Module 5

Firewalls

IDS

Need for Firewall

- If your PC is connected to the Internet, you are a potential target to an array of cyber threats, such as hackers, keyloggers, and Trojans that attack through unpatched security holes.
- This means that if you, like most people shop and bank online, are vulnerable to identity theft and other malicious attacks.

Why do u need Firewalls

- A firewall works as a barrier, or a shield, between your PC and cyber space.
- When you are connected to the Internet, you are constantly sending and receiving information in small units called packets.
- The firewall filters these packets to see if they meet certain criteria set by a series of rules, and thereafter blocks or allows the data.
- This way, hackers cannot get inside and steal information such as bank account numbers and passwords from you.

Firewall

- It is simply a router that is used to filter the packets
- Or a multicomputer that performs routing of packets with application level proxy services
- A group of routers to enforce access control - either to permit packets/or to block
-

Firewall basics

- Basic firewalls such as the one included in Windows XP, only monitor incoming traffic by default.
- This may give you a false sense of security. Keep in mind, outgoing traffic, with your credit card information, bank accounts, and social security number is not protected.
- A good firewall will monitor traffic in both directions, both your incoming data and your outgoing data, keeping your private information safe.
- In addition to preventing unauthorized access to your PC, it also makes your PC invisible when you're online, helping prevent attempted intrusions in the first place.

Firewall basics

- Although a firewall provides critical protection to keep your PC safe from unauthorized access, it cannot remove malware from a system that has already been infected.
- Therefore, a firewall should be used in conjunction with other proactive measures, such as anti-malware software, to strengthen your resistance to attacks.

Firewall Basics

- Hardware firewalls provide higher level of security and hence preferred for servers where security has the top most priority.
- The software firewalls are less expensive and hence preferred in home computers and laptops.
- Hardware firewalls usually come as an in-built unit of a router and provide maximum security by filtering the data at packet-level.

Firewall Definition

- A **check/choke point** of control and monitoring
- Interconnects networks with different trusts
- Imposes restrictions on network services
  - Only authorized traffic is allowed
- Auditing and controlling access
  - It can give alarm for abnormal behavior

Firewalls Characteristics

Design goals:

1. All traffic form the inside to outside must pass through the firewall (physically blocking all access to the local network except via firewall).
2. Only Authorized traffic (defined by the local security policy) will be allowed to pass.
3. The firewall itself is immune to penetration (use of trusted systems with secure operating systems).

Firewall Characteristics

Four General Technologies:

1. **Service Control**:
   - determines the types of the internet services that can be accessed, in bounded or out bounded.
   - The firewall may filter traffic on the basis of IP address, protocol, or port number
2. **Direction Control**: determines the direction in which particular services requests are allowed to flow
3. **User Control**: controls access to a service according to which user is attempting to access it.
4. **Behavior Control**: controls how particular service are used (e.g. filter e-mail)

Limitations of Firewalls

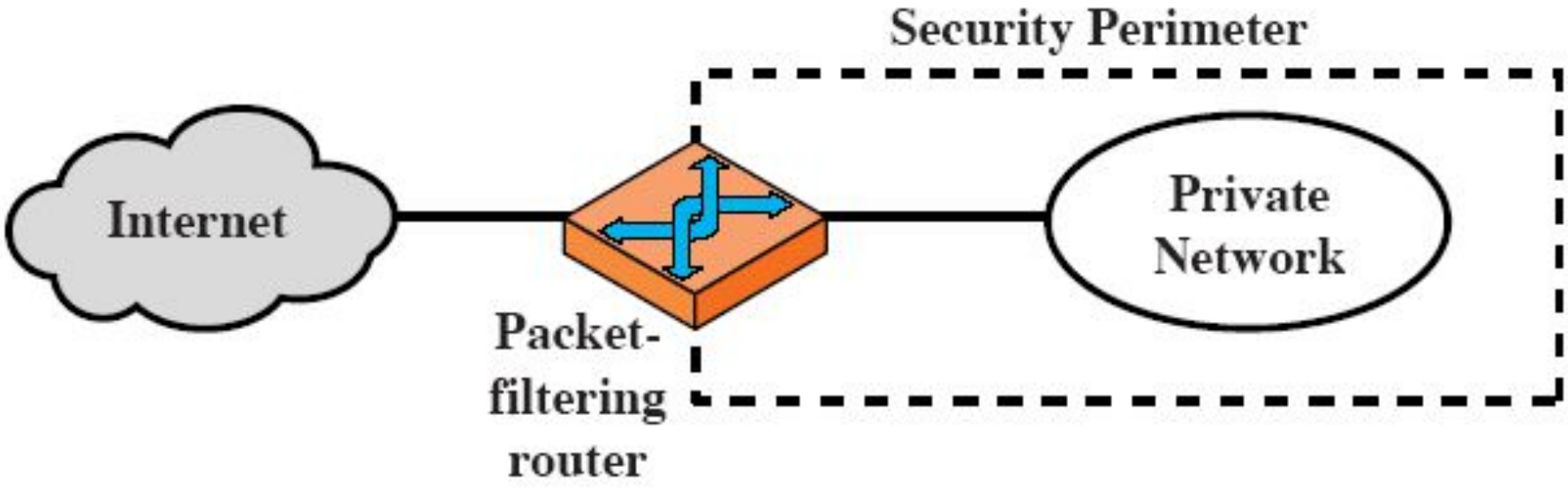
- **It cannot protect from attacks bypassing it**
  - Utility modems, trusted organizations, trusted services (e.g. SSL/SSH)
- **It cannot protect against internal threats**
  - e.g. disgruntled employee
- **It cannot protect against transfer of all virus infected programs or files**
  - because of huge range of O/S & file types

