# Network Security

Asim Rasheed

# Where we are …

- Introduction to network security
- Vulnerabilities in IP
- I. CRYPTOGRAPHY
  - Symmetric Encryption and Message Confidentiality
  - Public-Key Cryptography and Message Authentication
- II. NETWORK SECURITY APPLICATIONS
  - Authentication Applications (Kerberos, X.509)
  - Electronic Mail Security (PGP, S/MIME)
  - IP Security (IPSec, AH, ESP, IKE)
  - Web Security (SSL, TLS, SET)
- III. SYSTEM SECURITY
  - Intruders and intrusion detection
  - Malicious Software (viruses)
  - Firewalls and trusted systems

# Firewalls

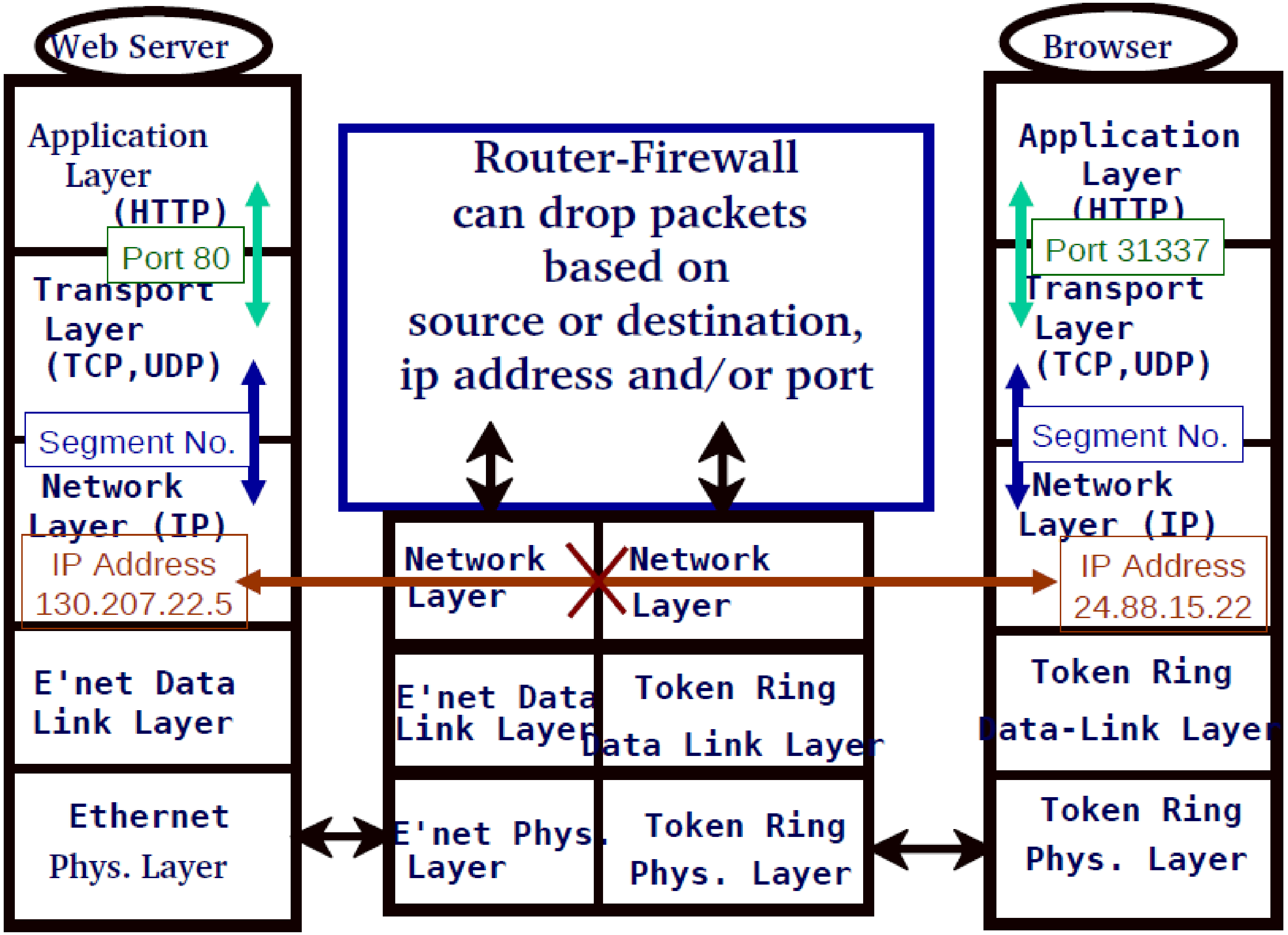
# Introduction

- Everyone wants to be on the Internet
- And to interconnect networks
- Such connectivity has persistent security concerns
  - can’t easily secure every system in organization
- Need "harm minimization"
- **Firewall is usually part of this**

# What is a Firewall?

- Any device, software, or arrangement or equipment that limits network access
- 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
- Is itself immune to penetration
- Provides **perimeter defense**

# Firewall


Web Server
Application Layer (HTTP)
Port 80
Transport Layer (TCP,UDP)
Segment No.
Network Layer (IP)
IP Address 130.207.22.5
E'net Data Link Layer
Ethernet Phys. Layer
Router-Firewall can drop packets based on source or destination, ip address and/or port
Network Layer
Network Layer
E'net Data Link Layer
Token Ring Data Link Layer
E'net Phys. Layer
Token Ring Phys. Layer
Browser
Application Layer (HTTP)
Port 31337
Transport Layer (TCP,UDP)
Segment No.
Network Layer (IP)
IP Address 24.88.15.22
Token Ring Data-Link Layer
Token Ring Phys. Layer

# Firewall Characteristics

- All traffic must pass through it
  - No other point of entrance
- Only authorized traffic must be allowed to pass
  - As defined by the local security policy
- Immune to penetration
  - Use trusted system with a secure OS

