Chapter 4

System Level Security

Intruders

- One of the two most publicized threats to security is the intruder (the other is viruses), generally referred to as a hacker or cracker.
- Three classes 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
  - Misfeasor: A legitimate user who accesses data, programs, or resources for which such access is not authorized, or who is authorized for such access but misuses his or her privileges
  - 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

Password File Protection

- The objective of the intruder is to gain access to a system and acquire information that should have been protected, by getting password
- A system must maintain a file that associates a password with each authorized user
- The password file can be protected in one of two ways:
  - One-way function: The system stores only the value of a function based on the user's password. When the user presents a password, the system transforms that password and compares it with the stored value
  - Access control: Access to the password file is limited to one or a very few accounts.

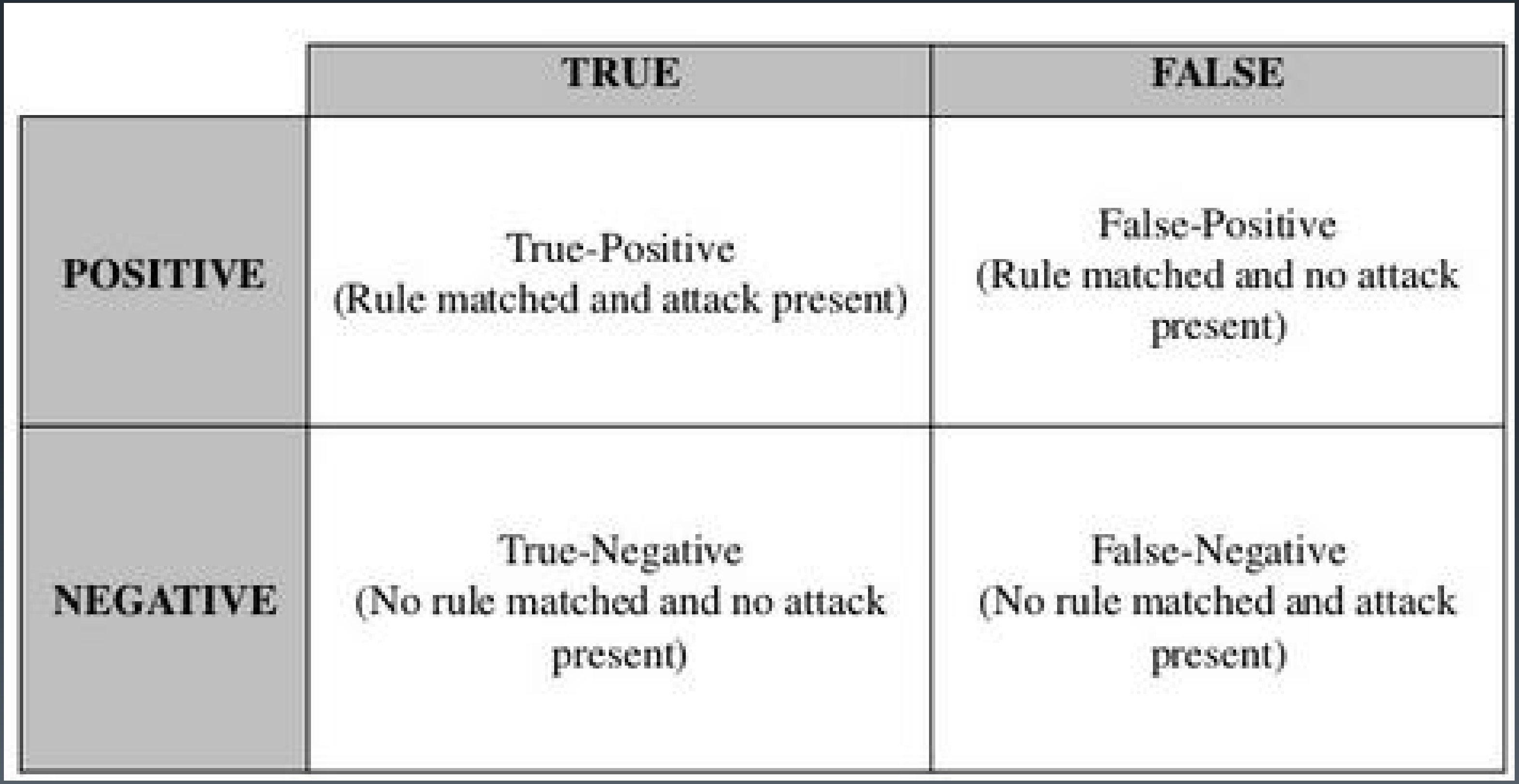
Intrusion Techniques

- Try default passwords
- Exhaustively try all short passwords
- Try a list of likely passwords
- Collect information about users
- Try users' phone numbers, Social Security numbers
- Try all legitimate license plate numbers for this state
- Use a Trojan horse
- Wiretap the line between a remote user and the host system

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
- Intrusion detection is based on the assumption that the behavior of the intruder differs from that of a legitimate user in ways that can be quantified
- Although the typical behavior of an intruder differs from the typical behavior of an authorized user, there is an overlap in these behaviors