Types of Firewalls

- Three common types of firewalls:

1. Packet-filtering-router.
2. Application-level-Gateways.
3. Circuit-level-Gateways.
4. (Bastion Host).

Firewalls – Packet Filters



(a) Packet-filtering router

Packet-Filtering-Router

- Applies a set of rules to each incoming IP packet and then forwards or discards the packet.
- Filter packets going in both directions.
- The packet filter is typically set up as a list of rule based on matches to fields in the IP or TCP header.
- Two default polices(discards or forwards).
- Filtering rules are based on information contained in a network packet.

1) Source IP Address
2) Destination IP Address
3) Source and destination transport –level address
4) IP Protocol field
5) Interface – which port

Packet-Filtering-Router

- Advantages:

1. Simplicity.
2. Transparency to users.
3. High speed
4. They shield the IP address from outside world
5.

Packet-Filtering-Router

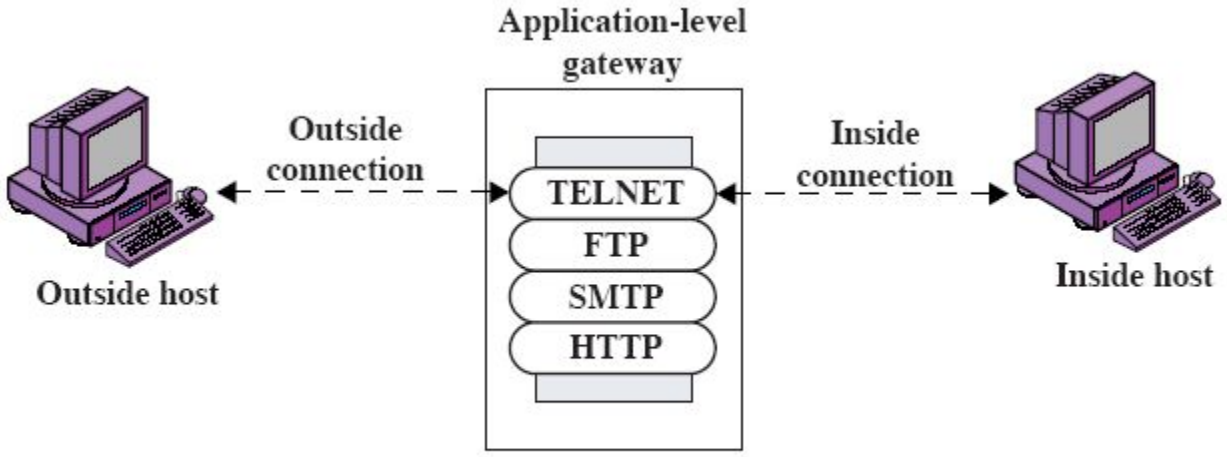
Disadvantages:

- packet filter firewalls do not examine upper-layer data thus they cannot prevent attacks that employ application-specific vulnerabilities or functions.
- limited information is available to the firewall thus the logging functionality present in packet filter firewalls is limited.
- Packet filter firewalls are generally vulnerable to attacks
- Packet filter firewalls do not support advanced user authentication schemes.

Attacks on Packet Filters

- **IP address spoofing**
  - Fake source address to be trusted
  - **Countermeasure:** Add filters on router to block
- **Source routing attacks**
  - **A**ttacker sets a route other than default
  - **Countermeasure:** discard all the packets that use this option
- **Tiny fragment attacks**
  - Split header info over several tiny packets
  - **Countermeasure:** discard the packets where the protocol type is TCP and IP fragment offset is equal to 1.

Firewalls - Application Level Gateway (or Proxy Server)



(b) Application-level gateway

Application-Level-Gateway

- Also called (Proxy Server).
- Acts as relay of application level traffic.

Firewalls - Application Level Gateway (or Proxy)

- **An application level gateway also called proxy server.**
- The user contacts the gateway using a TCP/IP application, such as Telnet or FTP, and the gateway asks the user for the name of the remote host to be accessed.
- When the user responds and provides a valid user ID and authentication information, the gateway contacts the application on the remote host and relays TCP segments containing the application data between the two end points.
- If the does not implement the proxy code for a specific application, the service is not supported and can not be forwarded across the firewall.

