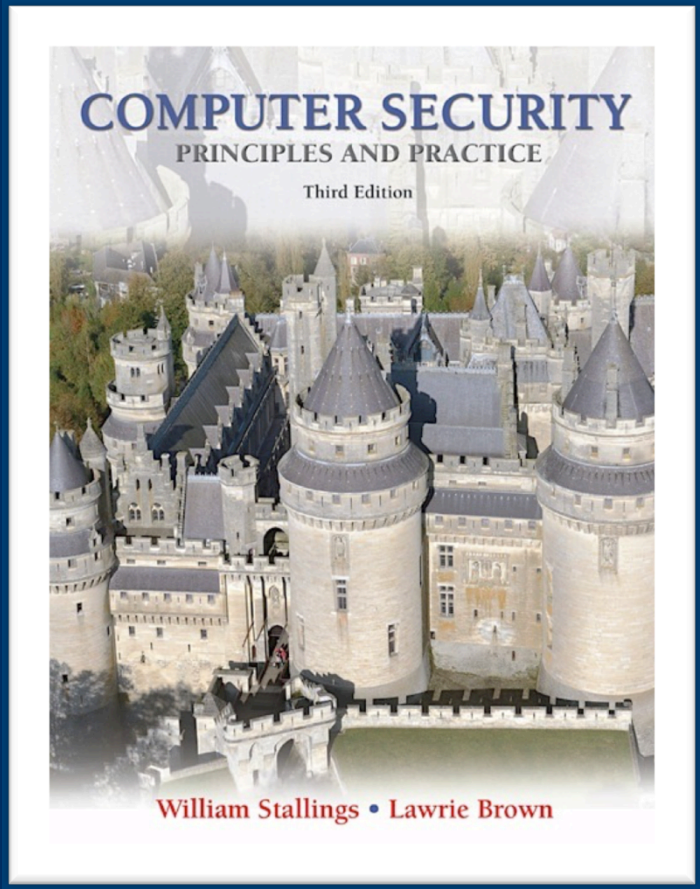
Lecture 14
Access Control



modified from slides of Lawrie Brown

Access Control

- **For short**--The restriction of access to the resources
- Comparing **user authentication** and **access control**
  - prevent unauthorized users from gaining access to resources
  - prevent legitimate users from accessing resources in an unauthorized manner

Access Control Policies

- Core of AC: AC policies
  - Embodied in the authorization database
- Dictates
  - what types of access are permitted,
  - under what circumstances,
  - by whom.
- Four classes
  - Discretionary access control; Mandatory access control; Role-based AC; Attribute-based AC

Access Control Basic Elements

- Subject: users and applications
  - Owner: creator of a resource
  - Group: a group of users who may also be granted access right
  - World: all the other user, with the minimum access right

Access Control Basic Elements

- Object: the resource to which access is controlled
  - Records, blocks, pages, segments, files, portions of files, directories, directory trees, mailboxes, messages, and programs (hardware and software)

Access Control Basic Elements

- Access right : describes the way in which a subject may access an object (how can a user operates over the resources)
  - Read: User may view information in a system resource
  - Write: User may add, modify, or delete data in system resource
  - Execute, delete, create, search

- **Discretionary access control**
- Mandatory access control
- **Role-based access control**
- **Attribute-based access control**

Mandatory Access Control (MAC)

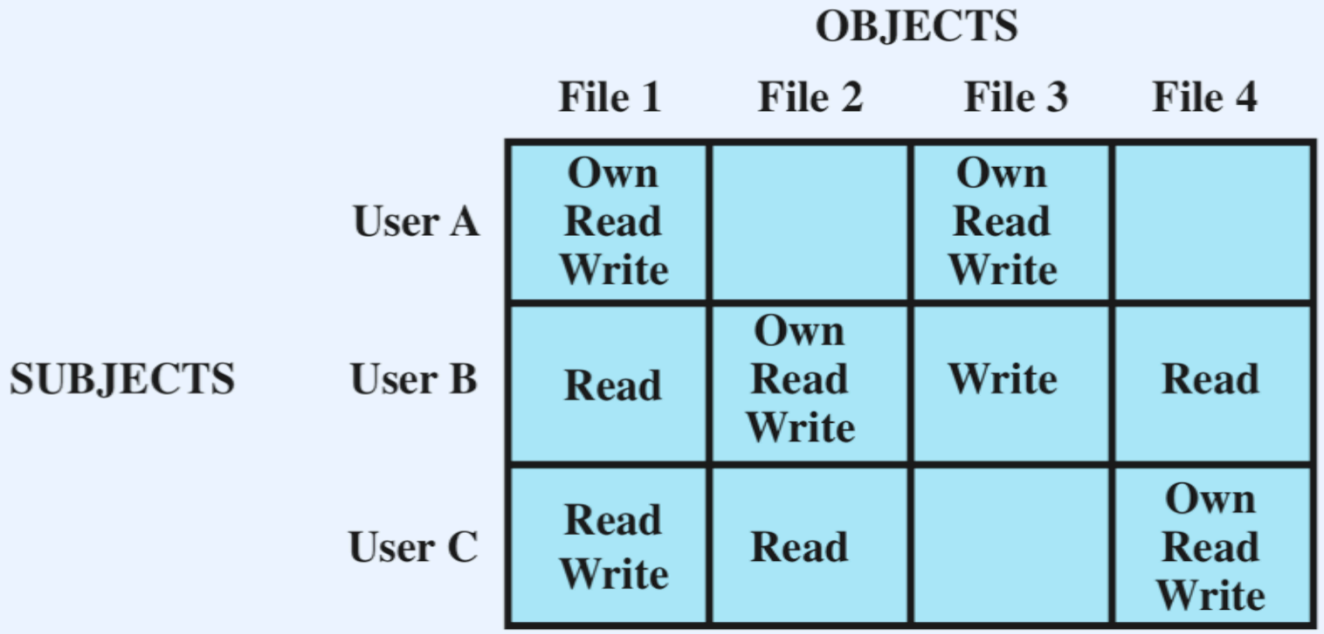
- When a system/security admin configures security rules that apply to users
- Users cannot change the rules set by admins, and are not usually considered to “own” files

