INTRUDERS

Key Points

- 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.
- A significant security problem for networked systems is hostile, or at least unwanted, trespass by users or software.
- User trespass can take the form of unauthorized logon to a machine or, in the case of an authorized user, acquisition of privileges or performance of actions beyond those that have been authorized.
- Software trespass can take the form of a virus, worm, or Trojan horse.

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.

- There are three classes of intruders:
  1. **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.
  2. **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.
  3. **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.

- The masquerader is likely to be an outsider; the misfeasor generally is an insider; and the clandestine user can be either an outsider or an insider.
- Intruder attacks range from the benign to the serious.
- At the benign end of the scale, there are many people who simply wish to explore internets and see what is out there.
- At the serious end are individuals who are attempting to read privileged data, perform unauthorized modifications to data, or disrupt the system.

Intrusion Techniques

- The objective of the intruder is to gain access to a system or to increase the range of privileges accessible on a system.
- Generally, this requires the intruder to acquire information that should have been protected.
- This information is in the form of a user password.
- With knowledge of some other user's password, an intruder can log in to a system and exercise all the privileges accorded to the legitimate user.
- Typically, a system must maintain a file that associates a password with each authorized user. If such a file is stored with no protection, then it is an easy matter to gain access to it and learn passwords.

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.
- In practice, the system usually performs a one-way transformation (not reversible) in which the password is used to generate a key for the one-way function and in which a fixed-length output is produced.

Access control

- Access to the password file is limited to one or a very few accounts.

Intrusion Detection Systems

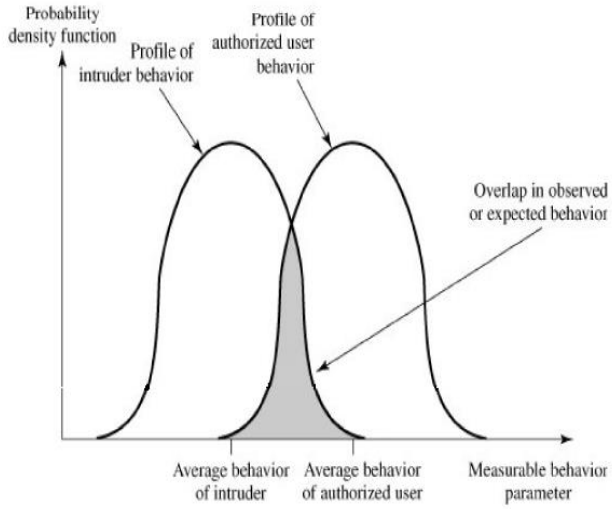
The need for intrusion detection systems:

- Building a completely secure system!!!
- Detect the attack as soon as possible and take appropriate action.
- If the intrusion detected quickly enough, the intruder can be identified and ejected from the system before any damage is done.
- An effective IDS can serve as a deterrent.
- Intrusion detection enables the collection of information about intrusion techniques.

Intrusion detection is based on the assumption that the behavior of the intruder differs from that of the a legitimate user.

Figure 18.1. Profiles of Behavior of Intruders and Authorized Users

(This item is displayed on page 571 in the print version)



- Intrusion detection is based on the assumption that the behavior of the intruder differs from that of the a legitimate user.
- We can divide the techniques of intrusion detection into two main types:

- Statistical anomaly detection.
- Rule-based detection.

Approaches to Intrusion Detection

- Statistical anomaly detection
  - Attempts to define normal/expected behavior
  - Threshold detection
  - Profile based
- Rule-based detection
  - Attempts to define proper behavior
  - Anomaly detection
  - Penetration identification

Statistical Anomaly Detection

- Threshold detection
  - count occurrences of specific event over time
  - if exceed reasonable value assume intrusion
  - alone is a crude & ineffective detector
- Profile based
  - characterize past behavior of users
  - detect significant deviations from this
  - profile usually multi-parameter

Audit Records

- Fundamental tool for intrusion detection
- Native audit records
  - part of all common multi-user O/S

- already present for use
- may not have info wanted in desired form

- Detection-specific audit records
  - created specifically to collect wanted info
  - at cost of additional overhead on system

Audit Record Analysis

- Foundation of statistical approaches
- Analyze records to get metrics over time
  - counter, gauge, interval timer, resource use
- Use various tests on these to determine if current behavior is acceptable
  - mean & standard deviation, multivariate, markov process, time series, operational
- Key advantage is no prior knowledge used

Rule-Based Intrusion Detection

- Rule-based penetration identification
  - Uses expert systems technology
  - With rules identifying known penetration, weakness patterns, or suspicious behavior
  - Compare audit records or states against rules
  - Rules usually machine & O/S specific
  - Rules are generated by experts who interview & codify knowledge of security admins
  - Quality depends on how well this is done
- Rule-based penetration identification takes a very different approach based on expert system technology. It uses rules for identifying known penetrations or penetrations that would

exploit known weaknesses, or identify suspicious behavior. The rules used are specific to machine and operating system. The rules are generated by "experts", from interviews of system administrators and security analysts. Thus the strength of the approach depends on the skill of those involved in setting up the rules.