Application-Level-Gateway

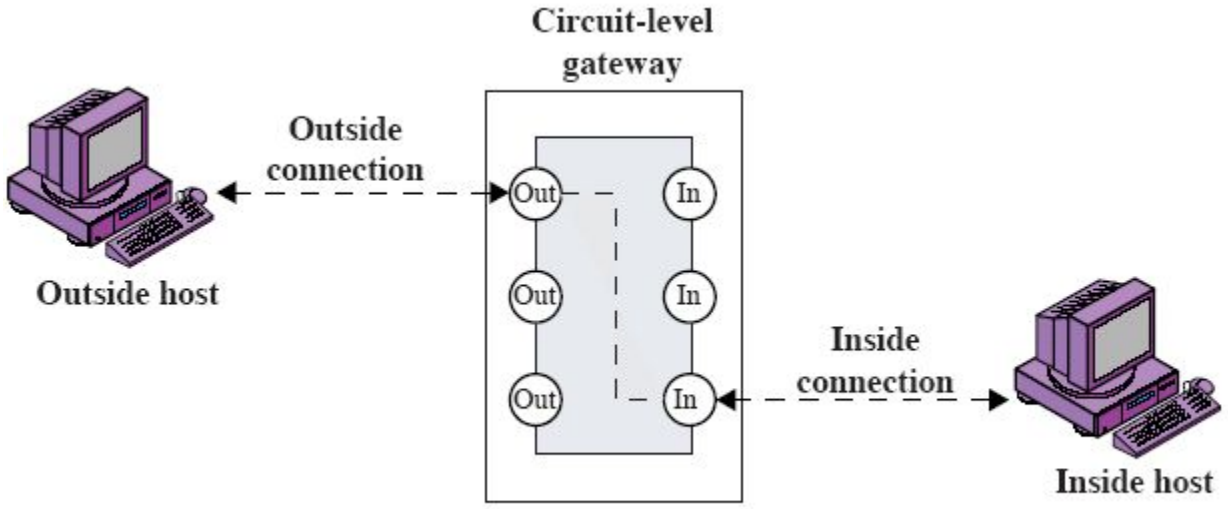
- Advantages:

1. Higher security than packet filter
2. Only need securitize a few allowable applications.
3. Easy to log and audit all incoming traffic.

- Disadvantages:

Additional processing overhead on each connection (Gateway as splice point).

Firewalls - Circuit Level Gateway



(c) Circuit-level gateway

Firewalls - Circuit Level Gateway

- It can be specialized function performed by an application level gateway for certain applications
- It does not permit an end to end TCP connections; rather, the gateway sets up two TCP connections.
- Once the two connections are established, the gateway usually relays traffic without examining the contents

Firewall Basing

- It is common to base a firewall on a stand-alone machine running a common operating system, such as UNIX or Linux.
- Firewall functionality can also be implemented as a software module in a router or LAN switch.

Bastion Host

- A bastion host is a system identified by the firewall administrator as a critical strong point in the network's security.
- Typically, the bastion host serves as a platform for an application-level or circuit-level gateway.
- On the Internet, a bastion host is the only host computer that a company allows to be addressed directly from the public network and that is designed to screen the rest of its network from security exposure.

Bastion Host

- A bastion host is a computer that is fully exposed to attack
- Indeed the firewalls and routers can be considered bastion hosts.
- Due to their exposure a great deal of effort must be put into designing and configuring bastion hosts to minimize the chances of penetration.

Intruder

- **Unauthorized intrusion** into a computer system or network is one of the most serious threats to computer security.
- Intrusion detection systems have been developed to provide early warning of an intrusion so that defensive action can be taken to prevent or minimize damage.
- Intrusion detection involves detecting unusual patterns of activity or patterns of activity that are known to correlate with intrusions.
- One important element of intrusion prevention is password management, with the goal of preventing unauthorized users from having access to the passwords of others.