- This overlap should not cause “false positive ” or “false negative”

IDS Matrix



	TRUE	FALSE
POSITIVE	True-Positive (Rule matched and attack present)	False-Positive (Rule matched and no attack present)
NEGATIVE	True-Negative (No rule matched and no attack present)	False-Negative (No rule matched and attack present)

Intrusion Detection Approaches

- Statistical anomaly detection: Involves the collection of data relating to the behavior of legitimate users over a period of time.
  - Threshold detection: This approach involves defining thresholds, for the frequency of occurrence of various events.
  - Profile based: A profile of the activity of each user is developed and used to detect changes in the behavior of individual accounts.
- Rule-based detection: Involves an attempt to define a set of rules that can be used to decide that a given behavior is that of an intruder.
  - Anomaly detection: Rules are developed to detect deviation from previous usage patterns.
  - Penetration identification: An expert system approach that searches for suspicious behavior.

Statistical Anomaly Detection

- Statistical anomaly detection techniques fall into two broad categories: threshold detection and profile-based systems
- Both the threshold and the time interval must be determined. Because of the variability across users, such thresholds are likely to generate either a lot of false positives or a lot of false negatives.
- However, simple threshold detectors may be useful in conjunction with more sophisticated techniques
- Profile-based anomaly detection focuses on characterizing the past behavior of individual users or and then detecting significant deviations.
- A profile may consist of a set of parameters, so that deviation on just a single parameter may not be sufficient in itself to signal an alert