- Rule-based penetration identification
    - Uses expert systems technology
    - With rules identifying known penetration, weakness patterns, or suspicious behavior
    - Compare audit records or states against rules
    - Rules usually machine & O/S specific
    - Rules are generated by experts who interview & codify knowledge of security admins
    - Quality depends on how well this is done
- Rule-based penetration identification takes a very different approach based on expert system technology. It uses rules for identifying known penetrations or penetrations that would exploit known weaknesses, or identify suspicious behavior. The rules used are specific to machine and operating system. The rules are generated by "experts", from interviews of system administrators and security analysts. Thus the strength of the approach depends on the skill of those involved in setting up the rules.

Base-Rate Fallacy

- Practically an intrusion detection system needs to detect a substantial percentage of intrusions with few false alarms
    - if too few intrusions detected -> false security
    - if too many false alarms -> ignore / waste time
- This is very hard to do
- Existing systems seem not to have a good record.
- To be of practical use, an intrusion detection system should detect a substantial percentage of intrusions while keeping the false alarm rate at an acceptable level. If only a modest percentage of actual intrusions are detected, the system provides a false sense of security. On the other hand, if the system frequently triggers an alert when there is no intrusion (a false alarm), then either system managers will begin to ignore the alarms, or much time will

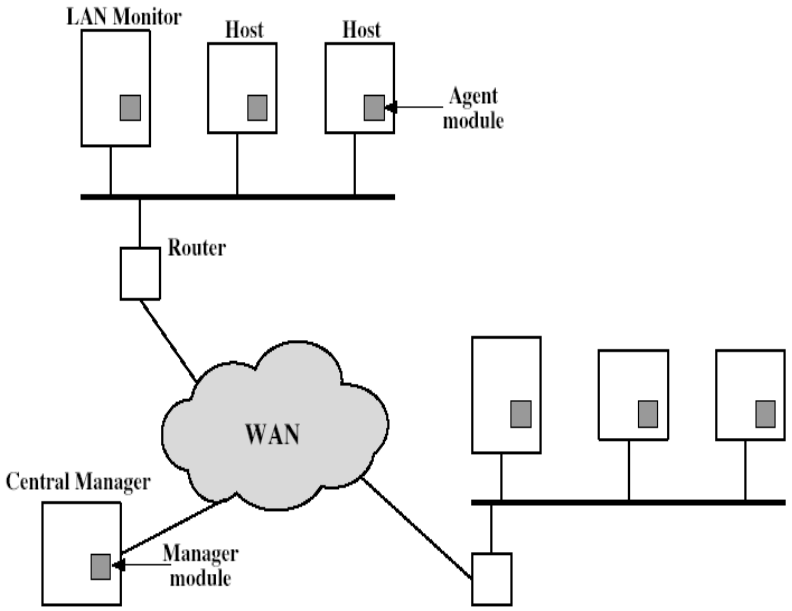
be wasted analyzing the false alarms. Unfortunately, because of the nature of the probabilities involved, it is very difficult to meet the standard of high rate of detections with a low rate of false alarms. A study of existing intrusion detection systems indicated that current systems have not overcome the problem of the base-rate fallacy.

Distributed Intrusion Detection

- Traditional focus is on single systems
- But typically have networked systems
- More effective defense has these working together to detect intrusions
- Issues
  - dealing with varying audit record formats
  - integrity & confidentiality of networked data
  - centralized or decentralized architecture
- Until recently, work on intrusion detection systems focused on single-system standalone facilities. The typical organization, however, needs to defend a distributed collection of hosts supported by a LAN or internetwork, where a more effective defense can be achieved by coordination and cooperation among intrusion detection systems across the network.
- Porras points out the following major issues in the design of a distributed IDS:
- • A distributed intrusion detection system may need to deal with different audit record formats
- • One or more nodes in the network will serve as collection and analysis points for the data, which must be securely transmitted to them
- • Either a centralized (single point, easier but bottleneck) or decentralized (multiple centers must coordinate) architecture can be used.
- A distributed intrusion detection system is one developed at the University of California at Davis.
- Which consists of three main components:
- **Host agent module:**An audit collection module operating as a background process on a monitored system.Its purpose is to collect data on security related events on the host and transmit these to the central manager.