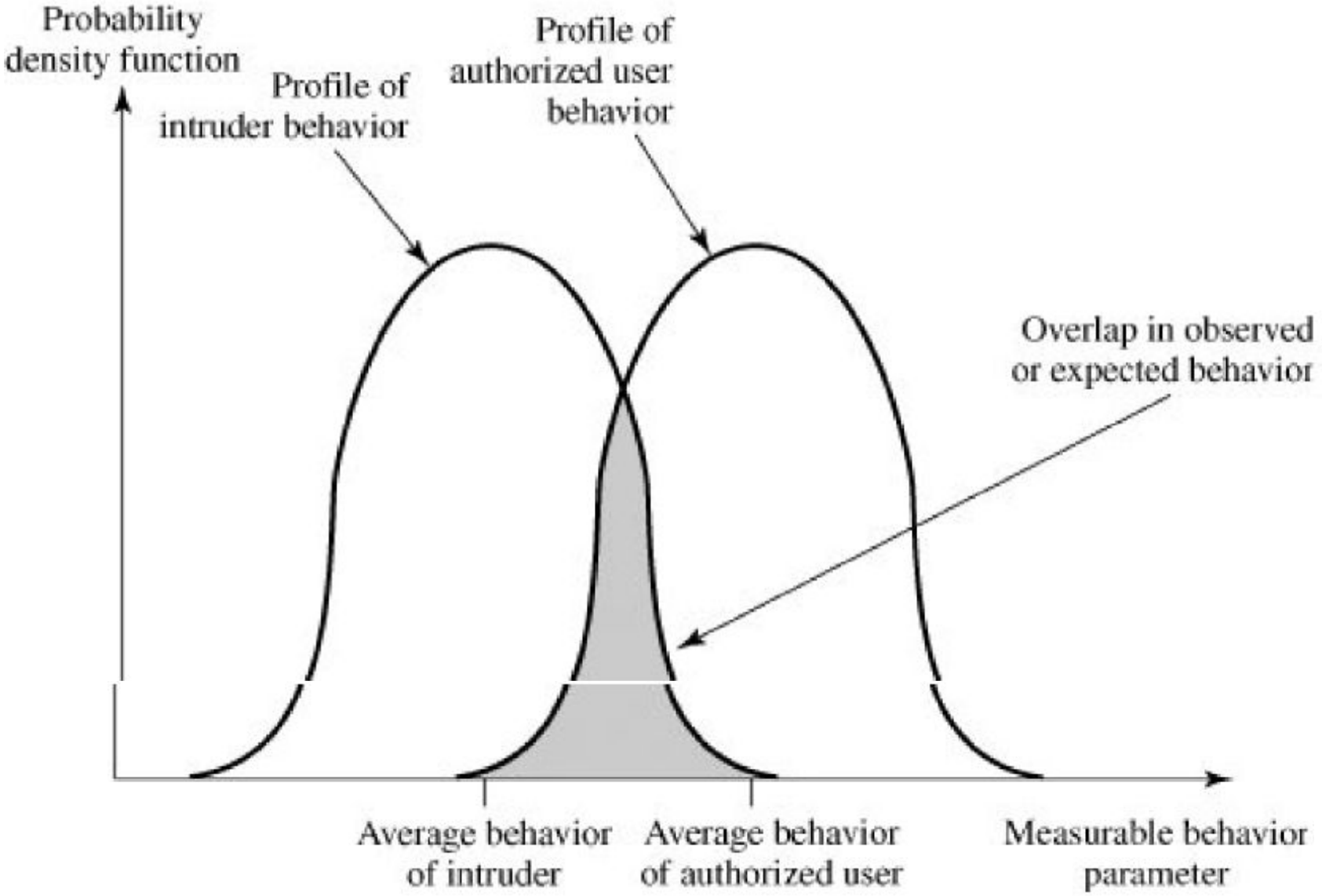
Types of Intruders

- **Masquerader:** An individual who is not authorized to use the computer and who penetrates a system's access controls to exploit a legitimate user's account **(Outsider)**
- **Misfeasor: A legitimate user who accesses data, programs, or resources for which such access is not authorized, or who is a**uthorized for such access but misuses his or her privileges **(Insider)**
- **Clandestine user: An individual who seizes supervisory control of the system and uses this control to evade auditing and** access controls or to suppress audit collection **(Outsider or Insider)**

Intrusion Detection

- If an intrusion is detected quickly enough, **the intruder can be identified and ejected from the system before any damage is done or any data are compromised.**
- Even if the detection is not sufficiently timely to preempt the intruder, the sooner that the intrusion is detected, the less the amount of damage and the more quickly that recovery can be achieved.
- **An effective intrusion detection system can serve as a deterrent, so acting to prevent intrusions.**
- Intrusion detection enables the collection of information about intrusion techniques that can be used to strengthen the intrusion prevention facility.

Profiles of Behaviour of Intruders and Authorized Users



Intrusion Techniques (Guessing Techniques)

- Try default passwords used with standard accounts that are shipped with the system. Many administrators do not bother to change these defaults.
- **Exhaustively try all short passwords (those of one to three characters).**
- Try words in the **system's online dictionary or a list of likely passwords**. Examples of the latter are readily available on hacker bulletin boards.
- Collect information about users, such as their full names, the names of their spouse and children, pictures in their office, and books in their office that are related to hobbies.
- Try users' phone numbers, Social Security numbers, and room numbers.
- Try all legitimate license plate numbers for this state.

Firewall/IDS

Firewall	IDS
A firewall is a hardware and/or software which functions in a networked environment to block unauthorized access while permitting authorized communications.	An Intrusion Detection System (IDS) is a software or hardware device installed on the network (NIDS) or host (HIDS) to detect and report intrusion attempts to the network.
A firewall can block an unauthorized access to network (E.g. A watchman standing at gate can block a thief)	An IDS can only report an intrusion; it cannot block it (E.g. A CCTV camera which can alert about a thief but cannot stop it)
A firewall cannot detect security breaches for traffic that does not pass through it (E.g. a gateman can watch only at front gate. He is not aware of wall-jumpers)	IDS is fully capable of internal security by collecting information from a variety of system and network resources and analyzing the symptoms of security problems

Firewall/IDS

Firewall	IDS
Firewall doesn't inspect content of permitted traffic. (A gateman will never suspect an employee of the company)	IDS keeps a check of overall network
No man-power is required to manage a firewall.	An administrator (man-power) is required to respond to threats issued by IDS
Firewalls are most visible part of a network to an outsider. Hence, more vulnerable to be attacked first. (A gateman will be the first person attacked by a thief!!)	IDS are very difficult to be spotted in a network (especially stealth mode of IDS).