- **Discretionary access control**
- Mandatory access control
- **Role-based access control**
- **Attribute-based access control**

Discretionary Access Control

- Scheme in which an entity may enable another entity to access some resource
  - often provided using an access matrix
    - one dimension consists of identified subjects that may attempt data access to the resources
    - the other dimension lists the objects that may be accessed
  - each entry in the matrix indicates the access rights of a particular subject for a particular object

Access Matrix



		OBJECTS			
		File 1	File 2	File 3	File 4
SUBJECTS	User A	Own Read Write		Own Read Write	
	User B	Read	Own Read Write	Write	Read
	User C	Read Write	Read		Own Read Write

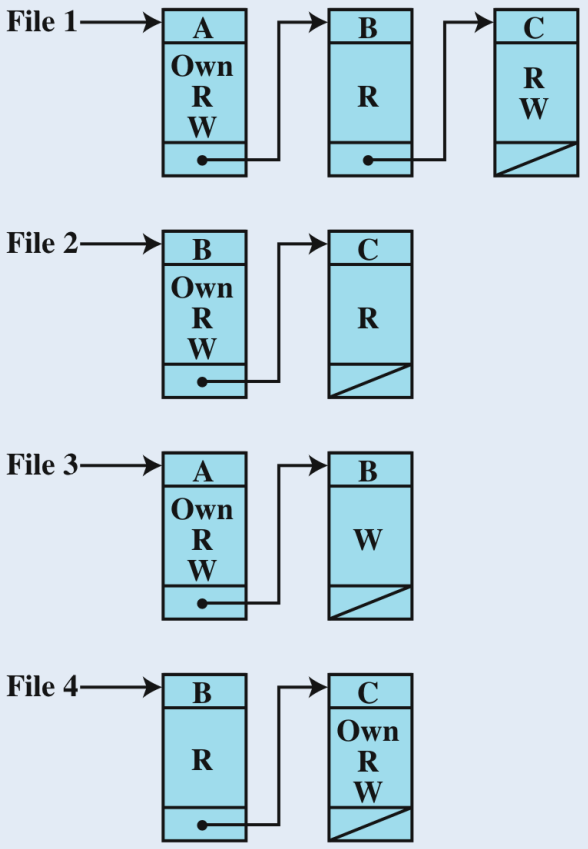
(a) Access matrix

Example of Access Control Structures

- An access matrix is usually sparse—it is implemented by decomposition in one of two ways
  - By columns: yielding access control list (ACL)
  - By rows: yielding capability tickets

Example of Access Control Structures

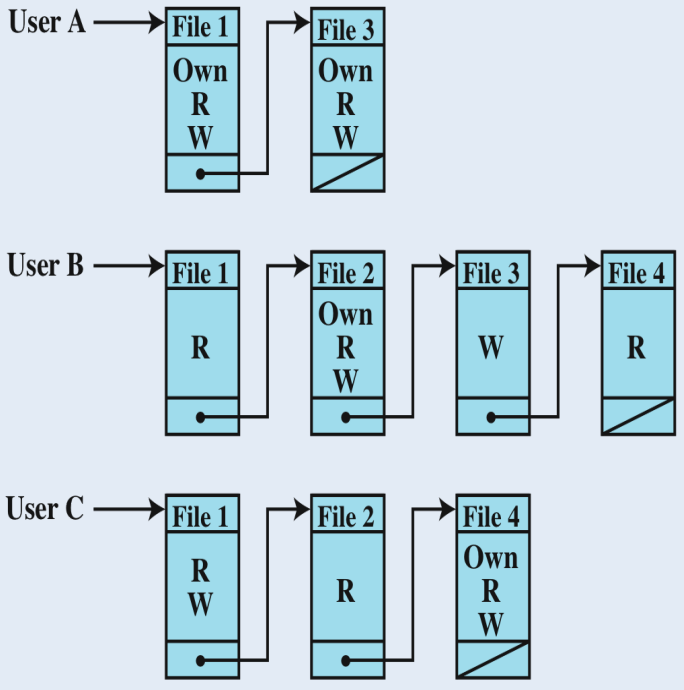
- By columns: yielding access control list (ACL)
- For each object, an ACL lists users and their permitted access rights



(b) Access control lists for files of part (a)

Example of Access Control Structures

- By rows: yielding capability tickets
- A capability ticket (A row) specifies authorized objects and operations for a particular user



(c) Capability lists for files of part (a)

- **Discretionary access control**
- Mandatory access control
- **Role-based access control**
- **Attribute-based access control**