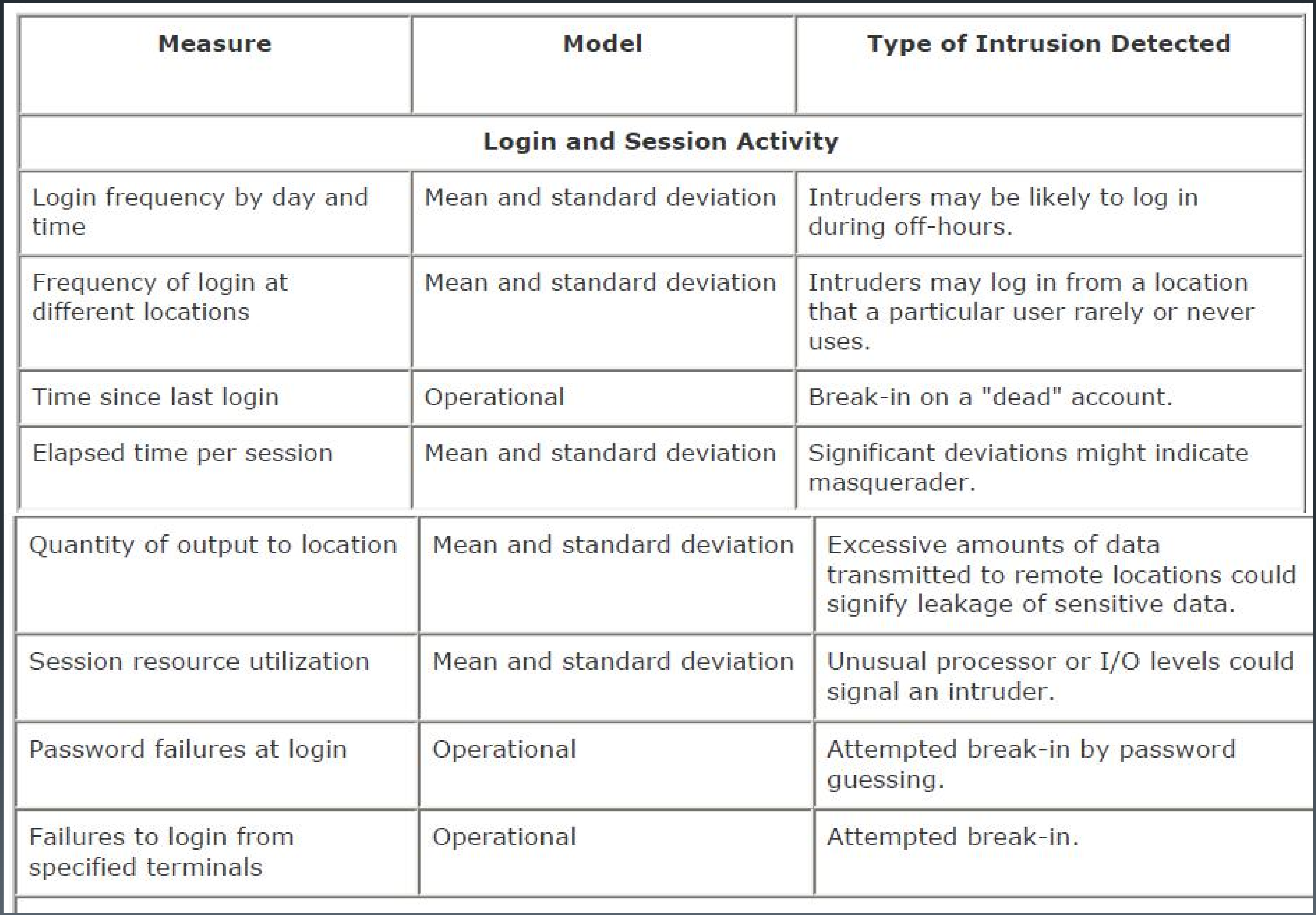
Profile Based Detection

- Metrics that are useful for profile-based intrusion detection:
  - Counter : number of logins by a single user during an hour, the number of times a given command is executed during a single user session, and the number of password failures during a minute.
  - Gauge : number of logical connections assigned to a user application and the number of outgoing messages queued for a user process.
  - Interval timer: the length of time between successive logins to an account.
  - Resource utilization: the number of pages printed during a user session and total time consumed by a program execution.