IDS

- Firewalls are the modern-day equivalent to dead bolts and security bars.
- The purpose of a firewall is to prevent unauthorized access.
- Just as locks can be manipulated, firewalls can also be compromised.
- Someone or something must be present to protect the company's assets once someone or something has breached the first line of defence.
- IDSs are the modern-day equivalent to the burglar alarm.
- IDSs constantly monitor the network to look for suspicious activity and, once discovered, can be configured to notify security personnel of the suspected intrusion.
- Unlike burglar alarms, which can only send an alert that a breach has been made, an IDS can also be configured to take action to prevent further access, while sending alarms and recording information about the intruder(s).

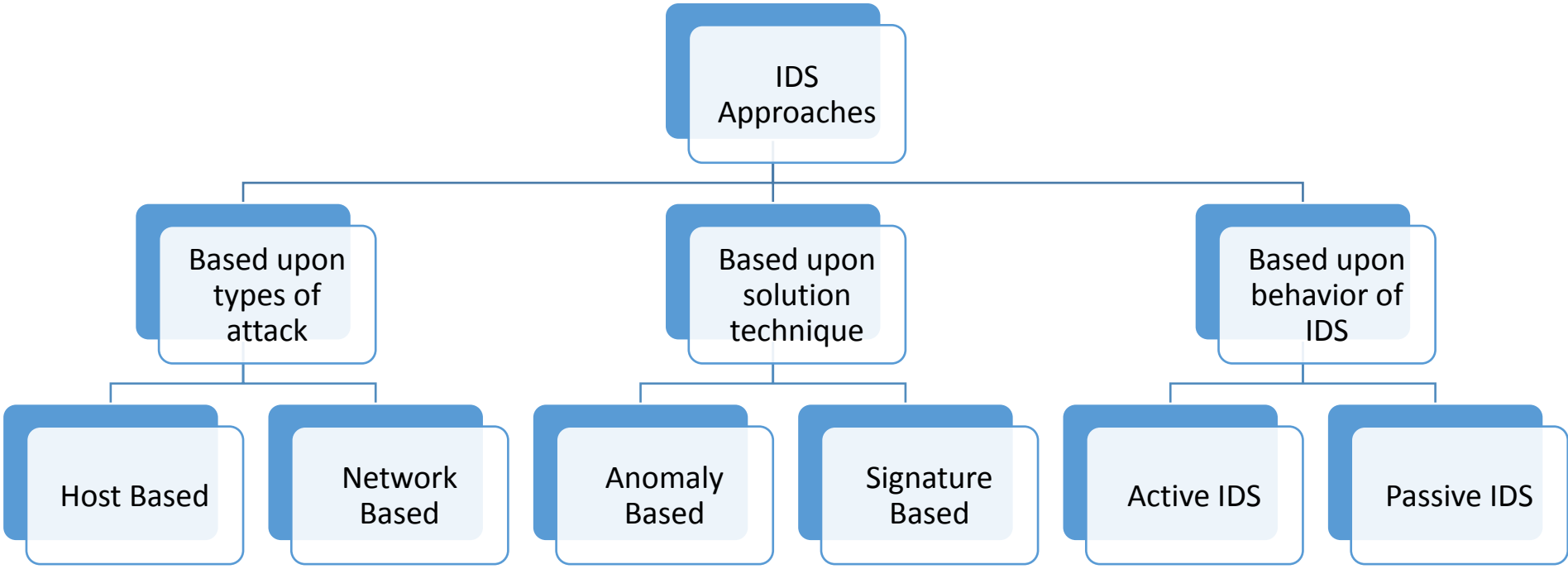
usages

- Identifying the existing threat to an organization
  - Quality control
  - Can raise alerts if no traffice is sen blocked
- Documenting the existing threats to an organization
  - Logs
- Preventive actions of IDPS
  - Terminating the network connection
  - Block access to the target
- Can reconfigure the firewalls
- Can change the content of the attack
  - Can act like a proxy, can unpack the payload, remove the header and nullify the attack

IDS

- It is similar to a burglar alarm system in your home or any organization which detects the presence of any unwanted intervention and alerts the system administrator.
- It is a type of software which is designed to automatically caution administrators when anyone is trying to breach through the system using malicious activities.
- It monitors and analysis the user and system activities.
- It performs auditing of the system files and other configurations and the operating system.
- It assesses the integrity of system and data files
- It conducts analysis of patterns based on known attacks.
- It detects errors in system configuration.
- It detects and cautions if the system is in danger.
- Intrusion detection systems help in sending an alarm against any malicious activity in the network, drop the packets, and reset the connection to save the IP address from any blockage.

Classification of IDS



Host Based IDS

- Host Intrusion Detection Systems are run on individual hosts or devices on the network.
- A HIDS monitors the inbound and outbound packets from the device only and will alert the user or administrator of suspicious activity is detected

Network Based IDS

- Network Intrusion Detection Systems are placed at a strategic point or points within the network to monitor traffic to and from all devices on the network.

Anomaly Detection based IDS

- An IDS which is anomaly based will monitor network traffic and compare it against an established baseline.
- The baseline will identify what is “normal” for that network- what sort of bandwidth is generally used, what protocols are used, what ports and devices generally connect to each other- and alert the administrator or user when traffic is detected which is anomalous, or significantly different, than the baseline.

