Chapter 11

Firewalls

Outline

- Firewall Design Principles
  - Firewall Characteristics
  - Types of Firewalls
  - Firewall Configurations
- Trusted Systems
  - Data Access Control
  - The Concept of Trusted systems
  - Trojan Horse Defense

Firewalls

- Effective means of protection for 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

Firewall Design Principles

- Information systems undergo a steady evolution (from small LAN`s to Internet connectivity)
- Strong security features for all workstations and servers are not established

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 outside to inside 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 policy) will be allowed to pass

Firewall Characteristics

- Design goals:
  - The firewall itself is immune to penetration .
    - Meaning use of trusted system with a secure operating system

Firewall Characteristics

❖Four general techniques:

- Service control
  - Determines the types of Internet services that can be accessed, inbound or outbound
  - May filter traffic on the basis of IP address and TCP port number; may provide proxy software; or host the server S/W itself, such as a Web or mail service
- Direction control
  - Determines the direction in which particular service requests are allowed to flow trough the Firewall

Firewall Characteristics

- 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; need authentication technique
- Behavior control
  - Controls how particular services are used (e.g. filter e-mail to eliminate spam), or it may enable external access to only a portion of the information on a local Web server

Types of Firewalls

- Three common types of Firewalls:
  - Packet-filtering routers
    - Using source/destination IP addresses and port # or Interface
  - Application-level gateways
  - Circuit-level gateways
  - (Bastion host)

Types of Firewalls

- Packet- or session-filtering router (filter)
- Proxy gateway
  - All incoming traffic is directed to firewall, all outgoing traffic appears to come from firewall
  - Application-level: separate proxy for each application
    - Different proxies for SMTP (email), HTTP, FTP, etc.
    - Filtering rules are application-specific
  - Circuit-level: application-independent, “transparent”
    - Only generic IP traffic filtering (example: SOCKS)
- Personal firewall with application-specific rules
  - E.g., no outbound telnet connections from email client

Packet Filtering

- For each packet, firewall decides whether to allow it to proceed
  - Decision must be made on per-packet basis
    - Stateless; cannot examine packet's context (TCP connection, application to which it belongs, etc.)
- To decide, use information available in the packet
  - IP source and destination addresses, ports
  - Protocol identifier (TCP, UDP, ICMP, etc.)
  - TCP flags (SYN, ACK, RST, PSH, FIN)
  - ICMP message type
- Filtering rules are based on pattern-matching

An Example: FTP Packet Filter

The following filtering rules allow a user to FTP from any IP address to the FTP server at 172.168.10.12

```
access-list 100 permit tcp any gt 1023 host 172.168.10.12 eq 21
access-list 100 permit tcp any gt 1023 host 172.168.10.12 eq 20
  ! Allows packets from any client to the FTP control and data ports
access-list 101 permit tcp host 172.168.10.12 eq 21 any gt 1023
access-list 101 permit tcp host 172.168.10.12 eq 20 any gt 1023
  ! Allows the FTP server to send packets back to any IP address with TCP ports > 1023

interface Ethernet 0
 access-list 100 in     ! Apply the first rule to inbound traffic
 access-list 101 out    ! Apply the second rule to outbound traffic
!
```

Anything not explicitly permitted by the access list is denied!

Packet Filtering Examples

A

action	ourhost	port	theirhost	port	comment
block	*	*	SPIGOT	*	we don't trust these people
allow	OUR-GW	25	*	*	connection to our SMTP port

B

action	ourhost	port	theirhost	port	comment
block	*	*	*	*	default

C

action	ourhost	port	theirhost	port	comment
allow	*	*	*	25	connection to their SMTP port

D

action	src	port	dest	port	flags	comment
allow	{our hosts}	*	*	25		our packets to their SMTP port
allow	*	25	*	*	ACK	their replies

E

action	src	port	dest	port	flags	comment
allow	{our hosts}	*	*	*		our outgoing calls
allow	*	*	*	*	ACK	replies to our calls
allow	*	*	*	>1024		traffic to nonservers

