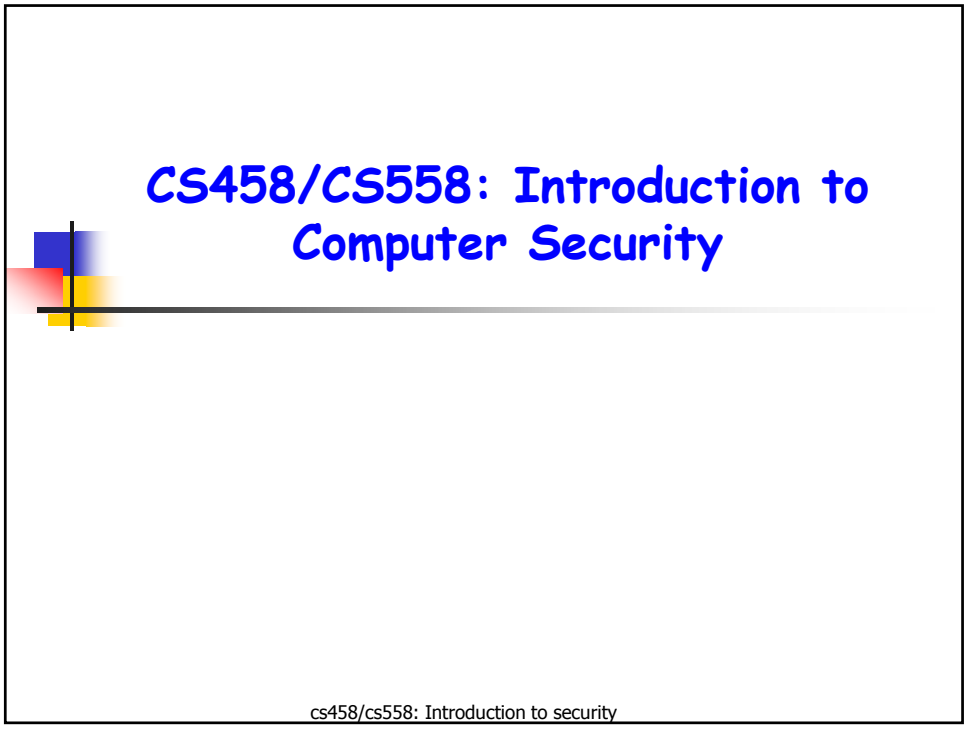


- This class
  - OSI security architecture
  - A model for network security
  - Introduction to Network and socket programming

OSI Security Architecture

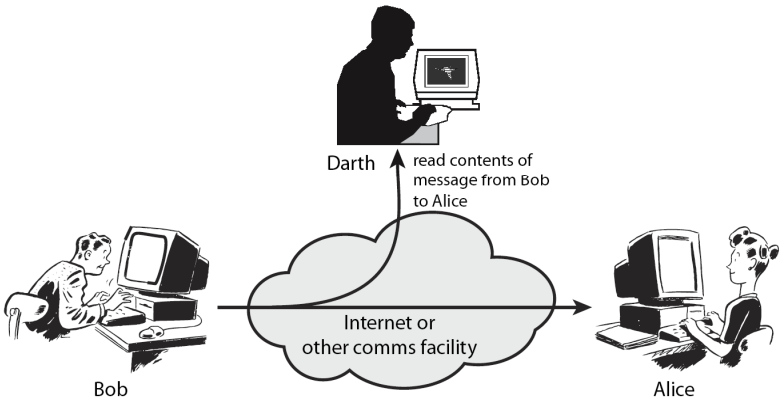
- ITU-T X.800: Security Architecture for OSI
  - ITU-T: International Telecommunication Union, Telecommunication standardization sector
  - OSI: Open Systems Interconnection - an effort to standardize networking
    - Started in 1982 by the Internationtional Organization for Standardization (ISO), along with the ITU-T
  - Systematic way of defining the requirements for security
- Consider 3 aspects of information security:
  - Security attacks
  - Security mechanisms
  - Security services

Security Attacks

- Any action that compromises the security of information owned by an organization
- Information security: how to prevent attacks and to detect attacks on information-based systems
- Can focus of generic types of attacks
  - Passive
  - Active

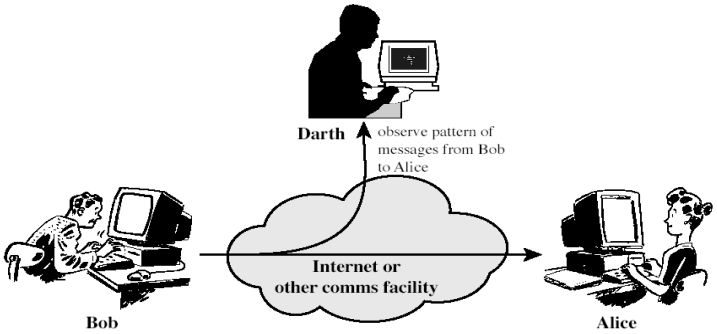
Passive Attacks

- Attempts to learn or make use of the information from the system but does not affect system resources
  - 1) The release of mesg. contents: eavesdropping on or monitoring of transmissions.



