M6L4

Firewalls

Information technology department

Computer network Security-ITC 502

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 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 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 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

- Design goals:
  - The firewall itself is immune to penetration (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
- Direction control
  - Determines the direction in which particular service requests are allowed to flow

Firewall Characteristics

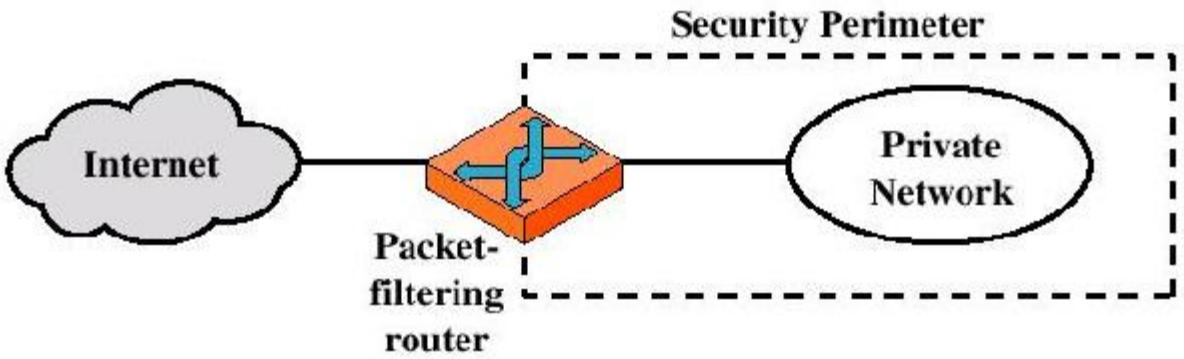
- User control
  - Controls access to a service according to which user is attempting to access it
- Behavior control
  - Controls how particular services are used (e.g. filter e-mail)

Types of Firewalls

- Three common types of Firewalls:
  - Packet-filtering routers
  - Application-level gateways
  - Circuit-level gateways
  - (Bastion host)

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

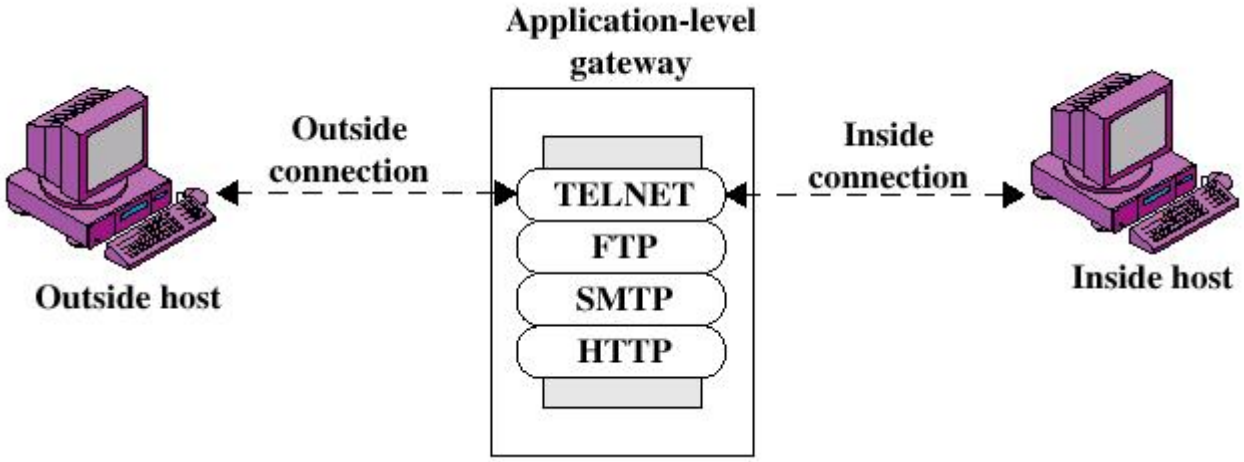
- Advantages:
  - Simplicity
  - Transparency to users
  - High speed
- Disadvantages:
  - Difficulty of setting up packet filter rules
  - Lack of Authentication