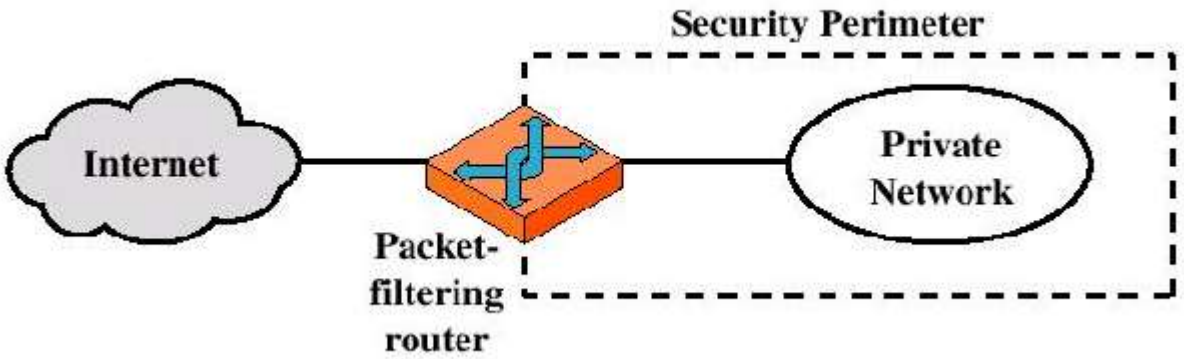
Example: Stateful Inspection Packet Filter

Table : Stateful Firewall Connection State Table

Source Address	Source Port	Destination Address	Destination Port	Connection State
192.168.1.100	1030	210.9.88.29	80	Established
192.168.1.102	1031	216.32.42.123	80	Established
192.168.1.101	1033	173.66.32.122	25	Established
192.168.1.106	1035	177.231.32.12	79	Established
223.43.21.231	1990	192.168.1.6	80	Established
219.22.123.32	2112	192.168.1.6	80	Established
210.99.212.18	3321	192.168.1.6	80	Established
24.102.32.23	1025	192.168.1.6	80	Established
223.212.212	1046	192.168.1.6	80	Established

Types of Firewalls

- Packet-filtering Router



Types of Firewalls

- 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)

Types of Firewalls

- Advantages:
  - Simplicity
  - Transparency to users
  - High speed
- Disadvantages:
  - Difficulty of setting up packet filter rules
  - Lack of Authentication

Types of Firewalls

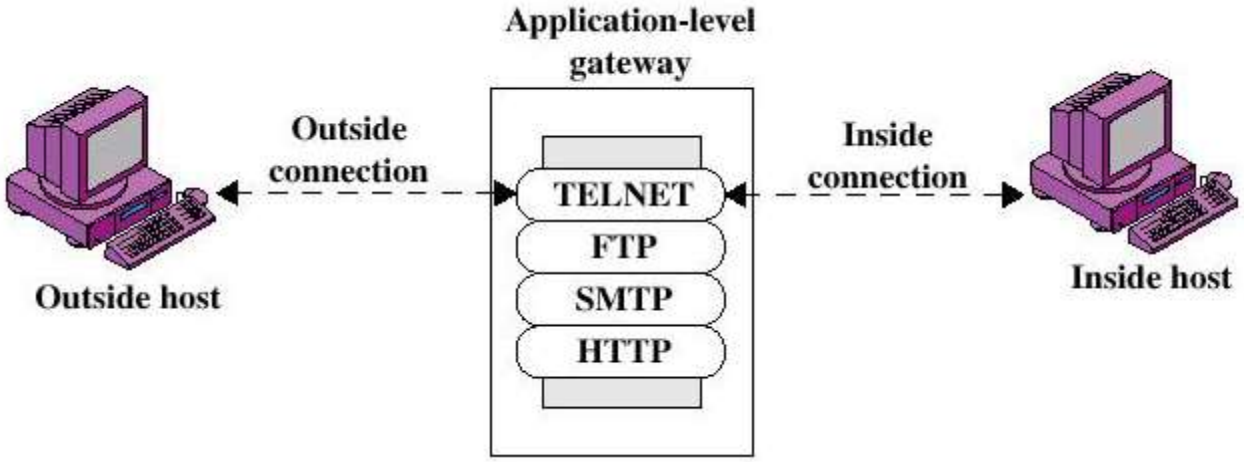
- Possible attacks and appropriate countermeasures
  - IP address spoofing
    - Ex) an address of an internal host
  - Source routing attacks
  - Tiny fragment attacks

