FIREWALLS

Dr. Vasudha Arora
Vasudha.arora@gdgu.org, vasudharora6@gmail.com
Department of Computer Science and Engineering
GD Goenka University, Gurugram

Outline

What are Firewalls

Firewall Design Principles

Firewall Characteristics

Types of Firewalls

Firewalls

Effective means of protecting a local system or network of systems from network-based security threats while affording access to the outside world via WAN`s or the Internet

The Nature of Today's Attackers

Who are these "hackers" who are trying to break into your computer?

- Most people imagine someone at a keyboard late at night, guessing passwords to steal confidential data from a computer system.
- This type of attack does happen, but it makes up a very small portion of the total network attacks that occur.
- Today, worms and viruses initiate the vast majority of attacks. Worms and viruses generally find their targets randomly.
- As a result, even organizations with little or no confidential information need firewalls to protect their networks from these automated attackers.

What Is a Firewall ?

The term firewall has been around for quite some time and originally was used to define a barrier constructed to prevent the spread of fire from one part of a building or structure to another. Network firewalls provide a barrier between networks that prevents or denies unwanted or unauthorized traffic.

Definition: A Network Firewall is a system or group of systems used to control access between two networks -- a trusted network and an untrusted ı

What Is a Firewall ?

- Device that provides secure connectivity between networks (internal/external; varying levels of trust)
- Used to implement and enforce a security policy for communication between networks
- Firewalls can either be hardware and/or software based.
- Firewalls can be composed of a single router, multiple routers, a single host system or multiple hosts running firewall software, hardware appliances specifically designed to provide firewall services, or any combination thereof. They vary greatly in design, functionality, architecture, and cost.
- A firewall is also called a Border Protection Device (BPD) in certain military contexts where a firewall separates networks by creating perimeter networks in a DMZ “Demilitarized Zone”.

What is a Firewall?

- a **choke point** of control and monitoring
- interconnects networks with differing trust
- imposes restrictions on network services
  - only authorized traffic is allowed
- auditing and controlling access
  - can implement alarms for abnormal behavior
- provide NAT & usage monitoring
- implement VPNs using IPSec
- must be immune to penetration

What Firewalls Do (Positive Effects)

User authentication.

Firewalls can be configured to require user authentication. This allows network administrators to control ,track specific user activity.

Auditing and logging.

By configuring a firewall to log and audit activity, information may be kept and analyzed at a later date.

Anti-Spoofing - Detecting when the source of the network traffic is being "spoofed", i.e., when an individual attempting to access a blocked service alters the source address in the message so that the traffic is allowed.

Network Address Translation (NAT) - Changing the network addresses of devices on any side of the firewall to hide their true addresses from devices on other sides. There are two ways NAT is performed:

One-to-One - where each true address is translated to a unique translated address.

Many-to-One - where all true addresses are translated to a single address, usually that of the firewall.

What Firewalls Do (Positive Effects)

Virtual Private Networks

VPNs are communications sessions traversing public networks that have been made virtually private through the use of encryption technology. VPN sessions are defined by creating a firewall rule that requires encryption for any session that meets specific criteria.

What Firewalls Do (Negative Effects)

Although firewall solutions provide many benefits, negative effects may also be experienced.

- **Traffic bottlenecks.** By forcing all network traffic to pass through the firewall, there is a greater chance that the network will become congested.
- **Single point of failure.** In most configurations where firewalls are the only link between networks, if they are not configured correctly or are unavailable, no traffic will be allowed through.
- **Increased management responsibilities.** A firewall often adds to network management responsibilities and makes network troubleshooting more complex.

Firewall Limitations

- The most common misconception about firewalls is that they guarantee security for your network.
- A firewall cannot and does not guarantee that your network is 100% secure.
- Firewalls cannot offer any protection against inside attacks. A high percentage of security incidents today come from inside the trusted network.
- cannot protect from attacks bypassing it
  - eg sneaker net, utility modems, trusted organisations, trusted services (eg SSL/SSH)
- cannot protect against access via WLAN
  - if improperly secured against external use

Firewall Design Principles

There are two security design logic approaches network firewalls use to make access control decisions.

- Everything not specifically permitted is denied.
- Everything not specifically denied is permitted.

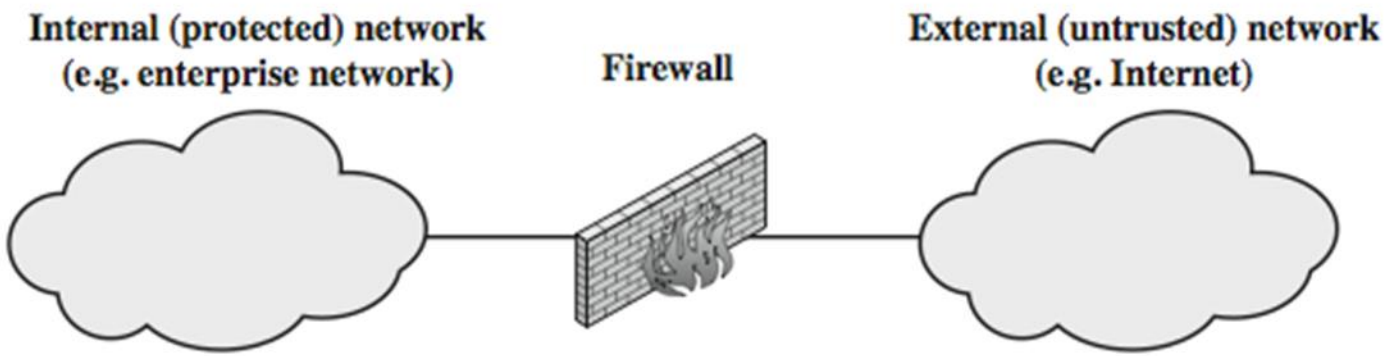
The one most often recommended is everything not specifically permitted is denied.