Types of Firewalls

- Possible attacks and appropriate countermeasures
  - IP address spoofing
  - Source routing attacks
  - Tiny fragment attacks

Types of Firewalls

- Application-level Gateway



Types of Firewalls

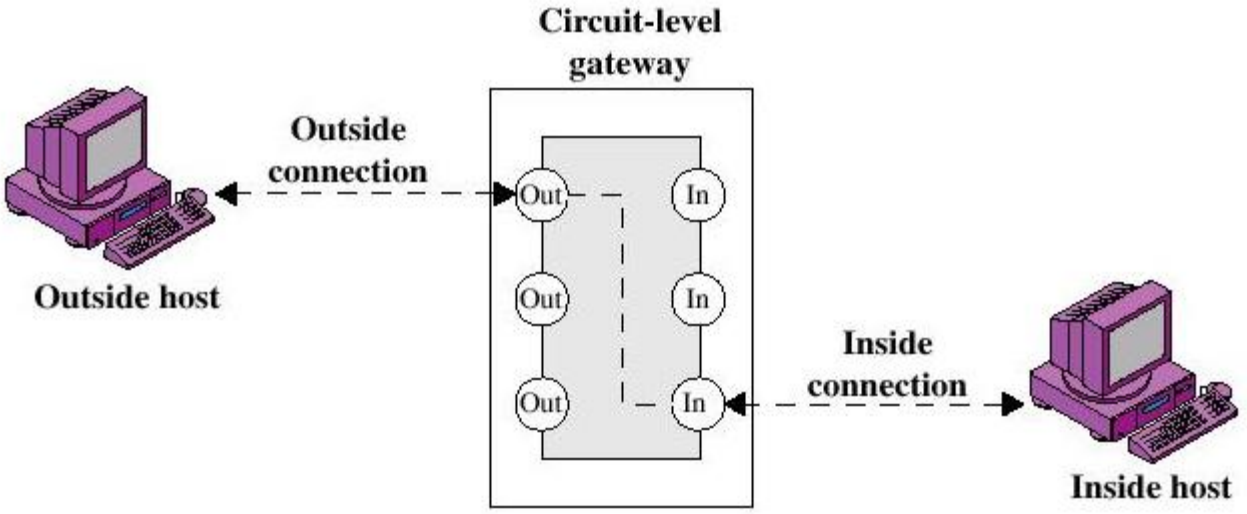
- Application-level Gateway
  - Also called proxy server
  - Acts as a relay of application-level traffic

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

Types of Firewalls

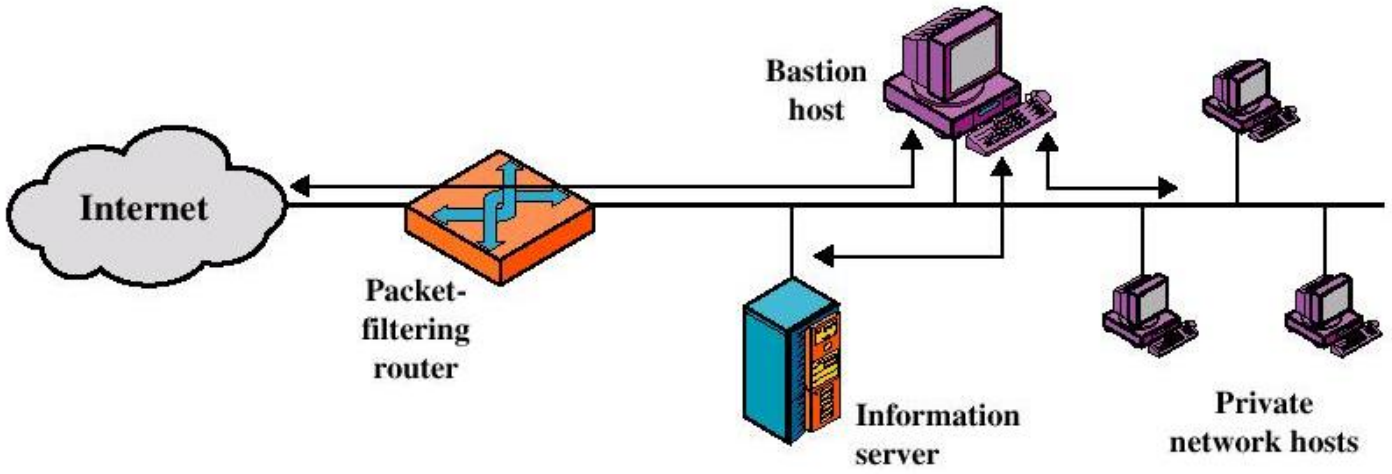
- Bastion Host
  - A system identified by the firewall administrator as a critical strong point in the network´s security
  - The bastion host serves as a platform for an application-level or circuit-level gateway