# Firewall Control Access

- Service control
  - Types of Internet services that can be accessed
  - Both inbound and outbound
  - May filter traffic on the basis of IP addresses
- Direction control
  - Direction in which particular service request may be initiated
- User control
  - Controls access to service that user is trying to use
  - Applied to users inside the firewall
  - May be applied to incoming traffic

# Firewall Control Access…

- Behavior control
  - Controls how particular services are used
  - e.g., may filter email to eliminate spam

# Firewall Capabilities

- Defines a single choke point that keeps unauthorized users out of protected network
- Provides a location for monitoring security-related events
- Convenient platform for several Internet functions that are not security related events
- Can serve as the platform for IPSec

# Firewall Limitations

- Cannot protect from attacks bypassing it
  - e.g., sneaker net, utility modems, trusted organizations, trusted services (eg SSL/SSH)
- Cannot protect against internal threats
  - e.g., disgruntled employee
- Cannot protect against transfer of virus infected programs or files
  - Because of huge range of O/S & file types

# General Firewall Configuration

## Policy

- No outside Web access.
- Outside connections to Public Web Server Only.
- Prevent Web-Radios from eating up the available bandwidth.
- Prevent your network from being used for a Smuft DoS attack.
- Prevent your network from being tracerouted or Ping scanned.

## Firewall Setting

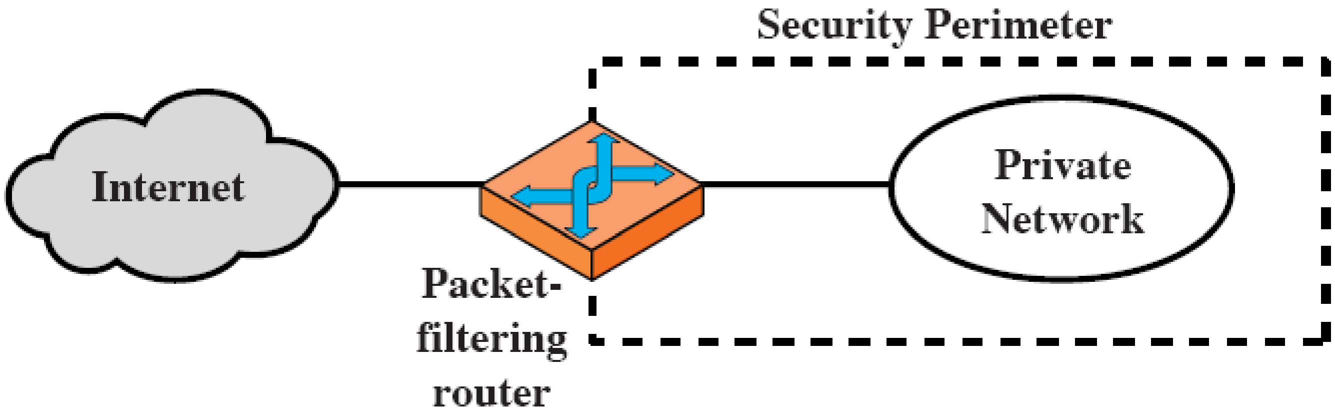
- Drop all outgoing packets to any IP, Port 80
- Drop all incoming TCP SYN packets to any IP except 130:207:244.203, port 80
- Drop all incoming UDP packets – except DNS and Router Broadcasts.
- Drop all ICMP packets going to a “broadcast” address (130.207.255.255 or 130.207.0.0)
- Drop all incoming ICMP, UDP, or TCP echo-request packets, drop all packets with TTL < 5.

# Types of Firewalls

- Packet-Filtering Router
- Application-level Gateways
- Circuit-level Gateways

- Characterized by protocol level it controls in packet filtering, circuit gateways, and application gateways
- Combination of above is dynamic packet filter

# Firewalls – Packet Filters



# Firewalls – Packet Filters

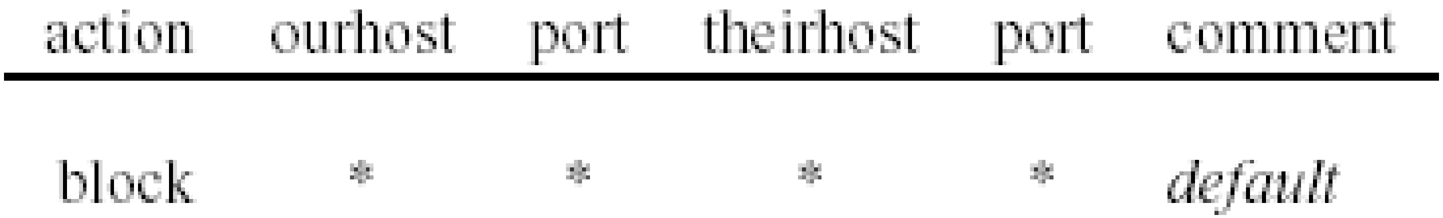
- Apply a set of rules to each incoming packet
- Cheap, useful level of gateway security
  - Filtering abilities come with router software
- Foundation of any firewall system
- Drop packets based on contents
- Incoming or outgoing interfaces
- Blocks spoofed packets
  - Ingress and egress filtering

# Packet Filters

- Permits or denies certain services
  - Requires intimate knowledge of TCP and UDP port utilization on a number of operating systems
- Possible default policies
  - That is not expressly permitted is prohibited
  - That is not expressly prohibited is permitted