Passive Attacks

- 2) Traffic analysis: may not be able to extract the information (encryption), but might still be able to observe the pattern of these massages
  - Observe the frequency and length of messages being exchanged.
  - Example: timing attack on the SSH protocol used timing information to deduce information about passwords

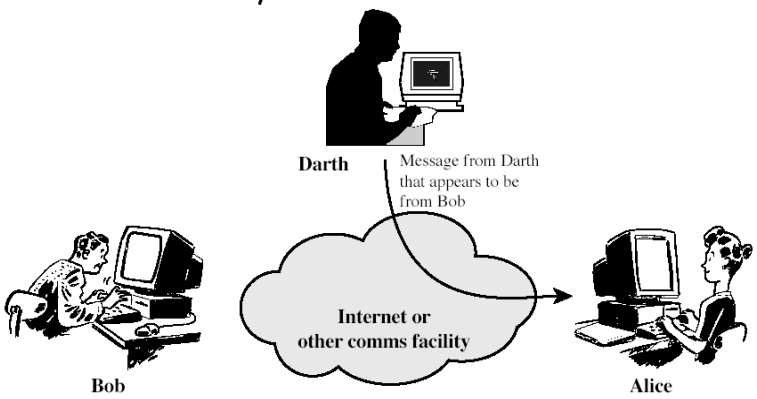


Passive Attacks

- Very difficult to detect because they do not involve any alteration of the data
- It is feasible to prevent the success of these attacks.
- The emphasis in dealing with passive attacks is on prevention rather than detection.

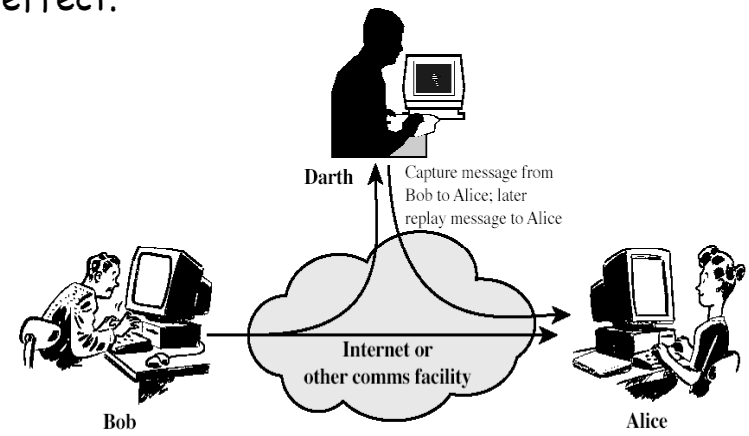
Active Attacks: Masquerade

- Attempts to alter system resources or affect their operation.
  - Masquerade: one entity pretends to be a different entity.



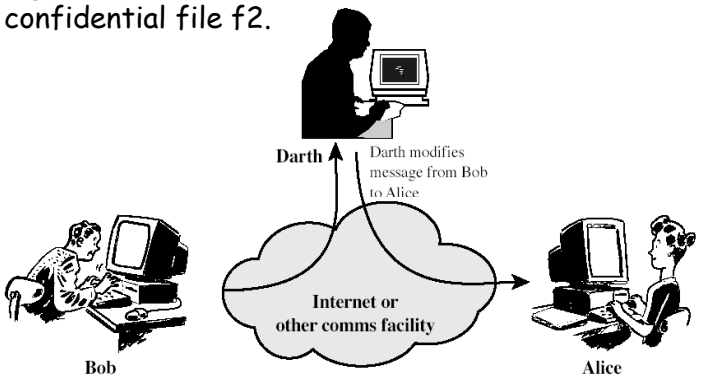
Active Attacks: Replay

- Replay: capture the data unit and transmit to the receiver later to produce an unauthorized effect.