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

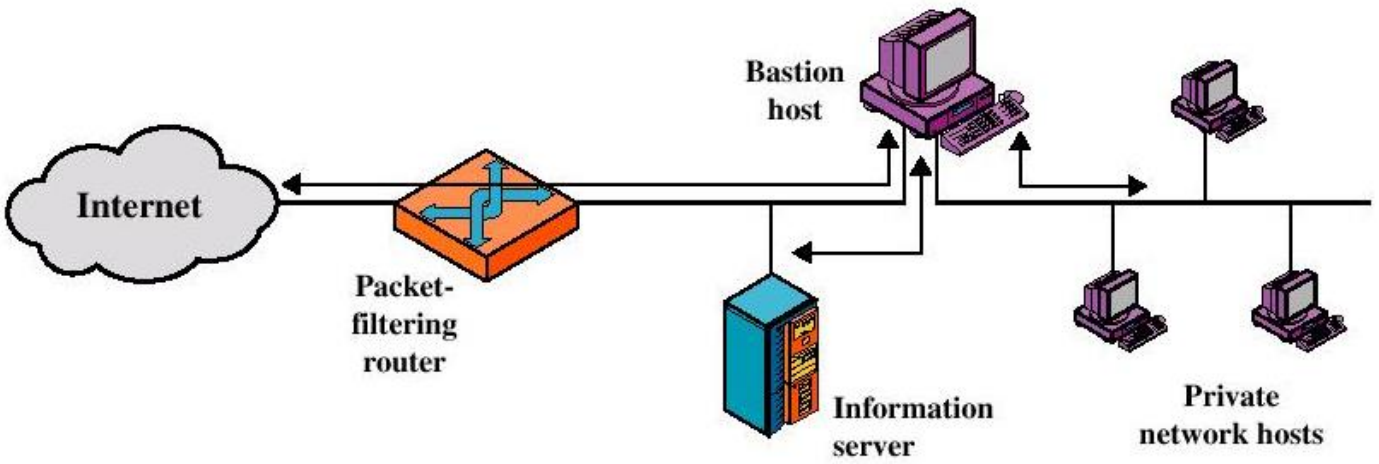
- Greater security than single configurations because of two reasons:
  - This configuration implements both packet-level and application-level filtering (allowing for flexibility in defining security policy)
  - An intruder must generally penetrate two separate systems

Firewall Configurations

- 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)

