Unit 7: Malicious Logic

Malicious logic is a set of instructions that cause a site's security policy to be violated. Malicious software, commonly known as malware, is any software that brings harm to a computer system. Malware can be in the form of worms, viruses, Trojans, spyware, adware and rootkits, etc., which steal protected data, delete documents or add software not approved by a user. Malware is software designed to cause harm to a computer and user.

Types of Malicious Logic:

The types of malicious logic are as follows:

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 d
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 ca

Keyloggers	Captures keystrokes on a compromised system
Rootkit	Set of hacker tools used after attacker has broken into a computer system and g
Zombie	Program activated on an infected machine that is activated to launch attacks on

Viruses:

- A computer virus is a program that inserts itself into one or more files and then performs some (possibly null) action.
- When the Trojan horse can propagate freely and insert a copy of itself into another file, it becomes a computer 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.
- 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 making thousands of flawless replicas of the original virus.
- Like its biological counterpart, 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.
- A virus can do anything that other programs do.
- The difference is that a virus attaches itself to another program and executes secretly when the host program is run.
- Once a virus is executing, it can perform any function, such as erasing files and programs that is allowed by the privileges of the current user.

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 safe but noticeable activity.

During its lifetime, a typical virus goes through the following four phases:

- **Dormant phase:** The virus is idle. The virus will eventually be activated by some event, such as a date, the presence of another program or file, or the capacity of the disk exceeding some limit. Not all viruses have this stage.
- **Propagation phase:** The virus places a copy of itself into other programs or into certain system areas on the disk. The copy may not be identical to the propagating version; viruses often morph to evade detection. Each infected program will now contain a clone of the virus, which will itself enter a propagation phase.
- **Triggering phase:** The virus is activated to perform the function for which it was intended. As with the dormant phase, the triggering phase can be caused by a variety of system events, including a count of the number of times that this copy of the virus has made copies of itself.
- **Execution phase:** The function is performed. The function may be harmless, such as a message on the screen, or damaging, such as the destruction of programs and data files.

- Most viruses carry out their work in a manner that is specific to a particular operating system and, in some cases, specific to a particular hardware platform.
- Thus, they are designed to take advantage of the details and weaknesses of particular systems.

```
beginvirus:
if spread-condition then begin
for some set of target files do begin
if target is not infected then begin
determine where to place virus instructions
copy instructions from beginvirus to endvirus into target
alter target to execute added instructions
end;
end;
end;
perform some action(s)
goto beginning of infected program
endvirus;
```

Worms:

- A worm is a program that can replicate itself and send copies from computer to computer across network connections.
- A computer virus infects other programs. A variant of the virus is a program that spreads from computer to computer, spawning copies of itself on each one.

- Upon arrival, the worm may be activated to replicate and propagate again. In addition to propagation, the worm usually performs some unwanted function.
- An e-mail virus has some of the characteristics of a worm because it propagates itself from system to system.
- However, we can still classify it as a virus because it uses a document modified to contain viral macro content and requires human action.
- A worm actively seeks out more machines to infect and each machine that is infected serves as an automated launching pad for attacks on other machines.
- Network worm programs use network connections to spread from system to system.
- Once active within a system, a network worm can behave as a computer virus or bacteria, or it could implant Trojan horse programs or perform any number of disruptive or destructive actions.
- To replicate itself, a network worm uses some sort of network vehicle. Examples include the following:
    - **Electronic mail facility:** A worm mails a copy of itself to other systems, so that its code is run when the e-mail or an attachment is received or viewed.
    - **Remote execution capability:** A worm executes a copy of itself on another system, either using an explicit remote execution facility or by exploiting a program flaw in a network service to subvert its operations.
    - **Remote login capability:** A worm logs onto a remote system as a user and then uses commands to copy itself from one system to the other, where it then executes.
- The new copy of the worm program is then run on the remote system where, in addition to any functions that it performs at that system, it continues to spread in the same fashion.
- A network worm exhibits the same characteristics as a computer virus: a dormant phase, a propagation phase, a triggering phase, and an execution phase.