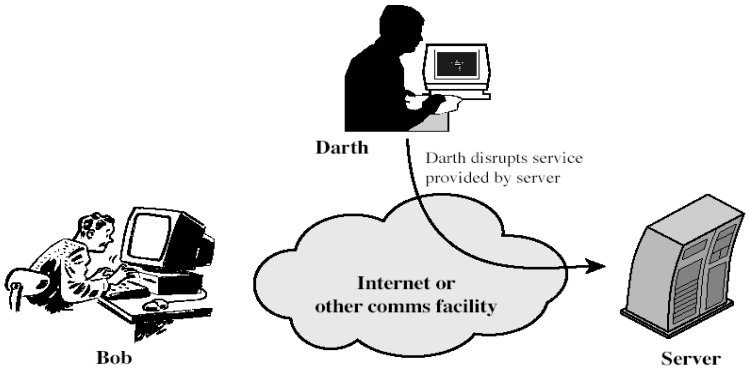
Active Attacks: Modification of Mesg.

- Modification of messages: some portion of a legitimate message is altered, or messages are delayed or reordered
  - E.g. Allow a to read confidential file f1 ➔ allow b to read confidential file f2.



Active Attacks: DOS

- Denial of service: prevents or inhibits the normal use or management of communications facilities
  - E.g. An entity may suppress all messages directed to a particular destination
  - E.g. disruption of an entire network by overloading it with messages so as to degrade performance



Security Services

- Provided by a system to give a specific kind of protection to system resources.
- Intended to counter security attacks
- Using one or more security mechanisms
- X800 divides these services into 5 categories and 14 specific services.

Security Services (X.800)

- Authentication: assurance that the communicating entity is the one claimed
- Access control: prevention of the unauthorized use of a resource
  - Controls who can have access to a resource.

Security Services (X.800)

- Data Confidentiality: protection of data from unauthorized disclosure
  - Protection of transmitted data from passive attacks.
  - Broader service: protects all user data transmitted between two users over a period of time (e.g. TCP connection).
  - Narrower service: protection of a single message or specific fields within a message

Security Services (X.800)

- Data Integrity: assurance that data received is as sent by an authorized entity
  - Integrity can apply to a stream of messages, a single message, or selected fields within a message.
  - Most useful: total stream protection
    - Connection-oriented integrity service: assures that messages are received as sent with no duplication, insertion, modification and denial of service

Security Services (X.800)

- Nonrepudiation: protection against denial by one of the parties in a communication
  - Proof that the message was sent by the specified party
  - Proof that the message was received by the specified party

Security Mechanism

- Feature designed to detect, prevent, or recover from a security attack
- No single mechanism that will support all services required
- However one particular element underlies many of the security mechanisms in use:
  - cryptographic techniques

Security Mechanisms (X.800)

- Specific security mechanisms:
  - Encipherment: the use of mathematical algorithms to transform data into a form that is not readily intelligible
  - Digital signatures: data appended to a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery
  - Access control: a variety of mechanism that enforce access rights to resources
  - Data integrity: a variety of mechanisms used to assure the integrity of a data unit or stream of data units.

Security Mechanisms (X.800)

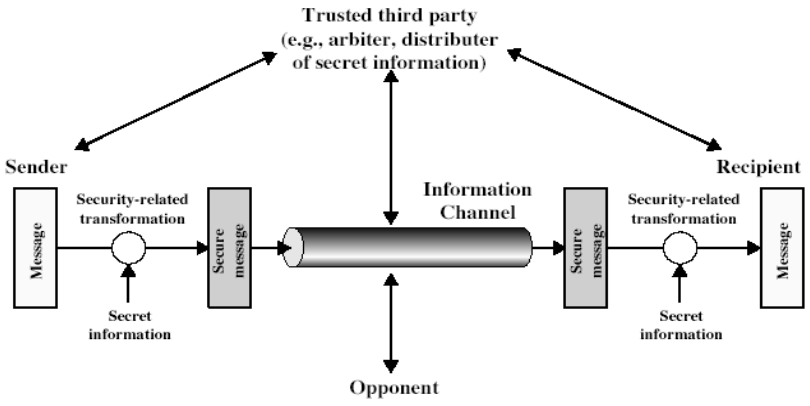
- Specific security mechanisms:
  - Authentication exchange: a mechanism intended to ensure the identity of an entity by means of information exchange.
  - Traffic padding: the insertion of bits into gaps in a data stream to frustrate traffic analysis
    - Make it difficult for an attacker to distinguish between true data flow and noise
    - Make it difficult to deduce the amount of traffic.