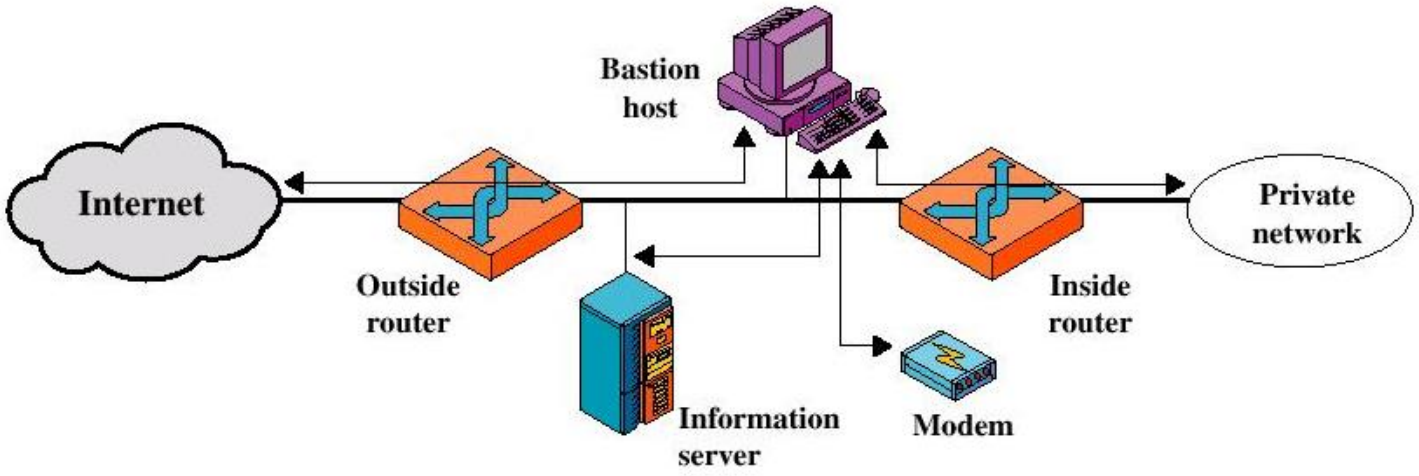


Firewall Configurations

- 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

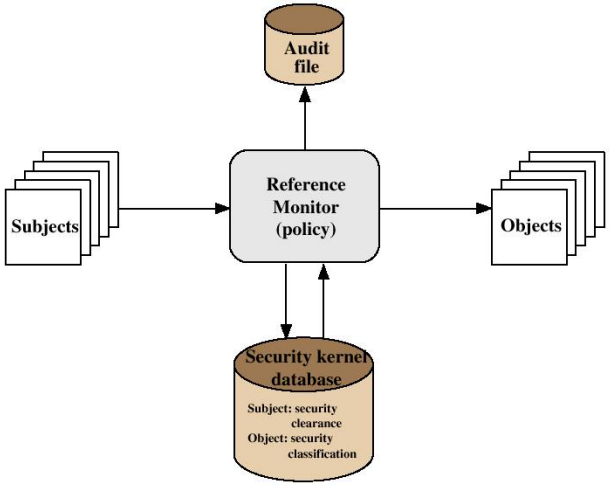
- Trusted Systems
  - Protection of data and resources on the basis of levels of security (e.g. military)
  - Users can be granted clearances to access certain categories of data