Signature Based IDS

- A signature based IDS will monitor packets on the network and compare them against a database of signatures or attributes from known malicious threats.
- This is similar to the way most antivirus software detects malware

Signature based IDS

- Ineffective against unknown attacks
-

Passive IDS

- A passive IDS simply detects and alerts. When suspicious or malicious traffic is detected an alert is generated and sent to the administrator or user and it is up to them to take action to block the activity or respond in some way

Active IDS

- A reactive IDS will not only detect suspicious or malicious traffic and alert the administrator, but will take pre-defined proactive actions to respond to the threat.
- Typically this means blocking any further network traffic from the source IP address or user.

What is malware

- Malware, or malicious software, is any program or file that is harmful to a computer user.
- Malware includes computer viruses, worms, Trojan horses and spyware.
- These malicious programs can perform a variety of functions,
  - Stealing
  - Encrypting
  - Deleting sensitive data
  - Altering or hijacking core computing functions
  - Monitoring users computer activity without their permission.

Causes of malware

- Drive-by download—Unintended download of computer software from the Internet
- Unsolicited email —Unwanted attachments or embedded links in electronic mail
- Physical media—Integrated or removable media such as USB drives
- Self propagation—Ability of malware to move itself from computer to computer or network to network, thus spreading on its own

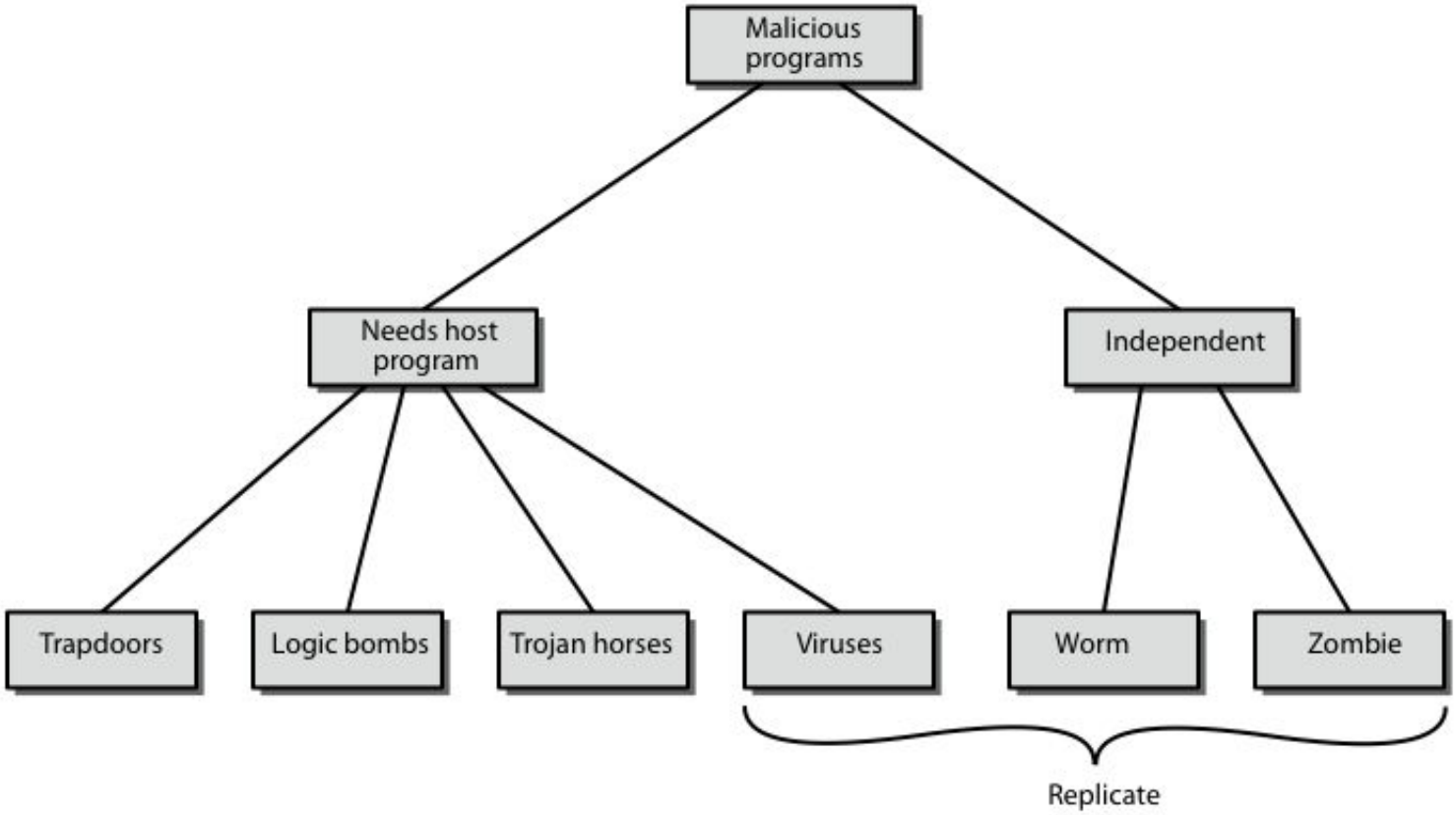
Malicious Software

- **Malicious software can be divided into two categories:** those that **need a host program, and those that are independent.**
- The former are essentially fragments of programs that cannot exist independently of some actual application program, utility, or system program.