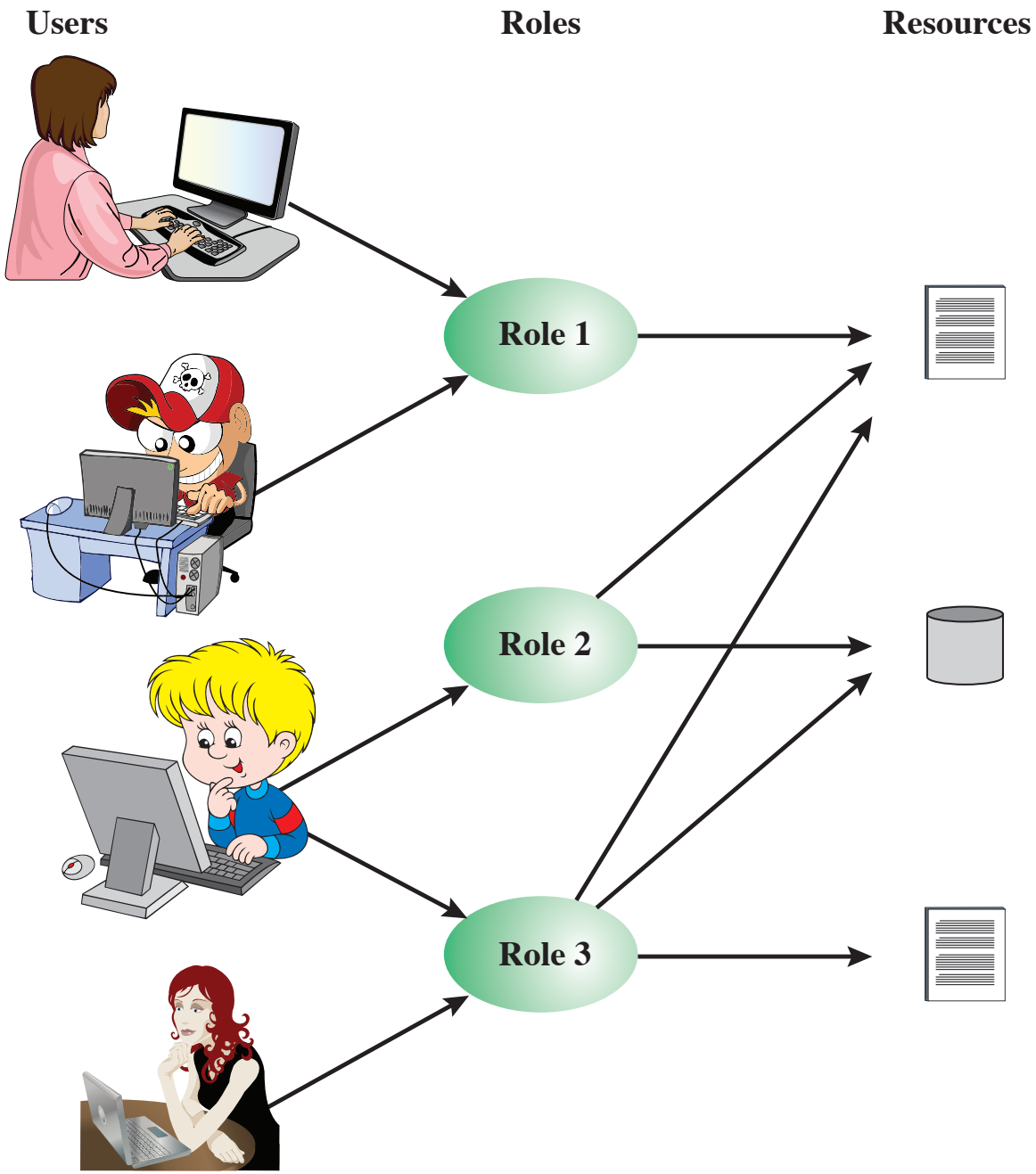
Role-Based Access Control

- Traditional DAC systems define the access rights of individual users
- RBAC is based on the roles that users assume in a system rather than the user's identity
  - WebCampus: faculties, students

Role-Based Access Control (RBAC)

Many to many

good aspects of RBAC?-consider a new user joins

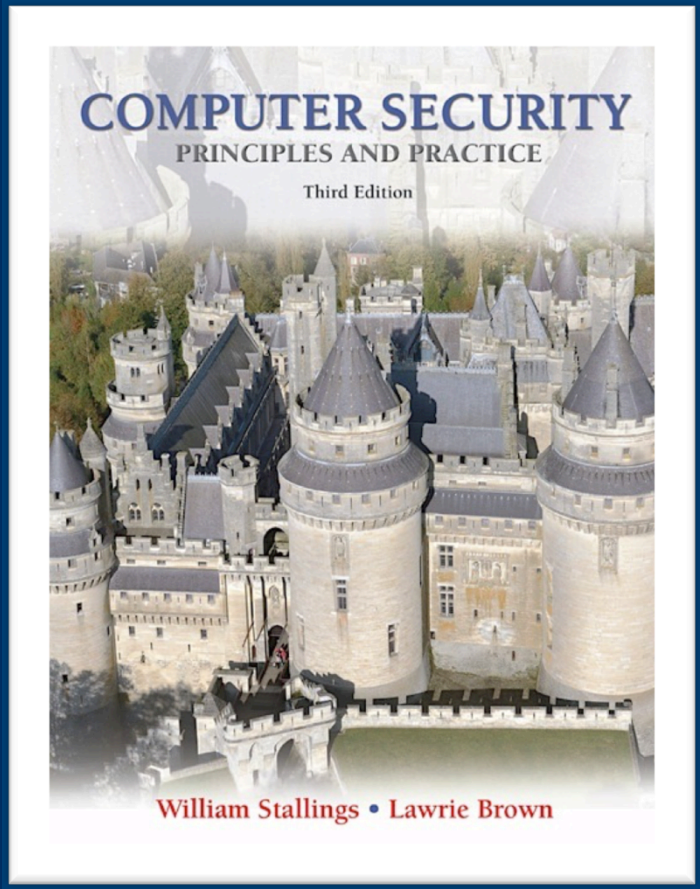


- **Discretionary access control**
- Mandatory access control
- **Role-based access control**
- **Attribute-based access control**

Attribute Based Access Control

- **Subject attributes**
  - Attributes define the identity and characteristics of the subject
- Object attributes
  - Objects have attributes that can be leverages to make access control decisions
- Environment attributes
  - Describe the operational, technical, and even situational environment or context in which the information access occurs

Lecture 15
Database Security



modified from slides of Lawrie Brown

Databases

- structured collection of data stored for use by one or more applications
  - contains the relationships between data items and groups of data items
  - can sometimes contain sensitive data
- database management system (DBMS)
  - suite of programs for constructing and maintaining the database
  - Query language
    - provides a uniform interface to the database

Relational Database Elements

- relation / table / file
- tuple / row / record
- attribute / column / field

primary key

- uniquely identifies a row
- consists of one or more column names

foreign key

- links one table to attributes in another

view / virtual table

- result of a query that returns selected rows and columns from one or more tables

