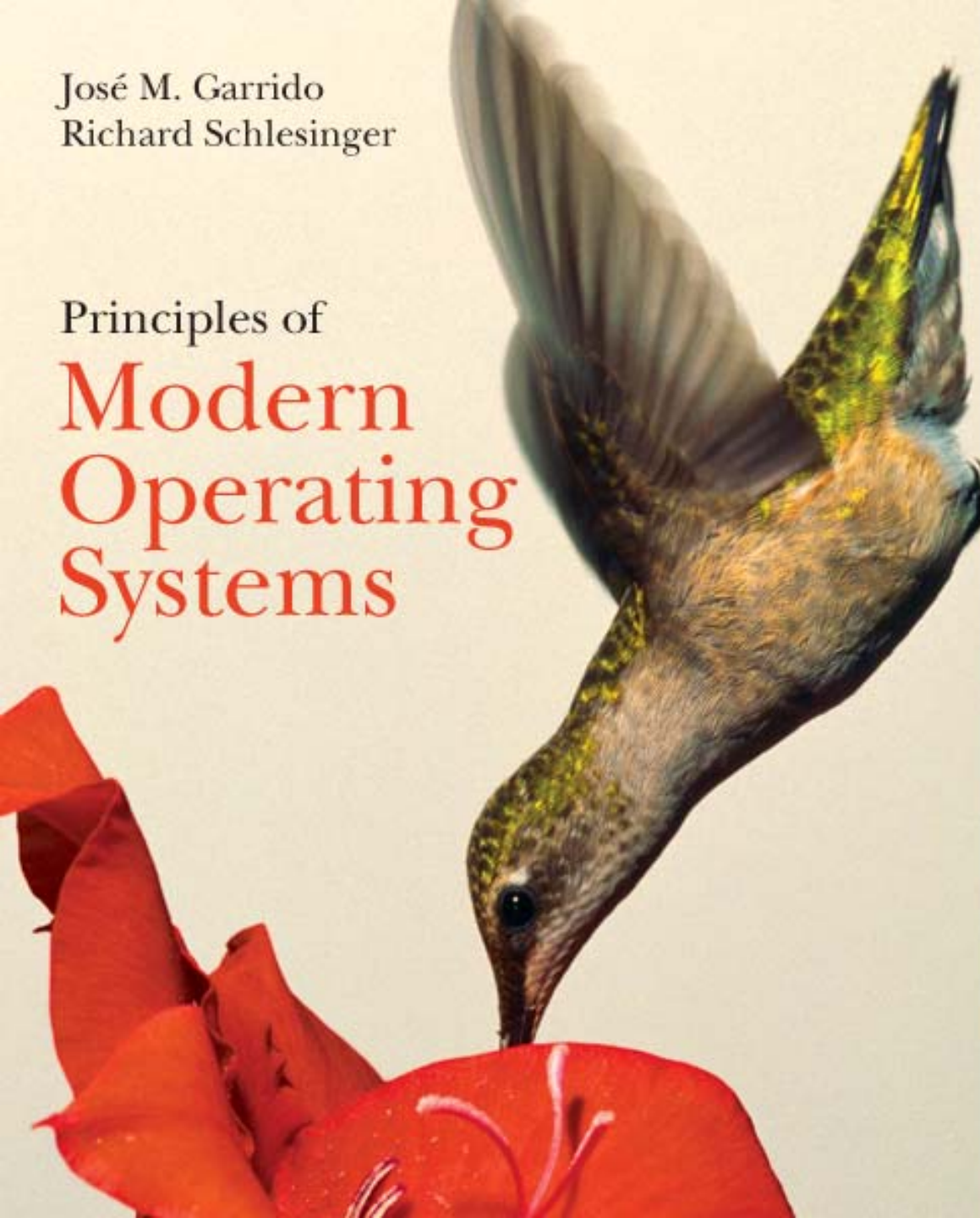


José M. Garrido
Richard Schlesinger

Principles of
**Modern
Operating
Systems**



Chapter 12

Firewalls and Network Security

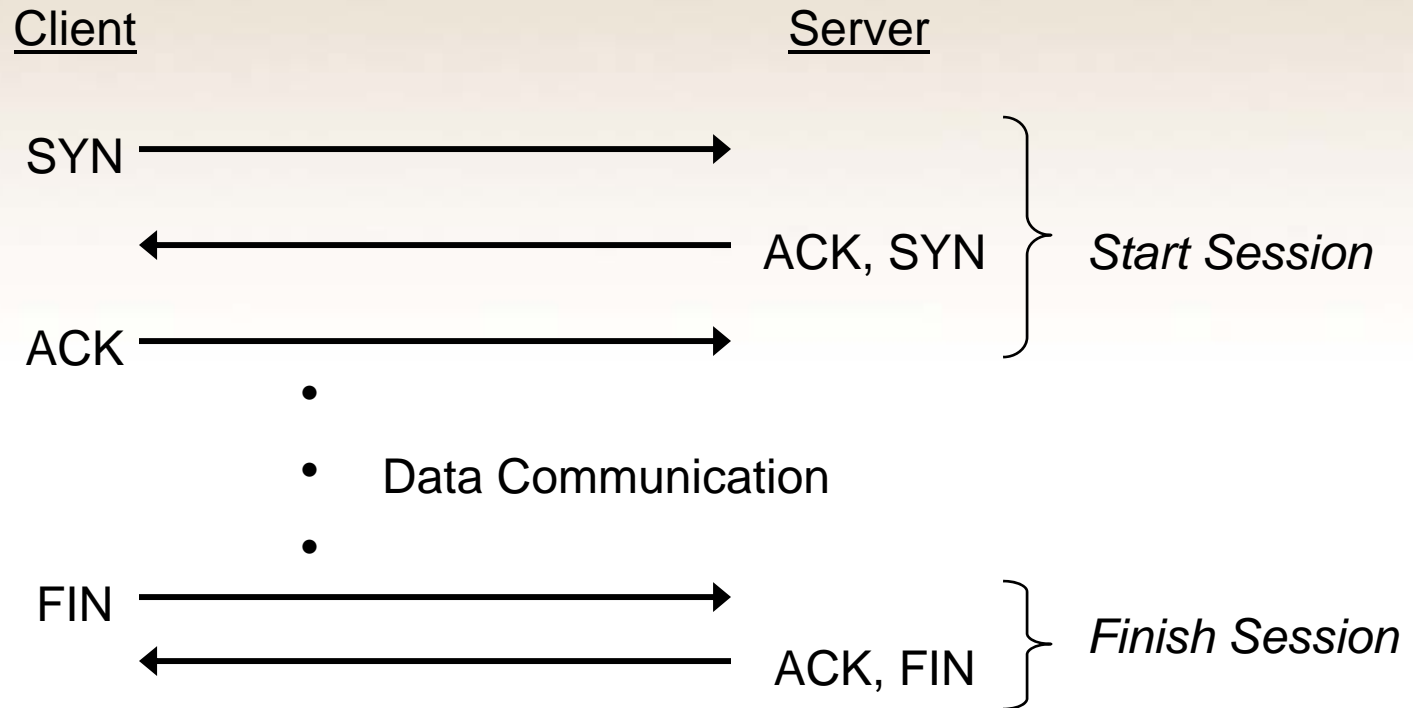
OSI Model



TCP/IP Communications

- IP protocol used for Network layer
- TCP and UDP protocols used for Transport layer
- Each computer on the network has an IP address, along with **ports** numbered 1 – 65535
 - Server applications (aka daemons) listen for incoming requests on one or more ports

TCP/IP Communications



IP Port Scanning

- A common practice is for attackers to send a short message (FIN) to each port on a computer
- Any port that responds indicates a server application is listening on that port and is a potential point of attack

Server Attacks

- Each type of server listens on a particular port
 - Example: Web Servers listen on port 80
- Once attacker knows there is a particular type of server listening
 - They can attempt to exploit known security flaws in those types of servers

Denial of Service

- Constantly sending SYN messages to a server and never responding to the server's ACK
 - Server is so busy handling these SYN messages, it cannot handle real service requests

Defending the Network

- Firewalls
- Monitoring tools

Firewalls

- Controls which messages can come in from outside and where they may go.
 - Tables are used to configure firewall
 - Example: From outside the local LAN...
 - Company web server is allowed to received only browser requests
 - Internal database server is never allowed to receive requests

Monitoring Tools

- Etherpeek
 - Monitors incoming packets
 - Records source IP address