- **LAN monitor agent module**:Operates in the same fashion as a host agent module except that it analyzes LAN traffic and reports the result to the central manager.
- **Central manager module:**Recieves reports from LAN r and host agent and processes and correlates these reports to detect intrusion**.**

Distributed Intrusion Detection – Architecture



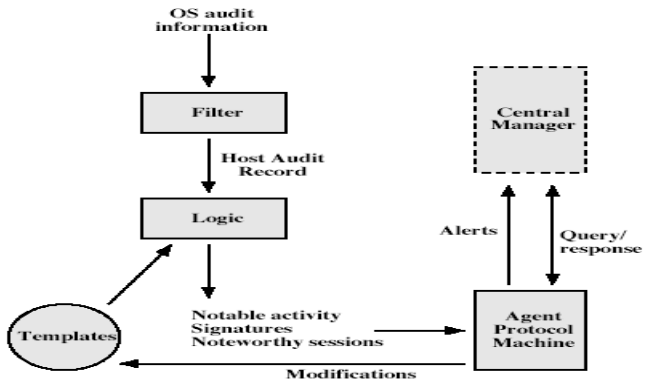
Stallings Figure18.2 shows the overall architecture, consisting of three main components, of the system independent distributed IDS developed at the University of California at Davis. The components are:

• Host agent module: audit collection module operating as a background process on a monitored system

• LAN monitor agent module: like a host agent module except it analyzes LAN traffic

• Central manager module: Receives reports from LAN monitor and host agents and processes and correlates these reports to detect intrusion

Distributed Intrusion Detection – Agent implementation



Stallings Figure 18.3 shows the general approach that is taken. The agent captures each native O/S audit record, & applies a filter that retains only records of security interest. These records are then reformatted into a standardized format (HAR). Then a template-driven logic module analyzes the records for suspicious activity. When suspicious activity is detected, an alert is sent to the central manager. The central manager includes an expert system that can draw inferences from received data. The manager may also query individual systems for copies of HARs to correlate with those from other agents.

Honeypots

- Decoy systems to lure attackers
  - away from accessing critical systems
  - to collect information of their activities
  - to encourage attacker to stay on system so administrator can respond
- Are filled with fabricated information
- Instrumented to collect detailed information on attackers activities
  - Single or multiple networked systems

- Honeypots are decoy systems, designed to lure a potential attacker away from critical systems, and:
- • 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 which any legitimate user of the system wouldn't access, thus, any access is suspect.
- They are instrumented with sensitive monitors and event loggers that detect these accesses and collect information about the attacker's activities.
- Have seen evolution from single host honeypots to honeynets of multiple dispersed systems.
- The IETF Intrusion Detection Working Group is currently drafting standards to support interoperability of IDS info (both honeypot and normal IDS) over a wide range of systems & O/S's.

Intrusion Detection Exchange Format

- To facilitate the development of distributed intrusion detection systems that can function across a wide range of platforms and environments ,standards are needed to support interoperability.
- Such standards are focus of the IETF Intrusion Detection Working Group.
- The outputs of this working group include the following:

1.A requirement document,which describes the high level functional requirements for communication between intrusion detection systems and with management systems,including the rationale for those requirements.

2.A common intrusion language specification,which describes data formats that satisfy the requirements.

3.A frame work document,which identifies existing protocols best used for communication between intrusion detection systems,and describes how the devised data formats relate to them.

VIRUSES

Definition:

"What is the concept of defense. The parrying of blow. What is its characteristics feature: Awaiting the blow." By -On War, Carl Von Clausewitz

Viruses:

- 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 connection.
- 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 legitimates users of a service from using that service.

Viruses and related threats

1. Malicious Programs

- Malicious software can be divided into two categories.

a) Those that need a host program

Eg: Viruses, logic bombs and backdoors.

b) Those that are independent

Eg: Worms and zombie programs

Terminology of Malicious Programs

1. Virus

- Attaches itself to a program and propagates copies of itself to other programs.
- It contains either a program fragment or an independent program that, when executed, may produce one or more copies of itself to be activated later on the same system or some other system.