Relationship Between Security Services and Mechanisms

Service	Mechanism							
	Enciph-erment	Digital signature	Access control	Data integrity	Authenti-cation exchange	Traffic padding	Routing control	Notari-zation
Peer entity authentication	Y	Y			Y			
Data origin authentication	Y	Y						
Access control			Y					
Confidentiality	Y						Y	
Traffic flow confidentiality	Y					Y	Y	
Data integrity	Y	Y		Y				
Non-repudiation		Y		Y				Y
Availability				Y	Y			

Model for Network Security

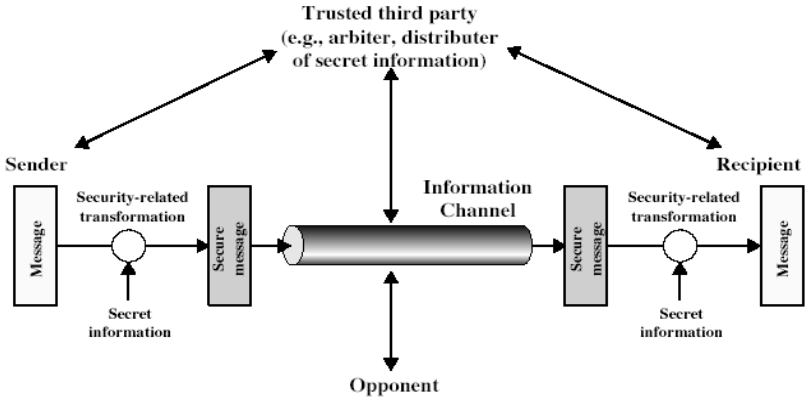
A logical information channel is established by defining a route through the internet from source to destination and by the use of communication protocols by the two principals.



Model for Network Security

Trusted third party

- Responsible for distributing the secret information to the two principals.
- arbitrate disputes between the two principals concerning the authenticity of a message transmission.



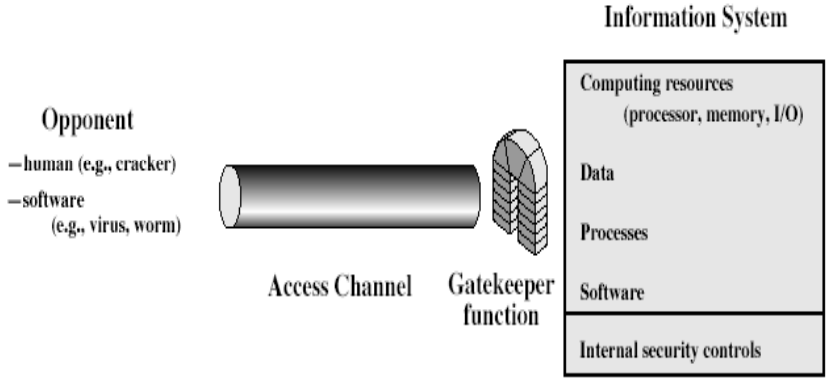
Model for Network Security

- Using this model requires us to:
  1. Design a suitable algorithm for the security transformation
  2. Generate the secret information (keys) used by the algorithm
  3. Develop methods to distribute and share the secret information

Model for Network Access Security

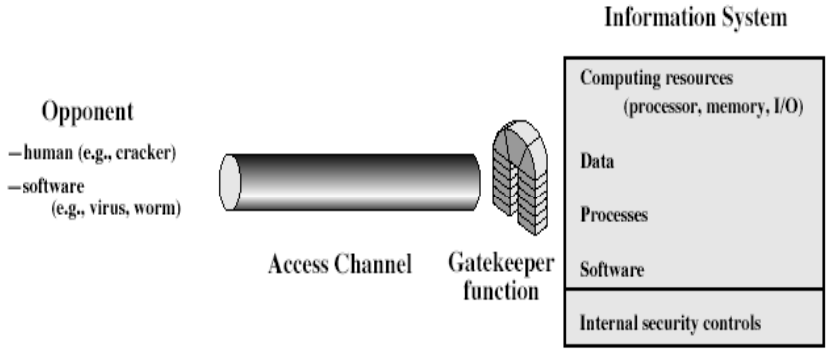
Concerned with controlled access to information or resources on a computer system, in the presence of possible opponents.