Firewall Design Principles

The firewall is inserted between the premises network and the Internet

Aims:

- Establish a controlled link
- Protect the premises network from Internet-based attacks
- Provide a single choke point



Firewall Characteristics

Design goals:

- All traffic from inside to outside must pass through the firewall (physically blocking all access to the local network except via the firewall)
- Only authorized traffic (defined by the local security police) will be allowed to pass

Firewall Characteristics

Four general techniques:

Service control

- Determines the types of Internet services that can be accessed, inbound or outbound

Direction control

- Determines the direction in which particular service requests are allowed to flow

Firewall Characteristics

User control
- Controls access to a service according to which user is attempting to access it

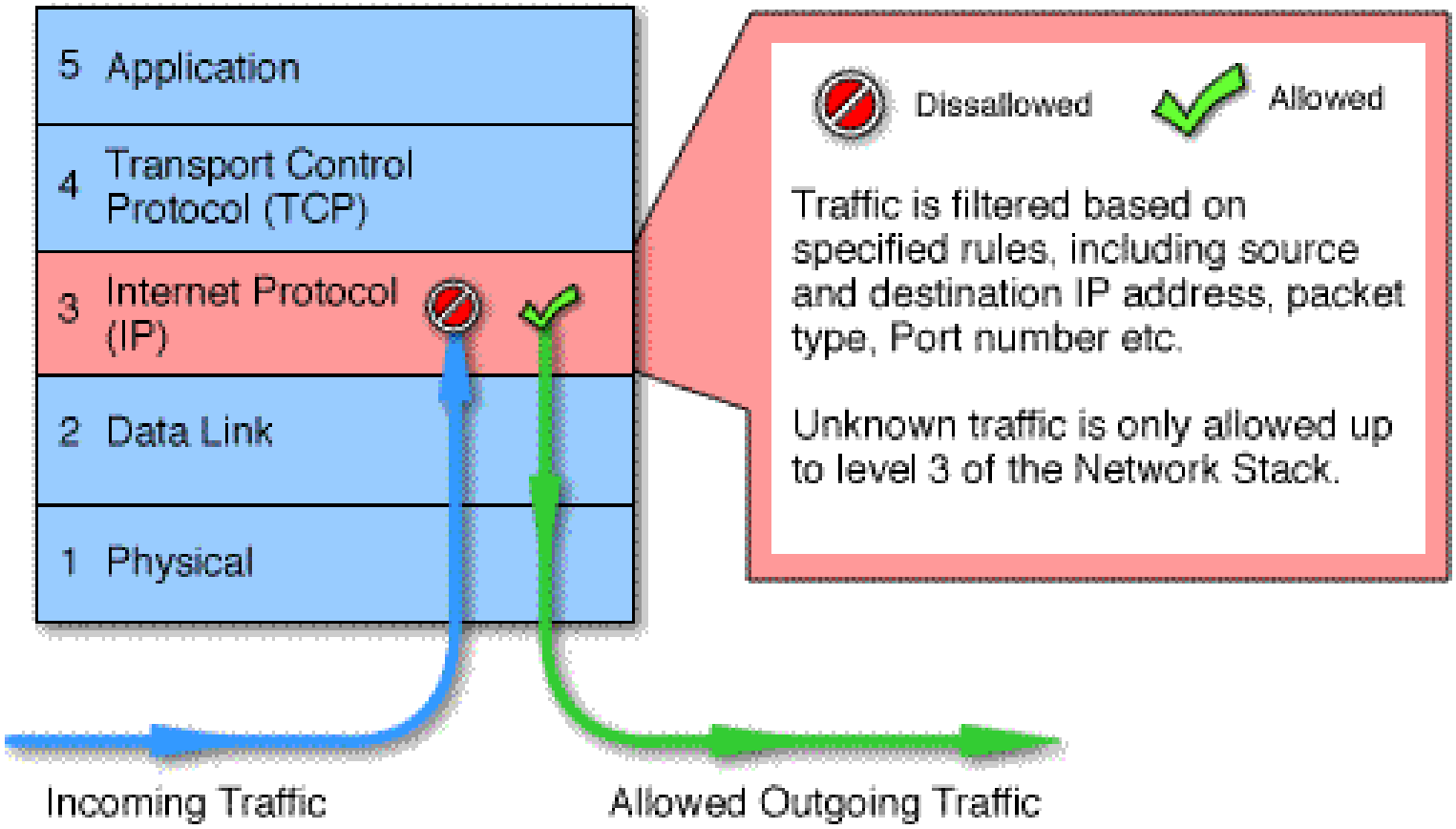
Behavior control
- Controls how particular services are used (e.g. filter e-mail)

Types of Firewalls

Three common types of Firewalls:

- Packet-filtering routers
- Application-level gateways
- Circuit-level gateways

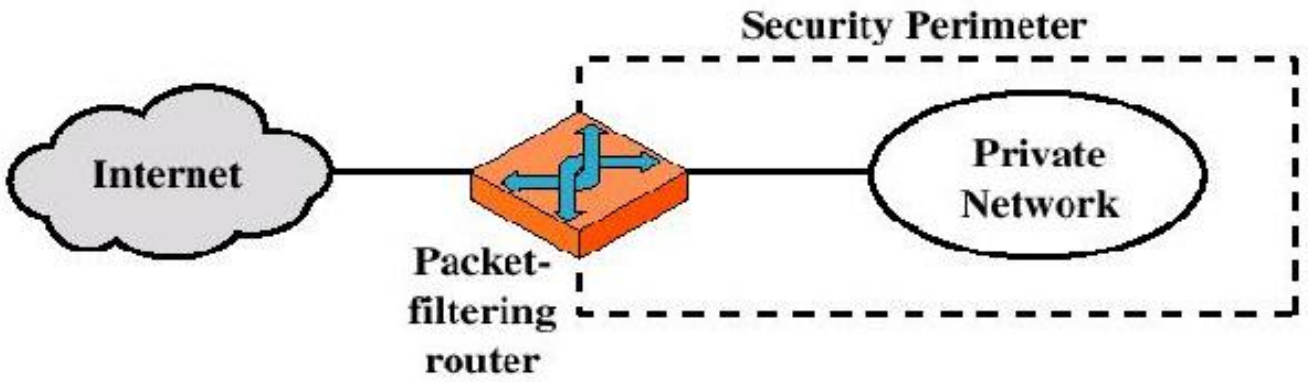
Packet-filtering Router



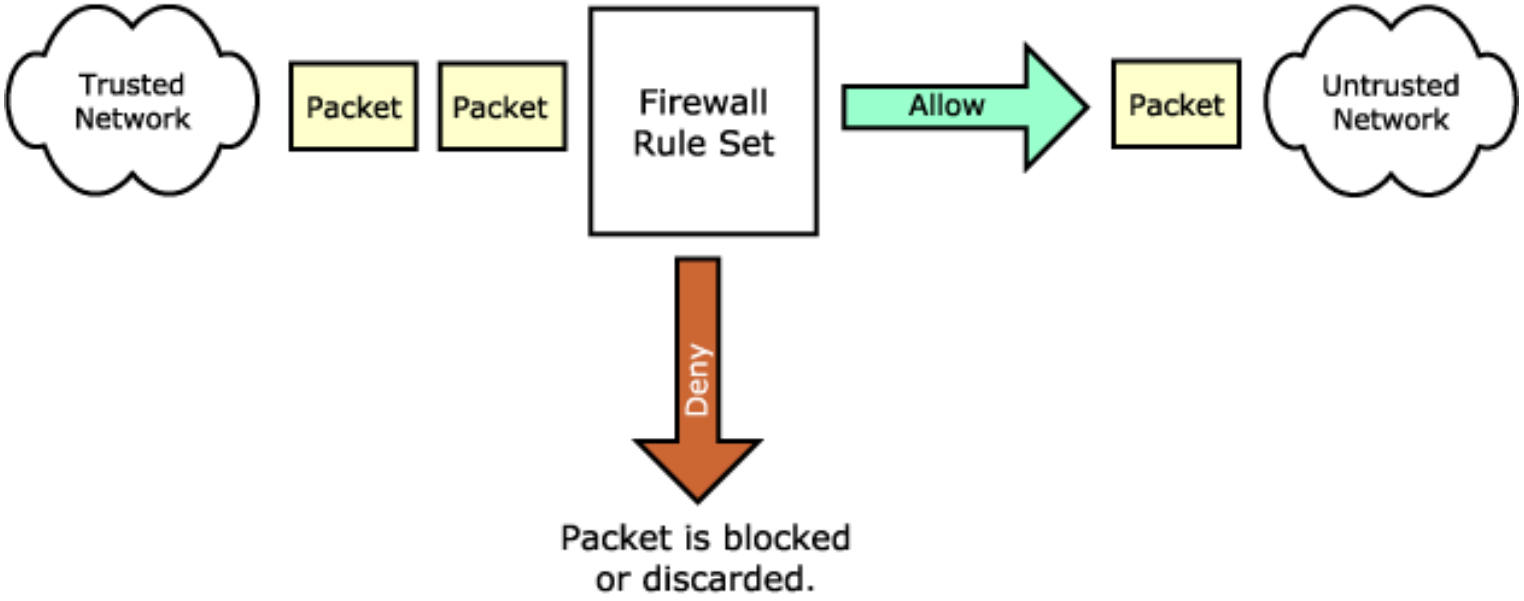
Packet-filtering Router

A packet filtering firewall does exactly what its name implies -- it filters packets.

As each packet passes through the firewall, it is examined and information contained in the header is compared to a pre-configured set of rules or filters. An allow or deny decision is made based on the results of the comparison. Each packet is examined individually without regard to other packets that are part of the same connection.



Packet-filtering Router



Packet-filtering Router

Packet-filtering Router

- Applies a set of rules to each incoming IP packet and then forwards or discards the packet
- Filter packets going in both directions
- The packet filter is typically set up as a list of rules based on matches to fields in the IP or TCP header
- Two default policies (discard or forward)

You can use packet filters to instruct a firewall to drop traffic that meets certain criteria.

For example, you could create a filter that would drop all ping requests. You can also configure filters with more complex exceptions to a rule.

Packet-filtering Router

Advantages:

- Simplicity
- Transparency to users
- High speed

Disadvantages:

- Difficulty of setting up packet filter rules
- Lack of Authentication

Packet-filtering Router

Possible attacks and appropriate countermeasures

IP address spoofing : fake source address to be trusted

- add filters on router to block

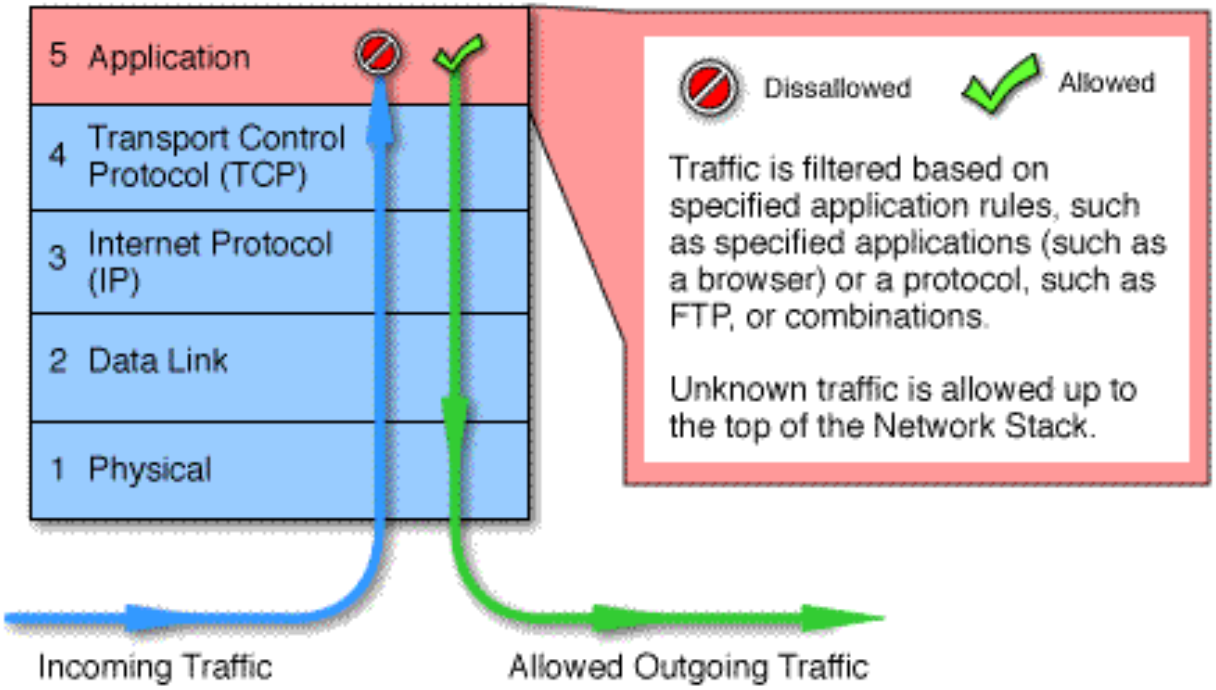
source routing attacks : attacker sets a route other than default