Rabbits and Bacteria:

- Some malicious logic multiplies so rapidly that resources become exhausted. This creates a denial of service attack.
- A bacterium or a rabbit is a program that absorbs all of some class of resource.
- Resources of a specific class, such as file descriptors or process table entry slots, may not affect currently running processes. They will affect new processes.
- Viruses not carrying a logic bomb, often referred to by experts as “bacteria” or “rabbits,” are not significantly destructive.
- Bacteria, or rabbit programs, make copies of themselves to overwhelm a computer system's resources.

- Bacteria do not explicitly damage any files. Their sole purpose is to replicate themselves.
- A typical bacteria program may do nothing more than execute two copies of itself simultaneously on multiprogramming systems, or perhaps create two new files, each of which is a copy of the original source file of the bacteria program.
- Both of those programs then may copy themselves twice, and so on.
- Bacteria reproduce exponentially, eventually taking up all the processor capacity, memory, or disk space, denying the user access to those resources.

Trojan Horse:

- A Trojan horse, or Trojan, is any malware which misleads users of its true intent. The term is derived from the Ancient Greek story of the deceptive Trojan Horse that led to the fall of the city of Troy.
- In other words, a Trojan horse is a program or command procedure containing hidden code that, when invoked, performs some unwanted or harmful function.
- In computing, a Trojan horse is a program downloaded and installed on a computer that appears harmless, but is, in fact, malicious. Unexpected changes to computer settings and unusual activity, even when the computer should be idle, are strong indications that a Trojan is residing on a computer.
- A Trojan horse is a program with an overt (documented or known) effect and a covert (undocumented or unexpected) effect.
- Trojan horses fit into one of three models:
    - Continuing to perform the function of the original program and additionally performing a separate malicious activity
    - Continuing to perform the function of the original program but modifying the function to perform malicious activity (e.g., a Trojan horse version of a login program that collects passwords) or to disguise other malicious activity.(e.g., a Trojan horse version of a process listing program that does not display certain processes that are malicious)
    - Performing a malicious function that completely replaces the function of the original program.

<u>Common types of Trojan malware:</u>

Backdoor Trojan:

This Trojan can create a “backdoor” on your computer. It lets an attacker access your computer and control it. Your data can be downloaded by a third party and stolen. Or more malware can be uploaded to your device.

Distributed Denial of Service (DDoS) attack Trojan:

This Trojan performs DDoS attacks. The idea is to take down a network by flooding it with traffic. That traffic comes from your infected computer and others.

Downloader Trojan:

This Trojan target your already-infected computer. It downloads and installs new versions of malicious programs. These can include Trojans and adware.

Fake AV Trojan:

This Trojan behaves like antivirus software, but demands money from you to detect and remove threats, whether they're real or fake.

Game-thief Trojan:

The losers here may be online gamers. This Trojan seeks to steal their account information.

Infostealer Trojan:

As it sounds, this Trojan is after data on your infected computer.

Mailfinder Trojan:

This Trojan seeks to steal the email addresses you've accumulated on your device.

Ransom Trojan:

This Trojan seeks a ransom to undo damage it has done to your computer. This can include blocking your data or impairing your computer's performance.

Remote Access Trojan:

This Trojan can give an attacker full control over your computer via a remote network connection. Its uses include stealing your information or spying on you.

Rootkit Trojan:

A rootkit aims to hide or obscure an object on your infected computer. The idea? To extend the time a malicious program runs on your device.

SMS Trojan:

This type of Trojan infects your mobile device and can send and intercept text messages. Texts to premium-rate numbers can drive up your phone costs.

Trojan banker:

This Trojan takes aim at your financial accounts. It's designed to steal your account information for all the things you do online. That includes banking, credit card, and bill pay data.

Trojan IM:

This Trojan target instant messaging. It steals your logins and passwords on IM platforms.