Profile Based Detection

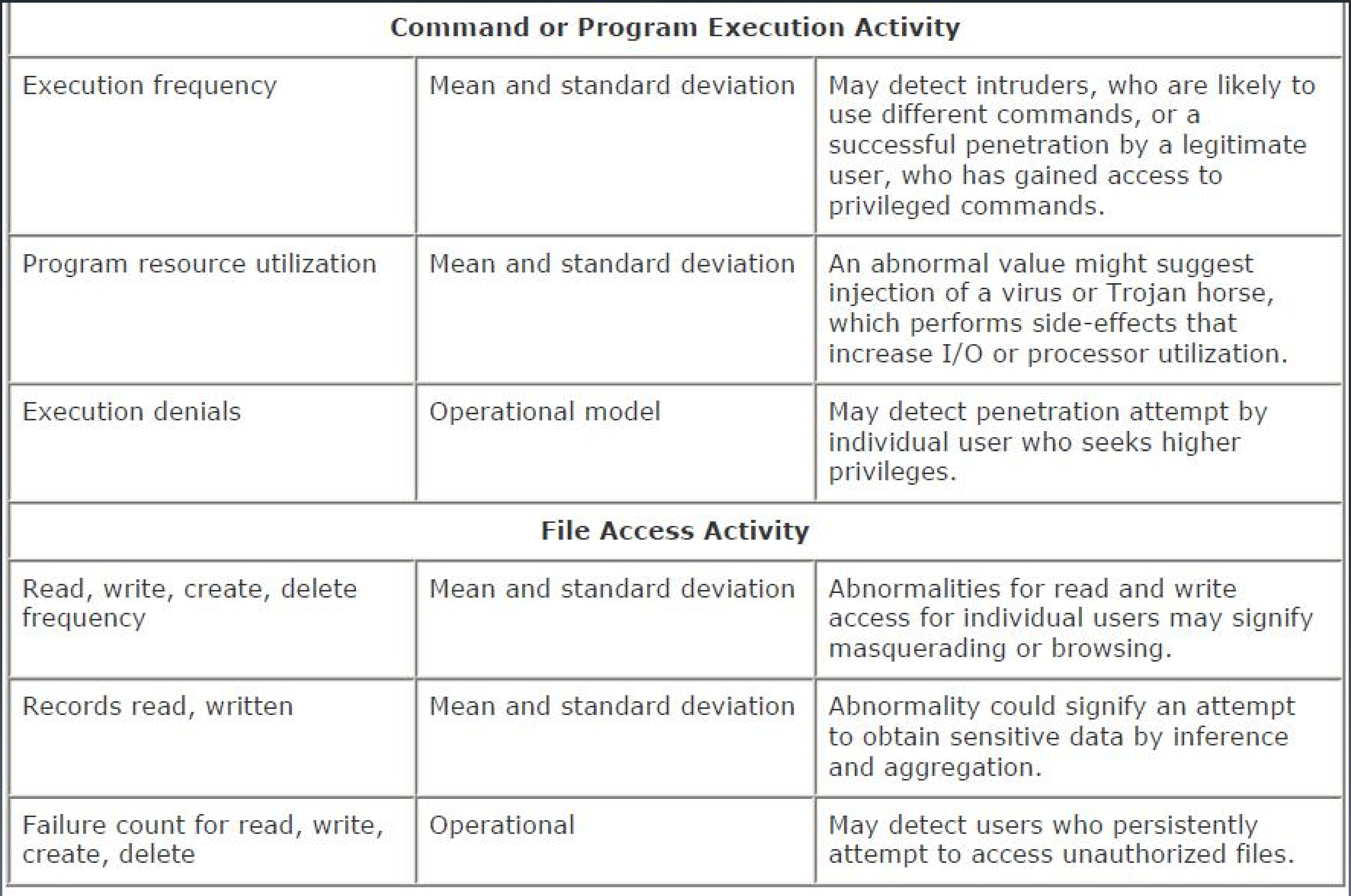
- Different approaches to decide intrusion:
  - ***Mean and standard deviation***: The use of mean and standard deviation is applicable to a wide variety of counters, timers, and resource measures
  - ***Multivariate***: based on correlations between two or more variables, for example, processor time and resource usage, or login frequency and session elapsed time
  - ***Markov process***: transition probabilities among various states, for example, transitions between certain commands.
  - ***Time series***: focuses on time intervals, looking for sequences of events that happen too rapidly or too slowly
  - ***Operational*** : judgment of what is considered abnormal, rather than an automated analysis of past audit records.

Measures That May Be Used for Intrusion Detection



Measure	Model	Type of Intrusion Detected
Login and Session Activity		
Login frequency by day and time	Mean and standard deviation	Intruders may be likely to log in during off-hours.
Frequency of login at different locations	Mean and standard deviation	Intruders may log in from a location that a particular user rarely or never uses.
Time since last login	Operational	Break-in on a "dead" account.
Elapsed time per session	Mean and standard deviation	Significant deviations might indicate masquerader.
Quantity of output to location	Mean and standard deviation	Excessive amounts of data transmitted to remote locations could signify leakage of sensitive data.
Session resource utilization	Mean and standard deviation	Unusual processor or I/O levels could signal an intruder.
Password failures at login	Operational	Attempted break-in by password guessing.
Failures to login from specified terminals	Operational	Attempted break-in.

