- Information gathering, processing, and distribution are key technologies today.
- Growing demand for sophisticated information processing due to increasing ability to gather, process, and distribute information.
- Computer systems are interconnected by a single technology, such as the Internet.
- The Internet has many uses including business applications, VoIP, home applications and mobile uses.
- The Internet raises social issues including network neutrality, content ownership, anonymity, censorship, and privacy.
- Different types of e-commerce: B2C (Business-to-consumer), B2B (Business-to-business), G2C (Government-to-consumer), C2C (Consumer-to-consumer), and P2P (Peer-to-peer).
- Mobile devices like tablets, laptops, and smartphones are popular; WiFi hotspots and 4G LTE provide wireless connectivity.
- Networks can be classified by transmission technology (Point-to-point, Broadcast) and network scale (PAN, LAN, MAN, WAN, Internet).
- Network security involves understanding how to defend networks against attacks and designing architectures that are immune to them.
- Malware can infiltrate hosts via the Internet, leading to data theft and botnet enrollment.
- Malware can enter a host system via the Internet, either through a virus (a self-replicating infection received/executed by an object like an email attachment) or a worm (a self-replicating infection received passively by an object that gets itself executed).
- Spyware malware can record keystrokes, websites visited, and upload info to a collection site.
- Infected hosts can be enrolled in a botnet and used for spam Distributed Denial of Service (DDoS) attacks.
- Attackers can overwhelm a server or network infrastructure with bogus traffic, rendering resources unavailable to legitimate traffic.
- Attackers can sniff packets, recording all packets that pass by using software like Wireshark.
- Attackers can use IP spoofing to send packets with a false source address.
- IEEE802.11 (WiFi) clients communicate via an Access Point (AP) that is wired to the rest of the network. Signals in the ISM band can vary in strength due to effects like multipath fading.
- The transport layer in network systems is implemented in the end systems but not in the network routers.
- A transport-layer protocol provides logical communication between processes running on different hosts.
- More than one transport layer protocol may be available to network applications, such as TCP and UDP in the Internet.
- The Internet's network-layer protocol, IP (Internet Protocol), provides logical communication between hosts but does not guarantee segment delivery, orderly delivery of segments, or the integrity of the data in the segments.
- The transport-layer multiplexing and demultiplexing extend the host-to-host delivery service to a process-to-process delivery service for applications running on the hosts.
- A TCP socket is identified by a four-tuple: source IP address, source port number, destination IP address, destination port number.
- The UDP checksum provides for error detection.
- TCP is connection-oriented and provides full-duplex service.
- A process called the server process manages the TCP connection.
- The client program establishes the connection by issuing the command: clientSocket.connect((serverName, serverPort)).
- The client first sends a special TCP segment, followed by the server responding with a second special TCP segment, and finally the client responds again with a third special segment.
- The first two segments carry no payload, while the third may carry a payload. This procedure is referred to as a three-way handshake.
- Once a TCP connection is established, the two application processes can send data to each other.
- Data is directed to the connection's send buffer, which is one of the buffers that is set aside during the initial three-way handshake.
- The maximum amount of application-layer data in a segment is limited by the maximum segment size (MSS).
- TCP pairs each chunk of client data with a TCP header, forming TCP segments, which are encapsulated within network-layer IP datagrams.
- When TCP receives a segment at the other end, the segment's data is placed in the TCP connection's receive buffer.
- The TCP segment structure consists of a Data field and Header fields. The Data field contains a chunk of application data, while the Header fields include source and destination port numbers, a checksum field, sequence and acknowledgment number fields, receive window field, header length field, and optional and variable-length options field.
- The flag field of the TCP segment structure contains 6 bits, which include the ACK bit, RST, SYN, and FIN bits, CWR and ECE bits, PSH bit, and URG bit.
- The sequence number for a segment is the byte-stream number of the first byte in the segment.
- TCP views data as an unstructured, but ordered, stream of bytes.
- In a given example, TCP constructs 500 segments out of a data stream of 500,000 bytes, with an MSS of 1,000 bytes, and assigns sequential sequence numbers to each segment.
- Field in the header
- Of the appropriate TCP segment