# Default Behavior

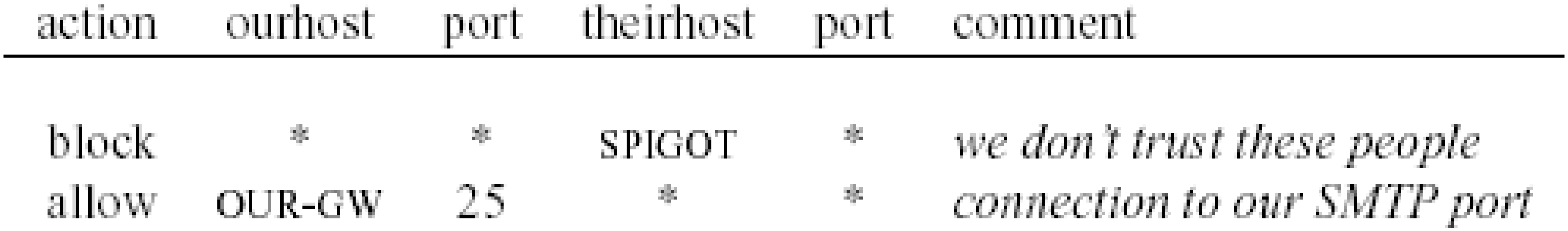
- Every rule set is followed by an implicit rule reading like this.



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

# Example 1:

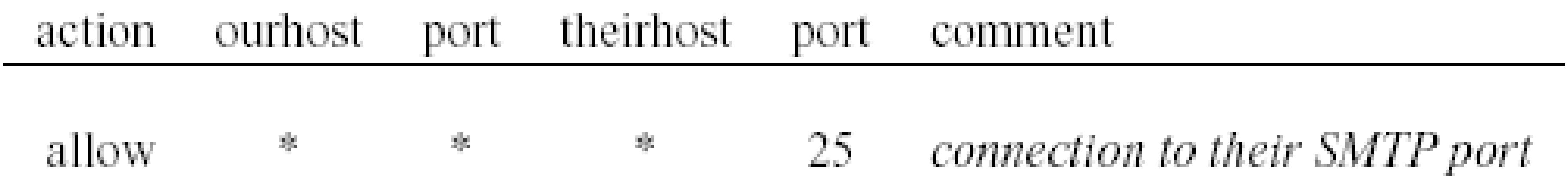
- Suppose we want to allow inbound mail (SMTP, port 25) but only to our gateway machine.
- Also suppose that mail from some particular site SPIGOT is to be blocked.



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

# Example 2:

- Now suppose that we want to implement the policy “any inside host can send mail to the outside”



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

# Solution

- This solution allows calls to come from any port on an inside machine, and will direct them to port 25 on the outside.

Simple enough…

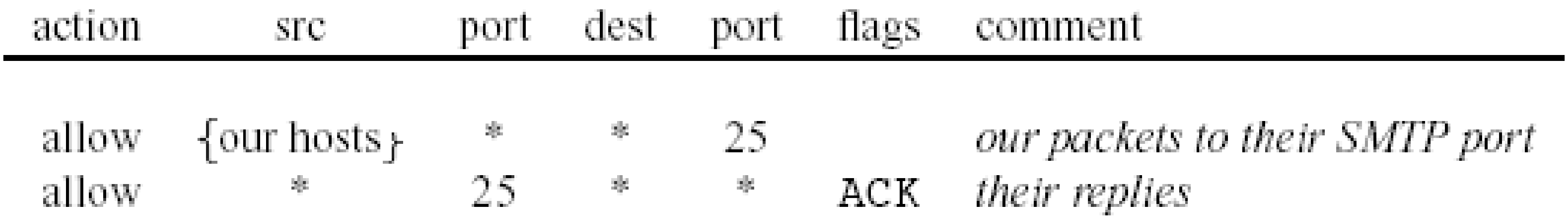
So is it wrong?

# Solution

- Our defined rule restricts solely the outside host’s port number, which we have no way of controlling.
- Now an enemy can access any internal machine and port by originating his call from port 25 on the outside machine.

Now for a better solution…

# Solution



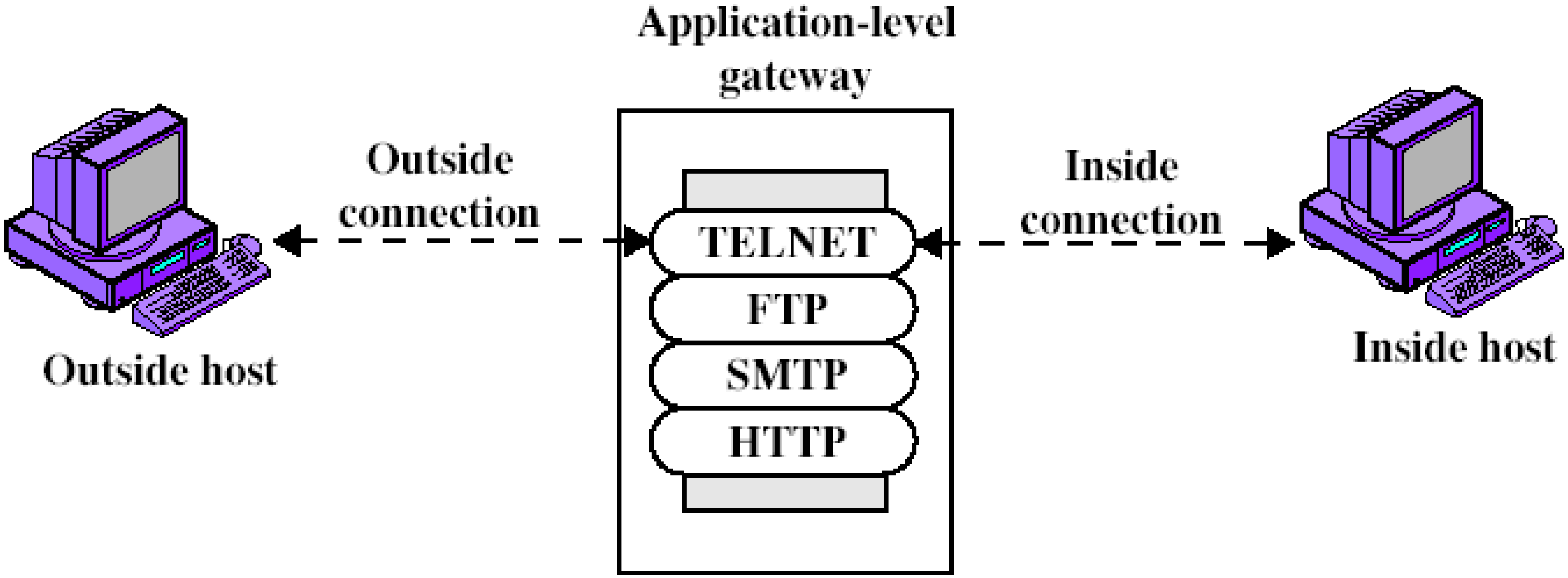
| action | src | port | dest | port | flags | comment |
|---|---|---|---|---|---|---|
| allow | {our hosts} | * | * | 25 | | *our packets to their SMTP port* |
| allow | * | 25 | * | * | ACK | *their replies* |