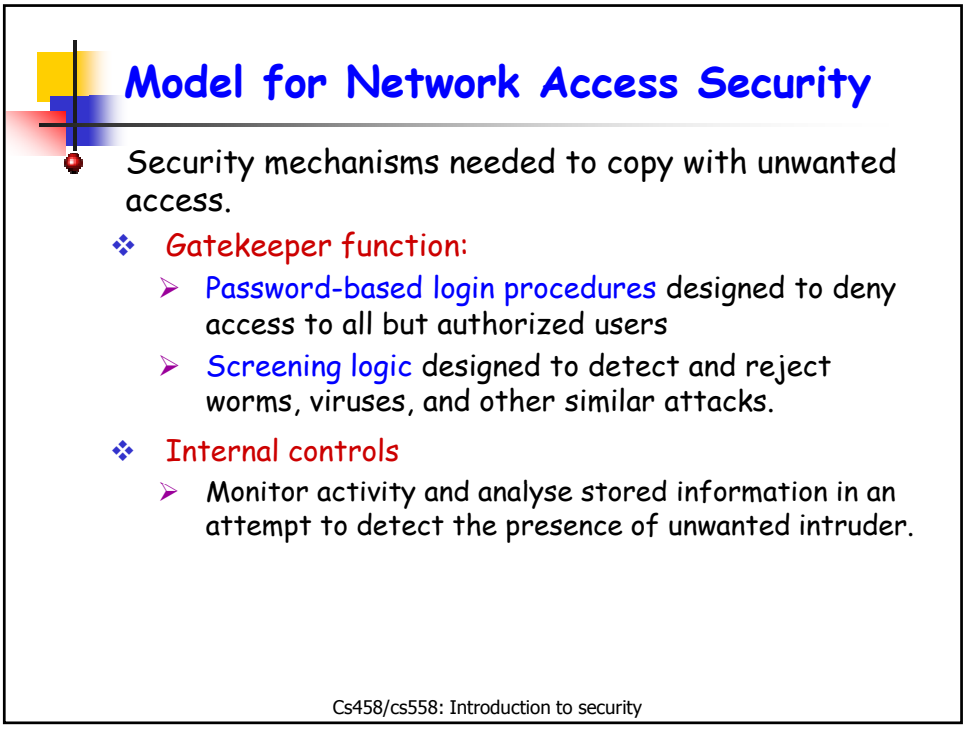
- Hackers: attempt to penetrate systems that can be accessed over a network



Model for Network Access Security

Virus and worms: software attacks. Such attacks can be introduced into a system by means of a disk or be inserted into a system across a network.

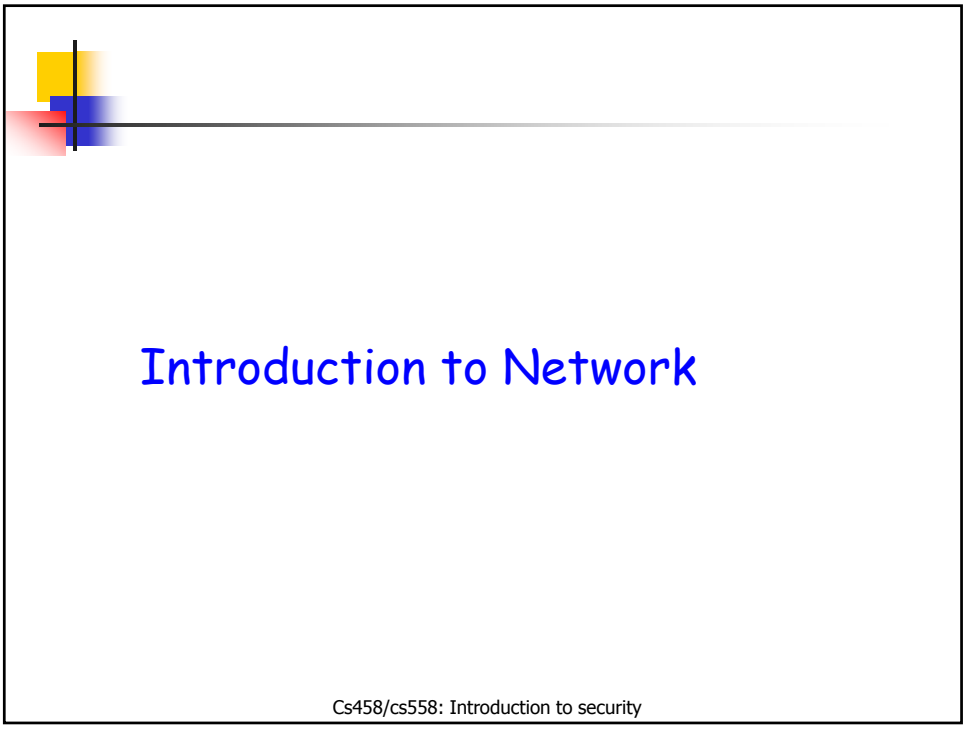




Model for Network Access Security

Security mechanisms needed to copy with unwanted access.