The Concept of Trusted Systems

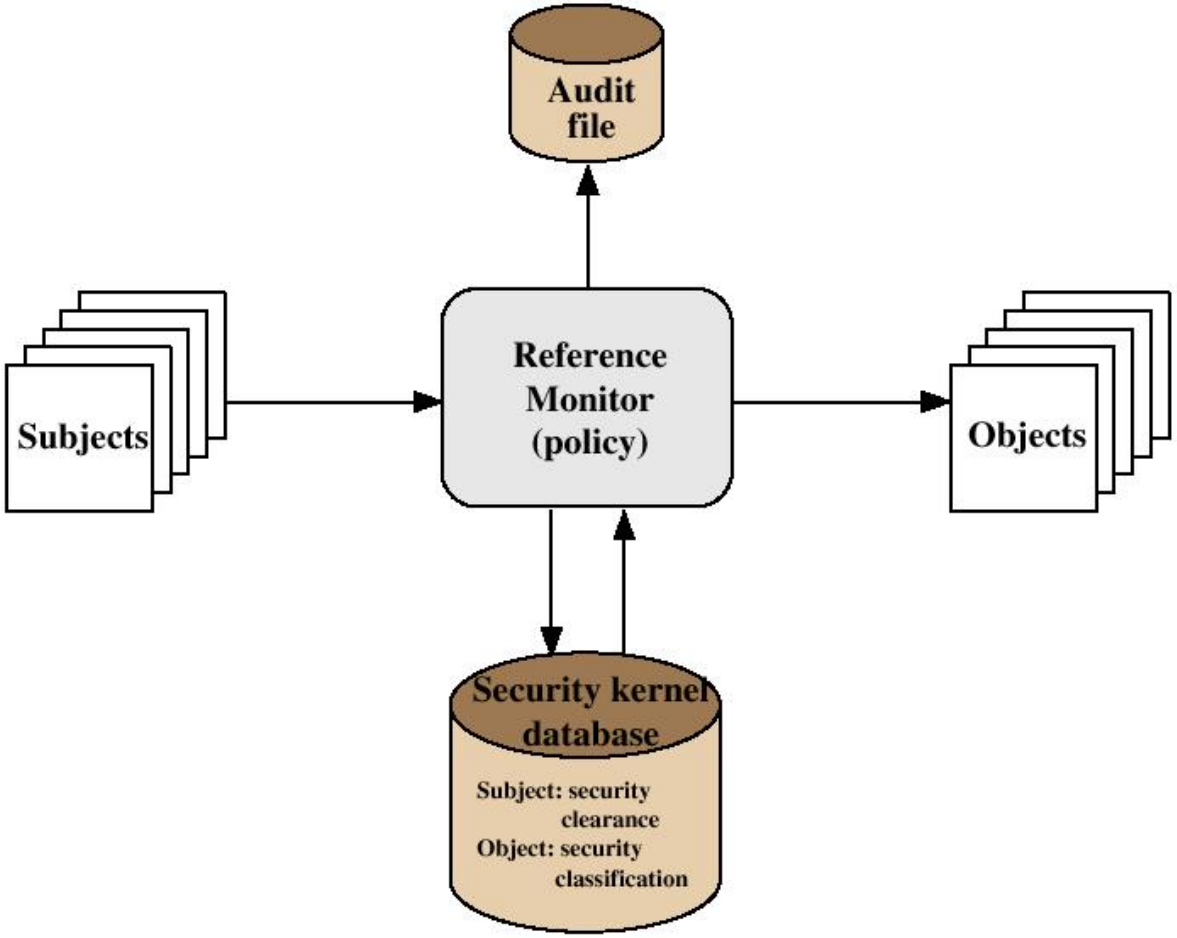
- Multilevel security
  - Definition of multiple categories or levels of data
- A multilevel secure system must enforce:
  - No read up: A subject can only read an object of less or equal security level (Simple Security Property)
  - No write down: A subject can only write into an object of greater or 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)