  Examples: Viruses, logic bombs, and backdoors
- The latter **are self-contained programs** that can be scheduled and run by the operating system.

  Examples: Worms and zombie programs

Malicious Software



Malicious Software

Name	Description
Virus	Attaches itself to a program and propagates copies of itself to other programs
Worm	Program that propagates copies of itself to other computers
Logic bomb	Triggers action when condition occurs
Trojan horse	Program that contains unexpected additional functionality
Backdoor (trapdoor)	Program modification that allows unauthorized access to functionality
Exploits	Code specific to a single vulnerability or set of vulnerabilities
Downloaders	Program that installs other items on a machine that is under attack. Usually, a downloader is sent in an e-mail.
Auto-rooter	Malicious hacker tools used to break into new machines remotely
Kit (virus generator)	Set of tools for generating new viruses automatically
Spammer programs	Used to send large volumes of unwanted e-mail
Flooders	Used to attack networked computer systems with a large volume of traffic to carry out a denial of service (DoS) attack
Keyloggers	Captures keystrokes on a compromised system
Rootkit	Set of hacker tools used after attacker has broken into a computer system and gained root-level access
Zombie	Program activated on an infected machine that is activated to launch attacks on other machines

Symptoms of malware

- Your computer slows down.
- A tidal wave of annoying ads that shouldn't be there washes over your screen. Unexpected pop-up ads are a typical sign of a malware infection. (adware)
- Your system repeatedly crashes, freezes, or displays a BSOD (Blue Screen of Death), which can occur on Windows systems after encountering a fatal error.
- You notice a mysterious loss of disk space.
- There's a weird increase in your system's Internet activity.
- Usage of your system resources is abnormally high and your computer's fan starts whirling away at full speed—signs of malware activity taking up system resources in the background.
- Your browser's homepage changes without your permission. Similarly, links you click send you to an unwanted web destination.
- New toolbars, extensions, or plugins unexpectedly populate your browser.
- Your antivirus product stops working and you cannot update it, leaving you unprotected against the sneaky malware that disabled it.
- Then there's the painfully obvious, intentionally non-stealthy malware attack. This famously happens with ransomware, which announces itself, tells you it has your data, and demands a ransom to return your files.

Virus

- A computer virus is a type of malware that propagates by inserting a copy of itself into and becoming part of another program.
- It spreads from one computer to another, leaving infections as it travels.
- Viruses can range in severity from causing mildly annoying effects to damaging data or software and causing denial-of-service (DoS) conditions.
- Almost all viruses are attached to an **executable file** which means the virus may exist on a system but will not be active or able to spread until a user runs or opens the malicious host file or program.
- When the host code is executed, the viral code is executed as well.
- Normally, the host program keeps functioning after it is infected by the virus.
- Some viruses overwrite other programs with copies of themselves, which destroys the host program altogether.
- Viruses spread when the software or document they are attached to is transferred from one computer to another using the network, a disk, file sharing, or infected email attachments.

Virus

- A computer virus is a piece of software that can “infect” other programs by modifying them
- The modification includes
  - injecting the original program with a routine to make copies of the virus program, which can then go on to infect other programs.
- Similar to Biological viruses are tiny scraps of genetic code—DNA or RNA—that can take over the machinery of a living cell and trick it into makin thousands of flawless replicas of the original virus.
- A computer virus carries in its instructional code the recipe for making perfect copies of itself.
- The typical virus becomes embedded in a program on a computer. Then, whenever the infected computer comes into contact with an uninfected piece of software, a fresh copy of the virus passes into the new program.
- Thus, the infection can be spread from computer to computer by unsuspecting users who either swap disks or send programs to one another over a network. In a network environment, the ability to access applications and system services on other computers provides a perfect culture for the spread of a virus.

Viruses

- a piece of self-replicating code attached to some other code
- attaches itself to another program and executes secretly when the host program is executed.
- propagates itself & carries a payload
  - carries code to make copies of itself
  - as well as code to perform some covert task

Virus

A computer virus has three parts

- **Infection mechanism:** The means by which a virus spreads, enabling it to replicate. The mechanism is also referred to as the **infection vector**.
- **Trigger:** The event or condition that determines when the payload is activated or delivered.
- **Payload:** What the virus does, besides spreading. The payload may involve damage or may involve benign but noticeable activity.

Virus Operation

- virus phases:
  - dormant – waiting on trigger event
  - propagation – replicating to programs/disks
  - triggering – by event to execute payload
  - execution – of payload
- details usually machine/OS specific
  - exploiting features/weaknesses

A simple virus

```
     program V :=

{goto main;
     1234567;

     subroutine infect-executable :=
          {loop:
          file := get-random-executable-file;
          if (first-line-of-file = 1234567)
             then goto loop
             else prepend V to file; }

     subroutine do-damage :=
          {whatever damage is to be done}

     subroutine trigger-pulled :=
          {return true if some condition holds}

main:    main-program :=
          {infect-executable;
          if trigger-pulled then do-damage;
          goto next;}
next:

}
```

Types of Viruses

Classification on basis of how they attack

- parasitic virus

  -attaches itself to executable files and replicates

- memory-resident virus

  -lodges in the main memory and infects every program that executes.

