to the IDS, in setting up a good IDS for the company network are:
  - *Operating Systems*. A good operating system that has logging and auditing features. Most of the modern operating systems including Windows, Unix, and other variants of Unix have these features. These features can be used to monitor security critical resources.
  - *Services*. All applications on servers such as Web servers, e-mail servers, and databases should include logging/auditing features as well.
  - *Firewalls*. A good firewall should have some network intrusion detection capabilities.
  - *Network management platform*. Whenever network management services such as OpenView are used, make sure that they do have tools to help in setting up alerts on suspicious activity.

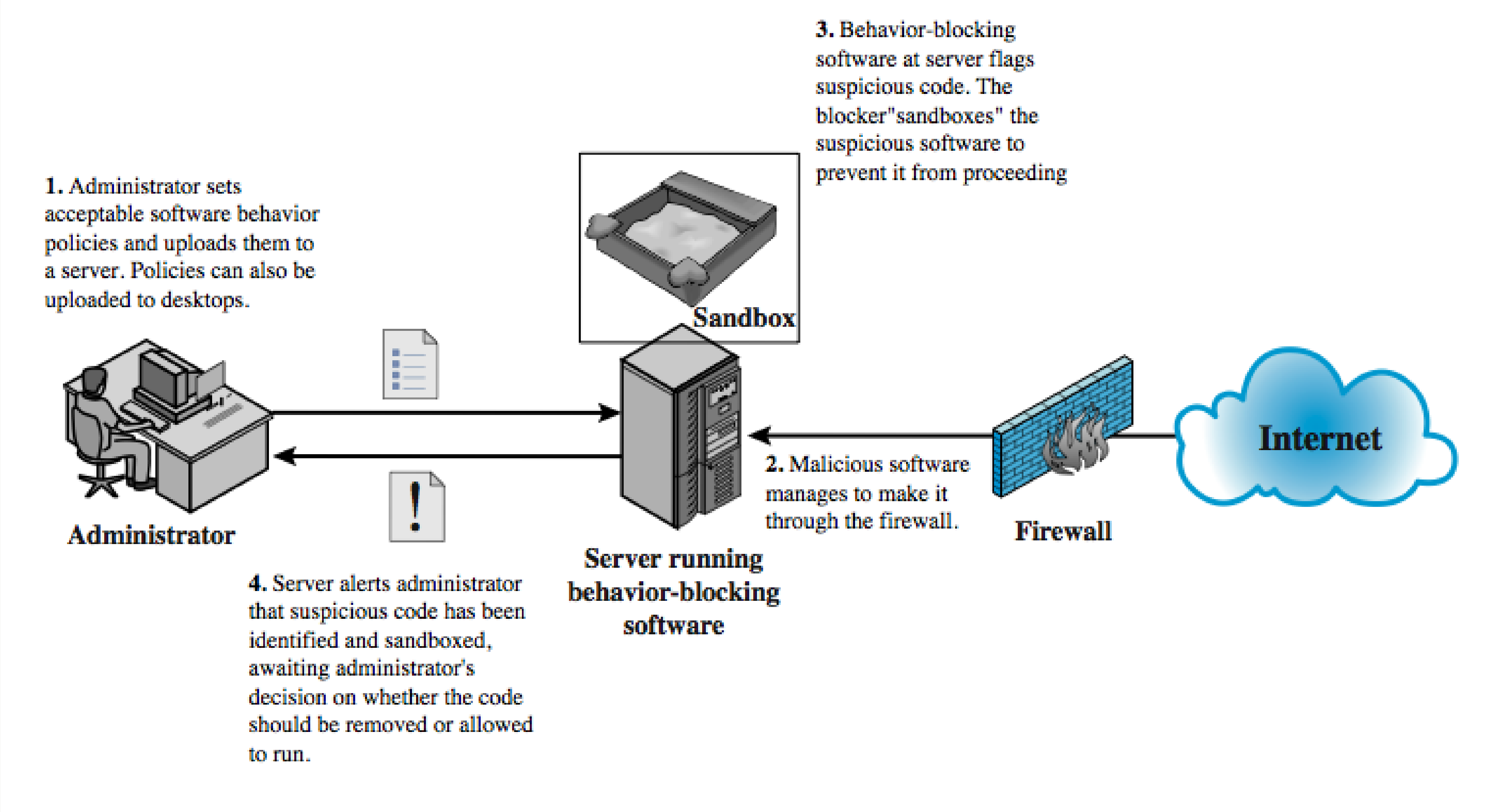
INTRUSION PREVENTION SYSTEMS (IPSS)

- Although IDS have been one of the cornerstones of network security, they have covered only one component of the total network security picture since they have been and they are a passive component which only detects and reports without preventing.
- A promising new model of intrusion is developing and picking up momentum. It is the *intrusion prevention system* (IPS) which, is to prevent attacks.
- Like their counterparts the IDS, IPS fall into two categories: network-based and host-based.

- Network-Based Intrusion Prevention Systems (NIPSs)
  - Because NIDSs are passively detecting intrusions into the network without preventing them from entering the networks, many organizations in recent times have been bundling up IDS and firewalls to create a model that can detect and then prevent.
  - The bundle works as follows.
    - The IDS fronts the network with a firewall behind it. On the detection of an attack, the IDS then goes into the prevention mode by altering the firewall access control rules on the firewall. The action may result in the attack being blocked based on all the access control regimes administered by the firewall.
    - The IDS can also affect prevention through the TCP resets; TCP utilizes the RST (reset) bit in the TCP header for resetting a TCP connection, usually sent as a response request to a non-existent connection. But this kind of bundling is both expensive and complex, especially to an untrained security team. It suffers from *latency* – the time it takes for the IDS to either modify the firewall rules or issue a TCP reset command. This period of time is critical in the success of an attack.

- Host-Based Intrusion Prevention Systems (HIPSs)
  - Most HIPSs work by *sand-boxing*, a process of restricting the definition of acceptable behavior rules used on HIPSs. HIPS prevention occurs at the agent residing at the host. The agent intercept system calls or system messages by utilizing dynamic linked libraries (dll) substitution.
  - The substitution is accomplished by injecting existing system dlls with vendor stub dlls that perform the interception.

BEHAVIOR-BLOCKING SOFTWARE



1. Administrator sets acceptable software behavior policies and uploads them to a server. Policies can also be uploaded to desktops.

2. Malicious software manages to make it through the firewall.

3. Behavior-blocking software at server flags suspicious code. The blocker"sandboxes" the suspicious software to prevent it from proceeding

4. Server alerts administrator that suspicious code has been identified and sandboxed, awaiting administrator's decision on whether the code should be removed or allowed to run.

Q/A

- End of Session 2

THANK YOU!