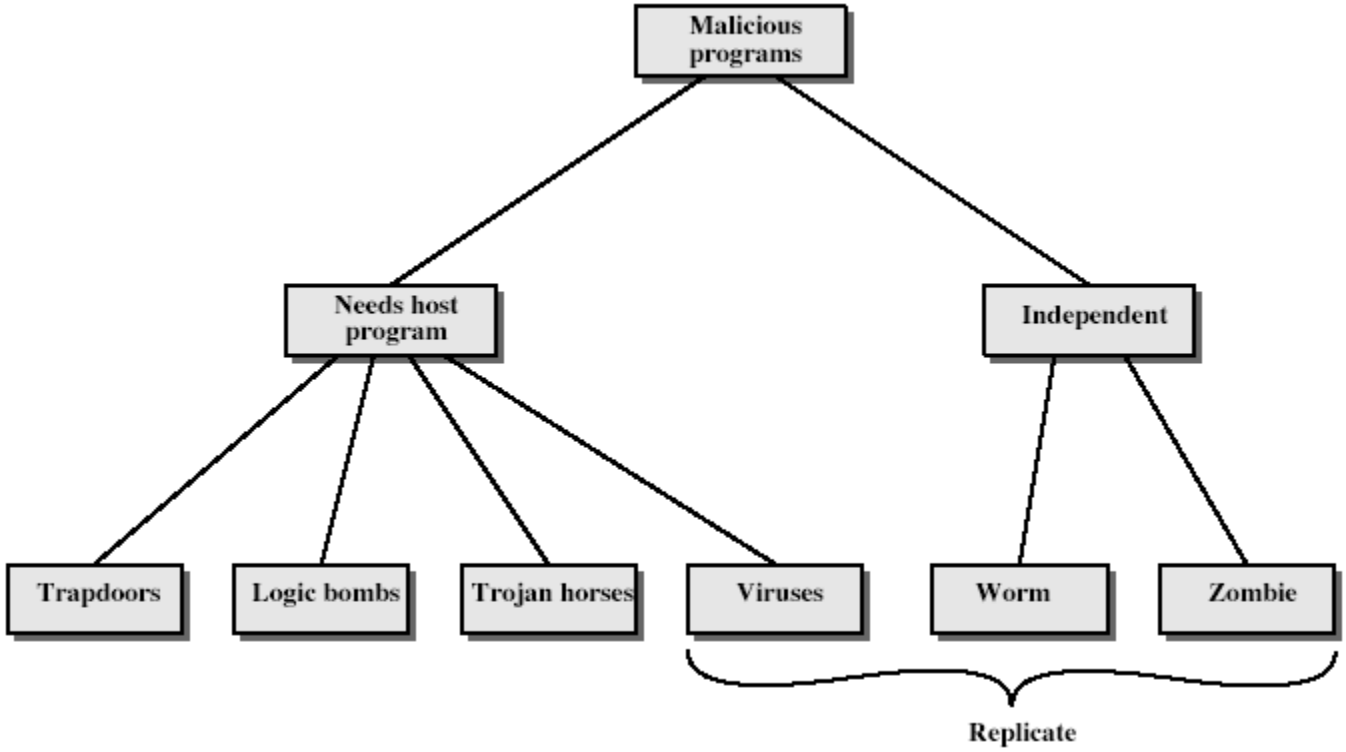
Unit VII. Malicious Logic

Presented by: Er. Kobid Karkee
Himalaya College of Engineering

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, 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.

Malicious Logic



Malicious Logic

Type	Characteristics
Trojan Horse	Contains unexpected, additional functionality
Virus	Attaches itself to a program and propagates copies of itself to other programs
Logic Bomb	Triggers action when condition occurs
Time Bomb	Triggers action when specified time occurs
Trapdoor	Allows unauthorized access to functionality
Worm	Propagates copies of itself through a network
Rabbit	Replicates itself without limit to exhaust resource

Trapdoors

- 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
- requires good s/w development & update

Logic Bomb

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

Virus

- 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.

Virus

- Whenever the infected computer encounters 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.
- 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.

Parts of Computer Virus

- 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.

Virus 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.

Virus Phases

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.

Types of Viruses

- can classify on basis of how they attack
- parasitic virus
- memory-resident virus
- boot sector virus
- stealth
- polymorphic virus
- macro virus

Macro Virus

- **macro code** attached to some **data file**
- interpreted by program using file
  - eg Word/Excel macros
  - esp. using auto command & command macros
- code is now platform independent
- is a major source of new viral infections
- blurs distinction between data and program files making task of detection much harder
- classic trade-off: "ease of use" vs "security"

Email Virus

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

Virus Countermeasures

- viral attacks exploit lack of integrity control on systems
- to defend need to add such controls
- typically by one or more of:
  - **prevention** - block virus infection mechanism
  - **detection** - of viruses in infected system
  - **reaction** - 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 program checksums 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

Advanced Anti-Virus Techniques

- generic decryption
  - use CPU simulator to check program signature & behavior before actually running it
- digital immune system (IBM)
  - general purpose emulation & virus detection
  - any virus entering org is captured, analyzed, detection/shielding created for it, removed

Behavior-Blocking Software

- integrated with host O/S
- monitors program behavior in real-time
  - eg file access, disk format, executable mods, system settings changes, network access
- for possibly malicious actions
  - if detected can block, terminate, or seek ok
- has advantage over scanners
- but malicious code runs before detection

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.