- The ACK signifies that the packet is part of an ongoing conversation
- Packets without the ACK are connection establishment messages, which we are only permitting from internal hosts

# Attacks on Packet Filters

- 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

# Firewalls - Application Level Gateway (or Proxy)



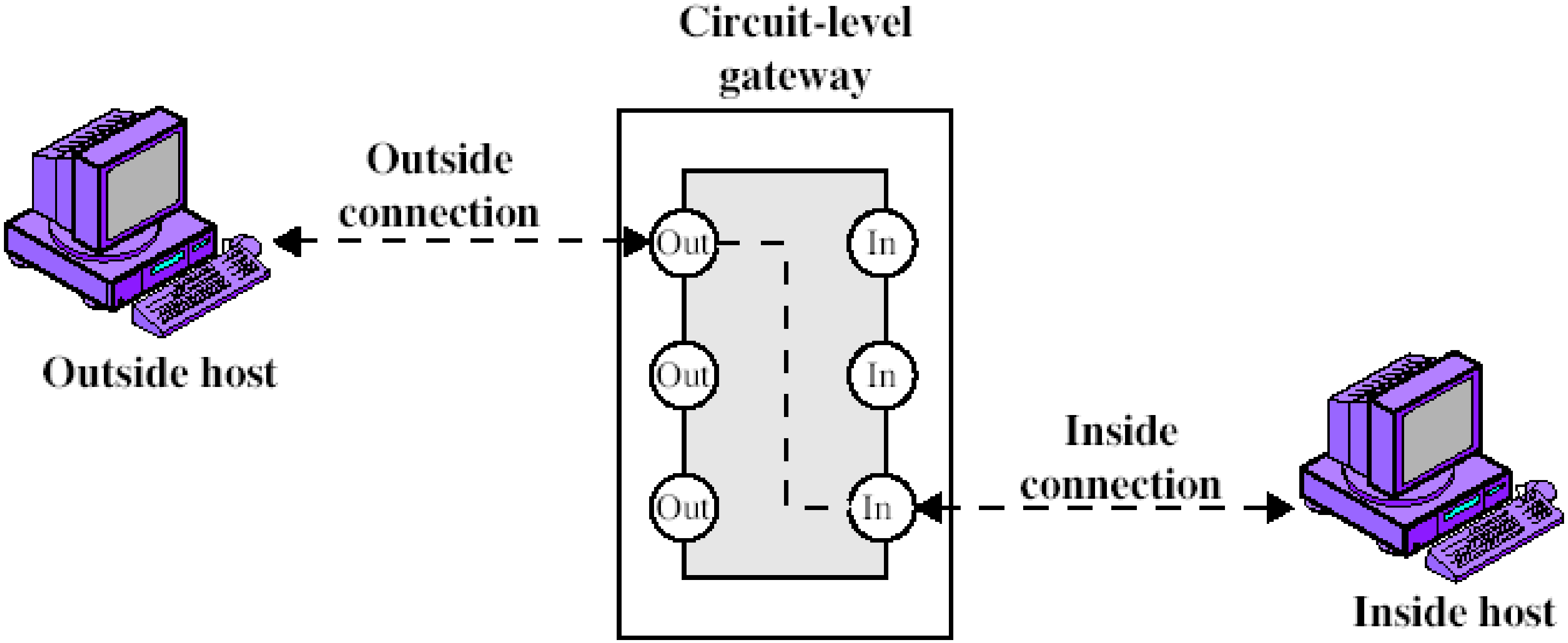
# Application-Level Filtering

- More complex than packet filtering – details
- Special-purpose code for each desired application
- Easy to log and control ALL incoming and outgoing traffic
- Only deals with attacks from outside
- Principal disadvantage
  - Need for specialized user program or variant user interface

# Firewalls - Application Level Gateway (or Proxy)

- Has full access to protocol
  - User requests service from proxy
  - Proxy validates request as legal
  - Then actions request and returns result to user
- Need separate proxies for each service
  - Some services naturally support proxying
  - Others are more problematic
  - Custom services generally not supported