2. Worm

- Program that propagates copies of itself to other computers.

3. Logical bomb

- Triggers action when condition occurs.
- It is a program or fragments of programs that are activated by a trigger.
- The logical bomb is code embedded in some legitimate program that is set to "explode" when certain conditions are met.

4. Trojan horse

- It is a program that contains unexpected additional functionality.
- It is useful, or apparently useful, program or command procedure containing hidden code that, when invoked, performs some unwanted or harmful function.
- Trojan horse programs can be used to accomplish functions indirectly that an unauthorized user could not accomplish directly.
- A common motivation for the Trojan horse is data construction.

5. Backdoor (trapdoor)

- It is a program modification that allows unauthorized access to functionality.
- Also, it 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.

- Programmers have used backdoors legitimately for many years to debug and test programmers.
- The backdoor is a code that recognizes some special sequence of input or is triggered by being run from a certain user ID or by an unlikely sequence of events.
- The program appears to be performing a useful function, but it may also be quietly deleting the user's files.
- Trojan horse was implanted in a graphics routine offered on an electronic bulletin board system.

6. Exploits

- Code specific to a single vulnerability or set of vulnerabilities.

7. down loaders

- It is a program that installs other items on a machine that is under attack. Usually, a downloader is sent in an e-mail.

8. Auto-rooter

- It is malicious hacker tools used to break into new machines remotely.

9. Kit

- It is a virus generator.
- It is a set of tools used to break into new machines remotely.

10. Spammer programs

- It is used to send large volumes of unwanted e-mail.

11. Zombie

- It is a program activated on an infected machine that is activated to launch attacks on other machines.
- Zombies are used in denial-of –service attacks, typically against target Web sites.

Nature of viruses

- 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 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, afresh copy of the virus pass into the new program.

A typical virus goes through the following four phases:

a) **Dormant phases:** 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.
b) **Propagation phase:** The virus places an identical copy of itself into other programs or into certain system areas on the disk. Each infected program will now contain a clone of the virus, which will itself enter a propagation phase.
c) **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.
d) **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.

Virus structure

- A virus can be prepended or postpended to an executable program, or it can be embedded in some other fashion.
- The key to its operation is that the infected program, when invoked, will first execute the virus code and then execute the original code of the program.
- A virus is easily detected because an infected version of a program is longer than the corresponding uninfected one.

Initial infection

- Once a virus has gained entry to a system by infecting a single program, it is in a position to infect some or all other executable files on that system when the infected program executes.
- Thus, vital infection can be completely prevented by preventing the virus from gaining entry in the first place.

Types of viruses

The most significant types of viruses are:

1. **Parasitic viruses:** The traditional and still most common form of virus. A parasitic virus attaches itself to executable file and replicates, when the infected program is executed, by finding other executable files to infect.

2. **Memory-resident virus:** Lodges in main memory as part of a resident system program. From that point on, the virus infects every program that executes.

3. **Boot sector virus:** Infects a master boot record or boot record and spreads when a system is booted from the disk containing the virus.

4. **Stealth virus:** A form of virus explicitly designed to hide itself from detection by antivirus software.
   - Stealth is not a term that applies to a virus as such, rather, is a technique used by a virus to evade detection.

5. **Polymorphic virus:** A virus that mutates with every infection, making detection by the "signature" of the virus impossible.
   - It creates copies during replication that are functionally equivalent but have distinctly different bit patterns.
   - The "signature of the virus will vary with each copy.
   - A more effective approach is to use encryption.
   - A portion of the virus, generally called a mutation engine, creates a random encryption key to encrypt the remainder of the virus.

6. **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.

Macro Viruses

- Macro viruses are particularly threatening for a number of reasons.
    i. A macro virus is platform independent.
    ii. Macro viruses infect documents, not executable portions of code.
    iii. Macro viruses are easily spread.

E-mail Viruses

- It is malicious software.
    1. The e-mail virus sends itself to everyone on the user's e-mail package.
    2. The virus does local damage.

Worms

- It is a program that can replicate itself and send copies from to computer across network connections.
- Eg: Electronic mail facility, Remote execution, Remote login capability.
- 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.
- The propagation phase generally performs the following functions:
    1. Search for other systems to infect by examining host tables or similar repositories of remote system address.
    2. Establish a connection with a remote system.
    3. Copy itself to the remote system and cause the copy to be run.