Measures That May Be Used for Intrusion Detection



Command or Program Execution Activity		
Execution frequency	Mean and standard deviation	May detect intruders, who are likely to use different commands, or a successful penetration by a legitimate user, who has gained access to privileged commands.
Program resource utilization	Mean and standard deviation	An abnormal value might suggest injection of a virus or Trojan horse, which performs side-effects that increase I/O or processor utilization.
Execution denials	Operational model	May detect penetration attempt by individual user who seeks higher privileges.
File Access Activity		
Read, write, create, delete frequency	Mean and standard deviation	Abnormalities for read and write access for individual users may signify masquerading or browsing.
Records read, written	Mean and standard deviation	Abnormality could signify an attempt to obtain sensitive data by inference and aggregation.
Failure count for read, write, create, delete	Operational	May detect users who persistently attempt to access unauthorized files.

Honeypots

- Honeypots are decoy systems that are designed to lure a potential attacker away from critical systems.
- Honeypots are designed to
  - divert an attacker from accessing critical systems
  - collect information about the attacker's activity
  - encourage the attacker to stay on the system long enough for administrators to respond
- These systems are filled with fabricated information designed to appear valuable but that a legitimate user of the system wouldn't access. Thus, any access to the honeypot is suspect

Password Protection

- Never use default password
- It should not be too small (at least 6 to 8 characters or digits)
- Should be combination of character, digit, upper case, lower case and special characters
- Should not contain personal information
- Different account must have different password
- Should not be a guessable word, but must be memorable

Password Protection

- The goal is to eliminate guessable passwords while allowing the user to select a password that is memorable. Four basic techniques are in use:
  - User education
  - Computer-generated passwords
  - Reactive password checking
  - Proactive password checking

Proactive Password Checking

- A user is allowed to select his or her own password. However, at the time of selection, the system checks to see if the password is allowable and, if not, rejects it.
- With sufficient guidance from the system, users can select memorable passwords from a fairly large password space that are not likely to be guessed in a dictionary attack.
- Another possible procedure is simply to compile a large dictionary of possible "bad" passwords

Malicious Program

- 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: Program modification that allows unauthorized access to functionality
- Zombie : Program activated on an infected machine that is activated to launch attacks on other machines

Backdoor

- A backdoor, also known as a trapdoor, is a secret entry point into a program that allows someone that is aware of the backdoor to gain access without going through the usual security access procedures
- To debug the program, the developer may wish to gain special privileges or to avoid all the necessary setup and authentication
- Backdoors become threats when untrustworthy, programmers use them to gain unauthorized access

Logic Bomb

- The logic bomb is code embedded in some legitimate program that is set to "explode" when certain conditions are met.
- Examples of conditions that can be used as triggers for a logic bomb are the presence or absence of certain files, a particular day of the week or date, or a particular user running the application.
- Once triggered, a bomb may alter or delete data or entire files, cause a machine halt, or do some other damage

Trojan Horses

- Unlike viruses, Trojan horses do not replicate themselves but they can be just as destructive.
- One of the most insidious types of Trojan horse is a program that claims to rid your computer of viruses but instead introduces viruses onto your computer.
- A Trojan horse is a type of malware that is often disguised as legitimate software
- By installing effective anti-malware software, you can defend your devices

Zombies

- A zombie is a program that secretly takes over another Internet-attached computer and then uses that computer to launch attacks that are difficult to trace to the zombie's creator.
- Zombies are used in denial of- service attacks
- The zombie is planted on hundreds of computers to overwhelm the target Web site by launching an overwhelming onslaught of Internet traffic

Virus

- Virus: It is a program code that attaches itself to a legitimate program and runs when the legitimate program runs.
- Viruses can be classified in following categories:
  - ***Parasitic virus***: attaches itself to executable files and keeps replicating
  - ***Memory resident*** : attaches to main memory and infects every executable program that is executable
  - ***Boot sector virus***: infects master boot record of the disk
  - ***Stealth virus***: prevents antivirus from detecting it
  - ***Polymorphic virus***: keeps changing its signature on every execution
  - ***Metamorphic virus***: in addition to changing signature, it keeps rewriting every time

Phases of Virus

- During its lifetime, a typical virus goes through the following four phases:
  - Dormant phase: The virus is idle it 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 an identical copy of itself into other programs or into certain system areas on the disk.
  - Triggering phase: The virus is activated to perform the function for which it was intended.
  - 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.