# Firewalls - Circuit Level Gateway

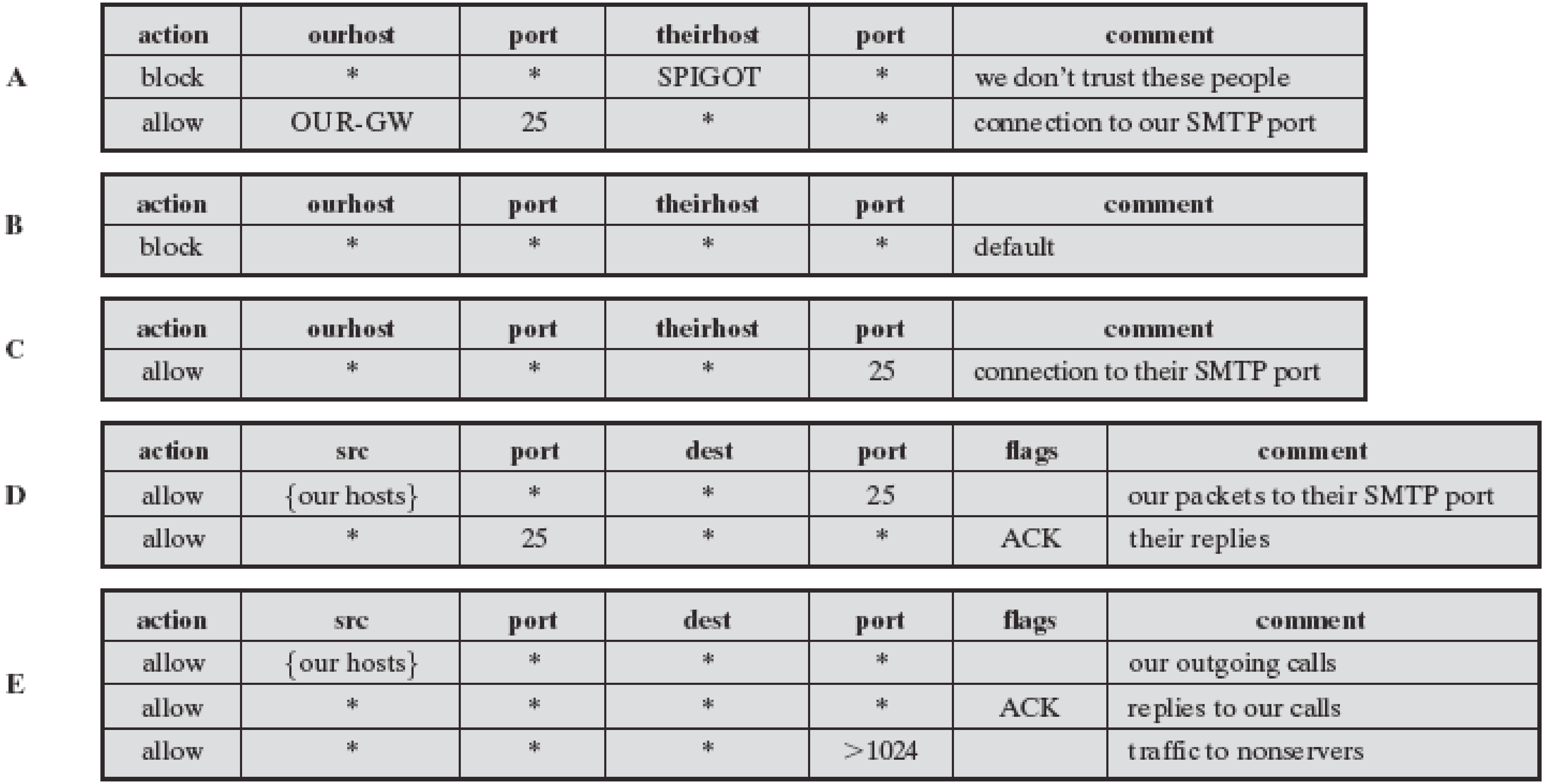


# Circuit-Level Gateways

- Work at TCP level
- Generally used to create specific connections between isolated networks
- SOCKS protocol – used in relay service
- Log the byte flow
  - Can’t catch all abuses, packet filter should be used
- Well suited for some UDP applications
- Once created usually relays traffic without examining contents
- Typically used when trust internal users by allowing general outbound connections

# Packet Filtering Example

Table 20.1 Packet-Filtering Examples



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

| | action | ourhost | port | theirhost | port | comment |
|---|---|---|---|---|---|---|
| B | block | * | * | * | * | default |

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

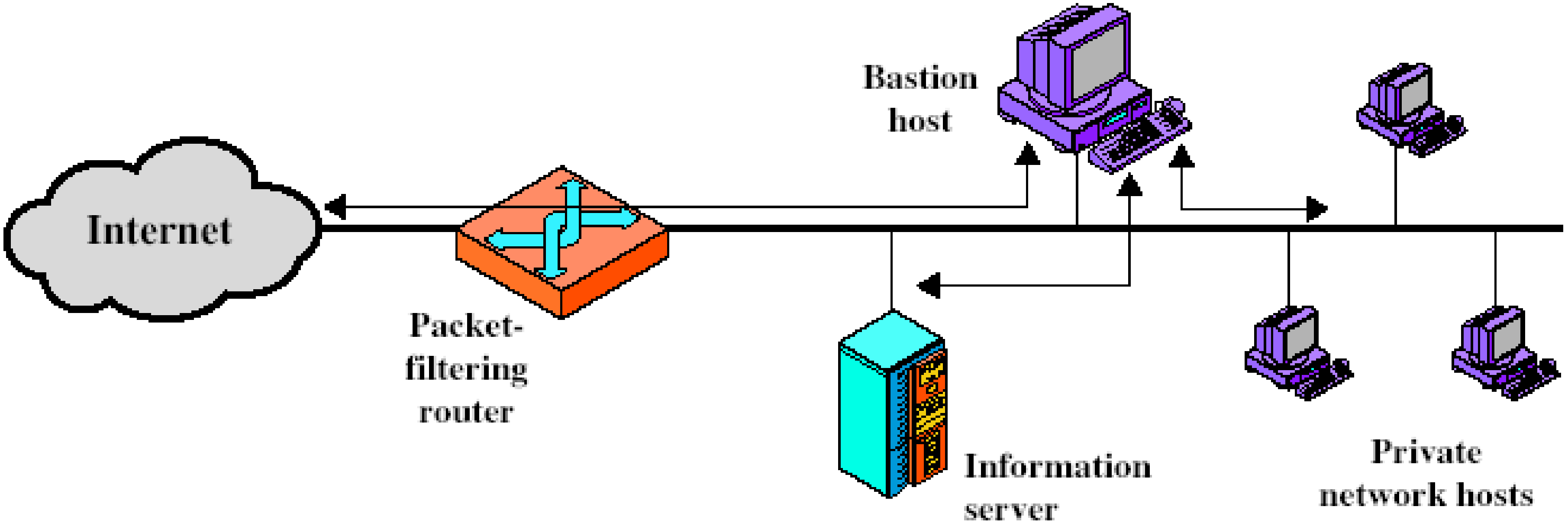
| | action | src | port | dest | port | flags | comment |
|---|---|---|---|---|---|---|---|
| D | allow | {our hosts} | * | * | 25 | | our packets to their SMTP port |
| | allow | * | 25 | * | * | ACK | their replies |