Morris Worm

- It was designed to spread on UNIX systems and used a number of different techniques for propagation.
- When a copy began execution, its first task was to discover other hosts known to this host that would allow entry from this host.

Recent Worm Attacks

- The contemporary era of worm threats began with the release of the Code Red worm in July of 2001.
- The worm probes random IP address to spread to other hosts.
- It then initiates a denial –of-service attack against a government Web site by flooding the site with packets from numerous hosts.
- The worm then spreads activities and reactivates periodically.

State of Worm Technology

- The state of the art in worm technology includes the following:
  - ✓ Multiplatform
  - ✓ Multiexploit
  - ✓ Ultrafast spreading
  - ✓ Polymorphic
  - ✓ Metamorphic
  - ✓ Transport vehicles
  - ✓ Zero-day exploit

Viruses' countermeasures

1. Antivirus Approaches

- The ideal solution to the threat of viruses is prevention. Do not allow a virus to get into the system in the first place.
- The next best approach is to be able to do the following:
  a. Detection
  b. Identification
  c. Removal

- Four generation of antivirus software :

    1. First generation: Simple scanners
    2. Second generation: heuristic scanners
    3. Third generation: activity traps
    4. Fourth generation: full-featured protection

2. Advanced Antivirus Techniques

- **Generic Decryption (GD):** This technology enables the antivirus program to easily detect even the most complex polymorphic viruses, while maintaining fast speeds.
- In order to detect such a structure, executable files are run through a GD scanner, which contains the following elements:

    1. **CPU emulator:** A software-based virtual computer.
    2. **Virus signature scanner:** A module that scans the target code looking for known virus signature.
    3. **Emulation control module:** Controls the execution of the target code.

- The most difficult design issue with a GD scanner is to determine how long to run each interpretation.

3. Digital Immune System

- It is a comprehensive approach to virus protection developed by IBM.
- Two major trends in Internet technology have had an increasing impact on the rate of virus propagation in recent years.

    I. Integrated mail system

    II. Mobile-program system

4. Behavior-Blocking Software

- The behavior blocking software then blocks potentially malicious actions before they have a chance to affect the system.
- Monitored behaviors can include the following:

    a. Attempts to open, view, delete, and/or modify files.

b. Attempts to format disk drives and other unrecoverable disk operations.

c. Modifications to the logic of executable files or macros.

d. Modifications of critical system settings, such as start-up settings.
e. Scripting of e-mail and instant messaging clients to send executable content.
f. Initiation of network communication.

- The ability to watch software as it runs in real time clearly confers a huge benefit to the behavior blocker.

FIREWALLS

What is a Firewall?

- A firewall :
  - Acts as a security gateway between two networks
  - Usually between trusted and untrusted networks (such as between a corporate network and the Internet)
  - Tracks and controls network communications
    - Decides whether to pass, reject, encrypt, or log communications (Access Control)
- A firewall forms a barrier through which the traffic going in each direction must pass. A firewall security policy dictates which traffic is authorized to pass in each direction.
- Firewalls can be an effective means of protecting a local system or network of systems from network-based security threats while at the same time affording access to the outside world via wide area networks and the Internet.

Firewall Design Principles

- Centralized data processing system, with a central mainframe supporting a number of directly connected terminals.
- Local area networks (LANs) interconnecting PCs and terminals to each other and the mainframe.

- Premises network, consisting of a number of LANs, interconnecting PCs, servers, and perhaps a mainframe or two.
- Enterprise-wide network, consisting of multiple, geographically distributed premises networks interconnected by a private wide area network (WAN).
- Internet connectivity, in which the various premises networks all hook into the Internet and may or may not also be connected by a private WAN.

Why Firewalls are needed

- Prevent attacks from untrusted networks
- Protect data integrity of critical information
- Preserve customer and partner confidence

Firewall Characteristics

- All traffic from inside to outside, and vice versa, must pass through the firewall. This is achieved by physically blocking all access to the local network except via the firewall.
- Only authorized traffic, as defined by the local security policy, will be allowed to pass.
- The firewall itself is immune to penetration. This implies that use of a trusted system with a secure operating system.

Firewalls focused primarily on service control, but they have since evolved to provide all four:

Service control

- Determines the types of Internet services that can be accessed, inbound or outbound.
- The firewall may filter traffic on the basis of IP address and TCP port number; may provide proxy software that receives and interprets each service request before passing it on; or may host the server software itself, such as a Web or mail service.

Direction control

- Determines the direction in which particular service requests may be initiated and allowed to flow through the firewall.