- boot sector virus

  -infects a boot record and spreads when the system is booted from the disk

Types of Viruses…

Classification on the basis of concealment strategy

- **Encrypted virus**
  - A portion of the virus creates a random encryption key and encrypts the remainder of the virus. The key is stored with the virus. When an infected program is invoked, the virus uses the stored random key to decrypt the virus. When the virus replicates, a different random key is selected. Because the bulk of the virus is encrypted with a different key for each instance, there is no constant bit pattern to observe.
- **Stealth virus**
  - A form of virus explicitly designed to hide itself from detection by antivirus software. Thus, the entire virus, not just a payload is hidden.

Types of Viruses…

Classification on the basis of concealment strategy

- **Polymorphic virus**
  - A virus that mutates with every infection, making detection by the "signature" of the virus impossible.
- **Metamorphic virus**
  - As with a polymorphic virus, a metamorphic virus mutates with every infection. The difference is that a metamorphic virus rewrites itself completely at each iteration, increasing the difficulty of detection. Metamorphic viruses may change their behavior as well as their appearance.

Email Virus

- spread using email with attachment containing a macro virus
- triggered when user opens attachment
- worse even when mail viewed by using scripting features in mail agent
- propagates very quickly
- usually targeted at Microsoft Outlook mail agent & Word/Excel documents

Worm

- Computer worms are similar to viruses in that they replicate functional copies of themselves
- In contrast to viruses, which require the spreading of an infected host file, worms are standalone software and do not require a host program or human help to propagate.
- A worm enters a computer through a vulnerability in the system and takes advantage of file-transport or information-transport features on the system, allowing it to travel unaided.
- More advanced worms leverage encryption, wipers, and ransomware technologies to harm their targets.

Worms

- replicating but not infecting program (does not attach itself to a program)
- typically spreads over a network
  - Morris Internet Worm in 1988
- using users distributed privileges or by exploiting system vulnerabilities worms perform unwanted functions
- widely used by hackers to create **zombie PC's**, subsequently used for further attacks, esp DoS
- major issue is lack of security of permanently connected systems, esp PC's

Worm Operation

- worm has phases like those of viruses:
  - dormant
  - propagation
    - search for other systems to infect
    - establish connection to target remote system
    - replicate self onto remote system
  - triggering
  - execution

Morris Worm

- best known classic worm
- released by Robert Morris in 1988
- targeted Unix systems
- using several propagation techniques
  - simple password cracking of local pw file
  - exploit bug in finger daemon
  - exploit debug trapdoor in sendmail daemon
- if any attack succeeds then replicated self

Malicious Software Cont..

- Malicious software is software that is intentionally included or inserted in a system for a harmful purpose.
- **A virus** is a piece of software that can "infect" other programs by modifying them; **the modification includes a copy of the virus program, which can then go on to infect other programs.**
- **A worm is a program that can replicate itself and send copies from computer to computer across network connections.** Upon arrival, the worm may be activated to replicate and propagate again. In addition to propagation, the worm usually performs some unwanted function.
- A **denial of service (DoS) attack** is an attempt to prevent legitimate users of a service from using that service.
- A **distributed denial of service attack** is launched from multiple coordinated sources.

Backdoor or Trapdoor

- secret entry point into a program
- allows those who know access bypassing usual security procedures
- have been commonly used by developers
- a threat when left in production programs allowing exploited by attackers
- very hard to block in O/S

Logic Bomb

- one of oldest types of malicious software
- code embedded in legitimate program
- activated when specified conditions met
  - E.g., presence/absence of some file
  - particular date/time
  - particular user
- when triggered typically damage system
  - modify/delete files/disks, halt machine, etc.

Trojan Horse

- program with hidden side-effects
- which is usually superficially attractive
  - E.g., game, s/w upgrade, etc.
- when run performs some additional tasks
  - allows attacker to indirectly gain access they do not have directly
- often used to propagate a virus/worm or install a backdoor or simply to destroy data
- Mail the password file.

Zombie

- program which secretly takes over another networked computer
- then uses it to indirectly launch attacks

(difficult to trace zombie's creator)

- often used to launch distributed denial of service (DDoS) attacks
- exploits known flaws in network systems

Virus Countermeasures

- best countermeasure is prevention

(do not allow a virus to get into the system in the first place.)

- but in general not possible
- hence need to do one or more of:
  - **detection** - of viruses in infected system
  - **identification** - of specific infecting virus
  - **removal** - restoring system to clean state

Anti-Virus Software

- **first-generation**
  - scanner uses virus signature to identify virus or change in length of programs
- **second-generation**
  - uses heuristic rules to spot viral infection or uses crypto hash of program to spot changes
- **third-generation**
  - memory-resident programs identify virus by actions
- **fourth-generation**
  - packages with a variety of antivirus techniques eg scanning & activity traps, access-controls
- arms race continues