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

# Bastion Host

- Highly secure host system
- Potentially exposed to "hostile" elements
- Hence is secured to withstand this
- May support 2 or more net connections
- May be trusted to enforce trusted separation between network connections
- Runs circuit/application level gateways
- Or provides externally accessible services

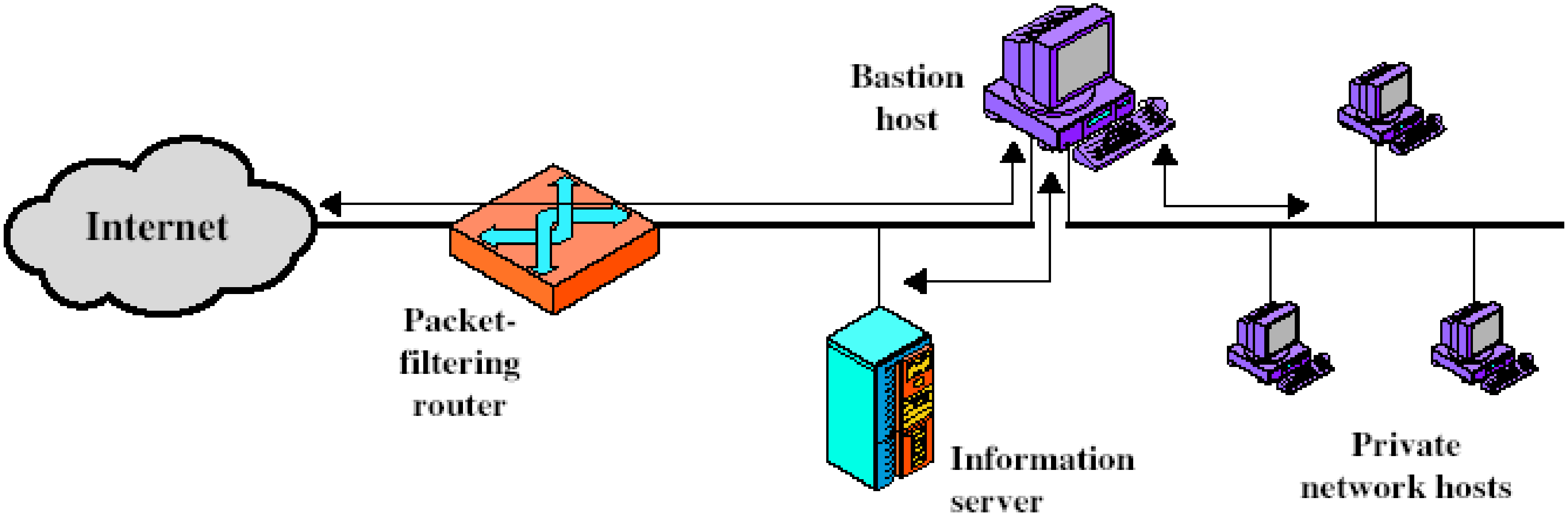
# Screened Host Firewall-Single Homed Bastion Host



# Screened Host Firewall- Single Homed Bastion Host

- Firewall consists of two systems
  - Packet filtering router
  - Bastion host
- Only IP packets destined for the bastion host are allowed in
- Only IP packets from the bastion host are allowed out
- Disadvantage:
  - If packet filtering router is compromised, traffic could flow directly

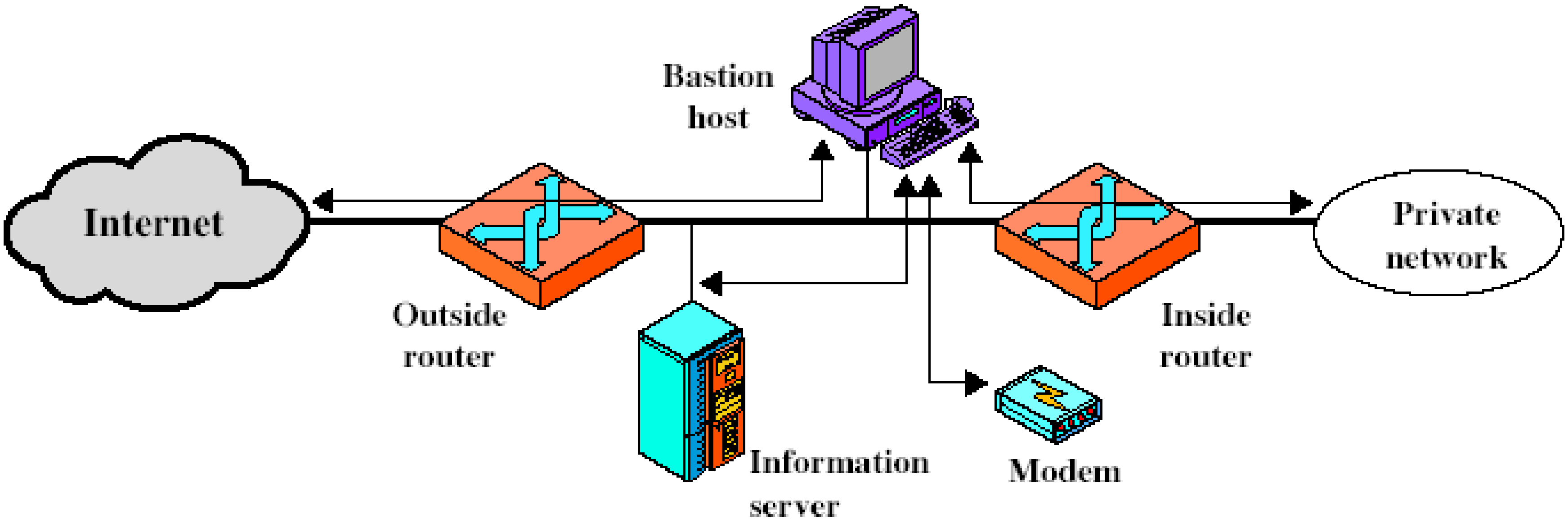
# Screened Host Firewall- Dual Homed Bastion Host