User control

- Controls access to a service according to which user is attempting to access it.
- This feature is typically applied to users inside the firewall perimeter (local users).
- It may also be applied to incoming traffic from external users; the latter requires some form of secure authentication technology, such as is provided in IPSec.

Behavior control

- Controls how particular services are used.
- For example, the firewall may filter e-mail to eliminate spam, or it may enable external access to only a portion of the information on a local Web server.

Scope of a firewall

1. A firewall defines a single choke point that keeps unauthorized users out of the protected network, prohibits potentially vulnerable services from entering or leaving the network, and provides protection from various kinds of IP spoofing and routing attacks.

   The use of a single choke point simplifies security management because security capabilities are consolidated on a single system or set of systems.

2. A firewall provides a location for monitoring security-related events. Audits and alarms can be implemented on the firewall system.

3. A firewall is a convenient platform for several Internet functions that are not security related. These include a network address translator, which maps local addresses to Internet addresses, and a network management function that audits or logs Internet usage.

4. A firewall can serve as the platform for IPSec. Using the tunnel mode capability the firewall can be used to implement virtual private networks.

Limitations

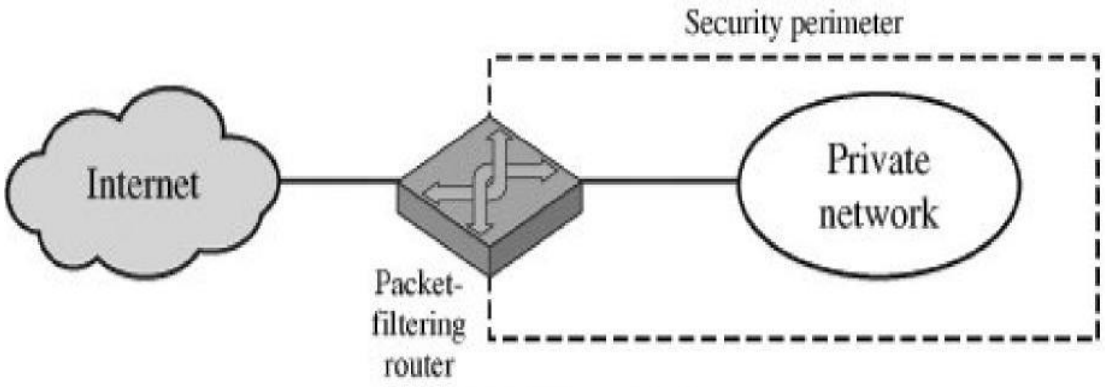
- The firewall cannot protect against attacks that bypass the firewall. Internal systems may have dial-out capability to connect to an ISP. An internal LAN may support a modem pool that provides dial-in capability for traveling employees and telecommuters.
- The firewall does not protect against internal threats, such as a disgruntled employee or an employee who unwittingly cooperates with an external attacker.

- The firewall cannot protect against the transfer of virus-infected programs or files. Because of the variety of operating systems and applications supported inside the perimeter, it would be impractical and perhaps impossible for the firewall to scan all incoming files, e-mail, and messages for viruses.

Types of Firewalls

1. Packet-Filtering Router
2. Stateful Inspection Firewalls
3. Application-Level Gateway

Packet-Filtering Router



(a) Packet-filtering router

- A packet-filtering router applies a set of rules to each incoming and outgoing IP packet and then forwards or discards the packet. The router is typically configured to filter packets going in both directions (from and to the internal network). Filtering rules are based on information contained in a network packet:

- **Source IP address**
  - The IP address of the system that originated the IP packet (e.g., 192.178.1.1)

- **Destination IP address**

  - The IP address of the system the IP packet is trying to reach (e.g., 192.168.1.2)

- **Source and destination transport-level address**
    - The transport level (e.g., TCP or UDP) port number, which defines applications such as SNMP or TELNET.
- **IP protocol field**
    - Defines the transport protocol
- **Interface**
    - For a router with three or more ports, which interface of the router the packet came from or which interface of the router the packet is destined for.
- The packet filter is typically set up as a list of rules based on matches to fields in the IP or TCP header.
- If there is a match to one of the rules, that rule is invoked to determine whether to forward or discard the packet.
- If there is no match to any rule, then a default action is taken.
- Two default policies are possible:
- **Default** = *discard*: That which is not expressly permitted is prohibited.
- **Default** = *forward*: That which is not expressly prohibited is permitted.
- One advantage of a packet-filtering router is its simplicity.
- Also, packet filters typically are transparent to users and are very fast.