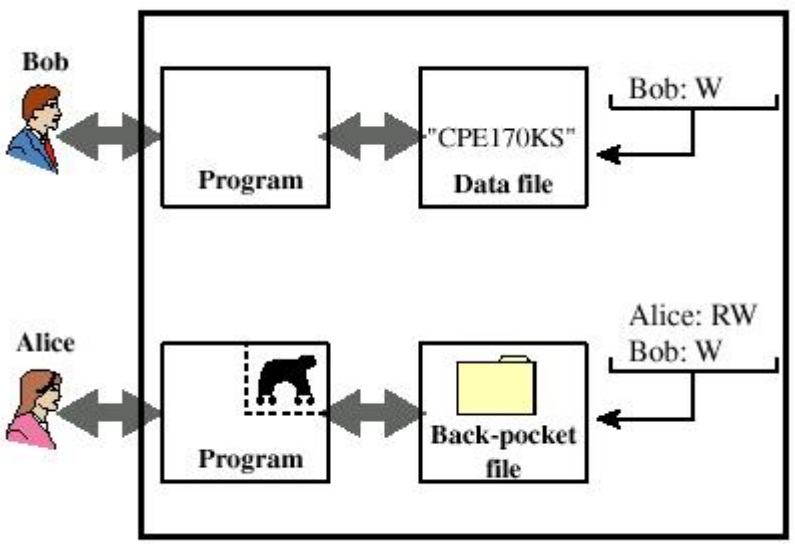
The Concept of Trusted Systems

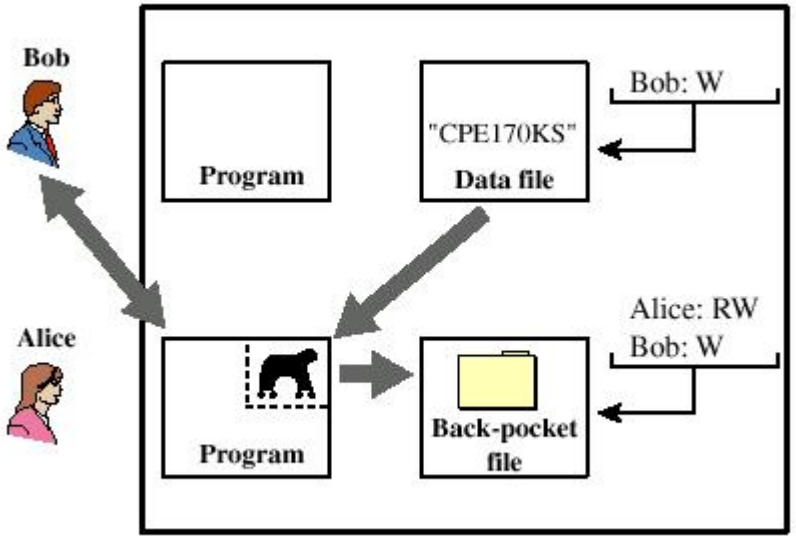
- A system that can provide such verifications (properties) is referred to as a trusted system

Trojan Horse Defense

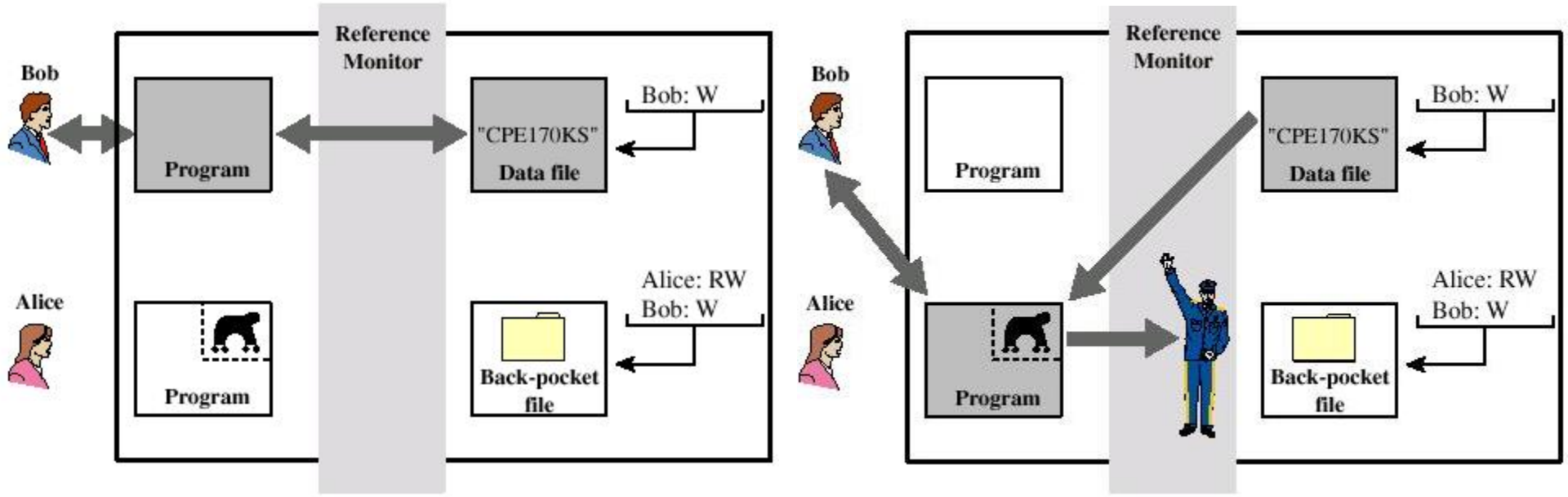
- Secure, trusted operating systems are one way to secure against Trojan Horse attacks

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