- Gatekeeper function:
  - Password-based login procedures designed to deny access to all but authorized users
  - Screening logic designed to detect and reject worms, viruses, and other similar attacks.
- Internal controls
  - Monitor activity and analyse stored information in an attempt to detect the presence of unwanted intruder.

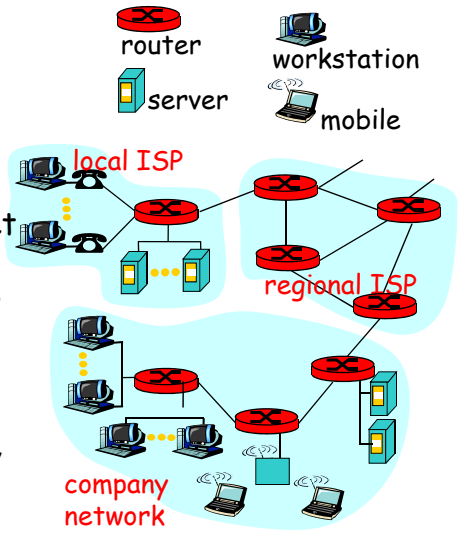


Introduction to Network

What's the Internet

What's the Internet

- A network that interconnects millions of computing devices (end systems) throughout the world.
- End systems access internet through Internet Service Providers (ISPs), companies that provide access to the Internet.
  - AT&T, Sprint, 56kbps dial-up modern access, cable modern, DSL, etc.



What's a protocol?…

- All communication activity in Internet governed by protocols
- A network protocol defines a language of rules and conventions for communication between network devices.
- Protocols define format, order of messages sent and received among network entities, and actions taken on message transmission

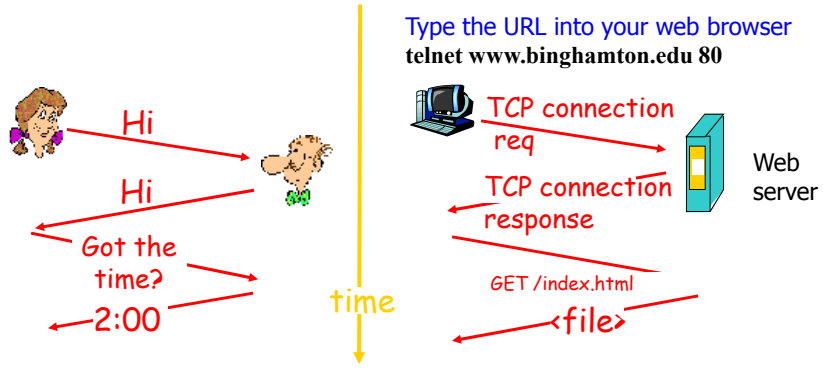
What's a protocol?…

- All communication activity in Internet governed by protocols
- A network protocol defines a language of rules and conventions for communication between network devices.
- Protocols define format, order of messages sent and received among network entities, and actions taken on message transmission
  - E.g. Transmission Control Protocol (TCP), Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP)

Cs458/cs558: Introduction to security

What's a protocol?

A human protocol and a computer network protocol:



A network protocol is similar to a human protocol except that the entities sending and receiving mesgs are hardware/software components of some device.

Protocol Layers

Protocol Layers

- Dealing with complex systems:
  - Provide a structural way to discuss system components.
  - Modularization eases maintenance, updating of system
    - Change of implementation of layer's service transparent to rest of system

Protocol Layers (Cont.)

- TCP/IP model: 5 layers

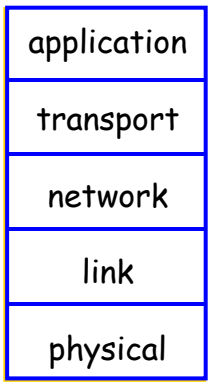
application
transport
network
link
physical

- OSI reference model: 7 layers

application
presentation
session
transport
network
link
physical

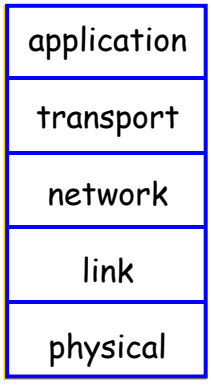
Internet protocol stack (TCP/IP Model)

- Application
  - Provides a means for the user to access information on the network through an application.
  - Supports network applications and application-layer protocols such as FTP, HTTP, SMTP.
  - Data sent over the network is passed into the application layer where it is encapsulated into the application layer protocol. The data is passed down into the transport layer.