Weaknesses of Packet Filters

- Do not prevent application-specific attacks
  - For example, if there is a buffer overflow in FTP server, firewall will not block an attack string
- No user authentication mechanisms
  - … except (spoofable) address-based authentication
  - Firewalls don't have any upper-level functionality
- Vulnerable to TCP/IP attacks such as spoofing
  - Solution: list of addresses for each interface (packets with internal addresses shouldn't come from outside)
- Security breaches due to misconfiguration

Types of Firewalls

- Application-level Gateway



Types of Firewalls

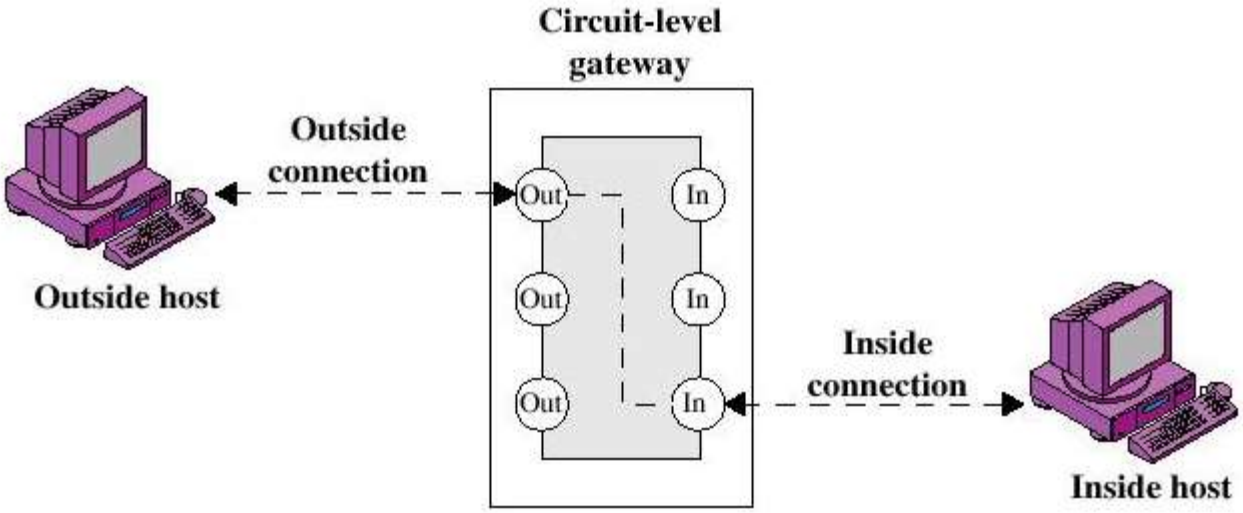
- Application-level Gateway
  - Also called proxy server
  - Acts as a relay of application-level traffic

Types of Firewalls

- Advantages:
  - Higher security than packet filters
  - Only need to scrutinize a few allowable applications
  - Easy to log and audit all incoming traffic
- Disadvantages:
  - Additional processing overhead on each connection (gateway as splice point)