Antivirus Approaches

- The goal of antivirus is to stop the virus from entering the system , which is almost impossible, that’s why the next approach is :
  - Detection
  - Identification
  - Removal
- If detection succeeds but either identification or removal is not possible, then the alternative is to discard the infected program and reload a clean backup version

Antivirus Approaches

- Four generations of antivirus software:
  - First generation: simple scanners
  - Second generation: heuristic scanners
  - Third generation: activity traps
  - Fourth generation: full-featured protection

Antivirus Approaches

- First generation
  - Requires a virus signature to identify a virus.
  - Such signature-specific scanners are limited to the detection of known viruses.
  - Another type of first-generation scanner maintains a record of the length of programs and looks for changes in length.

Antivirus Approaches

- Second generation:
  - The scanner uses heuristic rules to search for probable virus infection.
  - One class of such scanners looks for fragments of code that are often associated with viruses.
  - For example, a scanner may look for the beginning of an encryption loop used in a polymorphic virus and discover the encryption key. Once the key is discovered, the scanner can decrypt the virus to identify it, then remove the infection and return the program to service
  - A checksum/hash can be appended to each program. If a virus infects the program without changing the checksum, then an integrity check will catch the change

Antivirus Approaches

- Third-generation :
  - Memory-resident programs that identify a virus by its actions rather than its structure in an infected program.
  - Such programs have the advantage that it is not necessary to develop signatures and heuristics for a wide array of viruses.
  - Rather, it is necessary only to identify the small set of actions that indicate an infection is being attempted and then to intervene.

Antivirus Approaches

- Fourth-generation:
  - Packages consisting of a variety of antivirus techniques used in conjunction.
  - These include scanning and activity trap components. In addition, such a package includes access control capability, which limits the ability of viruses to penetrate a system and then limits the ability of a virus to update files in order to pass on the infection.