- block source routed packets

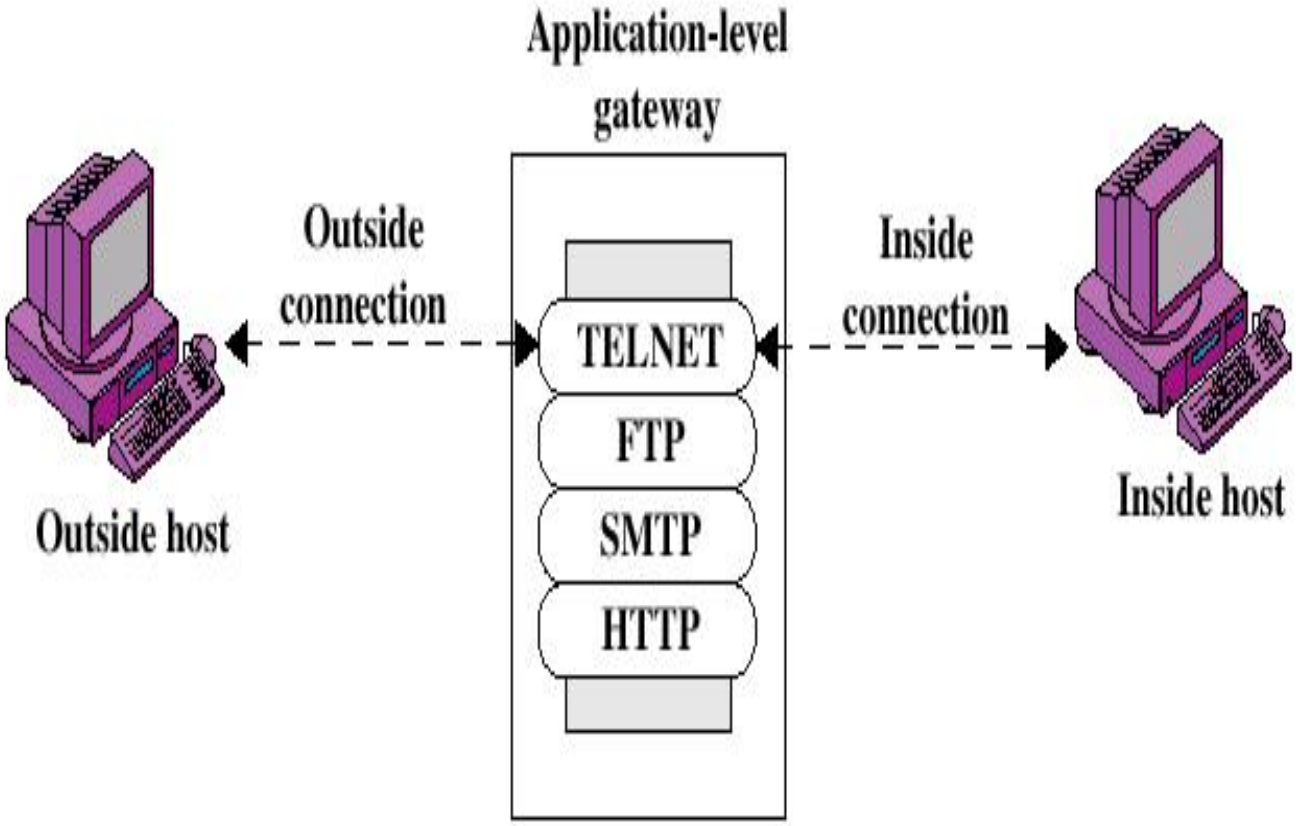
tiny fragment attacks: split header info over several tiny packets

- either discard or reassemble before check

Application-level Gateway



Application-level Gateway



Application-level Gateway

Application-level Gateway

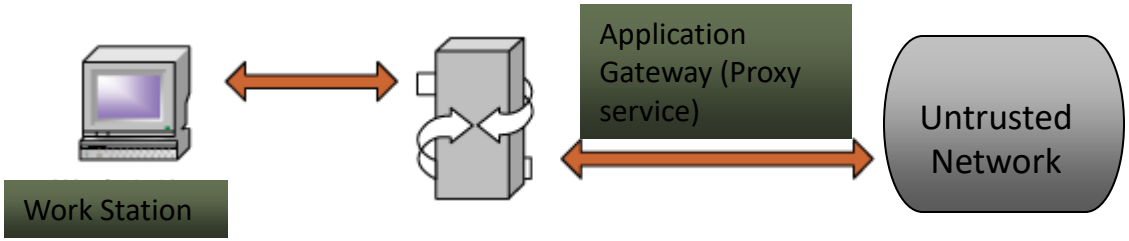
- Also called proxy server
- Acts as a relay of application-level traffic

The proxy plays middleman in all connection attempts.

The application gateway/proxy acts as an intermediary between the two endpoints. This packet screening method actually breaks the client/server model in that two connections are required: one from the source to the gateway/proxy and one from the gateway/proxy to the destination. Each endpoint can only communicate with the other by going through the gateway/proxy.

Application Gateways/Proxies Firewall

When a client issues a request from the untrusted network, a connection is established with the application gateway/proxy. The proxy determines if the request is valid (by comparing it to any rules or filters) and then sends a new request on behalf of the client to the destination. By using this method, a direct connection is never made from the trusted network to the untrusted network and the request appears to have originated from the application gateway/proxy.



Application Gateways/Proxies Firewall

The response is sent back to the application gateway/proxy, which determines if it is valid and then sends it on to the client.

By breaking the client/server model, this type of firewall can effectively hide the trusted network from the untrusted network.

It is important to note that the application gateway/proxy actually builds a new request, only copying known acceptable commands before sending it on to the destination.

Unlike packet filtering, an application gateway/proxy can see all aspects of the application layer so it can look for more specific pieces of information

Application-level Gateway

Advantages:

Application gateways/proxies do not allow a direct connection to be made between endpoints. They actually break the client/server model.

Typically have the best content filtering capabilities. Since they have the ability to examine the payload of the packet, they are capable of making decisions based on content.

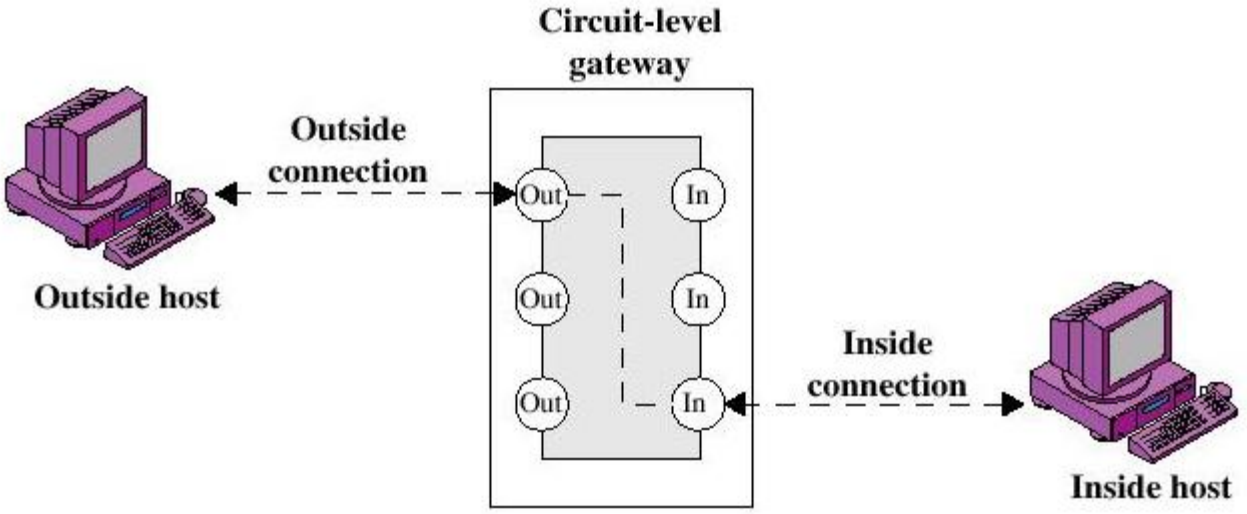
Allow the network administrator to have more control over traffic passing through the firewall. They can permit or deny specific applications or specific features of an application.