Types of Firewalls

- Circuit-level Gateway



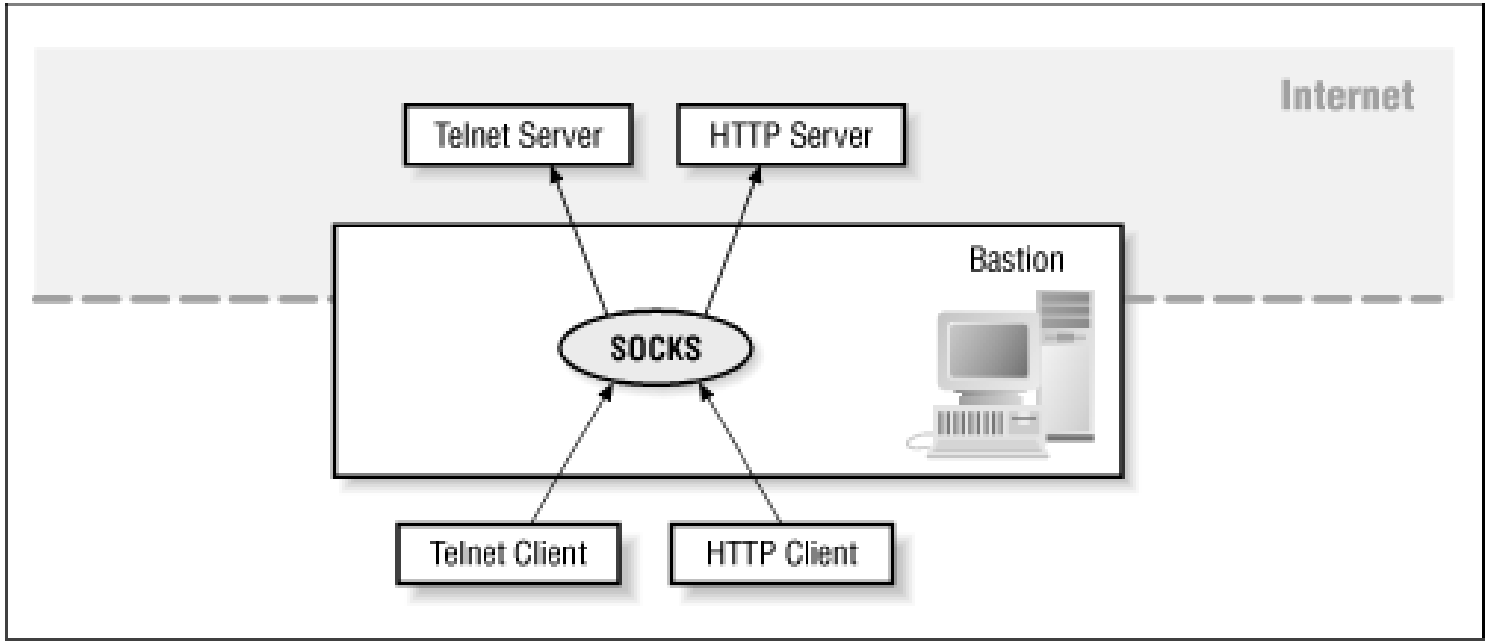
Types of Firewalls

- Circuit-level Gateway
  - Stand-alone system or
  - Specialized function performed by an Application-level Gateway
  - Sets up two TCP connections
  - The gateway typically relays TCP segments from one connection to the other without examining the contents

Types of Firewalls

- 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
  - An example is the SOCKS package

SOCKS for Proxying



Types of Firewalls

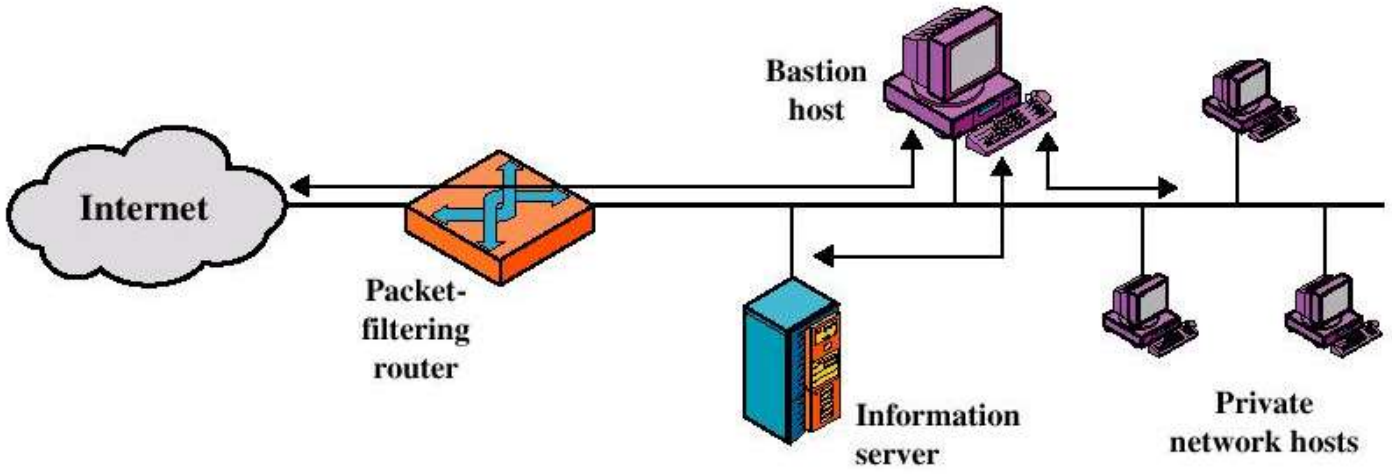
- Bastion Host
  - A system identified by the firewall administrator as a critical strong point in the network´s security
  - The bastion host serves as a platform for an application-level or circuit-level gateway