Weaknesses of packet filter firewalls

- Because packet filter firewalls do not examine upper-layer data, they cannot prevent attacks that employ application-specific vulnerabilities or functions. For example, a packet filter firewall cannot block specific application commands; if a packet filter firewall allows a given application, all functions available within that application will be permitted.
- Because of the limited information available to the firewall, the logging functionality present in packet filter firewalls is limited. Packet filter logs normally contain the same information used to make access control decisions (source address, destination address, and traffic type).
- Most packet filter firewalls do not support advanced user authentication schemes. Once again, this limitation is mostly due to the lack of upper-layer functionality by the firewall.

- They are generally vulnerable to attacks and exploits that take advantage of problems within the TCP/IP specification and protocol stack, such as *network layer address spoofing*. Many packet filter firewalls cannot detect a network packet in which the OSI Layer 3 addressing information has been altered. Spoofing attacks are generally employed by intruders to bypass the security controls implemented in a firewall platform.
- Finally, due to the small number of variables used in access control decisions, packet filter firewalls are susceptible to security breaches caused by improper configurations. In other words, it is easy to accidentally configure a packet filter firewall to allow traffic types, sources, and destinations that should be denied based on an organization's information security policy.

- **Some of the attacks that can be made on packet-filtering routers and the appropriate countermeasures are the following:** (refer text)
  - IP address spoofing
  - Source routing attacks
  - Tiny fragment attacks

Stateful Inspection Firewalls

- A stateful inspection packet filter tightens up the rules for TCP traffic by creating a directory of outbound TCP connections, There is an entry for each currently established connection.
- The packet filter will now allow incoming traffic to high-numbered ports only for those packets that fit the profile of one of the entries in this directory.

Application-Level Gateway

- An application-level gateway, also called a proxy server, acts as a relay of application-level traffic.
- Application-level gateways tend to be more secure than packet filters.
- Rather than trying to deal with the numerous possible combinations that are to be allowed and forbidden at the TCP and IP level, the application-level gateway need only scrutinize a few allowable applications.

- In addition, it is easy to log and audit all incoming traffic at the application level.
- **A prime disadvantage** of this type of gateway is the additional processing overhead on each connection.
- In effect, there are two spliced connections between the end users, with the gateway at the splice point, and the gateway must examine and forward all traffic in both directions.

Circuit-Level Gateway

- A third type of firewall
- This can be a stand-alone system or it can be a specialized function performed by an application level gateway for certain applications.
- A circuit-level gateway does not permit an end-to-end TCP connection.

Bastion Host

- A **bastion host** is a special purpose computer on a network specifically designed and configured to withstand attacks.

Common characteristics

- The bastion host hardware platform executes a secure version of its operating system, making it a trusted system.
- Only the services that the network administrator considers essential are installed on the bastion host.
- These include proxy applications such as Telnet, DNS, FTP, SMTP, and user authentication.
- The bastion host may require additional authentication before a user is allowed access to the proxy services.
- In addition, each proxy service may require its own authentication before granting user access.
- Each proxy is configured to support only a subset of the standard application's command set.
- Each proxy is configured to allow access only to specific host systems.
- Each proxy maintains detailed audit information by logging all traffic, each connection, and the duration of each connection.

- Each proxy module is a very small software package specifically designed for network security.
- Each proxy is independent of other proxies on the bastion host.
- Each proxy runs as a non-privileged user in a private and secured directory on the bastion host.
- A proxy generally performs no disk access other than to read its initial configuration file.

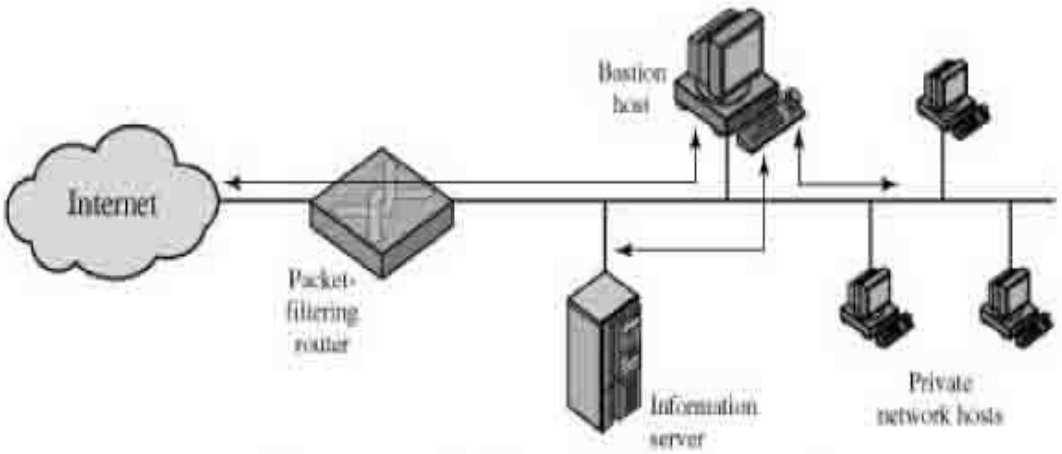
Firewall Configurations (refer text)

