

MODULE 3: NETWORKING, THE INTERNET, CYBERSECURITY AND ETHICAL ISSUES

PART I: NETWORKING AND THE INTERNET (Chapter 4)

4.1 NETWORK FUNDAMENTALS

Definition: A network is a linked computer system where computers are connected so that data can be transferred from machine to machine.

Purpose: Share information and resources among different computers

- Exchange messages
- Share printing capabilities
- Share software packages
- Share data storage facilities

Network Classifications

By Geographic Scope:

Network Type	Range	Description	Examples
PAN (Personal Area Network)	< few meters	Short-range communications between personal devices	Wireless headset and smartphone, wireless mouse and PC
LAN (Local Area Network)	Single building/building complex	Collection of computers in close proximity	University campus network, manufacturing plant network
MAN (Metropolitan Area Network)	Local community	Intermediate size network	City-wide network, local community network
WAN (Wide Area Network)	Greater distance	Links machines across cities, countries, worldwide	Neighboring cities, opposite sides of the world

By Design Ownership:

Network Type	Description	Characteristics
Open Network	Designs in public domain	Freely circulated; grow in popularity; prevail over proprietary approaches
Closed/Proprietary Network	Innovations owned/controlled by entity	Restricted by license fees and contract conditions

Example of Open System:

- **Internet** - governed by open collection of standards called **TCP/IP protocol suite**
- Anyone free to use these standards without paying fees or signing license agreements

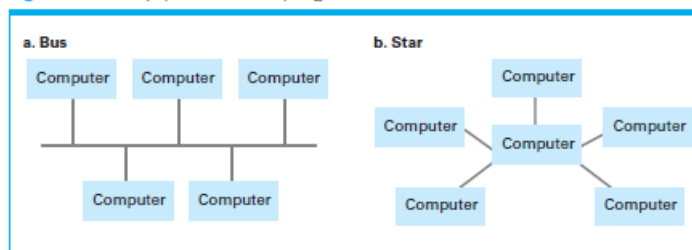
Example of Proprietary System:

- Novell Inc. - develops proprietary systems with ownership rights
- Company draws income from selling or leasing products

By Topology:

Two popular topologies are shown in FIGURE 4.1

Figure 4.1 Two popular network topologies



Topology	Description	Popularized By
Bus	Machines all connected to common communication line called bus	Ethernet (1990s)
Star	One machine serves as central focal point; all others connected to it	Wireless networks; central machine called Access Point (AP)

Important Distinction:

- Difference between bus and star is NOT always obvious by physical arrangement
- Bus network may have very short bus with long links to individual machines → looks like star
- **Hub**: Device at central location; all machines connect to it; relay signals back out to all machines
- Hub is little more than a very short bus
- Network looks like star but operates like bus

Protocols

Definition: Rules by which network activities are conducted

Importance:

- Developing and adopting protocol standards enables vendors to build compatible products
- Indispensable process in development of networking technologies

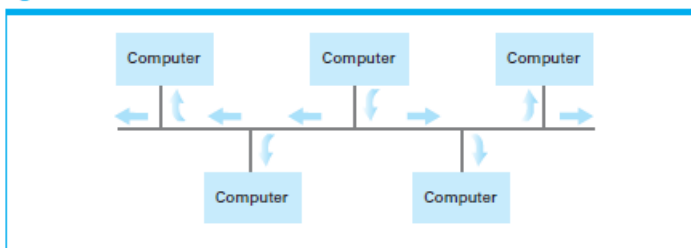
CSMA/CD (Carrier Sense, Multiple Access with Collision Detection):

- Protocol controlling right to transmit messages in bus network (Ethernet standards)

How CSMA/CD Works:

FIGURE 4.2

Figure 4.2 Communication over a bus network



Rules:

1. Each message broadcast to ALL machines on the bus
2. Each machine monitors all messages but keeps only those addressed to itself
3. To transmit: Wait until bus is silent, begin transmitting while continuing to monitor bus
4. If another machine also begins transmitting → both machines detect clash
5. Both pause for brief, independently RANDOM period of time

6. Try again after pause

Analogy: Small group of people in conversation

- If two people start to talk at once, both stop
- People: "I'm sorry, what were you going to say?" "No, no. You go first."
- CSMA/CD: Each machine tries again later

CSMA/CA (Carrier Sense, Multiple Access with Collision Avoidance):

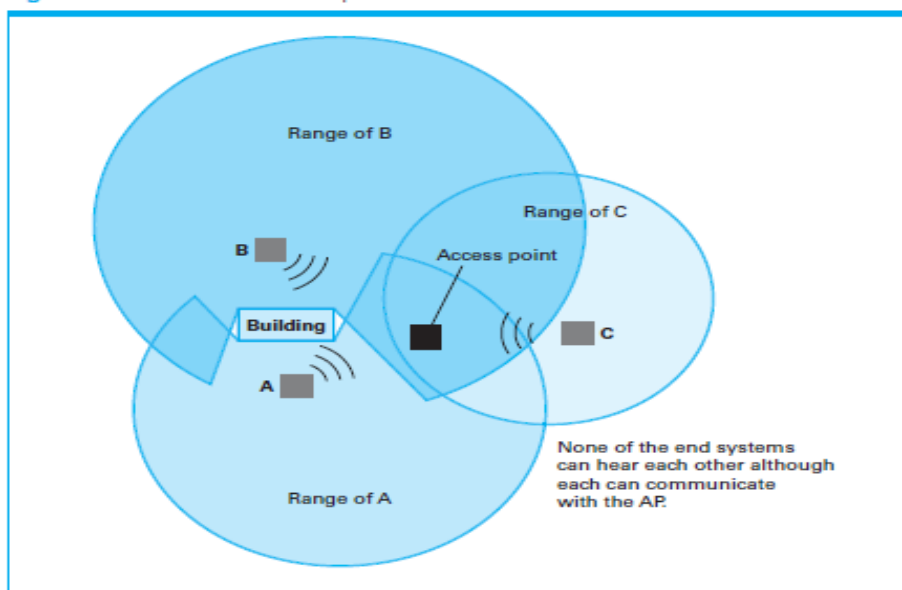
- Protocol for wireless star networks
- Standardized by IEEE within protocols defined in **IEEE 802.11**
- Commonly referred to as **WiFi**

Why CSMA/CD is NOT compatible with wireless star networks:

Problem	Description
Signal Drowning	Machine may not hear other's transmission because its own signal drowns out the other
Hidden Terminal Problem	Signals from different machines blocked from each other by objects or distance, even though they can all communicate with central AP

FIGURE 4.3: The hidden terminal problem

Figure 4.3 The hidden terminal problem



CSMA/CA Approach:

- Policy of trying to AVOID collisions rather than detect them
- Designed to avoid collisions but may not eliminate them completely
- When collisions occur, messages must be retransmitted

Common CSMA/CA Protocol:

1. When machine first needs to transmit and finds channel silent → does NOT start immediately
2. Waits for short period of time
3. Starts transmitting only if channel has remained silent throughout that period
4. If busy channel experienced during this process → waits for randomly determined period before trying again
5. Once this period exhausted → machine allowed to claim silent channel without hesitation

Result: Collisions between "newcomers" and those already waiting are avoided

- "Newcomer" not allowed to claim silent channel until any machine that has been waiting is given opportunity to start

Solving Hidden Terminal Problem:

- Protocol based on distinguishing silent vs. busy channel requires each station to hear all others
- Some WiFi networks: Each machine sends short "REQUEST" message to AP
- Waits until AP acknowledges request before transmitting entire message
- If AP busy (dealing with hidden terminal) → ignores request → requesting machine waits
- If AP acknowledges request → machine knows it is safe to transmit
- All machines hear all acknowledgments from AP → have good idea whether AP is busy

Combining Networks

Need: Sometimes necessary to connect existing networks to form extended communication system

Connecting Same Type Networks:

Device	Function	Behavior
Repeater	Passes signals back and forth between two original buses	Usually with amplification; without considering meaning of signals
Bridge	Connects two buses; does NOT necessarily pass all messages	Looks at destination address; forwards message across connection only when destined for computer on other side
Switch	Bridge with multiple connections	Connects several buses; forwards messages only into appropriate spoke; minimizes traffic in each spoke

Important Note:

- When networks connected via repeaters, bridges, and switches → result is SINGLE large network
- Entire system operates in same manner (using same protocols) as each original smaller network

Connecting Different/Incompatible Networks:

Internet (generic term):

- Network of networks
- Original networks maintain their individuality
- Continue to function as autonomous networks

Router:

- Special purpose computers used for forwarding messages
- Provide links between networks while allowing each network to maintain its unique internal characteristics
- Named because purpose is to forward messages in their proper directions

Forwarding Process:

1. Based on internet-wide addressing system

2. All devices in internet (machines in original networks AND routers) assigned unique addresses
3. Each machine has TWO addresses:
 - Original "local" address within its own network
 - Internet address
4. Machine wanting to send message to distant network:
 - Attaches internet address of destination to message
 - Directs message to its local router
5. Router forwards message in proper direction
6. Each router maintains **forwarding table**:
 - Contains router's knowledge about direction to send messages based on destination addresses

Gateway:

- The "point" at which one network is linked to an internet
- Serves as passageway between network and outside world
- Term used loosely
- Often merely the router through which network communicates with rest of internet
- Residential WiFi networks: term refers collectively to both network's AP and router (packaged in single unit)

Methods of Process Communication

Interprocess Communication:

- Communication between processes executing on different computers (or same machine via time-sharing/multitasking)
- Must often coordinate actions and perform designated tasks

Client/Server Model:

Role	Description
Client	Makes requests of other processes
Server	Satisfies requests made by clients

Early Applications:

Application	Server Type	Client Action
Office Network Printer	Print Server	Send print requests
Shared Magnetic Disk Storage	File Server	Request access to records/files

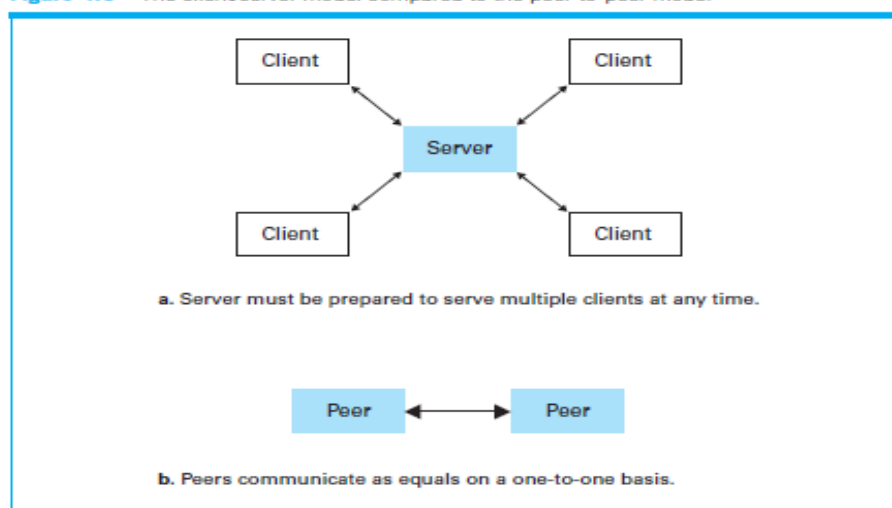
Today: Client/server model used extensively in network applications

Peer-to-Peer (P2P) Model:

Aspect	Client/Server	Peer-to-Peer
Service Direction	One-way (server serves clients)	Two-way (peers provide AND receive service)
Execution	Server must execute continuously	Peers execute on temporary basis
Examples	Web servers, file servers	Instant messaging, competitive interactive games

FIGURE 4.6

Figure 4.6 The client/server model compared to the peer-to-peer model



File Distribution - Swarm:

- Collection of peers participating in file distribution
- One peer receives file from another, then provides that file to other peers

- Replaces client/server model (central distribution center)

Why P2P Replaces Client/Server for File Sharing:

1. Distributes service task over many peers rather than concentrating at one server
2. Lack of centralized base → more efficient system
3. In cases of questionable legality: lack of central server makes legal efforts to enforce copyright laws more difficult

Important Terminology Note:

Peer-to-peer refers to system by which TWO PROCESSES communicate over a network

- NOT a property of the network itself
- Process might use P2P model for one communication and client/server for another over same network
- More accurate: "communicating by means of peer-to-peer model" NOT "communicating over peer-to-peer network"

Distributed Systems

Definition: Software systems consisting of software units that execute as processes on different computers

Examples:

- Global information retrieval systems
- Company-wide accounting and inventory systems
- Computer games
- Software that controls network's infrastructure

Evolution:

- Early distributed systems: developed independently from scratch
- Today: research reveals common infrastructure running throughout these systems
- Communication and security systems
- Prefabricated systems provide basic infrastructure
- Distributed applications constructed by developing only the part unique to the application

Types of Distributed Computing Systems:

System	Description	Characteristics
Cluster Computing	Many independent computers work closely together	Provides computation/services comparable to much larger machine; lower cost than supercomputer; higher reliability; lower maintenance costs
Grid Computing	More loosely coupled than clusters; work together to accomplish large tasks	Specialized software to distribute data and algorithms; machines volunteer computing power when not otherwise used; enabled by growing Internet connectivity
Cloud Computing	Huge pools of shared computers on network allocated for use by clients as needed	Eliminates need for entities to maintain their own generators; rent virtual computers by hour; reasonable guarantees of reliability and scalability; raises concerns about privacy and security

Examples:

- **Cluster:** High-availability systems, load-balancing
- **Grid:** University of Wisconsin's Condor system, Berkeley's Open Infrastructure for Network Computing (BOINC)
- **Cloud:** Amazon's Elastic Compute Cloud, Google Drive, Google Apps

4.2 THE INTERNET

Definition: The most notable example of an internet (uppercase I)

Origin:

- Research projects dating back to early 1960s
- Goal: Link variety of computer networks to function as connected system not disrupted by local disasters
- Sponsored by U.S. government through **DARPA (Defense Advanced Research Projects Agency)**

Evolution:

- Government-sponsored project → Academic research project → Commercial undertaking
- Links worldwide combination of PANs, LANs, MANs, and WANs
- Involves millions of computers

Internet Architecture

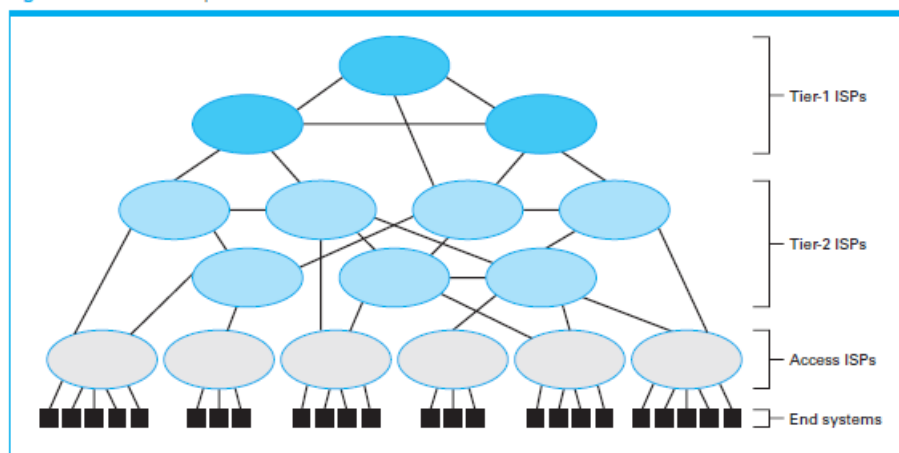
ISP (Internet Service Provider):

- Organizations that construct and maintain networks
- Also refers to the networks themselves
- "Connecting to an ISP" = connecting to network provided by ISP

Three-Tier ISP Hierarchy:

Below Figure 4.7 is the internet Composition

Figure 4.7 Internet composition



Tier	Description	Role
Tier-1 ISPs	Very high-speed, high-capacity, international WANs	Backbone of the Internet; operated by large communications companies
Tier-2 ISPs	More regional in scope; less potent	Connect to tier-1 ISPs; operated by communications companies
Access ISP/Tier-3 ISP	Independent internet (intranet) operated by single authority	Supplies Internet access to individual homes and businesses; examples: cable companies, telephone companies, universities, corporations

End Systems / Hosts:

- Devices individual users connect to access ISPs
- Laptops, PCs, telephones, video cameras, automobiles, home appliances

- Internet = communications system → any device that would benefit from communicating is potential end system

Connection Technologies:

Technology	Description
WiFi	Fastest growing; wireless connections; AP connected to access ISP; area within AP range = hot spot
Cellular	Similar to WiFi; hot spots known as cells ; routers coordinated to provide continuous service as end system moves
Telephone Lines	Direct connection or through customer's router; DSL modems
Cable/Satellite Systems	Direct connection or through customer's router; cable modems

Hot Spots:

- Area within AP or group of APs' range
- Particularly when network access is publicly available or free
- Found in: individual residences, hotel and office buildings, small businesses, parks, entire cities

Internet2:

- Intended as academic-only system
- Universities working in partnership with industry and government
- Goal: Research in internet applications requiring high bandwidth communication
- Examples: remote access and control of telescopes, medical diagnostic devices, remote surgery

The Last Mile Problem:

Definition: Issues arising from legacy analog linkages in older network infrastructure

Context:

- Telephone, cable television, satellite WANs (20th century) = designed to carry ANALOG communications
- Human voice, pre-digital television signals
- Modern networks = designed to carry DIGITAL data directly
- Older analog network infrastructure still comprises significant portion of Internet

Problem:

- Main arteries of WANs, MANs, LANs = relatively easy to modernize with high-speed digital technology (fiber optics)
- Far costlier to replace existing copper telephone lines and coaxial cables connecting these arteries to individual homes/offices
- Information may spend almost entire trip on high-speed digital connections
- Only to traverse "last mile" to end system over slow, century-old analog phone line

Solutions:

- DSL modems
- Cable modems
- Satellite uplinks
- Direct fiber-optic connections to the home

Result: Broadband Internet access to end users

Internet Addressing

IP Address:

- Internet-wide addressing system
- Assigns unique identifying address to each computer in the system
- Term IP = "Internet Protocol"
- Originally: 32-bit patterns
- Currently: converting to 128-bit addresses (IPv6)

ICANN (Internet Corporation for Assigned Names and Numbers):

- Nonprofit corporation
- Coordinates Internet's operation
- Awards blocks of consecutively numbered IP addresses to ISPs
- ISPs allocate addresses within their awarded blocks to machines in their region

Dotted Decimal Notation:

- Traditional way of writing IP addresses
- Bytes of address separated by periods
- Each byte expressed as integer in traditional base 10 notation

Examples:

- Pattern 5.2 = two-byte bit pattern 00000101 00000010
- Pattern 17.12.25 = three-byte bit pattern 00010001 00001100 00011001
- 32-bit IP address: 192.207.177.133

Domain Name System (Mnemonic Addressing):

- Alternative addressing system for human consumption
- Machines identified by mnemonic names
- Based on concept of **domain**

Domain:

- "Region" of Internet operated by single authority
- University, club, company, government agency
- May not correspond to physical area of Internet

Registration:

- Domain must be registered with ICANN
- Process handled by **registrars** (companies assigned this role by ICANN)
- Domain assigned mnemonic **domain name** (unique among all domain names throughout Internet)
- Domain names often descriptive of organization

Example:

- Marquette University domain name: mu.edu
- Suffix (edu) = **top-level domain (TLD)**

Top-Level Domains (TLDs):

TLD	Classification
edu	Educational institutions
com	Commercial institutions
gov	U.S. government institutions
org	Nonprofit organizations
museum	Museums
info	Unrestricted use
net	Originally for ISPs, now broader
au, ca, etc.	Country-code TLDs (Australia, Canada)

Domain Name Extension:

- Organization free to extend name for individual items within domain
- Example: eagle.mu.edu (individual host within Marquette University)
- Domain names extended to the left, separated by period
- Multiple extensions (**subdomains**) organize names within domain
- Example: overthruster.propulsion.yoyodyne.com
 - overthruster = computer
 - propulsion = subdomain
 - yoyodyne = domain
 - com = TLD

Important: Dotted notation in mnemonic addresses NOT related to dotted decimal notation for IP addresses

Domain Name System (DNS):

- Messages always transferred over Internet by IP addresses
- Mnemonic address must be converted into IP address before transmitting
- Conversion performed with aid of numerous **name servers**
- Name servers = directories providing address translation services to clients
- Collectively = Internet-wide directory system called **Domain Name System (DNS)**
- Process = **DNS lookup**

Name Server Models:

Model	Description
Original Model	Registered domain = physical region of Internet operated by local authority; organization maintains its own name server
Modern Model	Individuals/small organizations contract with access ISP; ISP registers domain name; name included in ISP's name server; DNS lookups directed to ISP's name server

Result: Many registered domains can reside within single ISP, each occupying small portion of single computer

Internet Applications

Historical:

- Most applications were separate, simple programs
- Each followed network protocol
- Newsreader: NNTP (Network News Transfer Protocol)
- File listing/copying: FTP (File Transfer Protocol)
- Remote access: Telnet protocol, later SSH (Secure Shell)

Today:

- More traditional network applications handled by webpages via HTTP
- More sophisticated web servers and browsers

Electronic Mail (Email):

SMTP (Simple Mail Transfer Protocol):

- Defines how two computers on network interact when transmitting email message
- Transmits email messages from one host to another
- Example exchange between mail servers:

text

```
1 220 mail.tardis.edu SMTP Sendmail Gallifrey-1.0; Fri, 23 Aug 2413 14:34:10
2 HELO mail.skaro.gov
3 250 mail.tardis.edu Hello mail.skaro.gov, pleased to meet you
4 MAIL From: dalek@skaro.gov
5 250 2.1.0 dalek@skaro.gov...Sender ok
6 RCPT To: doctor@tardis.edu
7 250 2.1.5 doctor@tardis.edu...Recipient ok
8 DATA
9 354 Enter mail, end with "." on a line by itself
10 Subject: Extermination.
11 EXTERMINATE!
13 Regards, Dalek
14 250 2.0.0 r7NJYAE1028071 Message accepted for delivery
16 QUIT
17 221 2.0.0 mail.tardis.edu closing connection
```

Protocol Characteristics:

- Keywords: HELO, MAIL, RCPT, DATA, QUIT precisely defined
- Remote server's numeric response codes enumerated and defined
- Software designers use protocol description to develop algorithms for sending/receiving email

Historical Note:

- Politeness ("pleased to meet you") neither appreciated by software nor essential to SMTP function
- Actual behavior built into popular SMTP mail server

- Held over from early Internet days when human operators frequently reviewed SMTP transcripts
- Debugged incompatibilities between mail servers
- Untold millions of these exchanges occur on network each day

SMTP Trust Problem:

- SMTP = example of protocol originally built on trust
- Subsequently abused by spammers and other Internet miscreants
- Modern mail servers use extended versions of SMTP to ensure secure transmission

MIME (Multipurpose Internet Mail Extensions):

- SMTP initially designed for transferring text messages encoded with ASCII
- Additional protocols developed to convert non-ASCII data to SMTP compatible form

Email Access Protocols:

Protocol	Full Name	Description
POP3	Post Office Protocol version 3	Simpler; user transfers (downloads) messages to local computer; read, stored, edited on local machine
IMAP	Internet Mail Access Protocol	User stores and manipulates messages on same machine as mail server; accessible from any remote computer

VoIP (Voice over Internet Protocol):

Definition: Internet infrastructure used to provide voice communication similar to traditional telephone systems

Simple Form: Two processes on different machines transferring audio data via P2P model

Complex Issues:

- Initiating and receiving calls
- Linking VoIP with traditional telephone systems
- Providing services such as emergency 911 communication
- Governments that own traditional telephone companies view VoIP as threat
- Taxed heavily or outlawed completely in some countries

Internet Multimedia Streaming:

Fact: Netflix streamed more than 4 billion hours of programming in first three months of 2013 alone

Fact: YouTube + Netflix consume more than half of bandwidth of Internet in 2014

N-unicast Approach:

- Internet radio station establishes server that sends program messages to each client who requested them
- **Unicast:** One sender sending messages to one receiver
- **N-unicast:** Single sender involved with multiple unicasts

Drawback:

- Places substantial burden on station's server
- Places substantial burden on server's immediate Internet neighbors
- Server must send individual messages to each client on real-time basis
- All these messages must be forwarded by server's neighbors

Alternatives to N-unicast:

Alternative	Description
P2P Model	Once peer has received data, begins distributing to peers still waiting; distribution problem transferred from source to peers
Multicast	Server transmits message to multiple clients via single address; relies on Internet routers to recognize significance of address; produce and forward copies to appropriate destinations

Multicast Support:

- Implemented in small networks
- Has yet to expand to global Internet
- Requires functionality of Internet routers expanded beyond original duties

On-Demand Streaming:

- Most important category
- End user expects to view/listen to media at arbitrary time of own choosing
- Start, pause, rewind content at own pace
- N-unicast and multicast technologies of little help

- Each on-demand stream = effectively unicast from media server storing content to end user retrieving it

Wireless Telephone Generations:

Generation	Characteristics
1G (First Generation)	Analog voice signals through air; like traditional telephones without copper wire
2G (Second Generation)	Digital signals to encode voice; more effective use of airwaves; transmission of other data (text messaging)
3G (Third Generation)	Higher data rates; mobile video calls; bandwidth-intensive activities
4G (Fourth Generation)	Even higher data rates; fully packet-switched IP network; smartphones enjoy connectivity and flexibility previously available only to broadband-enabled PCs

4.3 THE WORLD WIDE WEB

Origin:

- Work of Tim Berners-Lee (British scientist)
- Realized potential of combining internet technology with concept of linked-documents called **hypertext**
- First software for implementing Web released December 1990

Early Prototype:

- Did not yet support multimedia data
- Included key components of what we now recognize as World Wide Web:
 1. Hypertext document format for embedding **hyperlinks** to other documents
 2. Protocol for transferring hypertext across the network
 3. Server process that supplied hypertext pages upon request

Growth:

- Quickly grew to support images, audio, video
- By mid-1990s: dominant application powering growth of Internet

Web Implementation

Two Categories of Software Packages:

Type	Description	Examples
Browser	Resides on user's computer; obtains materials requested by user; presents materials in organized manner	Firefox, Safari, Internet Explorer
Webserver	Resides on computer containing hypertext documents; provides access to documents under its control as requested by clients	Apache, IIS, Nginx

HTTP (Hypertext Transfer Protocol):

- Protocol used to transfer hypertext documents between browsers and web servers

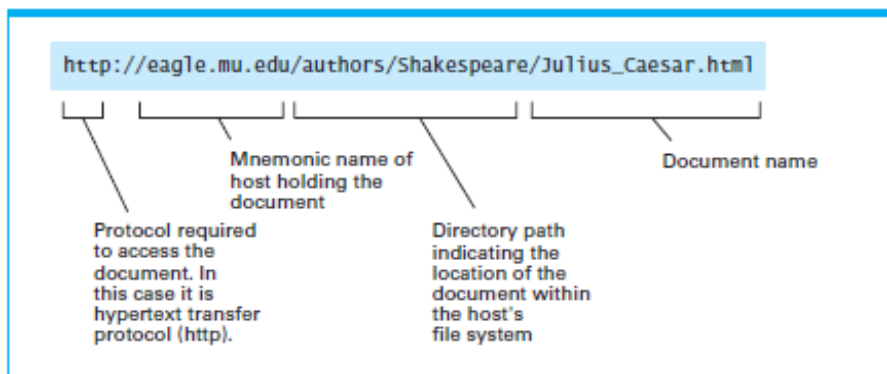
URL (Uniform Resource Locator):

- Unique address for each document on the Web
- Contains information needed by browser to contact proper server and request desired document

Components of a Typical URL:

FIGURE 4.8

Figure 4.8 A typical URL



Segment	Purpose
Protocol	Protocol to communicate with server controlling access to document
Machine Address	Mnemonic address of machine containing the server
Directory Path	Path needed for server to find directory containing document
Document Name	Name of the document itself

Shortened URLs:

- May not explicitly contain all segments
- No directory path if server doesn't need it
- URL consisting of only protocol and mnemonic address → webserver returns predetermined document (**home page**)
- Home page usually describes information available at that website

Example:

- `http://www.google.com` → leads to Google home page
- Contains hyperlinks to services, products, documents relating to company

Browser Assumption:

- Many browsers assume HTTP protocol should be used if no protocol identified
- Correctly retrieve Google home page when given URL consisting merely of `www.google.com`

HTML (Hypertext Markup Language)

Traditional Hypertext Document:

- Similar to text file
- Text encoded character by character using ASCII or Unicode
- Contains special symbols called **tags**

Tags:

- Describe how document should appear on display screen

- Indicate what multimedia resources (images) should accompany document
- Identify which items within document are linked to other documents

HTML:

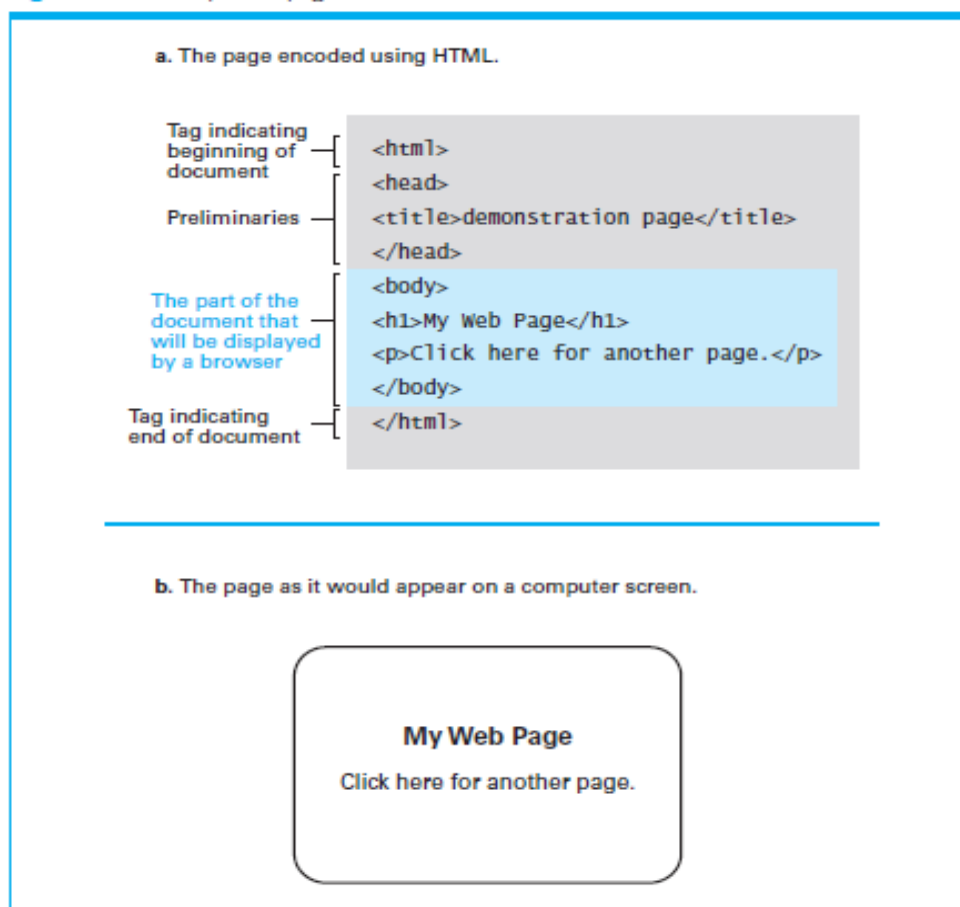
- System of tags for describing webpage presentation and links
- Author describes information browser needs to present page and find related documents

Analogy:

- Adding typesetting directions to plain typed text (using red pen)
- Typesetter knows how material should appear in final form
- HTML tags = red markings
- Browser = typesetter

Simple Webpage HTML code is shown in FIGURE 4.9

Figure 4.9 A simple webpage



Document Structure:

Section	Tags	Purpose
Head	<code><head> </head></code>	Preliminary information about document (title)
Body	<code><body> </body></code>	Material to be presented on computer screen

Common Tags:

Tag	Meaning	Description
<code><h1> </h1></code>	Level-one heading	Display text prominently
<code><p> </p></code>	Paragraph	Block of text
<code><title> </title></code>	Title	Documentation only; not displayed on screen

Adding Hyperlinks - Anchor Tags:

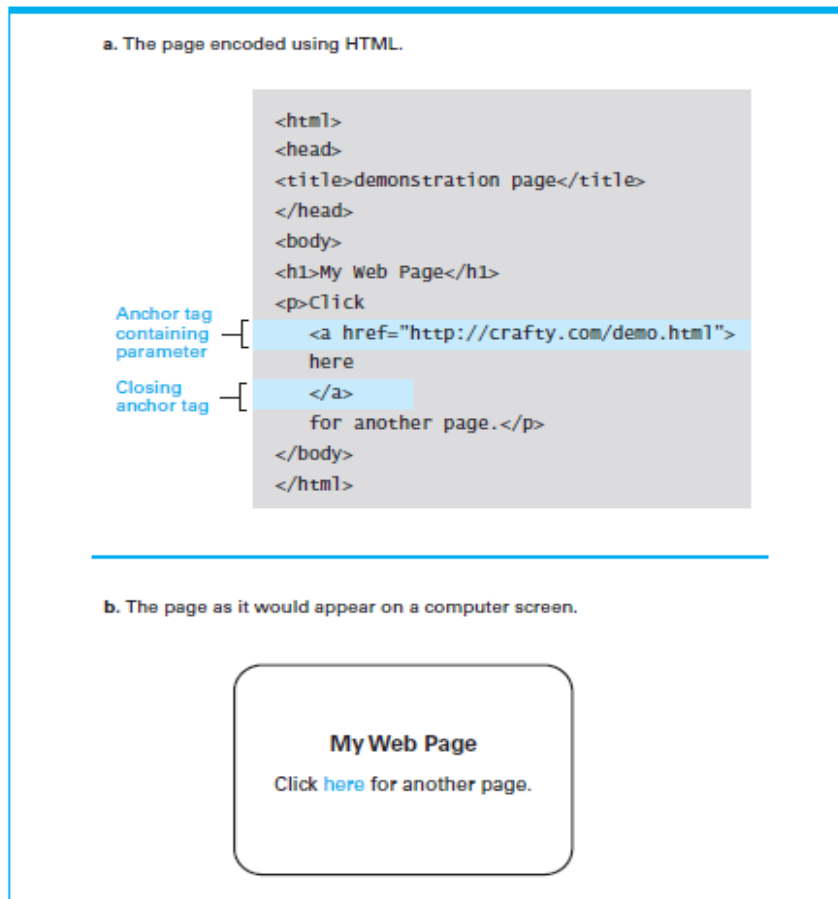
Purpose: Link word here to another document

URL Example: <http://crafty.com/demo.html>

HTML Code:

FIGURE 4.10

Figure 4.10 An enhanced simple webpage



Parameter: href = "http://crafty.com/demo.html"

- href = hypertext reference
- URL following equal sign = document to retrieve when link clicked

Adding Images:

Assumption: JPEG encoding of image stored as file OurPic.jpg in directory Images at Images.com, available via webserver

HTML Code:

text

```

```

Placement:

- Immediately after <body> tag → image at top of webpage
- Just before </body> tag → image at bottom of webpage

Parameter: src = "source"

- Information following equal sign indicates source of image to be displayed

Process:

1. Browser finds image tag
2. Sends message to HTTP server at Images.com requesting image OurPic.jpg
3. Displays image appropriately

XML (eXtensible Markup Language)

Concept:

- HTML = notational system for encoding text document + appearance as simple text file
- Similarly, encode nontextual material as text files
- Example: Sheet music

Music Encoding Example:

text

```
<staff clef="treble">
  <key>C minor</key>
  <time>2/4</time>
  <measure>
    <rest>egh</rest>
    <notes>egh G, egh G</notes>
  </measure>
  <measure>
    <notes>hlf E</notes>
  </measure>
</staff>
```

text

FIGURE 4.11

Figure 4.11 The first two bars of Beethoven's Fifth Symphony



Style Similarities with HTML:

- Tags delineated by < and >
- Beginning and end of structures indicated by tags of same name
- Ending tag designated by slash (</measure>)
- Special attributes within tags: clef="treble"

XML:

- Standardized style for designing notational systems for representing data as text files
- Simplified derivative of **SGML (Standard Generalized Markup Language)**
- Markup languages developed following XML standard for:
 - Mathematics
 - Multimedia presentations
 - Music

HTML and XML:

- HTML = markup language based on XML standard developed for representing webpages
- Original HTML developed before XML standard was solidified
- Some features of HTML do not strictly conform to XML
- **XHTML** = version of HTML that rigorously adheres to XML

Significance of XML:

- Standard for markup languages in GENERAL
- Not designing individual, unrelated markup languages
- Markup languages developed possess uniformity
- Can be combined to obtain markup languages for complex applications
- Example: text documents containing segments of sheet music AND mathematical expressions

Semantic vs. Appearance Markup:

Aspect	HTML (Appearance-oriented)	XML (Semantic-oriented)
Recipe ingredients	Marked as list; each ingredient on separate line	Marked as <ingredient> tags

Aspect	HTML (Appearance-oriented)	XML (Semantic-oriented)
Search capability	Find recipes containing/not containing certain WORDS	Find recipes containing/not containing certain INGREDIENTS

Example:

- Search for lasagna recipes without spinach
- Semantic tags: identify recipes where spinach is NOT an ingredient
- Word content search: skips over recipe starting with "This lasagna does not contain spinach"

World Wide Semantic Web:

- Using Internet-wide standard for marking documents according to semantics rather than appearance
- Would create Semantic Web (vs. today's Syntactic Web)

Client-Side and Server-Side Activities

Simple Webpage Retrieval Process:

1. Browser (client) uses URL to contact webserver
2. Requests copy of page
3. Server responds by sending text document (HTML source)
4. Browser interprets HTML tags
5. Displays page on screen
6. User clicks link → browser uses URL in anchor tag to contact appropriate server
7. Obtain and display another webpage

Process Summary: Browser fetches and displays webpages as directed by user

Need for Enhanced Activity:

- Webpage with animation
- Customer order form submission
- Requires additional activity by browser OR webserver

Type	Performed By	Description
Client-Side Activities	Client (browser)	Executed on user's computer
Server-Side Activities	Server (webserver)	Executed on server computer

Examples:

Application	Client-Side Activity	Server-Side Activity
Travel Agent	Customer specifies destinations/dates	Construct customized webpage; send to customer
Search Engine	User specifies topic of interest	Construct customized webpage identifying documents of possible interest
Web Mail	User creates messages; browser displays mail	Build webpages with information from mail server; forward messages to mail server

Technologies for Client/Server Activities:

Client-Side Technologies:

Technology	Description	Developer
JavaScript	Programs included within HTML source document; browser extracts and follows as needed	Netscape Communications, Inc.
Applets	Program units transferred to browser as requested within HTML source document	Sun Microsystems (Java)
Flash	Extensive multimedia client-side presentations	Macromedia

Server-Side Technologies:

Technology	Description	Developer
CGI (Common Gateway Interface)	Clients request execution of programs stored at server	Standards-based
Servlets	Clients cause program units to be executed at server side	Sun Microsystems
JSP (JavaServer Pages)	Webpage templates completed using information received from client	Sun Microsystems
ASP (Active Server Pages)	Templates for constructing customized webpages	Microsoft
PHP	Open source system for server-side functionality	Open source community

Security and Ethical Problems:

Server Side (Ethical):

- Webservers routinely transfer programs to clients where they are executed
- Ethical questions arise

Client Side (Security):

- Client blindly executes any program sent by webserver
- Opens itself to malicious activities by server

Server Side (Security):

- Clients can cause programs to be executed at server
- Server blindly executes any program sent by client
- Security breaches and potential damage at server can result

4.4 INTERNET PROTOCOLS

Goal: Understand how messages are transferred over the Internet

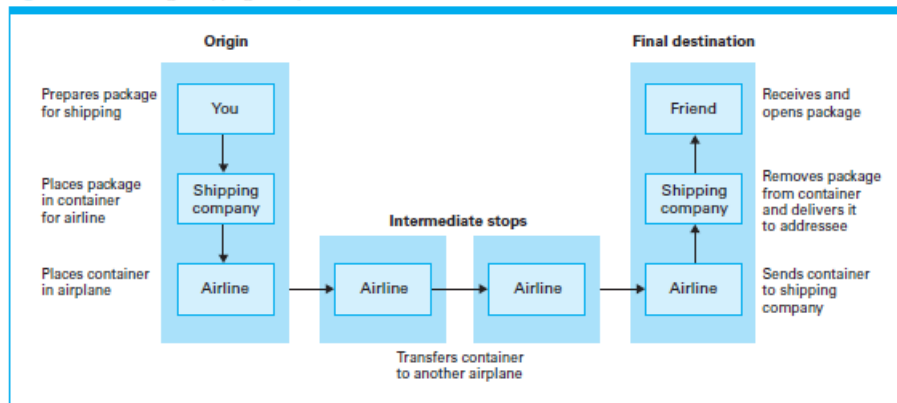
Key Insight:

- Transfer process requires cooperation of ALL computers in the system
- Software for controlling this process resides on EVERY computer in the Internet

The Layered Approach to Internet Software

Analogy - Shipping a Gift: Below FIGURE 4.12 shows the Package shipping example

Figure 4.12 Package-shipping example



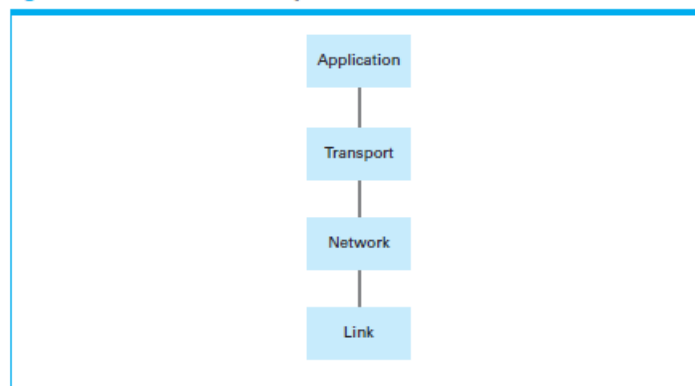
Key Properties:

- Three-level hierarchy
- Each level uses next lower level as abstract tool
- Each level has representatives at both origin and destination
- Destination representatives tend to do reverse of origin counterparts

Internet Software - Four Layers:

FIGURE 4.13 shows the Internet software layers

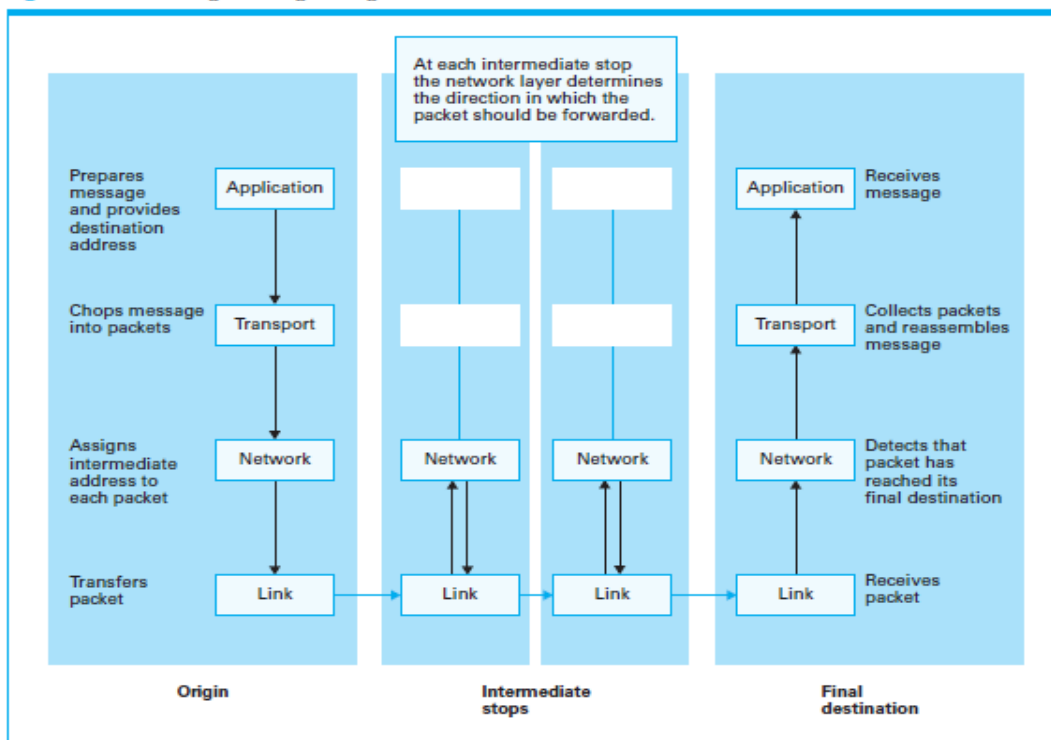
Figure 4.13 The Internet software layers



Layer	Function
Application Layer	Software units using Internet communication (clients, servers)
Transport Layer	Accept messages from application layer; ensure proper formatting; divide long messages into small segments; add sequence numbers; reassemble at destination
Network Layer	Decide direction packet should be sent at each step; maintain router's forwarding table
Link Layer	Transfer packet; handle communication details particular to individual network

Following a message through the internet is shown in the below FIGURE 4.14

Figure 4.14 Following a message through the Internet



Detailed Process:

1. Application Layer:

- Software units (clients, servers) that use Internet communication
- NOT restricted to application software classification

- Includes many utility packages (FTP, SSH)
- Provides address compatible with Internet infrastructure
- May use name servers to translate mnemonic addresses into IP addresses

2. Transport Layer:

- Accepts messages from application layer
- Ensures messages are properly formatted for transmission
- Divides long messages into small **segments**
- Adds **sequence numbers** to segments
- Hands these segments (now called **packets**) to network layer
- Packets treated as individual, unrelated messages until reaching destination transport layer
- Packets related to common message may follow different paths through Internet

3. Network Layer:

- Decides direction packet should be sent at each step
- Combination of network layer + link layer = software residing on Internet routers
- Maintains router's **forwarding table**
- Uses forwarding table to determine direction to forward packets
- At packet's origin: receives packet from transport layer, determines where packet should be sent, hands to link layer

4. Link Layer:

- Responsible for transferring packet
- Deals with communication details particular to individual network
- Ethernet: applies CSMA/CD
- WiFi: applies CSMA/CA

At Intermediate Stops (Routers):

- Only link and network layers are involved
- These are the only layers present on routers
- Network layer determines direction of packet's next step
- Returns packet to link layer to be forwarded

Router Performance:

- Time required for modern router to forward packet = millionths of a second

- Forwarding role of network layer within router closely integrated with link layer

At Destination:

- Network layer recognizes packet's journey is complete
- Hands packet to transport layer (not forwarding)
- Transport layer extracts message segments
- Reconstructs original message according to sequence numbers
- Hands message to appropriate unit within application layer

Port Numbers:

- Determine which unit within application layer should receive incoming message
- Unique port numbers assigned to various units
- Appropriate port number appended to message's address before starting journey
- Transport layer at destination hands message to application layer software at designated port number

Common Port Numbers:

Application	Port Number
HTTP Server(Hyper Text Transfer Protocol)	80
SMTP Mail Server(Simple Mail Transfer Protocol)	25

The TCP/IP Protocol Suite

Definition: Collection of protocol standards used by Internet to implement four-level communication hierarchy

TCP vs. UDP:

Feature	TCP	UDP
Connection	Connection-oriented (establishes connection before sending)	Connectionless (sends message and forgets)