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

Firewall Configurations

- 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
  - A bastion host

Firewall Configurations

- Configuration for the packet-filtering router:
  - Only packets from and to the bastion host are allowed to pass through the router
- The bastion host performs authentication and proxy functions

Firewall Configurations

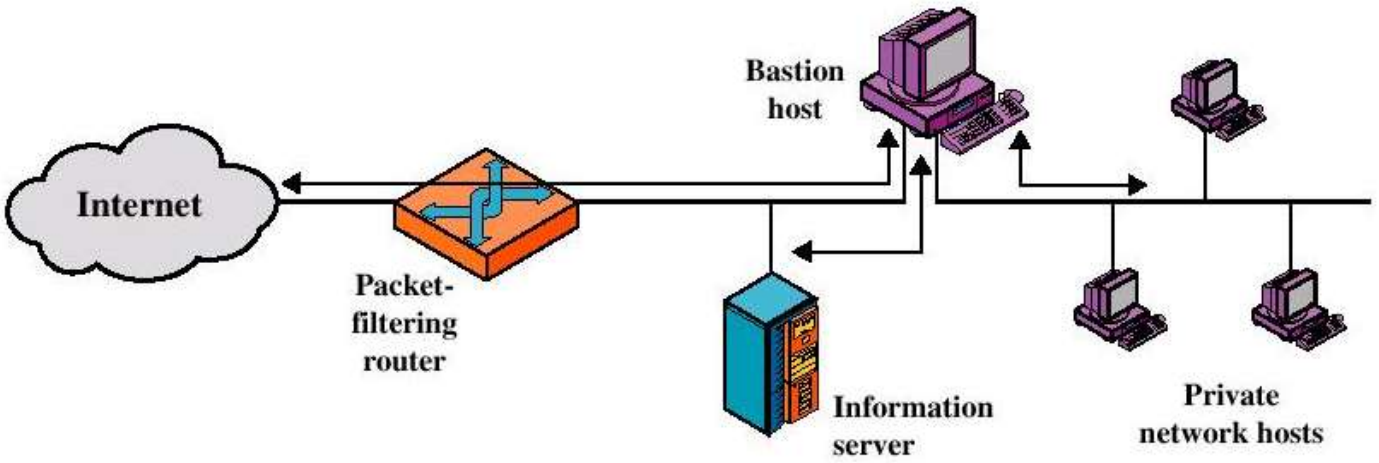
- Greater security than single configuration because of two reasons:
  - This configuration implements both packet-level and application-level filtering (allowing for flexibility in defining security policy)
  - An intruder must generally penetrate two separate systems

Firewall Configurations

- This configuration also affords flexibility in providing direct Internet access (public information server, e.g. Web server)