Worms

- 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
- A network worm exhibits the same characteristics as a computer virus: a dormant phase, a propagation phase, a triggering phase, and an execution phase.

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.

Trojan Horse

- 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.

Common Types of Trojan Malware

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.

Common Types of Trojan Malware

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.

Infostealer Trojan:

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

Common Types of Trojan Malware

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.

Common Types of Trojan Malware

SMS Trojan:

- This type of Trojan infects your mobile device and can send and intercept text messages.

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.

Zombies

- 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.
- 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.

Denial-of-Service Attack

- 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.
- 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.

Denial-of-Service Attack

- DoS cause the following problems:
  - Ineffective services
  - Inaccessible services
  - Interruption of network traffic
  - Connection interference

Distributed-Denial-of-Service Attack

- A distributed denial-of-service (DDoS) is a type of computer attack that uses several 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 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.

Distributed-Denial-of-Service Attack

- 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.

Intrusion and 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.

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.

Intrusion Detection

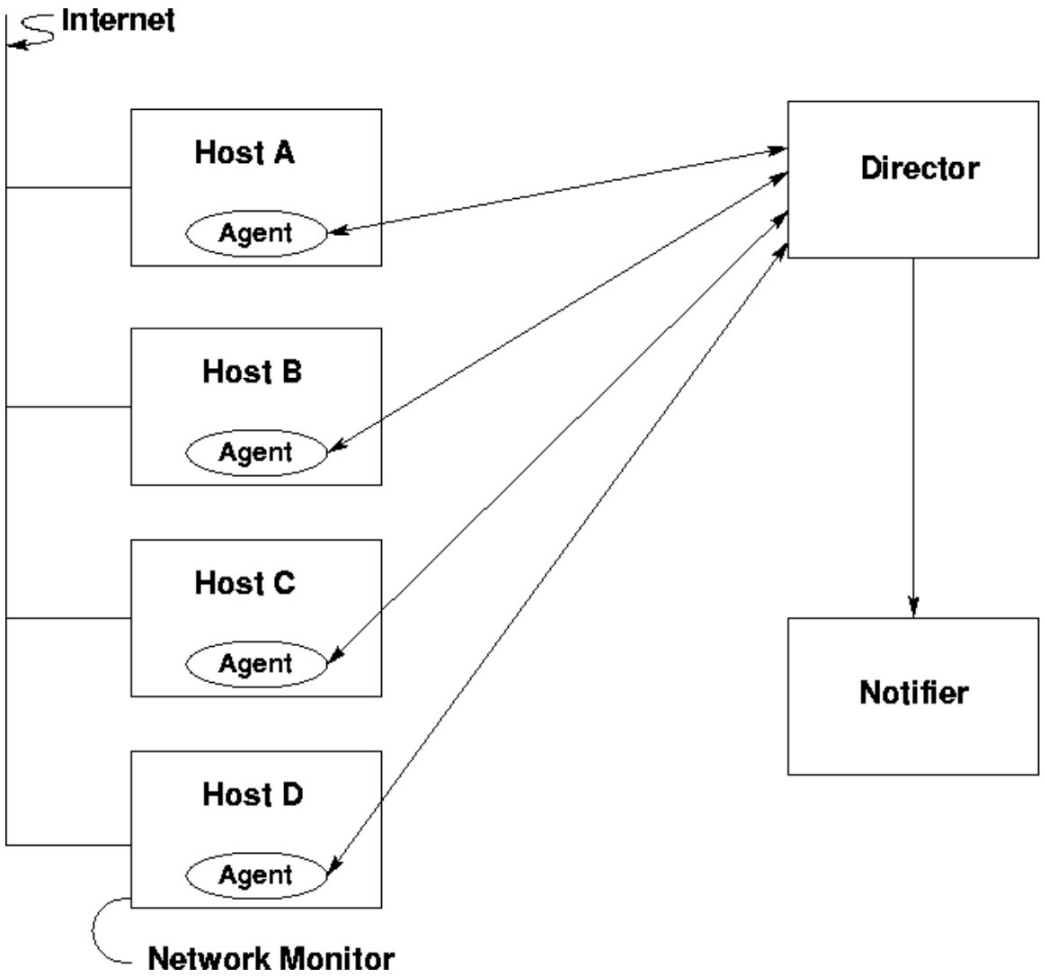
The goals of intrusion detection system are:

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

Architecture of IDS

- An intrusion detection system consists of three parts: an agent, a director, and a notifier.
- 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.

Architecture of IDS



Architecture of IDS

Agent

- An agent obtains information from a data sources.
- The source may be a log file, another process or a network.
- The information may be sent directly to the director.
- Usually, it is preprocessed into a specific format to save the director from having to do this.
- Also the agent may discard information that it deems irrelevant.

Architecture of IDS

Director

- The director determines if an attack is underway or a precursor to an attack is eminent.
- 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 a 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.
- This allows the system to be dedicated to the director's activity.

Architecture of IDS

Notifier

- 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.
- Take action to respond to attack
  - notify system security officer
  - email
  - log entries
  - pager

Approaches to Intrusion Detection:

- There are two general approaches to intrusion detection:

1. Statistical Anomaly Detection, and
2. 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.

Statistical Anomaly Detection

The two phases of most anomaly detection systems consist of:

- the training phase (where a profile of normal behaviors is built), and
- the testing phase (where current traffic is compared with the profile created in the training phase).

Rule Based Anomaly 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.

Rule Based Anomaly detection

- 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.