Structured Query Language (SQL)

- originally developed by IBM in the mid-1970s
- standardized language to define, manipulate, and query data in a relational database
- several similar versions of ANSI/ISO standard

SQL statements can be used to:

- create tables
- insert and delete data in tables
- create views
- retrieve data with query statements

Structured Query Language (SQL)

- The basic command for retrieving information is the SELECT statement. Consider this example:

  – SELECT Ename, Eid, Ephone
    FROM Employee
    WHERE Did 15

- This query returns the Ename, Eid, and Ephone fields from the Employee table for all employees assigned to department 15

SQL Injection Attacks (SQLi)

- One of the most prevalent and dangerous network-based security threats
- Designed to exploit the nature of Web application pages
- Sends malicious SQL commands to the database server
- Most common attack goal is bulk extraction of data
- Depending on the environment SQL injection can also be exploited to:
  - Modify or delete data
  - Execute arbitrary operating system commands
  - Launch denial-of-service (DoS) attacks

Injection Techniques

var Shipcity;

ShipCity = Request.form (“ShipCity”);

var sql = “select * from OrdersTable where ShipCity = ‘ ” + ShipCity + “ ‘ ”

Intention: a user will enter the name of a city. When the script is executed, the user is prompted to enter a city, and if the user enters SF, then the following SQL query is generated

Injection Techniques

- SELECT * FROM OrderTable WHERE ShipCity = ‘SF’
- Suppose, however, the user enters the following
- ‘SF’; DROP table OrderTable --
- This results in the following SQL query:
- SELECT * FROM OrderTable WHERE ShipCity = ‘SF’; DROP table OrderTable--

SQL Access Controls

- two commands for managing access rights:
  - grant
    - used to grant one or more access rights or can be used to assign a user to a role
  - revoke
    - revokes the access rights

```
GRANT { privileges | role }
[ON table]
TO { user | role | PUBLIC }
[IDENTIFIED BY password]
[WITH GRANT OPTION]
```

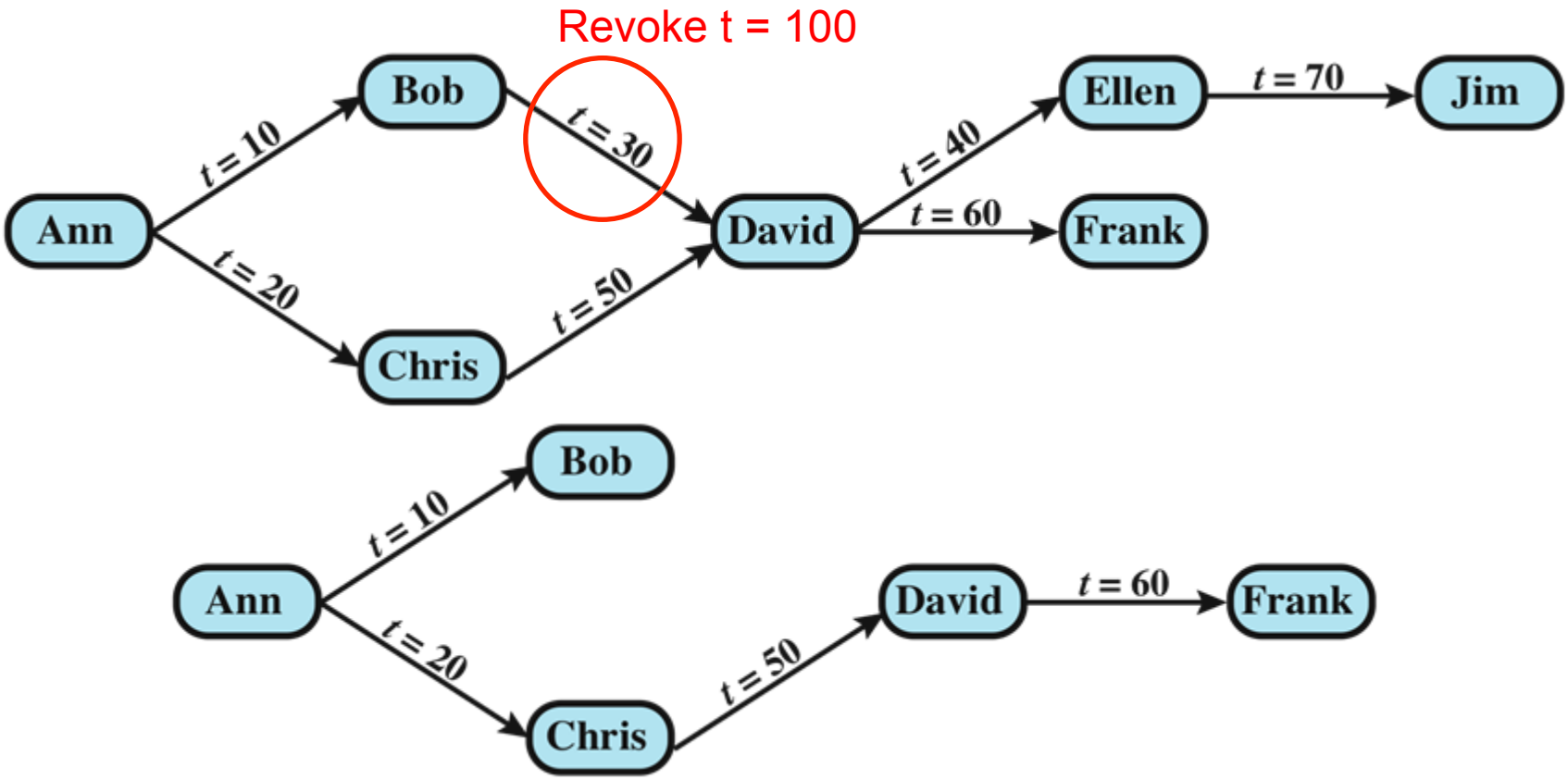
```
REVOKE { privileges | role }
[ON table]
FROM { user | role | PUBLIC }
```