# Screened Host Firewall-
# Dual Homed Bastion Host

- Dual layers of security also present here
- Overcomes the threat of single point of failure

# Screened Subnet Firewall



# Screened Subnet Firewall

- Most secure configuration
- Two packet filtering routers
  - One b/w the bastion host and the Internet
  - One b/w the bastion host and the internal network
- Creates an isolated subnet, which may consist of:
  - Bastion host
  - One or more information servers
  - Modem for dial-in capability

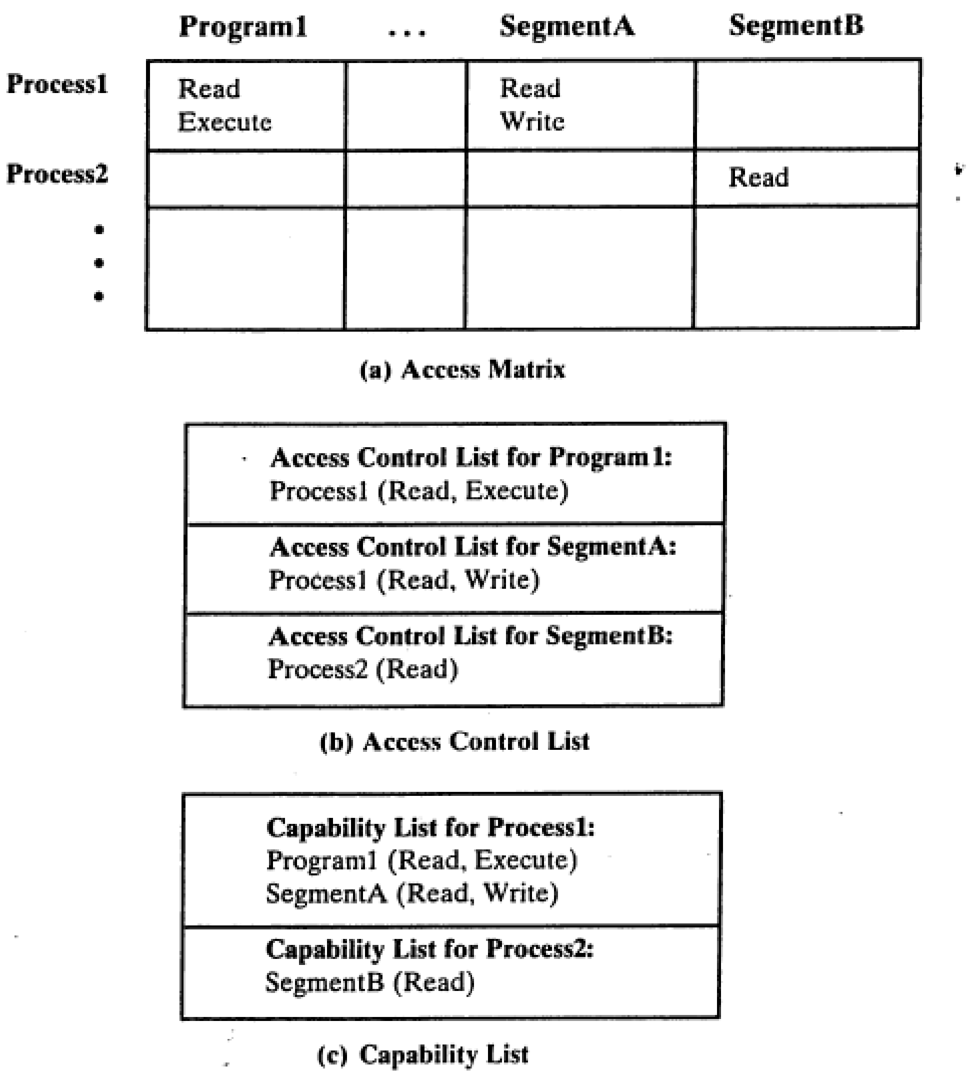
# Advantages

- Three levels of defense
- Internal network is invisible to the Internet
  - Outside router advertises only the existence of the screened subnet
- Systems on the inside cannot create direct routes to the Internet
  - Inside router advertises only the existence of screened subnet

# Access Control

- Given system has identified a user
- Determines what resources user can access
- General model is that of Access Matrix with
  - **Subject - entity capable of accessing objects (user,** process)
  - **Object – anything to which access is controlled e.g.,** files, programs, etc.
  - **Access right – way object can be accessed e.g., read,** write and execute
- Matrix can be decomposed
  - Columns as Access Control Lists
  - Rows as Capability List

# Access Control Matrix



|  | Program1 | . . . | SegmentA | SegmentB |
|---|---|---|---|---|
| Process1 | Read<br>Execute |  | Read<br>Write |  |
| Process2 |  |  |  | Read |
| •<br>•<br>• |  |  |  |  |