Disadvantages:

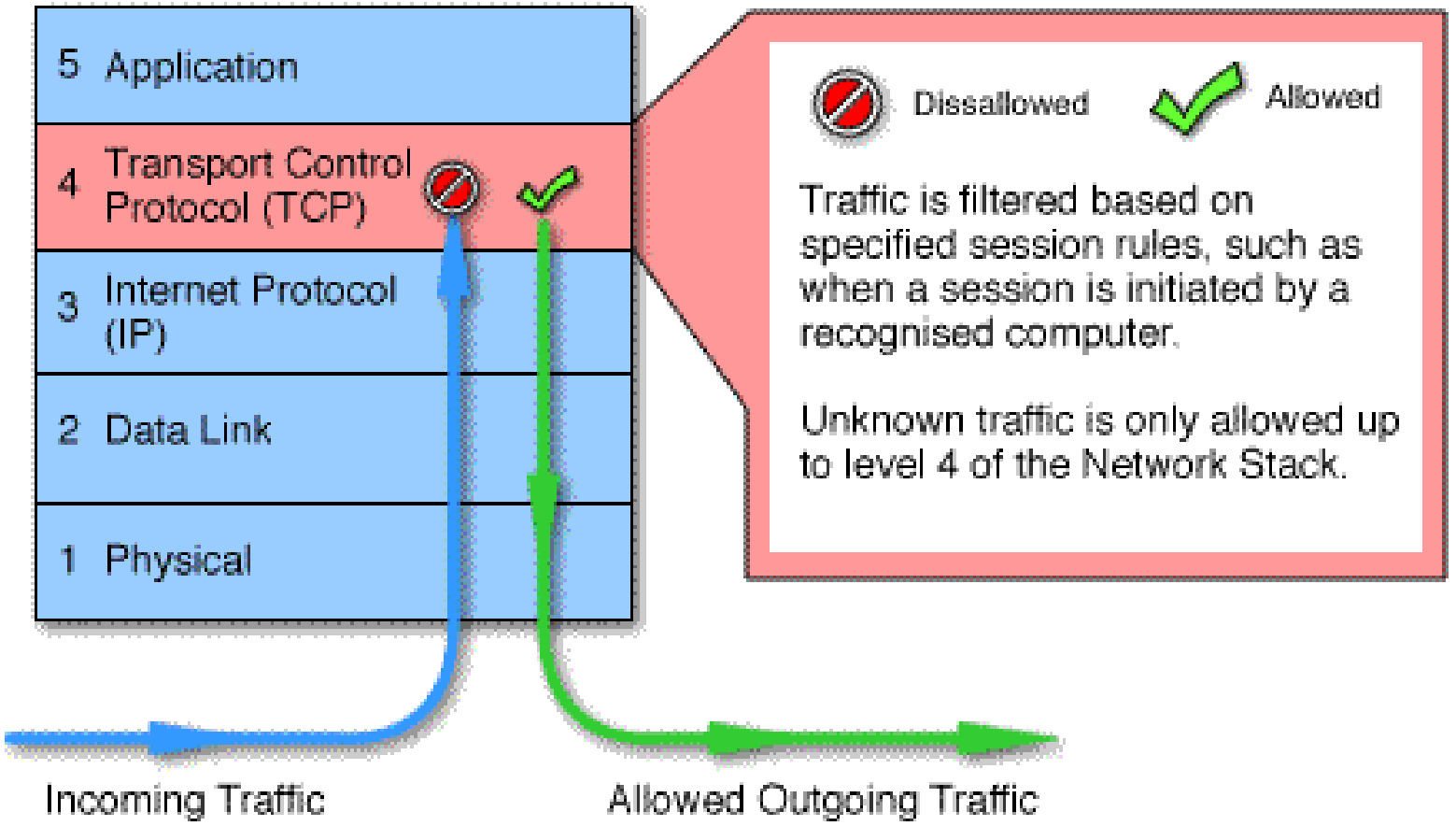
The most significant weakness is the impact they can have on performance. it requires more processing power and has the potential to become a bottleneck for the network.

Typically require additional client configuration. Clients on the network may require specialized software or configuration changes to be able to connect to the application gateway/proxy.

Circuit-level Gateway



Circuit-level Gateway



Circuit-level Gateway

Circuit-level Gateway

- Unlike a packet filtering firewall, a circuit-level gateway does not examine individual packets. Instead, circuit-level gateways monitor TCP or UDP sessions.
- Once a session has been established, it leaves the port open to allow all other packets belonging to that session to pass. The port is closed when the session is terminated.
- circuit-level gateways operate at the transport layer (layer 4) of the OSI model.

Circuit-level Gateway

- The security function consists of determining which connections will be allowed
- Typically use is a situation in which the system administrator trusts the internal users

Firewall Configurations

In addition to the use of simple configuration of a single system (single packet filtering router or single gateway), more complex configurations are possible

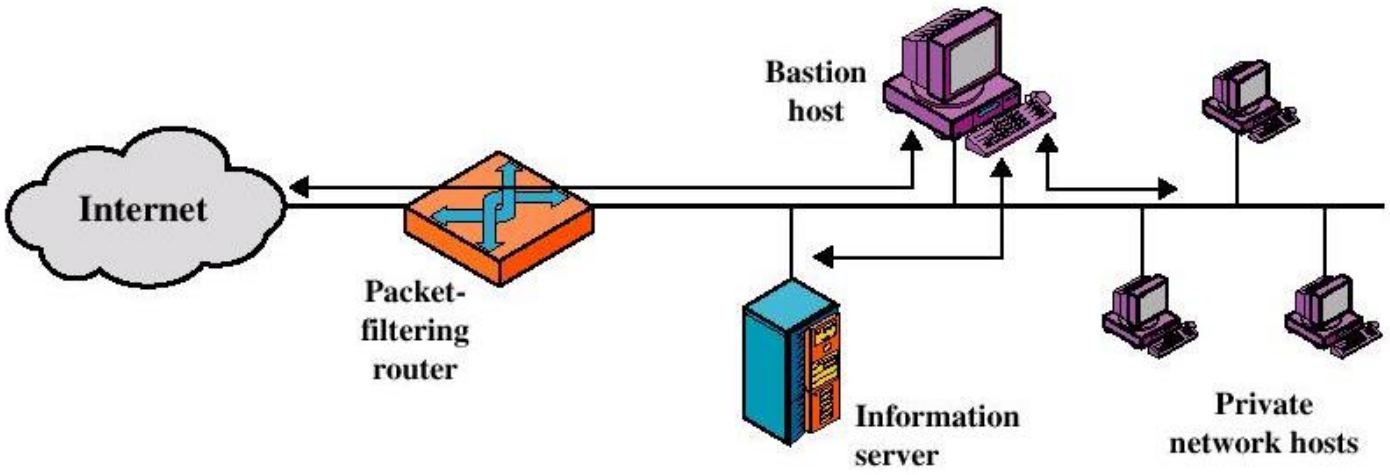
Three common configurations:

1. Screened host firewall system (single-homed bastion host)
2. Screened host firewall system (dual-homed bastion host)
3. Screened-subnet firewall system

bastion host

A **bastion host** is a special-purpose computer on a network specifically designed and configured to withstand attacks. The computer generally **hosts** a single application, for example a proxy server, and all other services are removed or limited to reduce the threat to the computer.

Screened host firewall system (single-homed bastion host)



Firewall Configurations

Screened host firewall, single-homed bastion configuration

Firewall consists of two systems:

- A packet-filtering router : allows Internet packets to/from bastion only
- A bastion host : performs authentication and proxy functions

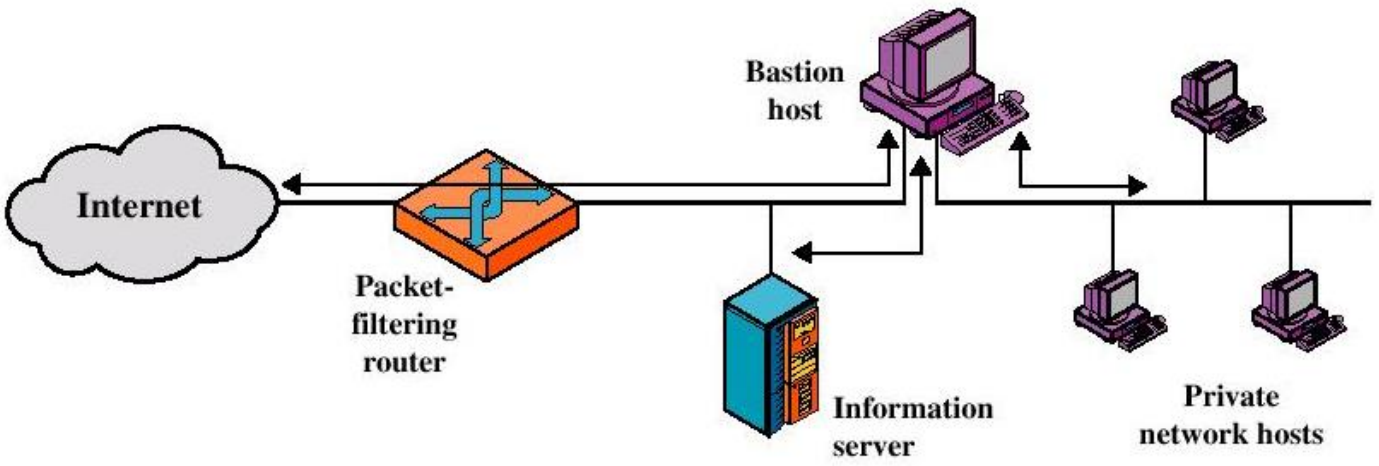
Firewall Configurations

Greater security than single configurations because of two reasons:

- This configuration implements both packet-level and application-level filtering (allowing for flexibility in defining security policy)
- An intruder must generally penetrate two separate systems

Firewall Configurations

Screened host firewall system (dual-homed bastion host)



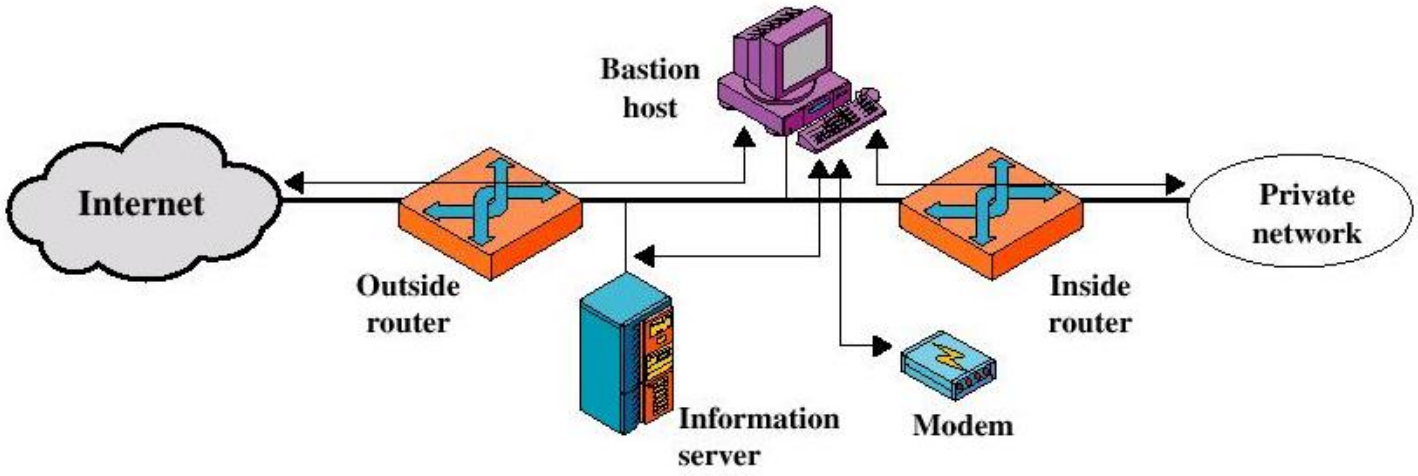
Firewall Configurations

Screened host firewall, dual-homed bastion configuration

- The packet-filtering router is not completely compromised
- Traffic between the Internet and other hosts on the private network has to flow through the bastion host

Firewall Configurations

Screened-subnet firewall system



Firewall Configurations

Screened subnet firewall configuration

- Most secure configuration of the three
- Two packet-filtering routers are used
- Creation of an isolated sub-network

Firewall Configurations

Advantages:

- Three levels of defense to thwart intruders
- The outside router advertises only the existence of the screened subnet to the Internet (internal network is invisible to the Internet)