SQL Access Controls

GRANT { privileges | role }
[ON table]
TO { user | role | PUBLIC }
[IDENTIFIED BY password]
[WITH GRANT OPTION]

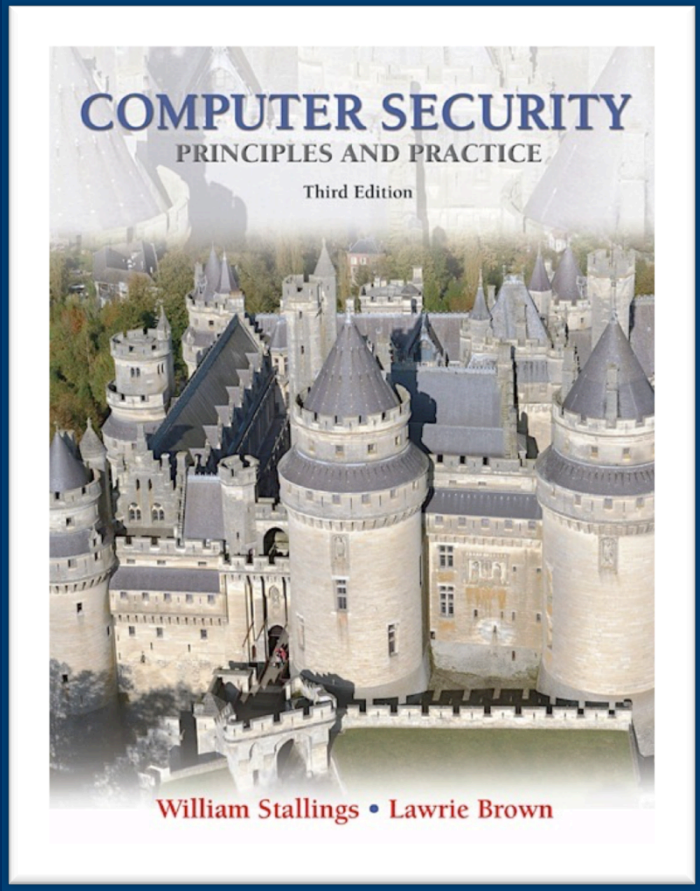
- typical access rights are:
  - select, insert, update, delete, references

Cascading Authorizations



Rule: When user A revokes an access right, any cascaded access right is also revoked

Lecture 17
Denial of Service Attacks



modified from slides of Lawrie Brown

Denial-of-Service (DoS) Attack

- DoS: a form of attack on the availability of some service
- In the context of computer and communication security, it focuses on **network services** that are attacked over their **network connection**
- Different from attacks that cause damage or deconstruction of IT infrastructure

Distributed Denial of Service (DDoS) Attacks

- The attack source is more than one-and often thousands of unique IP addresses
- Use of multiple systems to generate attacks
- Attacker uses a flaw in operating system or in a common application to gain access and installs their program on it (zombie)
  - Backdoor program

DDoS Attack Architecture

- **Advantage of hierarchical DDoS attack structure**
  - The attacker can send a single command to a handler, which then automatically forwards it to all the agents under its control
  - Lower physical capacity requirement
  - More difficult to identify the attacker

Application-based Bandwidth Attack

- To force the target to execute resource-consuming operations
- Two protocols for this kind of attack
  - SIP flood
  - HTTP based attack

SIP Flood

- A single INVITE request triggers considerable resource consumption
- The attacker can flood a SIP proxy with numerous INVITE requests with spoofed IP addresses
  - The proxy server resources are depleted in processing the INVITE requests
  - The server's network capacity is consumed