- Single homed bastion host
- Dual homed bastion host
- Screened subnet firewall system

Router Configuration

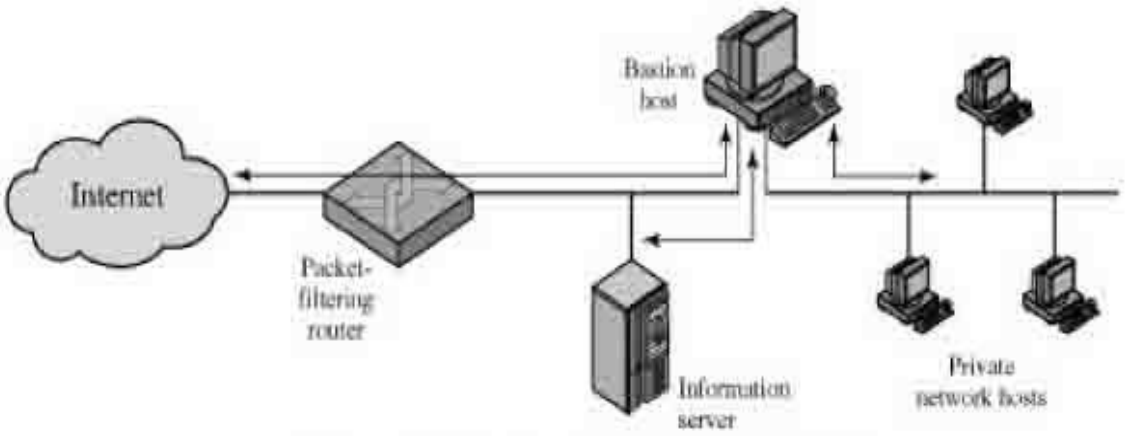
1. For traffic from the Internet, only IP packets destined for the bastion host are allowed in.
2. For traffic from the internal network, only IP packets from the bastion host are allowed out.

Single homed bastion host



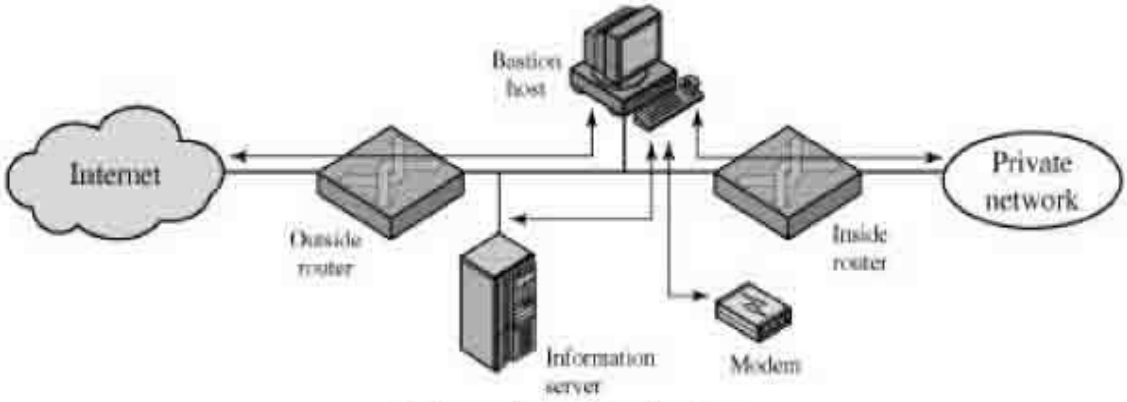
(a) Screened host firewall system (single-homed bastion host)

Dual homed bastion host



(b) Screened host firewall system (dual-homed bastion host)

Screened subnet firewall system



(c) Screened-subnet firewall system