Feature	TCP	UDP
Reliability	Reliable protocol; acknowledgments and retransmissions assure successful transfer	Unreliable protocol; no retransmission services
Flow Control	Can reduce transmission rate to keep from overwhelming destination	No flow control
Congestion Control	Can adjust transmission rate to alleviate congestion	No congestion control
Efficiency	Less efficient (more overhead)	More streamlined, efficient
Typical Uses	Email, web pages	DNS lookups, VoIP

IP (Internet Protocol):

- Internet's standard for implementing tasks assigned to network layer

Two Main Tasks:

Task	Description
Forwarding	Relaying packets through the Internet
Routing	Updating layer's forwarding table to reflect changing conditions

Routing Reasons:

- Router malfunctions → traffic should no longer be forwarded in its direction
- Section of Internet becomes congested → traffic should be routed around blockage

Hop Count (Time to Live):

- Value appended to packet when IP network layer prepares packet
- Limit to number of times packet should be forwarded
- Each time IP network layer forwards packet → decrements hop count by 1
- Protects Internet from packets circling endlessly within system

- Initial hop count of 64 = more than sufficient for packet to find way through today's ISPs

IPv4 vs. IPv6:

Version	Address Size	Status
IPv4 (IP version four)	32-bit	Used for years; Internet rapidly outgrowing
IPv6 (IP version six)	128-bit	Established; conversion underway; expected 32-bit addresses extinct by 2025

Additional IPv6 Improvements:

- Multicast
- Other protocol enhancements

4.5 SECURITY

Problem: When computer connected to network → subject to unauthorized access

Forms of Attack

Malware (Malicious Software):

- Transferred to and executed on the computer itself
- Attacks computer from a distance

Types of Malware:

Type	Description	Behavior
Virus	Software that infects computer by inserting itself into programs already in machine	Executed when host program executed; replicates to other programs; may degrade OS, erase mass storage, corrupt data

Type	Description	Behavior
Worm	Autonomous program that transfers itself through network; takes up residence; forwards copies of itself	Replicates; performs vandalism; explosion of copies degrades legitimate applications; can overload entire network/internet
Trojan Horse	Program disguised as desirable program (game, utility) willingly imported by victim	Performs additional harmful activities; may start immediately or lie dormant until triggered; often arrive as email attachments
Spyware (Sniffing Software)	Software that collects information about activities at computer; reports back to instigator	Building customer profiles (questionable ethical merit); recording keystrokes in search of passwords/credit card numbers

Trojan Horse Warning: Email attachments from unknown sources should NEVER be opened

Phishing:

- Technique of obtaining information explicitly by simply asking for it
- Term is play on "fishing" (cast numerous "lines" hoping someone will "take the bait")
- Carried out via email
- Little more than old telephone con

Process:

1. Perpetrator sends email messages posing as financial institution, government bureau, law enforcement agency
2. Email asks potential victim for information supposedly needed for legitimate purposes
3. Information obtained used by perpetrator for hostile purposes

Denial of Service (DoS) Attack:

- Process of overloading a computer with messages
- Launched against large commercial web servers on the Internet
- Goal: Disrupt company's business
- Some cases: brought company's commercial activity to a halt

Requirements:

- Generation of large number of messages over brief period of time
- Attacker usually plants software on numerous unsuspecting computers (**botnet**)
- When signal given, all computers swamp target with messages

Implication:

- Availability of unsuspecting computers to use as accomplices
- All PC users discouraged from leaving computers connected to Internet when not in use
- Estimated: once PC connected to Internet, at least one intruder will attempt to exploit its existence within 20 minutes
- Unprotected PC = significant threat to integrity of the Internet

Spam:

- Proliferation of unwanted junk email
- Unlike DoS attack: volume rarely sufficient to overwhelm computer system
- Effect: overwhelm the PERSON receiving the spam
- Widely adopted medium for:
 - Phishing
 - Instigating Trojan horses
 - Spreading viruses and other detrimental software

Protection and Cures

Firewall:

- Program that filters traffic passing through a point in the network
- Installed at gateway of organization's intranet

Firewall Functions:

Function	Description
Block outgoing messages	With certain destination addresses
Block incoming messages	From origins known to be sources of trouble

Function	Description
Terminate DoS attacks	Block traffic from attacking computers
Block spoofing	Block incoming messages with origin addresses within the region accessed through gateway (outsider pretending to be insider)

Spoofing:

- Masquerading as a party other than one's self

Firewall for Individual Computers:

- Protect individual computers, not entire networks/domains
- If computer not used as webserver, name server, email server → block all incoming traffic addressed to such applications
- Intruder may gain entry by establishing contact through "hole" left by nonexistent server
- Spyware: retrieve information by establishing clandestine server on infected computer
- Properly installed firewall blocks messages from malicious clients

Spam Filters:

- Firewalls designed to block unwanted email
- Use sophisticated techniques to distinguish between desirable email and spam
- Some learn to make distinction via training process
- User identifies items of spam until filter acquires enough examples to make decisions on its own
- Examples of how probability theory and artificial intelligence contribute to developments in other fields

Proxy Server:

- Software unit that acts as intermediary between client and server
- Goal: Shield client from adverse actions of server

Without Proxy Server:

- Client communicates directly with server
- Server has opportunity to learn certain amount about client

- Over time, server can collect multitude of information about intranet's internal structure
- Information can later be used for malicious activity

With Proxy Server:

1. Organization establishes proxy server for particular kind of service (FTP, HTTP, telnet)
2. Each time client within intranet tries to contact server of that type → client actually placed in contact with proxy server
3. Proxy server, playing role of client, contacts actual server
4. Proxy server plays role of intermediary between actual client and actual server
5. Relays messages back and forth

Advantages:

1. Actual server has no way of knowing proxy server is not true client
2. Actual server never aware of actual client's existence
3. Actual server has no way of learning about intranet's internal features
4. Proxy server in position to filter all messages sent from server to client
 - Example: FTP proxy server could check all incoming files for presence of known viruses
 - Block all infected files

Network Auditing Software:

- Similar to auditing software in operating system security
- System administrator can:
 - Detect sudden increase in message traffic at various locations
 - Monitor activities of system's firewalls
 - Analyze pattern of requests being made by individual computers to detect irregularities
- Administrator's primary tool for identifying problems before they grow out of control

Antivirus Software:

- Used to detect and remove presence of known viruses and other infections
- Represents broad class of software products
- Many products specialize in virus control

- Others specialize in spyware protection

Important for Users to Understand:

- New computer infections constantly coming on scene
- Require updated vaccines
- Antivirus software must be routinely maintained
- Download updates from software's vendor

Limitations:

- Even this does not guarantee safety of computer
- New virus must first infect some computers before discovered and vaccine produced

Wise Computer User Practices:

- Never open email attachments from unfamiliar sources
- Do not download software without first confirming reliability
- Do not respond to pop-up ads
- Do not leave PC connected to Internet when such connection is not necessary

Encryption

Purpose: Protect information when transferred over networks and internets where messages are relayed by unknown entities

Even if data falls into unscrupulous hands, encoded information remains confidential

Secure Versions:

- Traditional Internet applications altered to incorporate encryption techniques
- "Secure versions" of applications

HTTPS:

- Secure version of HTTP
- Used by most financial institutions to provide customers with secure Internet access to accounts
- Backbone of HTTPS = **SSL (Secure Sockets Layer)**
- Originally developed by Netscape
- Provides secure communication links between Web clients and servers

Browser Indication of SSL:

- Most browsers display tiny padlock icon on computer screen

- Some: presence/absence of icon indicates whether SSL is being used
- Others: display padlock in locked or unlocked position

Public-Key Encryption:

Definition: Encryption systems designed so that having knowledge about how messages are encrypted does NOT allow one to decrypt messages

Two Keys:

Key	Usage	Distribution
Public Key	Used to encrypt messages	Distributed to those who need to send messages to particular destination
Private Key	Required to decrypt messages	Held in confidence at destination

Process:

1. Bob creates public-key encryption system
2. Gives both Alice and Carol the public key
3. Both Alice and Carol can encrypt messages to Bob
4. Neither can spy on the other's communication
5. If Carol intercepts message from Alice → cannot decrypt it
6. This is true even though Carol knows how Alice encrypted it!

Subtle Problems:

1. Key Authentication:

- Ensure public key being used is proper key for the destination party
- Example: Communicating with bank → want to be sure public key is bank's key, not impostor's key
- **Spoofing:** Impostor presents itself as bank, gives you its public key
- Messages you encrypt and send to "bank" would be meaningful to impostor, not your bank

Solution - Certificate Authorities:

- Trusted Internet sites
- Task: maintain accurate lists of parties and their public keys
- Act as servers, provide reliable public-key information to clients
- Information packaged in **certificates**

Certificate:

- Package containing party's name and that party's public key
- Many commercial certificate authorities available on Internet
- Organizations may maintain their own certificate authorities
- Tighter control over security of organization's communication

2. Authentication (Digital Signatures):

Key Property:

- In some public-key encryption systems, roles of encryption and decryption keys can be REVERSED
- Text can be encrypted with PRIVATE key
- Only one party has access to that key
- Any text so encrypted must have originated from that party

Digital Signature:

- Bit pattern that only the holder of private key knows how to produce
- Attach signature to message → sender marks message as authentic
- Simple form: encrypted version of the message itself

Process:

1. Sender encrypts message being transmitted using his/her PRIVATE key
2. Message received
3. Receiver uses sender's PUBLIC key to decrypt the signature
4. Message revealed is guaranteed to be authentic
5. Only holder of private key could have produced the encrypted version

Legal Approaches to Network Security

Two Obstacles:

Obstacle	Description
1. Making action illegal does not preclude action	Only provides legal recourse, doesn't prevent the action
2. International nature of networking	Obtaining recourse often very difficult; what is illegal in one country may be legal in another

U.S. Federal Laws (Examples):

Computer Fraud and Abuse Act (1984, amended several times):

- Addresses proliferation of malware
- Requires proof that defendant knowingly caused transmission of program or data that intentionally caused damage
- Covers cases involving theft of information
- Outlaws obtaining anything of value via unauthorized access of computer
- Courts assign broad interpretation to "anything of value"
- Applied to more than theft of information
- Mere use of computer may constitute "anything of value"

Electronic Communication Privacy Act (ECPA) of 1986:

- Origins in legislation to control wiretapping
- Addresses right of privacy

Key Provisions:

- "Except as otherwise specifically provided... any person who intentionally intercepts... any wire, oral, or electronic communication... shall be punished..."
- "... any person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication... on that service to any person or entity other than an addressee or intended recipient..."