Firewall Configurations

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

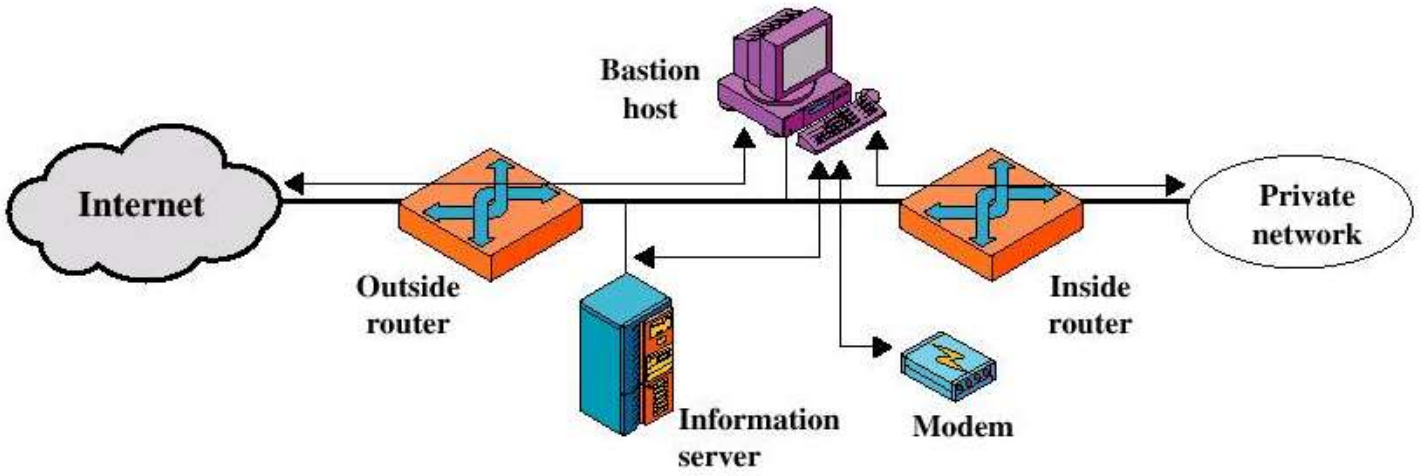


Firewall Configurations

- 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

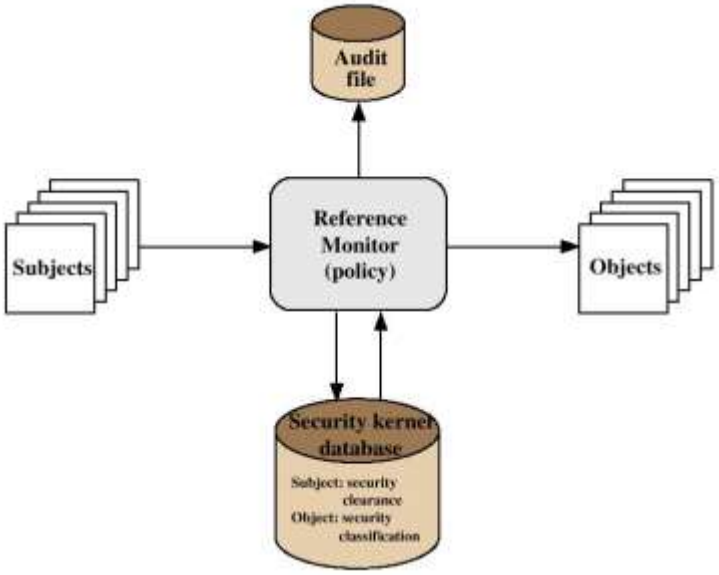
- Trusted Systems
  - Protection of data and resources on the basis of levels of security (e.g. military)
    - U: unclassified
    - C: confidential
    - S: secret
    - TS: to secret
    - beyond
  - Users can be granted clearances to access certain categories of data

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

- 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 about enforcing security rule and providing complete mediation and isolation (mathematically)