Zombies:

- A zombie is a computer connected to the Internet that has been compromised by a hacker, computer virus or trojan horse program and can be used to perform malicious tasks of one sort or another under remote direction.
- Botnets of zombie computers are often used to spread e-mail spam and launch denial-of-service attacks (DoS attacks).
- Most owners of zombie computers do not realize that their system is being used in this way, hence the comparison with the living dead. They are also used in DDoS attacks in coordination with botnets in a way that resembles the typical zombie attacks of horror films.
- A bot, short for "robot", is a type of software application or script that performs automated tasks on command. Bad bots perform malicious tasks that allow an attacker to remotely take control over an affected computer. Once infected, these machines may also be referred to as zombies.
- In addition to the worm-like ability to self-propagate, bots can include the ability to log keystrokes, gather passwords, capture and analyze packets, gather financial information, launch Denial of Service (DOS) Attacks, relay spam, and open backdoors on the infected host.
- Bots have all the advantages of worms, but are generally much more versatile in their infection vector and are often modified within hours of publication of a new exploit.
- They have been known to exploit backdoors opened by worms and viruses, which allows them to access networks that have good perimeter control.
- Bots rarely announce their presence with high scan rates that damage network infrastructure; instead, they infect networks in a way that escapes immediate notice.

Denial of Service Attacks:

- A denial-of-service (DoS) is any type of attack where the attackers (hackers) attempt to prevent legitimate users from accessing the service.
- In a DoS attack, the attacker usually sends excessive messages asking the network or server to authenticate requests that have invalid return addresses.
- The network or server will not be able to find the return address of the attacker when sending the authentication approval, causing the server to wait before closing the connection.
- When the server closes the connection, the attacker sends more authentication messages with invalid return addresses. Hence, the process of authentication and server wait will begin again, keeping the network or server busy.
- A DoS attack can be done in a several ways. The basic types of DoS attack include:
    - Flooding the network to prevent legitimate network traffic
    - Disrupting the connections between two machines, thus preventing access to a service
    - Preventing a particular individual from accessing a service.
    - Disrupting a service to a specific system or individual
    - Disrupting the state of information, such resetting of TCP sessions
- DoS attacks can cause the following problems:
    - Ineffective services
    - Inaccessible services
    - Interruption of network traffic
    - Connection interference

Distributed Denial of Service (DDoS) Attack:

- A distributed denial-of-service (DDoS) is a type of computer attack that uses a number of hosts to overwhelm a server, causing a website to experience a complete system crash.
- This type of denial-of-service attack is perpetrated by hackers to target large-scale, far-reaching and popular websites in an effort to disable them, either temporarily or permanently.
- This is often done by bombarding the targeted server with information requests, which disables the main system and prevents it from operating. This leaves the site's users unable to access the targeted website.
- DDoS differs from a denial-of-service (DoS) attack in that it uses several hosts to bombard a server, whereas in a DoS attack, a single host is used.
- In a standard DDoS attack, an attacker starts the process by taking advantage of a vulnerability in a computer system. The hacker makes this compromised computer the DDoS master.
- Using this master system, the hacker detects, communicates and infects other systems and makes them a part of the compromised systems.
- A compromised computer system within the control of a hacker is called a zombie or bot, while a set of compromised computers is called a zombie army or a botnet.
- The hacker loads several cracking tools on the compromised systems (sometimes thousands of systems).
- Using a single command, the attacker instructs these zombie machines to trigger several flood attacks toward a particular target. This packet flooding process causes a denial of service.

Intrusion & Intruders:

- Intrusion is a phenomenon that performs an activity that compromises a computer system by breaking the security or causing it to enter into an insecure state.
- A set of attempts to compromise a computer or a computer network resource security is regarded as an intrusion.
- The entity involved to perform such activity is called intruder.
- Intruders are also referred as attackers, interceptors or hackers.

Types of Intruders:

Masquerader

An unauthorized user who penetrates a system's access control to exploit other's account. Most likely an outsider to the system.

Misfeasor

A legitimate user but accesses data, program or resources for which he/she is not authorized. Generally, an insider.

Clandestine

An individual who seizes supervisory control and evades auditing and access control. May be an insider or outsider.

Again, there are two levels of Intruders:

- People with high level of system expertise: Personally constructed methods for breaking into systems.
- Others are “foot soldiers”, uses cracking programs developed and distributed by others: willing to spend countless hours looking for weakest links.