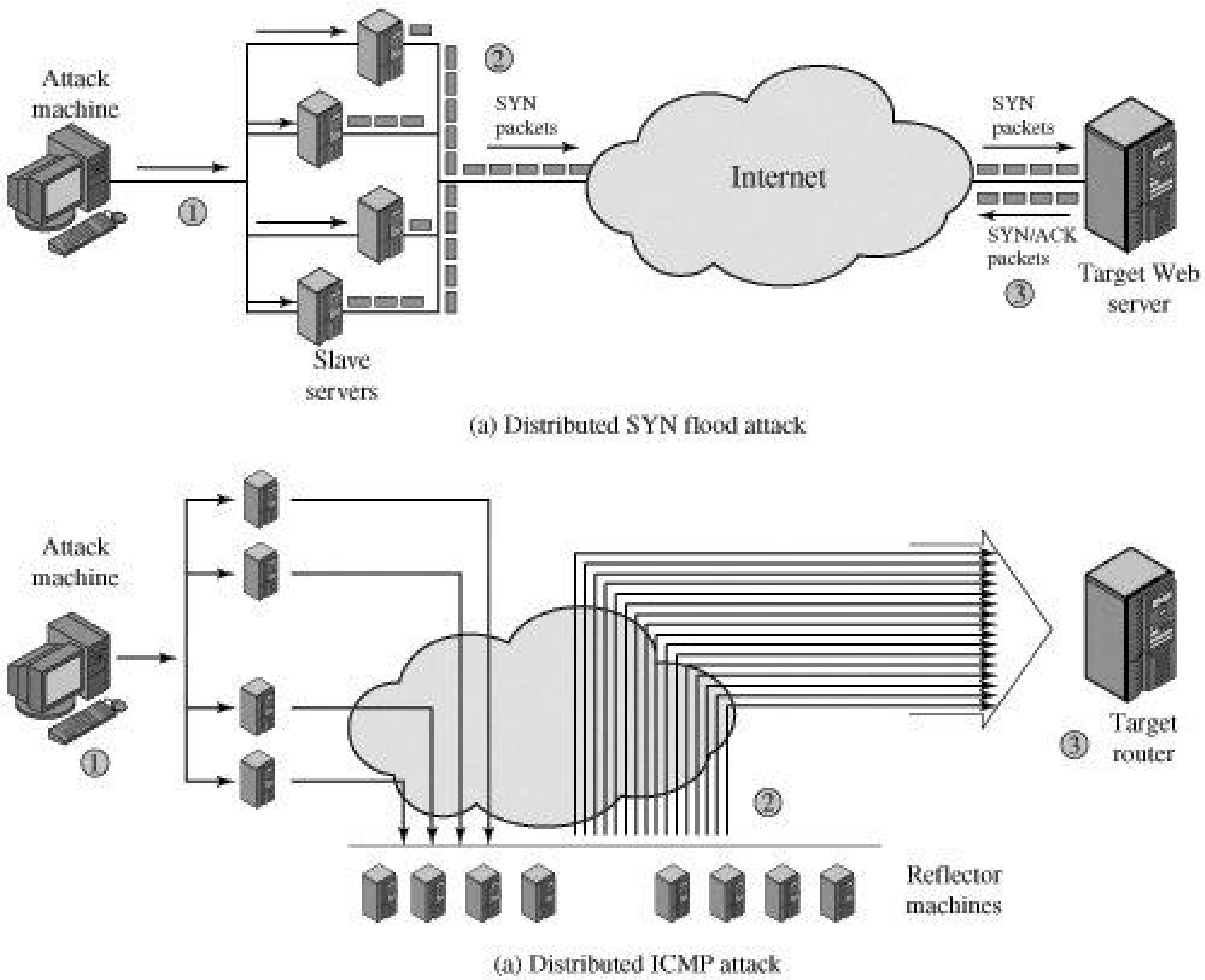
Behavior-Blocking Software

- Behavior-blocking software integrates with the operating system of a host computer and monitors program behavior in real-time for malicious actions
- Monitored behaviors can include the following:
  - Attempts to open, view, delete, and/or modify files
  - Attempts to format disk drives and other unrecoverable disk operations
  - Modifications to the logic of executable files
  - Modification of critical system settings, such as start-up settings
  - Scripting of e-mail and instant messaging clients to send executable content
  - Initiation of network communications