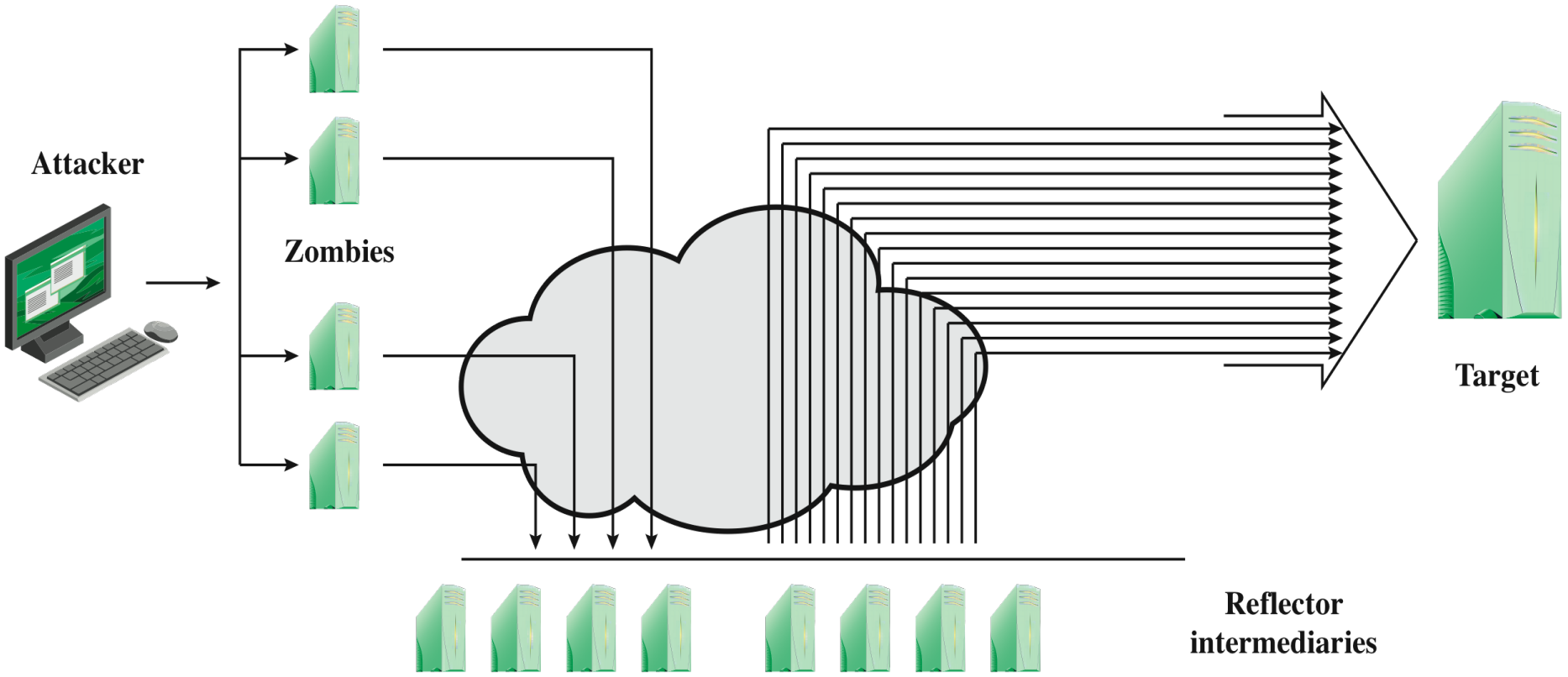
HTTP based Attack-Slowlories

- A common server uses multiple threads to support multiple requests to the same server application
- Basic idea
  - It consumes all of the available request handling threads on the Web server by sending HTTP requests that never complete
  - Since each request consumes a thread, the Slowloris attack eventually consumes all of the Web server's connection capacity, effectively denying access to legitimate users

Reflection Attacks

- attacker sends packets to a known service on the intermediary with a spoofed source address of the actual target system
- when intermediary responds, the response is sent to the target
- goal is to generate enough volumes of packets to flood the link to the target system without alerting the intermediary

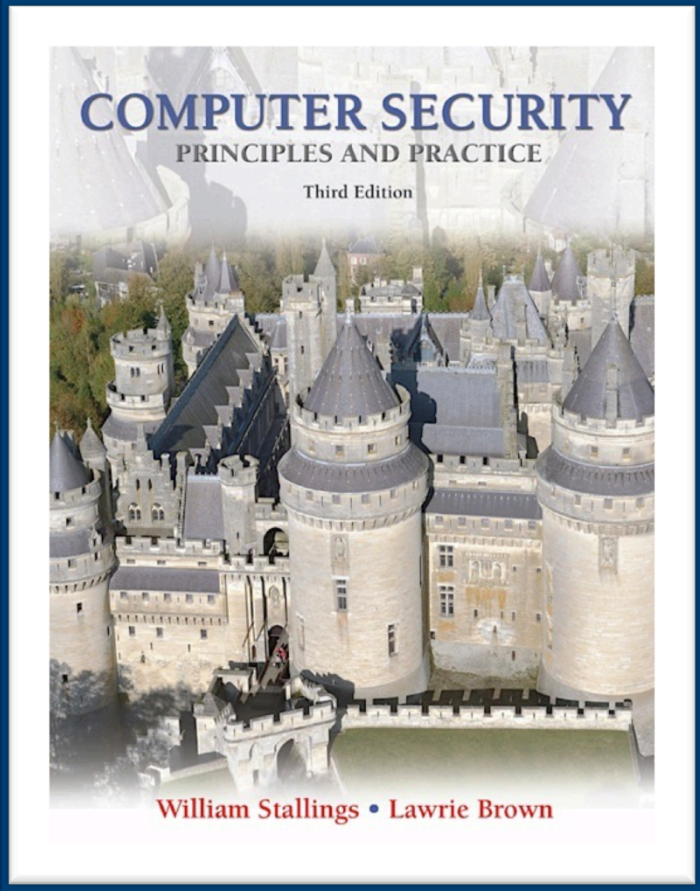
Amplification Attacks



DoS Attack Defenses

- these attacks cannot be prevented entirely
- high traffic volumes may be legitimate
  - high publicity about a specific site
  - activity on a very popular site
  - described as slashdotted, flash crowd, or flash event

Lecture 18
Intrusion Detection



modified from slides of Lawrie Brown

Definition

- A significant security problem for networked systems; hostile, or at least unwanted, trespass by users or software
- Trespass
  - Unauthorized login (user)
  - Authorized user: acquisition of privileges beyond authorization (user)
  - Take the form of virus, worm or Trojan horse (software)

Classes of Intruders

- Cyber criminals
- Activists
- State-sponsored organizations
- Others

Intrusion Detection

- **Intrusion Detection** : A security service that monitors and analyzes system events for the purpose of finding, and providing real-time or near real-time warning of, attempts to access system resources in an unauthorized manner.

Intrusion Detection Systems (IDSs)

- host-based IDS
  - monitors the characteristics of a single host suspicious activity
- network-based IDS
  - monitors network traffic and analyzes network, transport, and application protocols to identify suspicious activity
- Distributed or hybrid IDS
  - Combines information from a number of sensors, in a central analyzer that is able to better identify and respond to intrusion activity

Intrusion Detection Systems (IDSs)

- comprises three logical components:
  - Sensors
    - collect data
  - analyzers
    - determine if intrusion has occurred
  - user interface
    - view output or control system behavior