Communications Assistance for Law Enforcement Act (CALEA):

- Goal: Establish capabilities for monitoring communications

- Requires telecommunication carriers to modify equipment to accommodate law enforcement taps
- Complex and expensive to meet

Encryption vs. Government Monitoring:

- Clash between government's right to monitor communications and public's right to use encryption
 - If messages are well encrypted → tapping communication is of limited value to law enforcement
 - Governments in United States, Canada, Europe considering systems requiring registration of ciphering keys
 - Such demands being fought by corporations
 - Corporate espionage → requiring registration of ciphering keys makes law-abiding corporations and citizens uncomfortable
 - Question: How secure can the registration system be?
-

Anti cybersquatting Consumer Protection Act of 1999:

- Designed to protect organizations from impostors who establish look-alike domain names (**cybersquatting**)
- Prohibits use of domain names that are identical or confusingly similar to another's trademark or "common law trademark"

Effect:

- Does NOT outlaw domain name speculation (registering potentially desirable domain names, later selling rights)
 - Limits practice to GENERIC domain names
 - Domain name speculator may legally register generic name: GreatUsedCars.com
 - May NOT be able to claim rights to BigAlUsedCars.com if Big Al is already in used car business
-

PART II: CYBERSECURITY (Textbook 2, Chapter 16)

16.1 OVERVIEW - WHAT IS CYBERSECURITY?

Definition: Cybersecurity is the practice of protecting systems, networks, programs, and data from digital attacks, damage, or unauthorized access.

Core Objectives:

Objective	Description
Confidentiality	Ensuring information is not disclosed to unauthorized individuals, entities, or processes
Integrity	Maintaining and assuring the accuracy and completeness of data over its entire lifecycle
Availability	Ensuring information and systems are accessible when needed by authorized users

CIA Triad: The three fundamental principles of information security

16.2 BRIEF HISTORY OF CYBERSECURITY EVENTS

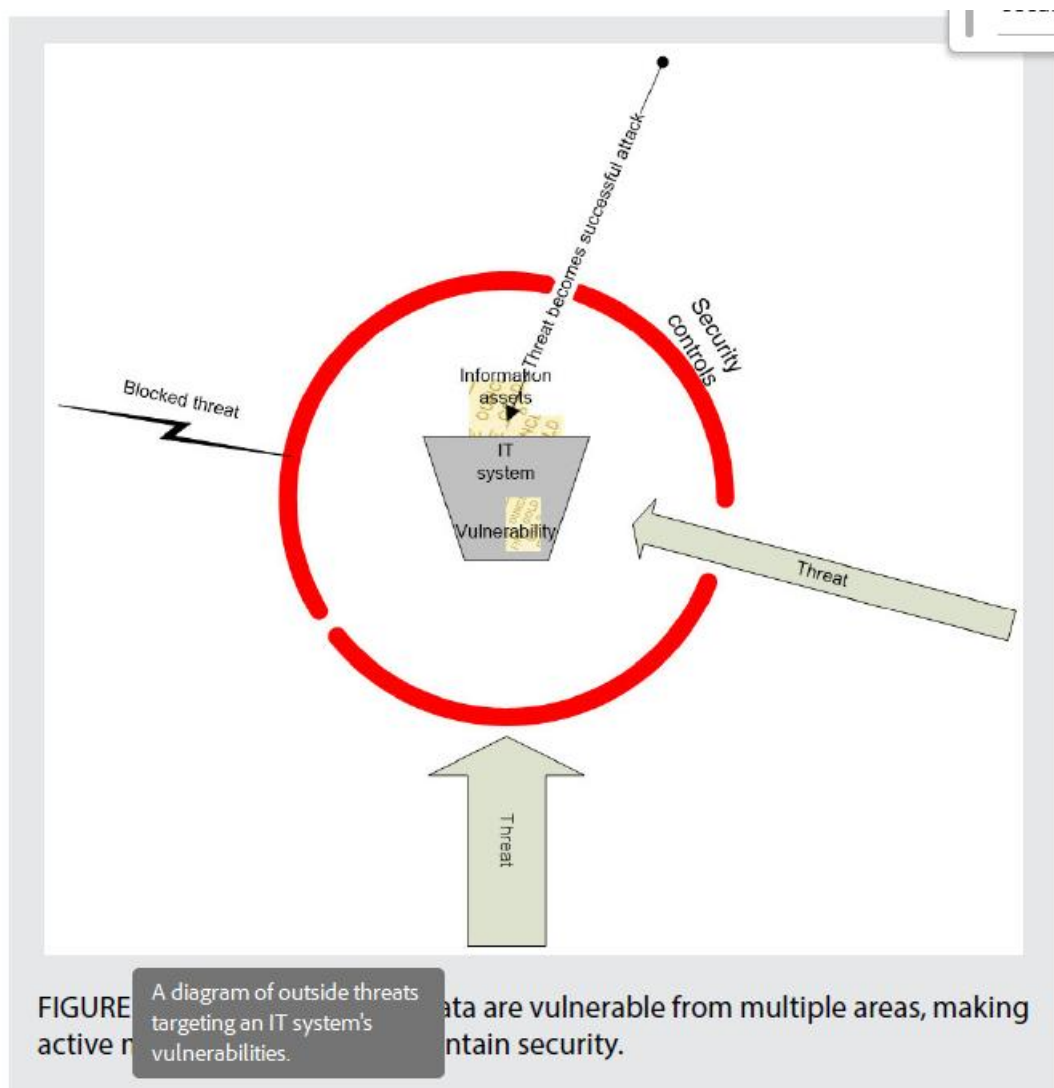
Timeline of Significant Cybersecurity Events:

Era	Event	Significance
1940s-1950s	Early computing	Security not a major concern; systems were isolated and physically secured
1960s	Multi-user systems	Passwords introduced to protect user accounts
1970s	ARPANET	First network security incidents; researchers experiment with network vulnerabilities
1980s	First computer viruses	"Elk Cloner" (1982) on Apple II; "Brain" (1986) first IBM PC virus
1988	Morris Worm	First major Internet worm; infected ~10% of Internet; led to CERT formation
1990s	Commercial Internet	Rise of firewalls, antivirus software; e-commerce security concerns
2000s	Cybercrime era	Identity theft, phishing, botnets, spyware; organized criminal groups

Era	Event	Significance
2010s	Advanced Persistent Threats	State-sponsored attacks; Stuxnet; massive data breaches (Target, Equifax, Yahoo)
2020s	Ransomware pandemic	Colonial Pipeline, JBS Foods; supply chain attacks; SolarWinds

16.3 THE BASIC INFORMATION SECURITY MODEL

Core Components:



Component	Description
People	Users, administrators, attackers; human factor is often weakest link
Process	Policies, procedures, guidelines for security
Technology	Hardware and software security tools
Data	Information being protected

16.4 CYBER HYGIENE

Definition: Cyber hygiene refers to practices and steps that users take to maintain system health and improve online security.

Basic Cyber Hygiene Practices:

Practice	Description
Strong Passwords	Use complex, unique passwords for different accounts; minimum 12+ characters
Multi-Factor Authentication (MFA)	Require two or more verification factors
Regular Software Updates	Patch operating systems and applications promptly
Antivirus/Antimalware	Install and maintain security software
Firewall	Enable hardware and software firewalls
Data Backup	Regular backups; 3-2-1 rule (3 copies, 2 media, 1 offsite)
Safe Browsing	Avoid suspicious links; verify HTTPS

Practice	Description
Email Caution	Do not open attachments from unknown senders
Least Privilege	Users have minimum access necessary
Screen Lock	Lock device when unattended
Password Best Practices:	
Do	Don't
Use passphrases (correct-horse-battery-staple)	Use dictionary words
Use different passwords for each account	Reuse passwords across sites
Use password manager	Write passwords on sticky notes
Enable MFA when available	Share passwords with others
3-2-1 Backup Rule:	
• 3 copies of data • 2 different media types • 1 copy stored offsite	

16.5 TEAMS IN CYBERSECURITY

Blue Team:

- Defensive security team
- Protects organization's systems and data
- Monitors for threats, responds to incidents
- Implements security controls

Red Team:

- Offensive security team
- Simulates attacks to test defenses

- Ethical hackers who think like adversaries
- Identifies vulnerabilities before real attackers do

Purple Team:

- Collaborative approach
- Combines Red and Blue teams
- Shares knowledge and improves overall security posture

Security Operations Center (SOC):

- Centralized unit dealing with security issues
- 24/7 monitoring and analysis
- Incident response team

Computer Security Incident Response Team (CSIRT):

- Handles security incidents
- Investigates breaches
- Coordinates response and recovery

PART III: ETHICAL ISSUES IN INFORMATION TECHNOLOGY (Textbook 2, Chapter 17)

17.1 OVERVIEW

Definition: Ethics is the branch of philosophy that deals with moral principles governing behavior and conduct.