Another classification scheme, based on intrusion types, classifies intrusions into the following six types:

- Attempted break-in: often detected by atypical behavior profiles or violations of security constraints.
- Masquerade attack: often detected by a typical behavior profiles or violations of security constraints.
- Penetration of the security control system: usually detected by monitoring for specific patterns of activity.
- Leakage: often detected by a typical usage of I/O resources.
- Denial of Service: often detected by atypical usage of system resources.
- Malicious use: often detected by a typical behavior profiles, violations of security constraints, or use of special privileges.

Intrusion Detection:

- In addition to security services (e.g. data confidentiality, integrity, authentication, etc.), intrusion detection (ID) techniques are used to strengthen the system security and increase its resistance to internal and external attacks.
- These techniques are implemented by an intrusion detection system (IDS).
- Generally, IDS main task is to detect an intrusion and, if necessary or possible, to undertake some measures eliminating it.

The goals of intrusion detection system are:

  - Detect a wide variety of intrusions.
  - Detect intrusions in a timely fashion.
  - Present the analysis in a simple, easy-to-understand format.
  - Be accurate.

- Formalizing this type of analysis provides a statistical and analytical basis for monitoring a system for intrusions.
- Three types of analyses—anomaly detection, misuse (or signature) detection, and specification detection.

Architecture of IDS:

- An intrusion detection system consists of three parts.
- The agent corresponds to the logger. It acquires information from a target (such as a computer system).

- The director corresponds to the analyzer. It analyzes the data from the agents as required (usually to determine if an attack is in progress or has occurred).
- The director then passes this information to the notifier, which determines whether, and how, to notify the requisite entity.
- The notifier may communicate with the agents to adjust the logging if appropriate.