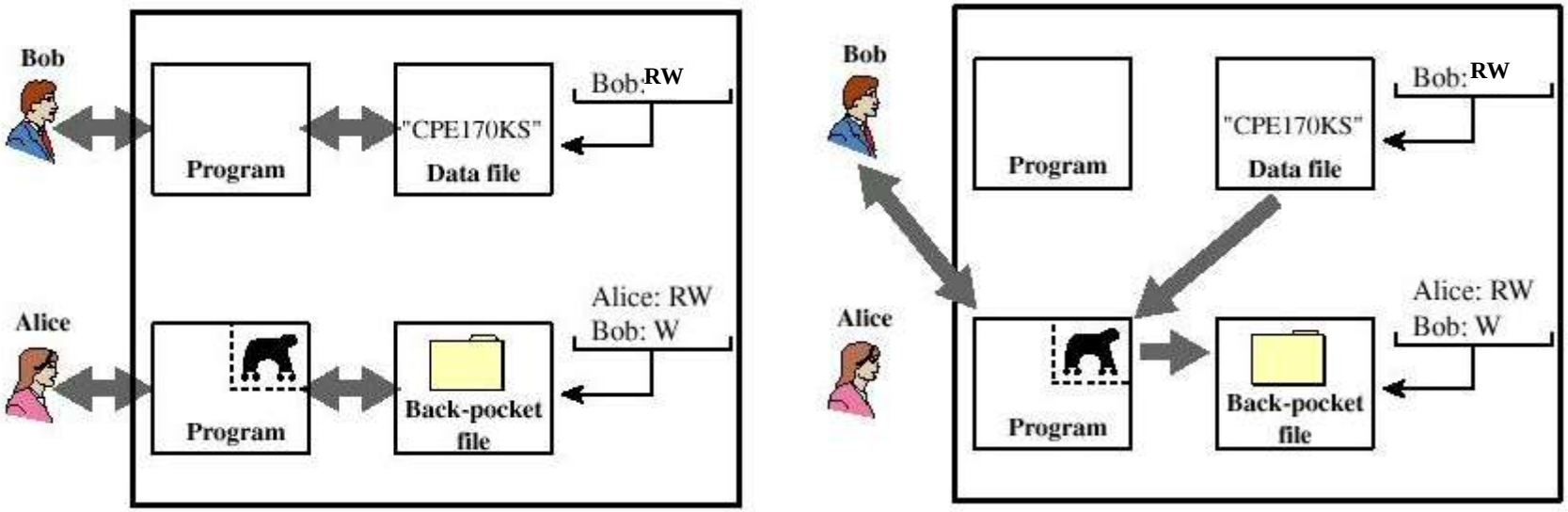
The Concept of Trusted Systems

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

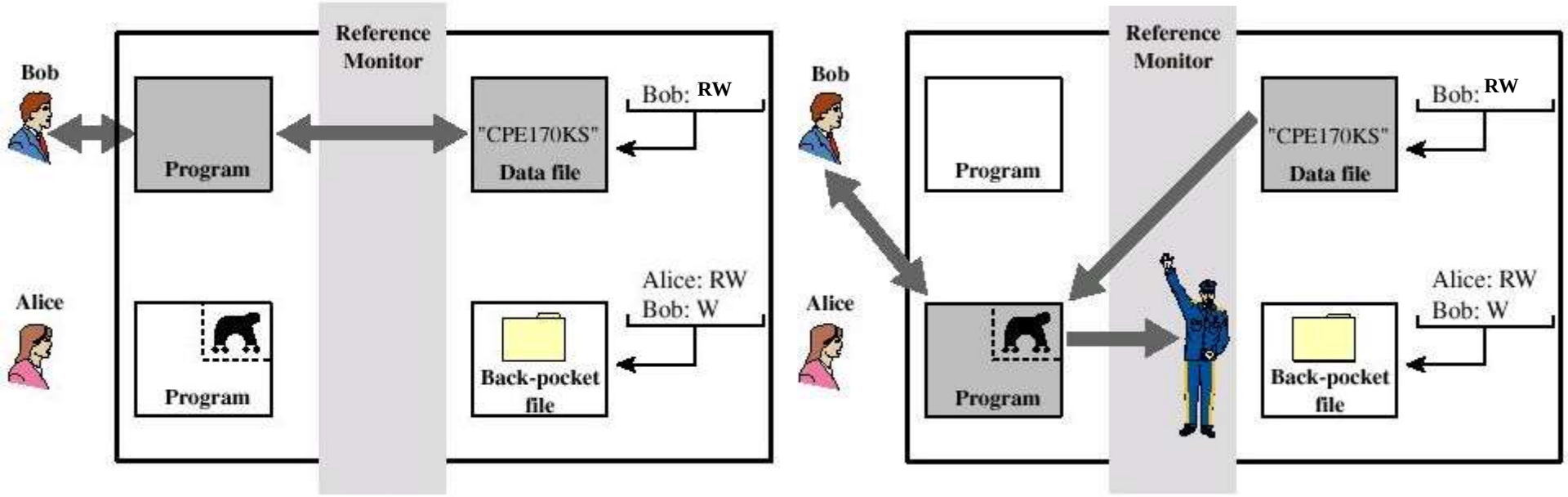
Trojan Horse Defense

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

Trojan Horse Defense



Trojan Horse Defense



Summary

- 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.
- A firewall may be designed to operate as a filter at the level of IP packets, or may operate at a higher protocol layer.
- A trust system is a computer and operating system that can be verified to implement a given security policy. Typically, the focus of a trusted system is access control.
- The common criteria for information technology security is an international standards initiative to define a common set of security requirements and a systematic means of evaluating products against those requirements.