Information Technology Ethics: The application of ethical principles to the use, development, and management of information technology.

Key Questions:

- What are our rights regarding information about ourselves?
- What are our responsibilities regarding information about others?
- How should intellectual property be protected in digital age?
- What constitutes acceptable use of technology?

17.2 OWNERSHIP RULES

Intellectual Property:

- Creations of the mind (inventions, literary/artistic works, symbols, names, images, designs)

- Protected by law through patents, copyright, trademarks, trade secrets

Copyright:

- Protects original works of authorship
- Books, music, films, software, artwork
- Grants creator exclusive rights to reproduce, distribute, perform, display work
- Duration: life of author + 70 years (US)

What Copyright Protects:

- Expression of ideas
- NOT the underlying ideas themselves

Software Copyright:

- Source code
- Object code
- Structure, sequence, organization

Patent:

- Protects inventions and discoveries
- Grants exclusive right to make, use, sell invention
- Duration: 20 years from filing date
- Requires: novel, useful, non-obvious

Software Patents:

- Controversial
- Protect processes, algorithms, methods of doing business
- Not all countries permit software patents

Trademark:

- Protects words, phrases, symbols, designs identifying source of goods/services
- Duration: indefinite while in use
- Prevents consumer confusion

Trade Secret:

- Confidential business information providing competitive advantage
- No registration required
- Protected indefinitely if kept secret
- Examples: Coca-Cola formula, Google search algorithm

Digital Rights Management (DRM):

- Technological protection measures to control use of digital content
- Prevent unauthorized copying, sharing, modification
- Controversial: can restrict legitimate uses

17.3 ETHICS AND ONLINE CONTENT

Plagiarism:

- Using others' work without attribution
- Presenting someone else's work as your own
- Includes copying text, images, code, ideas
- Easy with digital content; still unethical and often illegal

Proper Attribution:

- Cite sources
- Use quotation marks for direct quotes
- Obtain permission when required

Piracy:

- Unauthorized copying/distribution of copyrighted material
- Software, music, movies, games, books
- Widespread due to ease of digital copying
- Economic impact on creators and industries

Arguments Against Piracy:

- Violates copyright law
- Deprives creators of income
- Discourages creation of new works

- May contain malware

Arguments For (Debated):

- Builds audience
- Some users wouldn't purchase anyway
- Pricing may be unreasonable
- Availability issues

Deepfakes:

- Synthetic media where person's likeness is replaced with someone else's
- AI-generated videos, images, audio
- Realistic and difficult to detect

Ethical Concerns:

- Misinformation/disinformation
- Non-consensual pornography
- Political manipulation
- Erosion of trust in media
- Fraud and impersonation

Online Harassment and Cyberbullying:

- Using digital technologies to harass, threaten, embarrass target
- Social media, messaging, email, gaming platforms

Forms:

- Trolling
- Doxing (publishing private information)
- Revenge porn
- Hate speech
- Threats of violence

Ethical Responsibilities:

- Platforms: content moderation, reporting mechanisms
- Users: treat others with respect, report abuse

- Bystanders: intervene or report

Freedom of Speech vs. Content Moderation:

- First Amendment protects from government censorship
- Private platforms may set their own content policies
- Tension between free expression and preventing harm

Key Issues:

- Hate speech
- Misinformation
- Harassment
- Extremist content
- Platform liability

Digital Divide:

- Gap between those with/without access to technology and Internet
- Based on socioeconomic status, geography, age, education

Ethical Implications:

- Unequal access to information and opportunities
- Educational disparities
- Economic disadvantages
- Civic participation gaps

Bridging the Divide:

- Public Internet access (libraries, community centers)
- Affordable connectivity programs
- Digital literacy training
- Accessible technology design

Environmental Ethics in IT:

- E-waste: discarded electronics, toxic materials
- Energy consumption: data centers, cryptocurrency mining

- Resource depletion: rare earth metals
- Carbon footprint of manufacturing and operation

Sustainable IT Practices:

- Extend device lifespan
- Recycle electronics properly
- Energy-efficient hardware
- Cloud computing efficiency
- Green data centers

Professional Ethics in Computing:**ACM Code of Ethics:**

1. Contribute to society and human well-being
2. Avoid harm
3. Be honest and trustworthy
4. Be fair and take action not to discriminate
5. Honor property rights including copyrights and patent
6. Give proper credit for intellectual property
7. Respect the privacy of others
8. Honor confidentiality

IEEE Code of Ethics:

- Accept responsibility in making decisions consistent with safety, health, welfare of public
- Avoid real or perceived conflicts of interest
- Be honest and realistic in stating claims or estimates
- Reject bribery in all forms
- Improve understanding of technology, its appropriate application, potential consequences

SUMMARY - KEY TERMS TO REMEMBER (MODULE 3)

Networking and Internet

Term	Definition
PAN	Personal Area Network; < few meters range
LAN	Local Area Network; single building/building complex
MAN	Metropolitan Area Network; local community
WAN	Wide Area Network; greater distance
Bus Topology	All machines connected to common communication line
Star Topology	Central focal point (AP/hub) connects all machines
Protocol	Rules by which network activities are conducted
CSMA/CD	Carrier Sense, Multiple Access with Collision Detection (Ethernet)
CSMA/CA	Carrier Sense, Multiple Access with Collision Avoidance (WiFi)
Hidden Terminal Problem	Nodes cannot hear each other but both can hear AP
Repeater	Passes signals between buses without considering meaning
Bridge	Connects two buses; forwards only messages destined for other side
Switch	Bridge with multiple connections; minimizes traffic
Router	Forwards messages between networks; allows networks to maintain unique characteristics

Term	Definition
Gateway	Point where network links to internet
Client/Server	Client makes requests; Server satisfies requests
P2P	Peer-to-peer; processes provide and receive service
ISP	Internet Service Provider
Tier-1 ISP	Backbone; high-speed, high-capacity international WANs
Tier-2 ISP	Regional scope; connects to tier-1
Access ISP/Tier-3	Provides Internet access to homes/businesses
Intranet	Independent internet operated by single authority
Hot Spot	Area within AP range with network access
Last Mile Problem	Legacy analog links to individual homes/offices
IP Address	32-bit (IPv4) or 128-bit (IPv6) unique identifier
Dotted Decimal	Notation for IP addresses (192.168.1.1)
Domain Name	Mnemonic address (mu.edu)
TLD	Top-Level Domain (com, edu, gov, org)
DNS	Domain Name System; translates domain names to IP addresses
Name Server	Directory providing address translation
SMTP	Simple Mail Transfer Protocol; email transmission

Term	Definition
POP3	Post Office Protocol version 3; download email to local computer
IMAP	Internet Mail Access Protocol; store/manage email on server
VoIP	Voice over Internet Protocol; voice communication over Internet
HTTP	Hypertext Transfer Protocol; transfers web documents
HTTPS	Secure HTTP; uses SSL/TLS encryption
HTML	Hypertext Markup Language; webpage formatting
XML	eXtensible Markup Language; standard for markup languages
URL	Uniform Resource Locator; unique document address
Browser	Client software for accessing web
Webserver	Server software providing web documents
Application Layer	Software using Internet communication
Transport Layer	Formats messages; divides into packets; reassembles
Network Layer	Directs packets; maintains forwarding tables
Link Layer	Transfers packets; handles network-specific details
TCP	Transmission Control Protocol; connection-oriented, reliable
UDP	User Datagram Protocol; connectionless, efficient
IP	Internet Protocol; forwarding and routing

Term	Definition
Hop Count/TTL	Limit on packet forwarding; prevents endless circulation
Cybersecurity	
Term	Definition
Cybersecurity	Protecting systems, networks, programs, data from digital attacks
CIA Triad	Confidentiality, Integrity, Availability
Malware	Malicious software
Virus	Self-replicating code attaching to programs
Worm	Autonomous self-replicating network program
Trojan Horse	Malware disguised as legitimate software
Spyware	Software that collects information without consent
Phishing	Obtaining information by deceptive requests
DoS	Denial of Service; overloading system with messages
Botnet	Network of compromised computers controlled by attacker
Spam	Unwanted junk email
Firewall	Filters network traffic
Spoofing	Masquerading as another party
Proxy Server	Intermediary shielding client from server

Term	Definition
Antivirus	Software detecting/removing malware
Encryption	Encoding information to prevent unauthorized access
Public Key	Key used to encrypt messages; publicly distributed
Private Key	Key used to decrypt messages; kept secret
SSL/TLS	Secure Sockets Layer/Transport Layer Security
Certificate	Package containing party's name and public key
Digital Signature	Encrypted message authenticating sender
Cyber Hygiene	Practices maintaining system health and online security
MFA	Multi-Factor Authentication
Blue Team	Defensive security team
Red Team	Offensive security team (ethical hackers)
Purple Team	Collaborative security approach
SOC	Security Operations Center
CSIRT	Computer Security Incident Response Team
Ethical Issues	

Term	Definition
Ethics	Moral principles governing behavior and conduct

Term	Definition
Intellectual Property	Creations of the mind protected by law
Copyright	Protects original works of authorship
Patent	Protects inventions and discoveries
Trademark	Protects source-identifying marks
Trade Secret	Confidential business information
DRM	Digital Rights Management; technological protection measures
Plagiarism	Using others' work without attribution
Piracy	Unauthorized copying/distribution of copyrighted material
Deepfake	AI-generated synthetic media replacing likeness
Cyberbullying	Using digital technologies to harass
Doxing	Publishing private information maliciously
Digital Divide	Gap between those with/without technology access
E-waste	Discarded electronic devices
ACM Code of Ethics	Professional ethics guidelines for computing
IEEE Code of Ethics	Professional ethics guidelines for engineering