Analysis Approaches

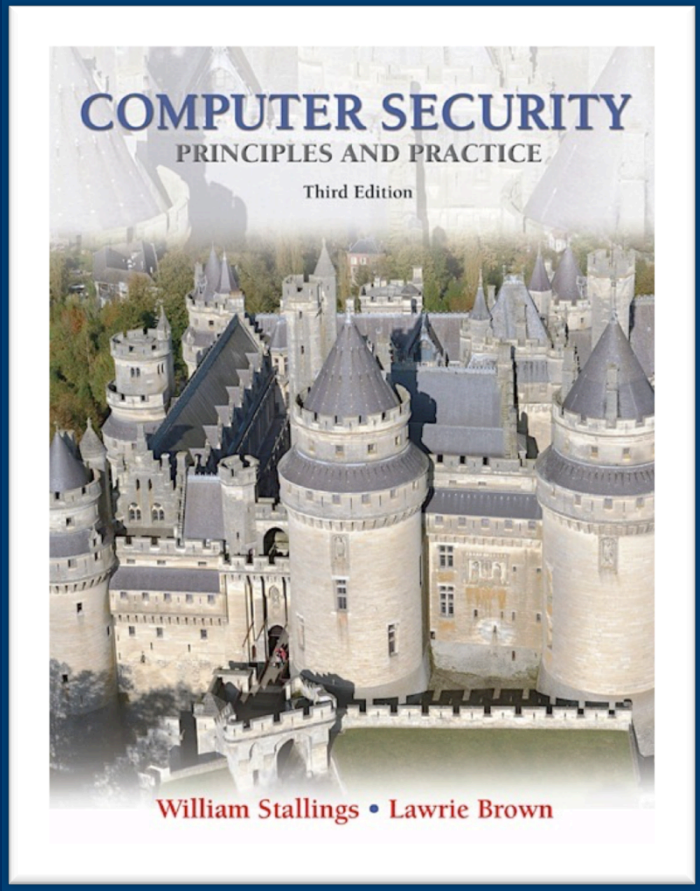
Anomaly detection

- Involves the collection of data relating to the **behavior of legitimate users** over a period of time
- Then current observed behavior is analyzed to determine whether this behavior is that of a legitimate user or that of an intruder

Signature/Heuristic detection

- Uses a set of **known malicious data patterns** or attack rules that are compared with current behavior
- Can only identify known attacks for which it has patterns or rules

Lecture 19
Firewalls



modified from slides of Lawrie Brown

The Need For Firewalls

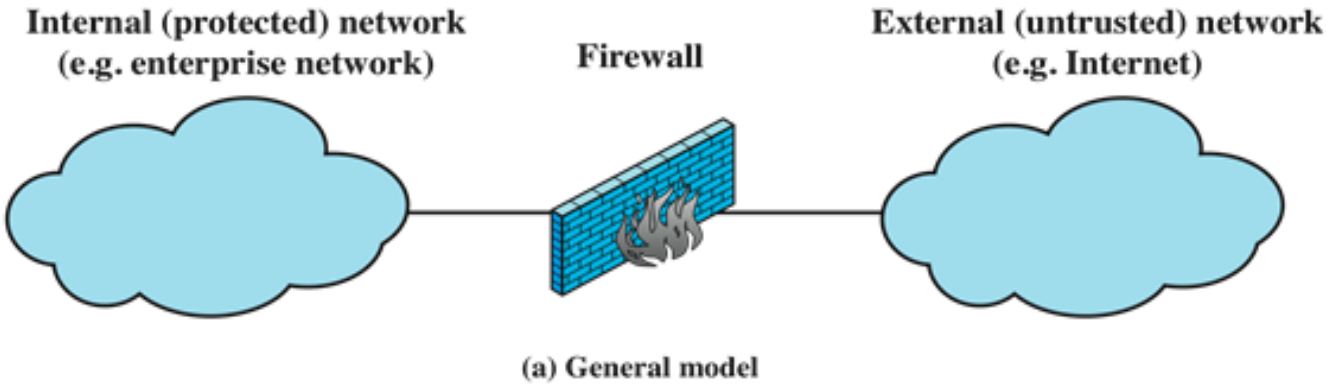
- Inserted between the premises network and the Internet to establish a controlled link
  - Aim--protect the premise network from Internet-based attacks and to provide a single choke point where security and auditing can be imposed
  - can be a single computer or a set of two or more systems working together to perform firewall function

Firewall Capabilities And Limits

- capabilities:
  - defines a single choke point
  - provides a location for monitoring security events
  - can serve as the platform for IPSec
- limitations:
  - cannot protect against attacks bypassing firewall
  - may not protect fully against internal threats
  - laptop, PDA, or portable storage device may be infected outside the corporate network then used internally

Types of Firewalls

- Packet filtering firewalls
- Stateful inspection firewalls
- Application-level firewalls
- Circuit-level firewalls



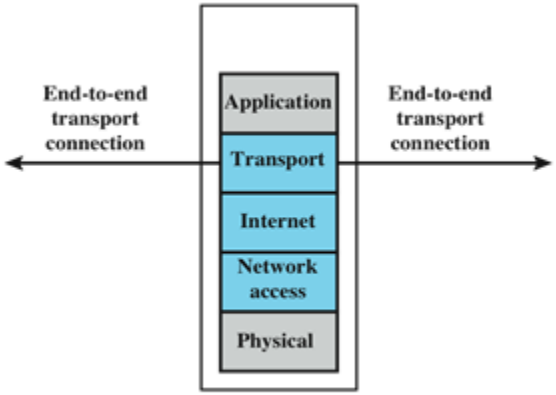
(a) General model

Packet Filtering Firewall

- applies rules to each incoming and outgoing IP packet
  - typically a list of rules based on matches in the TCP/IP header
  - forwards or discards the packet based on rules match

Filtering rules are based on information contained in a network packet

- Source IP address
- Destination IP address
- Source and destination transport-level address
- IP protocol field
- Interface



(b) Packet filtering firewall

- two default policies:
  - **discard** - prohibit unless expressly permitted
    - more conservative, controlled, visible to users
  - **forward** - permit unless expressly prohibited
    - easier to manage and use but less secure

Packet Filtering Rule Example

Rule	Direction	Src address	Dest addresss	Protocol	Dest port	Action
1	In	External	Internal	TCP	25	Permit
2	Out	Internal	External	TCP	>1023	Permit
3	Out	Internal	External	TCP	25	Permit
4	In	External	Internal	TCP	>1023	Permit
5	Either	Any	Any	Any	Any	Deny