Firewall Configurations

Advantages:

- The inside router advertises only the existence of the screened subnet to the internal network (the systems on the inside network cannot construct direct routes to the Internet)

Trusted Systems

One way to enhance the ability of a system to defend against intruders and malicious programs is to implement trusted system technology

Data Access Control

Through the user access control procedure (log on), a user can be identified to the system

Associated with each user, there can be a profile that specifies permissible operations and file accesses

The operation system can enforce rules based on the user profile

Data Access Control

General models of access control:

- Access matrix
- Access control list
- Capability list

Data Access Control

Access Matrix

	Program1	• • •	SegmentA	SegmentB
Process1	Read Execute		Read Write	
Process2				Read
•				
•				
•				

Data Access Control

Access Matrix: Basic elements of the model

- Subject: An entity capable of accessing objects, the concept of subject equates with that of process
- Object: Anything to which access is controlled (e.g. files, programs)
- Access right: The way in which an object is accessed by a subject (e.g. read, write, execute)

Data Access Control

Access Control List: Decomposition of the matrix by columns

Access Control List for Program1: Process1 (Read, Execute)
Access Control List for SegmentA: Process1 (Read, Write)
Access Control List for SegmentB: Process2 (Read)

Data Access Control

Access Control List

- An access control list lists users and their permitted access right
- The list may contain a default or public entry

Data Access Control

Capability list: Decomposition of the matrix by rows

Capability List for Process1:
Program1 (Read, Execute)
SegmentA (Read, Write)
Capability List for Process2:
SegmentB (Read)

Data Access Control

Capability list

- A capability ticket specifies authorized objects and operations for a user
- Each user have a number of tickets

The Concept of Trusted Systems

Trusted Systems

- Protection of data and resources on the basis of levels of security (e.g. military)
- Users can be granted clearances to access certain categories of data

The Concept of Trusted Systems

Multilevel security

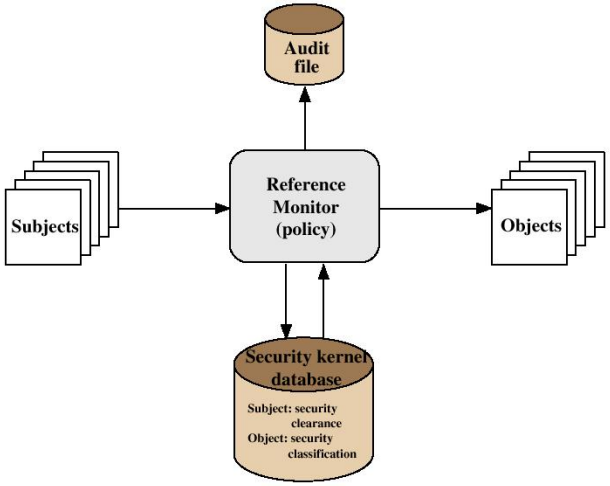
- Definition of multiple categories or levels of data

A multilevel secure system must enforce:

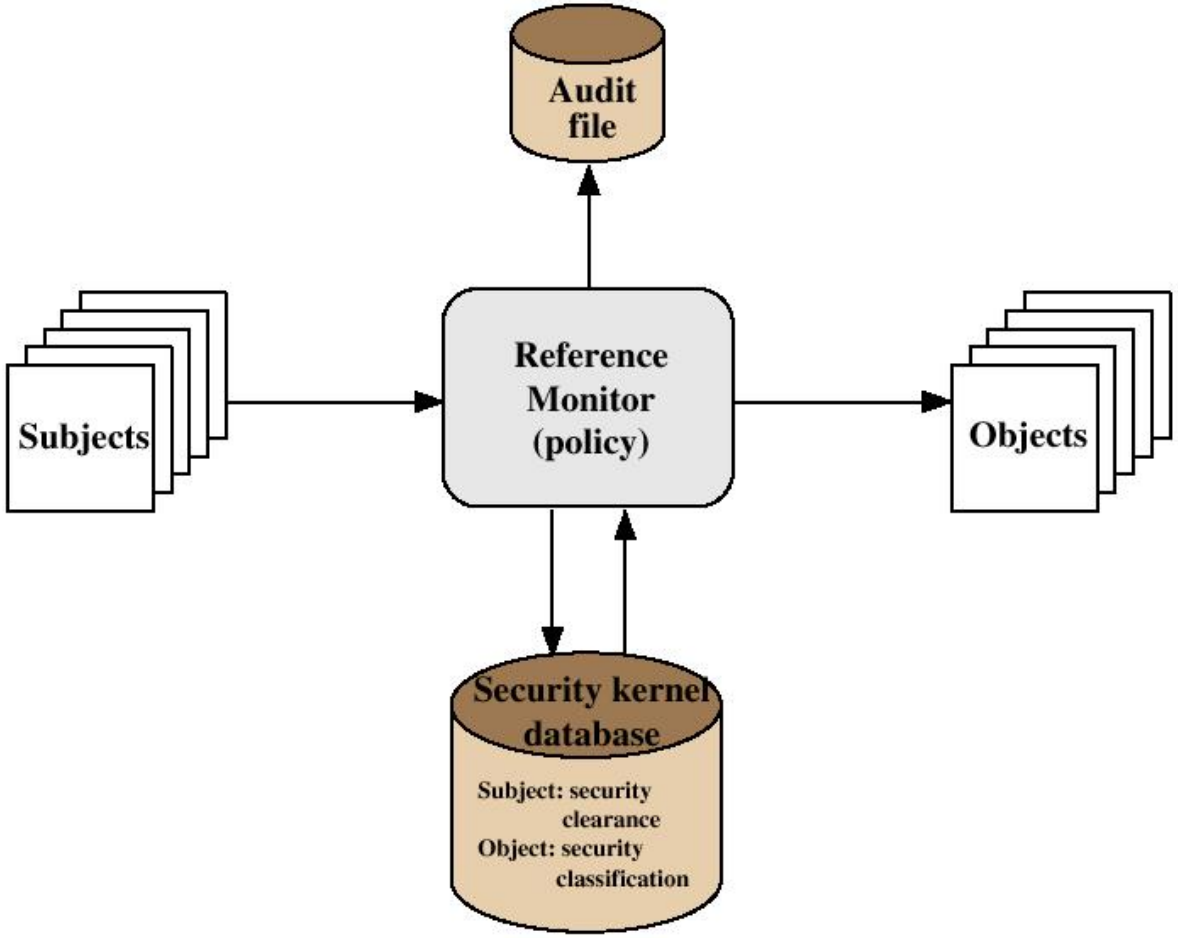
- No read up: A subject can only read an object of less or equal security level (Simple Security Property)
- No write down: A subject can only write into an object of greater or equal security level (*-Property)