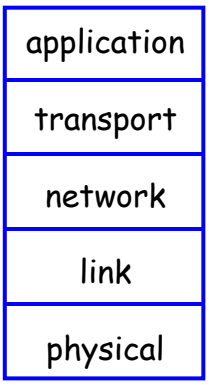
Internet protocol stack (TCP/IP Model)

- Transport
  - Provides transparent transfer of data between end users
  - Controls the reliability of a given link through flow control, segmentation/ desegmentation, and error control
  - Converts messages into TCP segments or User Datagram Protocol (UDP), etc.
    - TCP: a reliable connection-oriented protocol
    - UDP: an unreliable, connectionless protocol, application: e.g. streaming media (audio, video, voice over IP etc).



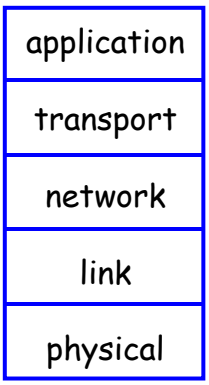
Internet protocol stack (TCP/IP Model)

- Network: routes datagrams from source to destination
  - Routers operate at this layer
  - IP, routing protocols
- Link: provides the functional and procedural means to transfer data between network entities
  - Bridges and link-layer switches operate.

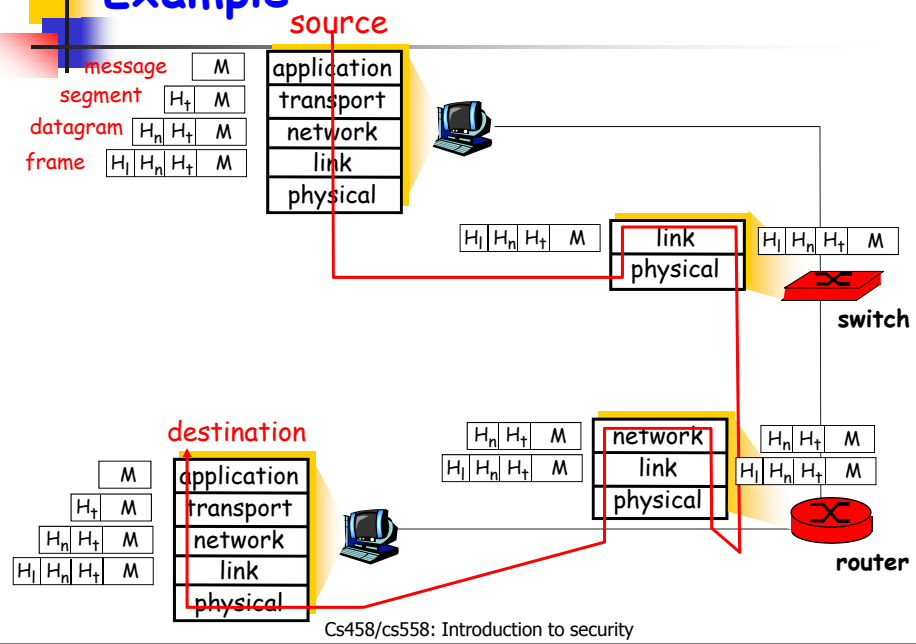


Internet protocol stack (TCP/IP Model)

- Physical: encodes and transmits raw data over network communications media (e.g. optical fiber).
  - Make sure that when one side sends a 1 bit, it is received by the other side as 1 bit.



Example



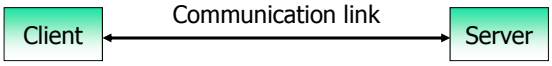
Reference

- TCP/IP model:
  http://en.wikipedia.org/wiki/TCP/IP_model

Socket Programming

Client-Server Model

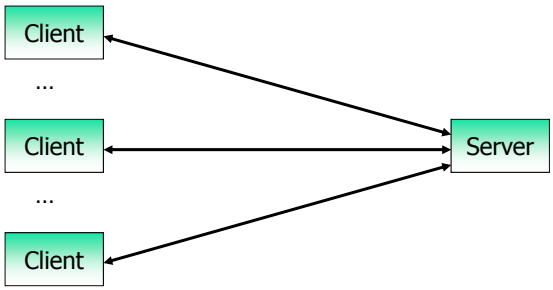
- Most network applications use the client-server model.