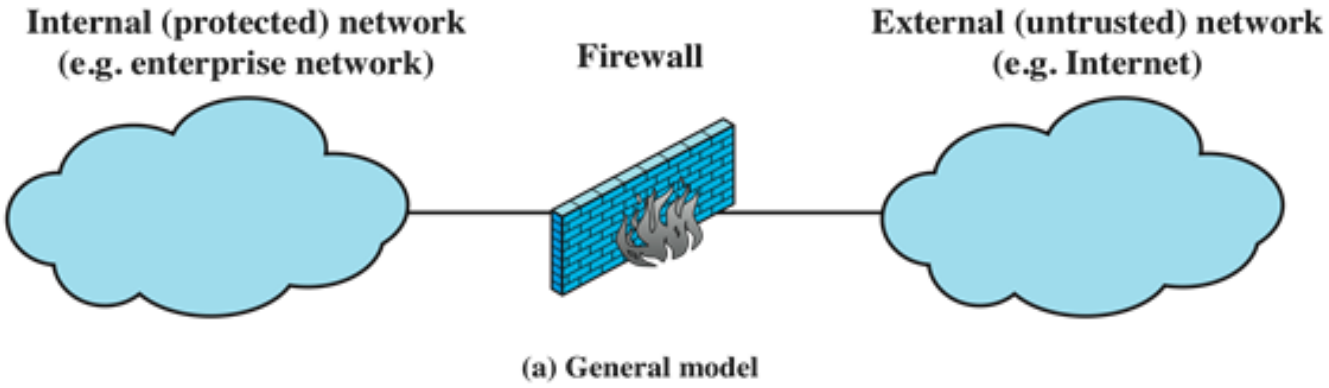
- Inbound mail is allowed (port 25 is for SMTP incoming)
- Allow a response to an inbound SMTP connection
- Outbound mail to an external source is allowed
- Allow a response to an inbound SMTP connection
- Discard default policy

Packet Filter Firewalls: Advantages And Weaknesses

- advantages
  - simplicity
  - typically transparent to users and are very fast
- weaknesses
  - cannot prevent attacks that employ application specific vulnerabilities or functions
  - do not support advanced user authentication
  - improper configuration can lead to breaches

Types of Firewalls

- Packet filtering firewalls
- Stateful inspection firewalls
- Application-level firewalls (gateway)
- Circuit-level firewalls



(a) General model

Stateful Inspection Firewall

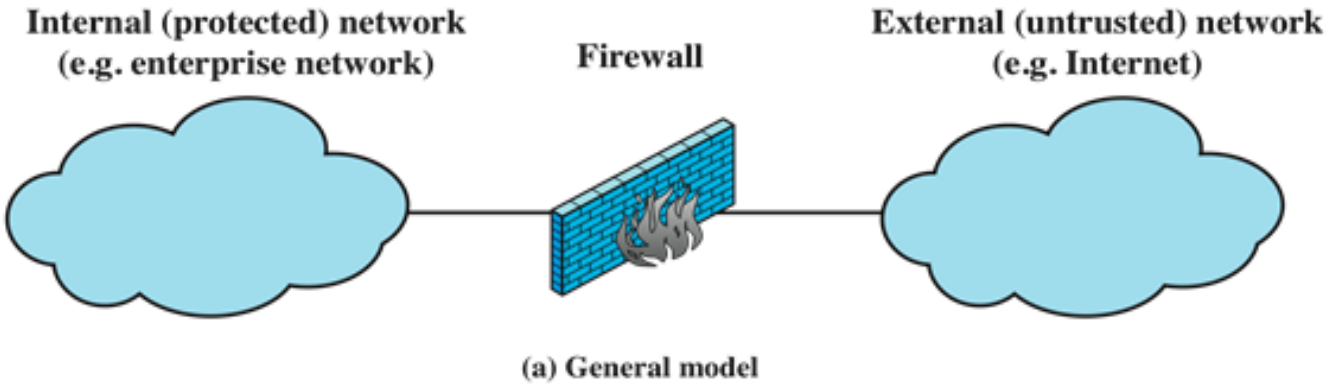
- tightens rules for TCP traffic by creating a directory of current TCP connections and their information (stateful)
  - there is an entry for each currently established connection
  - packet filter allows incoming packets that fit the profile of one of the entries
  - Consider the SMTP example ; the TCP client port value is valid if it belongs to 1024-65,535—wide accepting range for firewall filter; the attacker can exploit this property→stateful inspection
  - How about the first packet?

Stateful Firewall Connection State

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
223.21.22.12	1046	192.168.1.6	80	Established

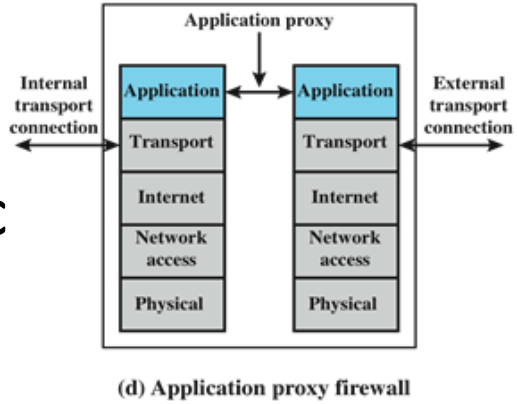
Types of Firewalls

- Packet filtering firewalls
- Stateful inspection firewalls
- Application-level firewalls (gateway)
- Circuit-level firewalls



(a) General model

Application-Level Gateway



(d) Application proxy firewall

- also called an **application proxy**
- acts as a relay of application-level traffic
  - user contacts gateway using a TCP/IP appl.
  - user is authenticated
  - gateway contacts application on remote host and relays TCP segments between server and user
- tend to be more secure than packet filters
  - The application-level gateway only needs to check a few allowable applications