(a) Access Matrix

**Access Control List for Program1:**
Process1 (Read, Execute)

**Access Control List for SegmentA:**
Process1 (Read, Write)

**Access Control List for SegmentB:**
Process2 (Read)

(b) Access Control List

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

**Capability List for Process2:**
SegmentB (Read)

(c) Capability List

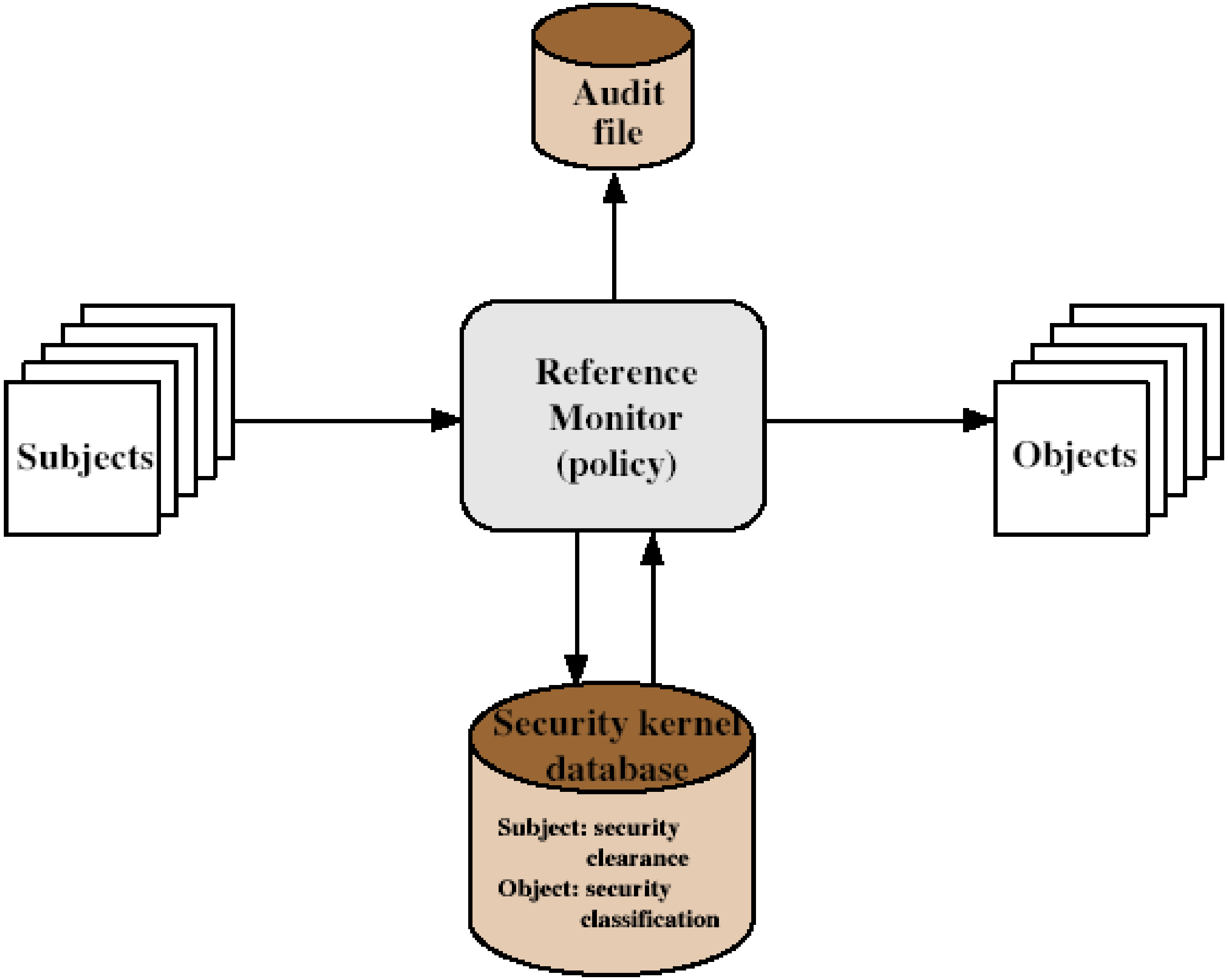
# Trusted Computer Systems

- Information security is increasingly important
- Have varying degrees of sensitivity of information
  - like military information classifications: confidential, secret, etc.
- Subjects (people or programs) have varying rights of access to objects (information)
- Want to consider ways of increasing confidence in systems to enforce these rights
- Known as multilevel security
  - Subjects have **max & current security** level
  - Objects have a fixed security level **classification**

# Multilevel Security

- Implemented as mandatory policies on system
- Has two key policies:
- **no read up (simple security property)**
  - a subject can only read/write an object if the current security level of the subject dominates (>=) the level of the object
- **no write down (*-property)**
  - a subject can only append/write to an object if the current security level of the subject is dominated by (<=) the level of the object

# Reference Monitor


Audit file
Subjects
Reference Monitor (policy)
Objects
Security kernel database
Subject: security clearance
Object: security classification

# Reference Monitor

- Controlling element in the hardware and OS
- Regulates the access of subjects to objects based on security kernel database
- Has following properties
  - Complex Mediation
    - Security rules are enforced on every access
  - Isolation
    - Reference monitor and database are protected from unauthorized modification
  - Verifiability
    - Reference monitor's correctness must be provable

# Evaluated Computer Systems

- Governments can evaluate IT systems
- Against a range of standards:
  - TCSEC, IPSEC and now Common Criteria
- Define a number of “levels” of evaluation with increasingly stringent checking
- Have published lists of evaluated products
  - Though aimed at government/defense use
  - Can be useful in industry also

# Trojan Horse Defense

- Use secure and trusted OS
- Two security levels
  - Sensitive & Public
  - Assigned to subjects on the basis of user and terminal being used
- Intruder's file and processes are restricted to public
- Legitimate user is assigned sensitive
- Therefore attempt to write in intruder's file is denied based on No Write Down rule

# Any question ?