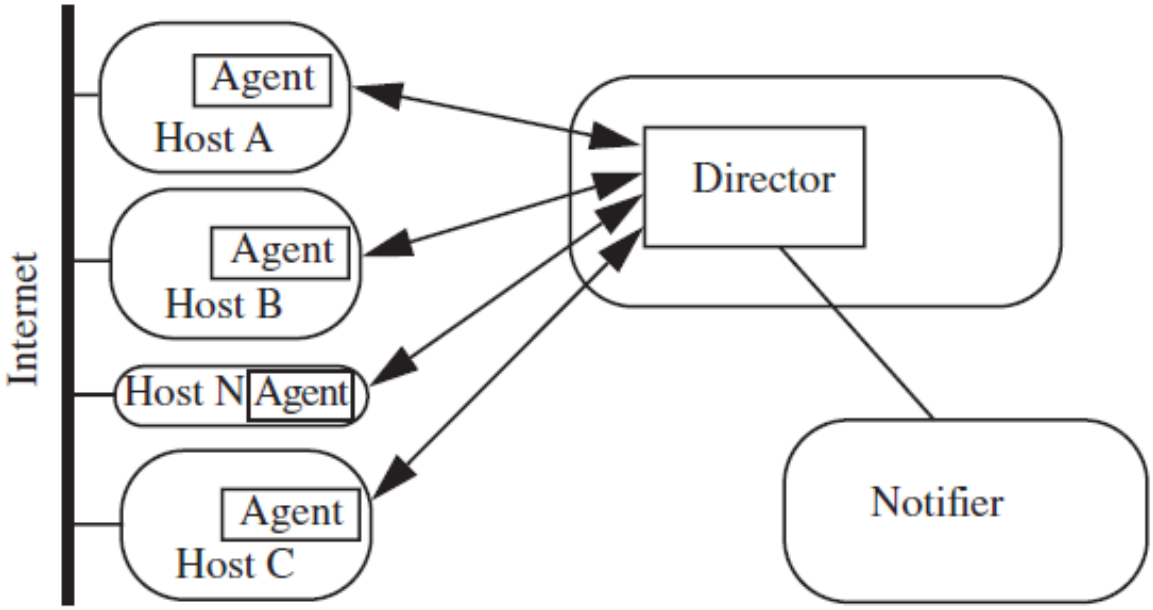

Fig: Architecture of an intrusion detection system

- An agent obtains information from a data source (or set of data sources).
- The source may be a log file, another process, or a network.
- The information, once acquired, may be sent directly to the director.
- Usually, however, it is preprocessed into a specific format to save the director from having to do this.
- Also, the agent may discard information that it considers irrelevant.
- The director may determine that it needs more information from a particular information source.
- In that case, the director can instruct the agent to collect additional data, or to process the data it collects differently.
- The director can use this to cut down on the amount of processing it must do, but can increase the level of information it receives when an attack is suspected.
- An agent can obtain information from a single host, from a set of hosts or from a network.
- The agent, or the director, must either obtain information at the level of abstraction at which it looks for security problems or be able to map the information into an appropriate level.
- The director itself reduces the incoming log entries to eliminate unnecessary and redundant records. It then uses an analysis engine to determine if an attack (or the precursor to an attack) is underway.
- The analysis engine may use any of, or a mixture of, several techniques to perform its analysis.

- Because the functioning of the director is critical to the effectiveness of the intrusion detection system, it is usually run on a separate system.
- The notifier accepts information from the director and takes the appropriate action.
- In some cases, this is simply a notification to the system security officer that an attack is believed to be underway.
- In other cases, the notifier may take some action to respond to the attack.

Classification of Intrusion Detection System:

Host Intrusion Detection System (HIDS):

- Host intrusion detection systems (HIDS) run on independent hosts or devices on the network. A
- HIDS monitors the incoming and outgoing packets from the device only and will alert the administrator if suspicious or malicious activity is detected.
- It takes a snapshot of existing system files and compares it with the previous snapshot. If the analytical system files were edited or deleted, an alert is sent to the administrator to investigate.
- An example of HIDS usage can be seen on mission critical machines, which are not expected to change their layout.

Network Intrusion Detection System (NIDS):

- Network intrusion detection systems (NIDS) are set up at a planned point within the network to examine traffic from all devices on the network.
- It performs an observation of passing traffic on the entire subnet and matches the traffic that is passed on the subnets to the collection of known attacks.
- Once an attack is identified or abnormal behavior is observed, the alert can be sent to the administrator.
- An example of a NIDS is installing it on the subnet where firewalls are located in order to see if someone is trying crack the firewall.

Approaches to Intrusion detection:

There are two general approaches to intrusion detection: Statistical Anomaly Detection and Rule Based Anomaly detection.

Statistical Anomaly Detection:

- An anomaly-based intrusion detection system, is an intrusion detection system for detecting both network and computer intrusions and misuse by monitoring system activity and classifying it as either normal or anomalous.
- Statistical Anomaly based IDS monitors network traffic and compares it against an established baseline.
- The baseline will identify what is normal for that network and what protocols are used. However, it may raise a false alarm if the baselines are not intelligently configured.
- The two phases of a majority of anomaly detection systems consist of the training phase (where a profile of normal behaviors is built) and testing phase (where current traffic is compared with the profile created in the training phase).

- Network-based anomalous intrusion detection systems often provide a second line of defense to detect anomalous traffic at the physical and network layers after it has passed through a firewall or other security appliance on the border of a network.
- Host-based anomalous intrusion detection systems are one of the last layers of defense and reside on computer end points.

Rule Based Detection:

- Rule based intrusion detection determines whether a sequence of instructions being executed is known to violate the security policy being executed.
- If so, it reports a potential intrusion.
- In some contexts, the term “misuse” refers to an attack by an insider or authorized user.
- In the context of intrusion detection systems, it means “rule-based detection.”
- Modeling of misuse requires a knowledge of system vulnerabilities or potential vulnerabilities that attackers attempt to exploit.
- The intrusion detection system incorporates this knowledge into a rule set.
- When data is passed to the intrusion detection system, it applies the rule set to the data to determine if any sequences of data match any of the rules.
- If so, it reports that a possible intrusion is underway.
- Misuse-based intrusion detection systems often use expert systems to analyze the data and apply the rule set.
- These systems cannot detect attacks that are unknown to the developers of the rule set.