The Concept of Trusted Systems

Reference Monitor Concept: Multilevel security for a data processing system



The Concept of Trusted Systems



The Concept of Trusted Systems

Reference Monitor

- Controlling element in the hardware and operating system of a computer that regulates the access of subjects to objects on basis of security parameters
- The monitor has access to a file (security kernel database)
- The monitor enforces the security rules (no read up, no write down)

The Concept of Trusted Systems

Properties of the Reference Monitor

- Complete mediation: Security rules are enforced on every access
- Isolation: The reference monitor and database are protected from unauthorized modification
- Verifiability: The reference monitor's correctness must be provable (mathematically)

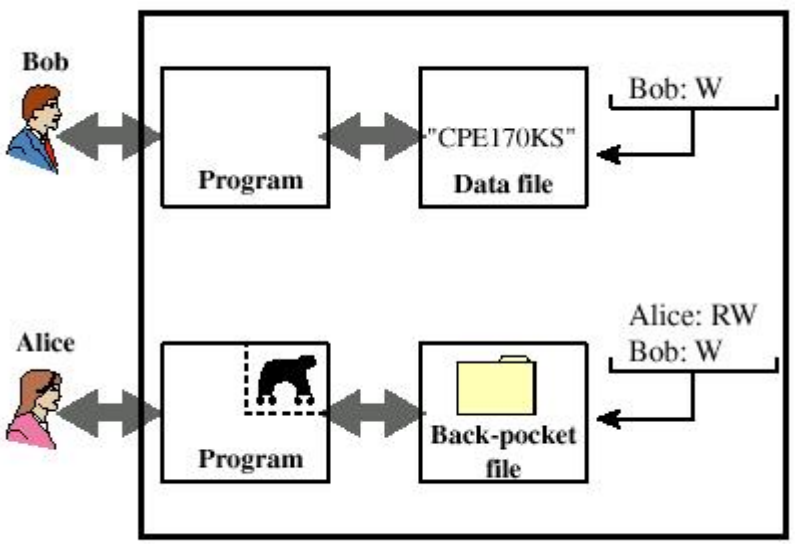
The Concept of Trusted Systems

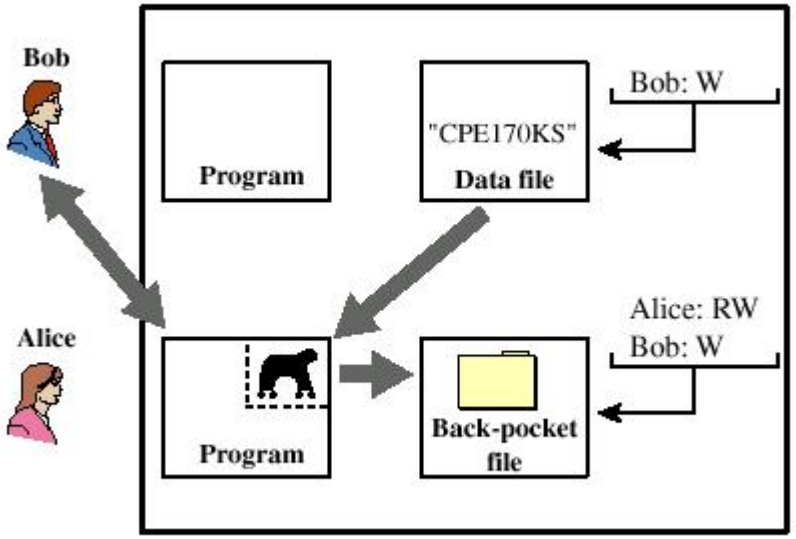
A system that can provide such verifications (properties) is referred to as a trusted system

Trojan Horse Defense

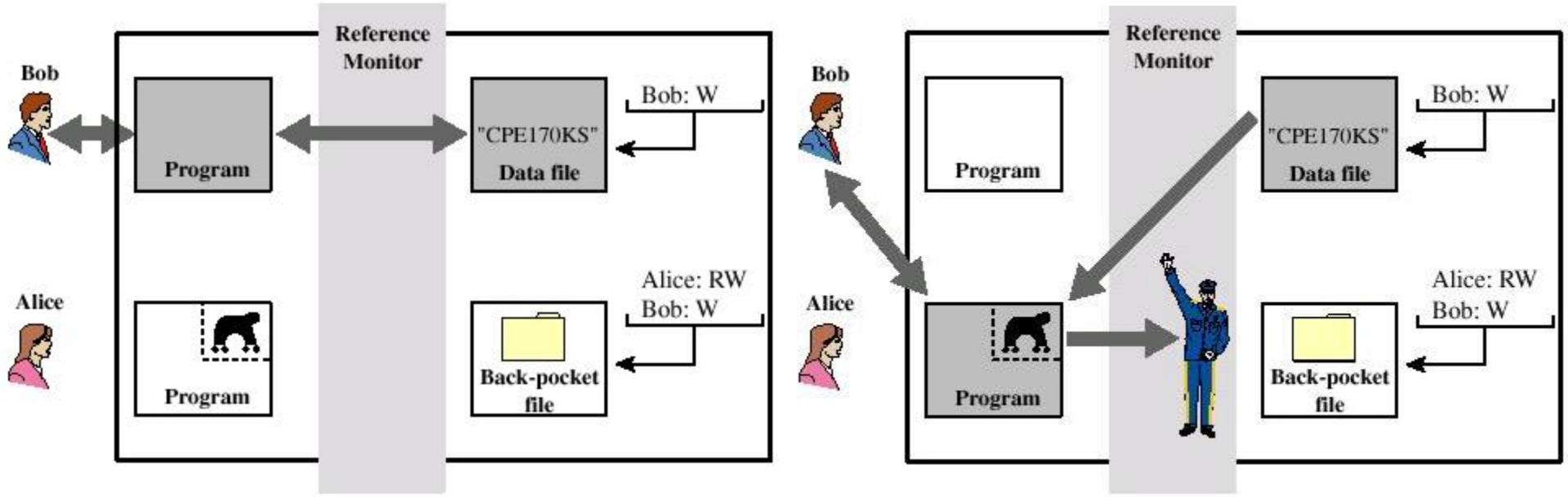
Secure, trusted operating systems are one way to secure against Trojan Horse attacks

Trojan Horse Defense





Trojan Horse Defense



Recommended Reading

Chapman, D., and Zwicky, E. Building Internet Firewalls. O'Reilly, 1995

Cheswick, W., and Bellovin, S. Firewalls and Internet Security: Repelling the Wily Hacker. Addison-Wesley, 2000

Gasser, M. Building a Secure Computer System. Reinhold, 1988

Pfleeger, C. Security in Computing. Prentice Hall, 1997