Distributed Denial of Service Attacks

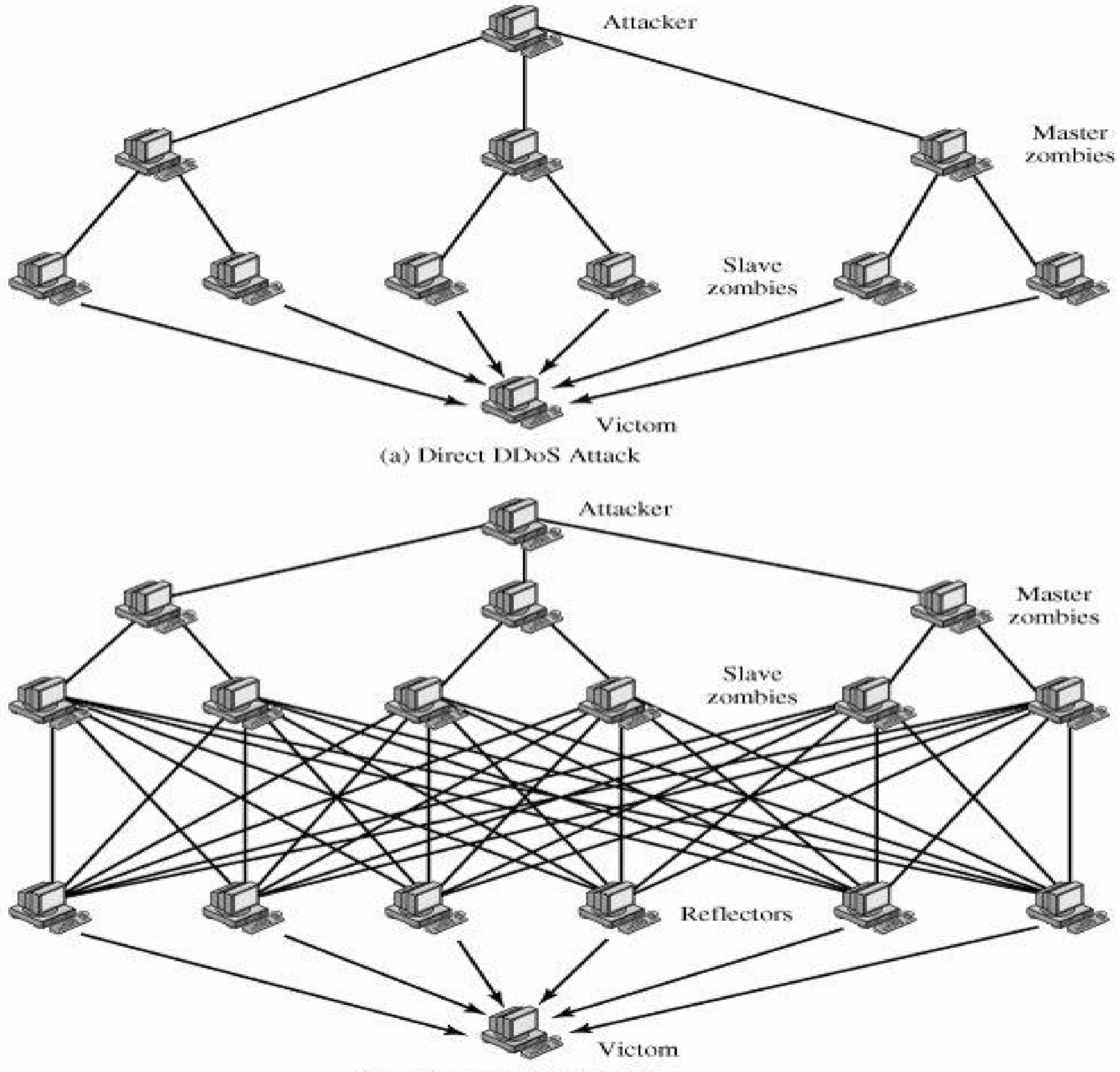
- DDoS attacks make computer systems inaccessible by flooding servers, networks, or even end user systems with useless traffic so that legitimate users can no longer gain access to those resources.
- In a typical DDoS attack, a large number of compromised hosts are amassed to send useless packets.
- When this attack comes from a single host or network node, then it is simply referred to as a DoS attack
- In a DDoS attack, an attacker is able to recruit a number of hosts throughout the Internet to simultaneously or in a coordinated fashion launch an attack upon the target

DDoS



(a) Distributed SYN flood attack

(a) Distributed ICMP attack



(a) Direct DDoS Attack

(b) Reflector DDoS Attack

DDoS Countermeasures

- **Attack prevention (before the attack):** These mechanisms enable the victim to endure attack attempts without denying service to legitimate clients. Techniques include enforcing policies for resource consumption and providing backup resources available on demand
- **Attack detection and filtering (during the attack):** These mechanisms attempt to detect the attack as it begins and respond immediately. Detection involves looking for suspicious patterns of behavior
- **Attack source trace back and identification (during and after the attack):** This is an attempt to identify the source of the attack as a first step in preventing future attacks.

Firewall

- While Internet access provides benefits to the organization, it enables the outside world to reach and interact with local network assets. This creates a threat to the organization.
- Rather than equip each workstation and server on the premises network with strong security features, such as intrusion protection, firewall is more practical solution.
- The firewall is inserted between the premises network and the Internet
- The aim of this perimeter is to protect the premises network from Internet-based attacks.

Firewall Goals/Principle

- All traffic from inside to outside, and vice versa, must pass through the firewall
- Only authorized traffic, as defined by the local security policy, will be allowed to pass
- The firewall itself is immune to penetration
- General techniques that firewalls use to control access and enforce the site's security policy
  - Service control
  - Direction control
  - User control
  - Behavior control

Firewall Limitations

- The firewall cannot protect against attacks that bypass the firewall. An internal LAN may support a modem pool that provides dial-in capability for traveling employees and telecommuters.
- The firewall does not protect against internal threats.
- The firewall cannot protect against the transfer of virus-infected programs or files. It would be impractical and perhaps impossible for the firewall to scan all incoming files, e-mail, and messages for viruses.