  - Client: requests, receives service from an always-on server
    - Needs to know of the existence of and the address of the server.
  - Server does not need to know the address of the client prior to the connection being established.
  - Once a connection is established, both sides can send and receive information.
  - A good analogy is a person who makes a phone call to another person.
  - e.g. Web browser/server; email client/server

Client-Server Model

- Most network applications use the client-server model.



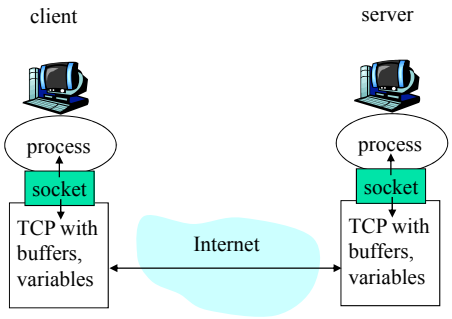
  - Clients usually communicate with one server a time
  - It is not unusual for a server to be communicating with multiple clients

Socket

- The system calls for establishing a connection are different for the client and the server
- But both involve the basic construct of a socket.

Sockets

- Process sends/receives messages to/from its socket
- Socket analogous to door
  - Sending process shoves message out door
  - Transport infrastructure brings message to the door at receiving process



Addressing Processes

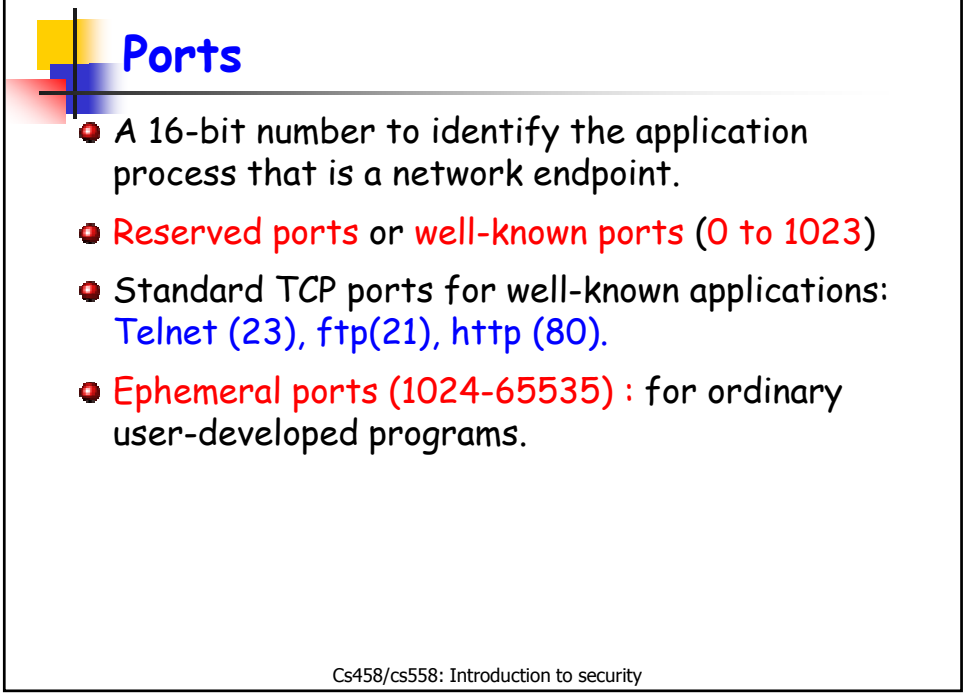
- For a process to receive messages, it must have an identifier.

Addressing Processes

- For a process to receive messages, it must have an identifier.
- Identifier includes both the IP address and port number associated with the process on the host.
  - A host has an IP address
  - Does the IP address of the host on which the process runs suffice for identifying the process?
    - Answer: no, many processes can be running on same host
  - Port: A 16-bit number to identify the application process that is a network endpoint.

IP Address (IPv4)

- An identifier for each machine connected to an IP network.
  - 32 bit binary number
  - Represented as dotted decimal notation:
    - 4 decimal values, each representing 8 bits (octet), in the range 0 to 255.
- Example:
  - Dotted Decimal: 140.179.220.200
  - Binary: 10001100.10110011.11011100.11001000


Ports
A 16-bit number to identify the application process that is a network endpoint.
Reserved ports or well-known ports (0 to 1023)
Standard TCP ports for well-known applications: Telnet (23), ftp(21), http (80).
Ephemeral ports (1024-65535) : for ordinary user-developed programs.
Cs458/cs558: Introduction to security