Department of Electrical and Computer Engineering

CMP2205 CAT2

Date: 04/18/2016 **Duration: 1hr 40min**

Answer any FOUR questions

Question 1

a) Explain client-server model of computing? [2 marks]

The client–server model of computing is a distributed application structure that partitions tasks or workloads between the providers of a resource or service, called servers, and service requesters, called clients. A client-server network consists of two or more clients, or users, computers and at least one server computer. The client computers do not use each other's resources, only those of the server.

b) Explain any three distinguishing characteristics of client – server systems [6 marks]

Service: The client/server is primarily a relationship between processes running on separate machines. The server process is a provider of services. The client is a consumer of services. In essence, client-server provides a clean separation of function based on the idea of service.

Shared Resources: A server can service many clients at the same time and regulate their access to shared resources.

Asymmetrical protocols: There is a many-to-one relationship between the clients and the server. Clients always initiate the dialog by requesting a service. Servers are passively awaiting request from the clients.

Transparency of location: The server is a process that can reside on the same machine as the client or on a different machine across a network. Client-Server software usually masks the location of the server from the clients by the redirecting the service calls when needed. A program can be a client, a server, or both.

Message-based exchanges:

Clients and servers are loosely coupled systems that interact through a message-passing mechanism. The message is the delivery mechanism for the service request and replies.

Mix-and-match:

The ideal client-server software is independent of hardware or operating system software platforms.

Encapsulation of services:

Scalability:

Client-Server systems can be scaled horizontally or vertically. Horizontal scaling means adding or removing client workstations with only a slight performance impact. Vertical scaling means either migrating to a larger and faster server machine or distributing the processing load across multiple servers.

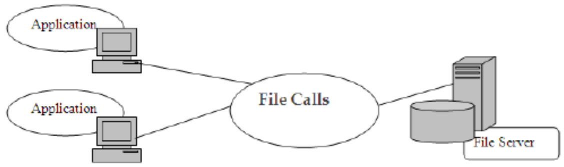
Integrity:

The server code and server data is centrally managed, which results in cheaper maintenance and the guarding of shared data integrity. At the same time, the clients remain personal and independent

c) Describe any three types of servers [6 Marks]

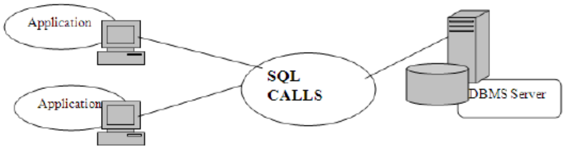
File Server

Useful for sharing information across the network. The client passes a request for file records over a network to the file server. The file servers provide access to the remote server processors.



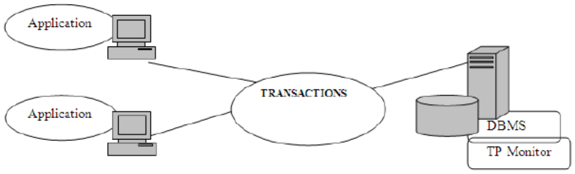
Database Server

The client passes the SQL requests as messages to the database server; the result of each SQL command is returned over the network. The code, which processes the SQL request and the data, reside in the same machine, the server uses its own processing power to find the requested data back to the client,



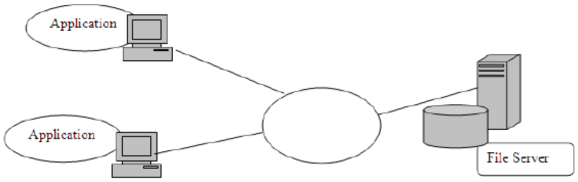
Transaction Servers

The client can invoke remote procedure or services that reside on the server with an SQL database engine using the transaction server. The network exchange consists of a single request/ reply. The SQL statements either all succeed or fail as a unit. These grouped SQL statements are called transactions.



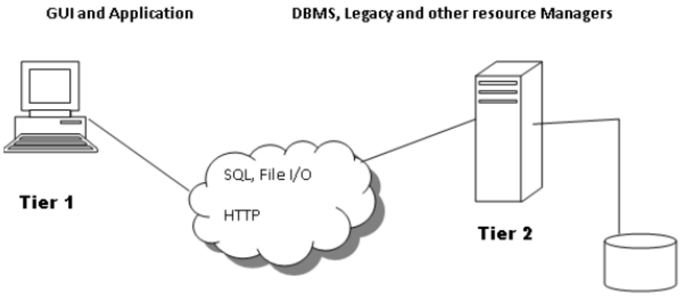
Groupware Servers

It involves the management of semi-structured information such as text, image, mail, bulletin boards and the flow of work. This client-server system places people in direct contact with other people. E.g. webmail servers



d) Using relevant diagrams explain the following type of client/server architecture:

i. 2-tier architecture [3 marks]



Two tier architectures consist of three components distributed in two layers: client (requester of services) and server (provider of services).

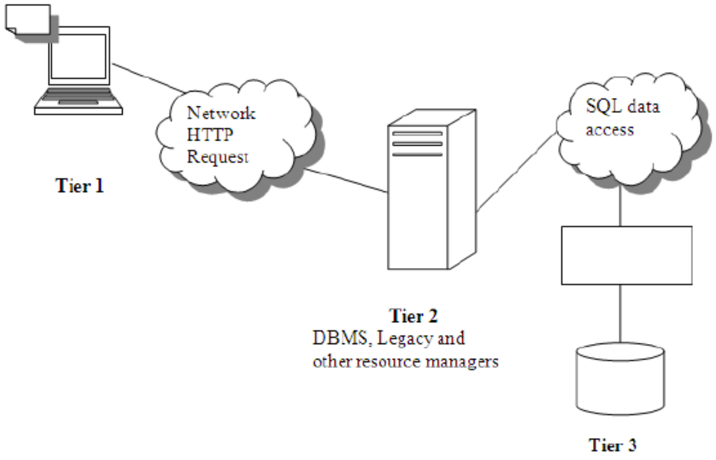
1. User System Interface (such as session, text input, dialog, and display management services)

2. Processing Management (such as process development, process enactment, process monitoring, and process resource services)

3. Database Management (such as data and file services)

The two-tier design allocates the user system interface exclusively to the client. It places database management on the server and splits the processing management between client and server, creating two layers. E.t.c

ii. 3-tier architecture [3 marks]



Overcomes the limitations of the two-tier architecture. The third tier (middle tier server) is between the user interface (client) and the data management (server) components. This middle tier provides process management where business logic and rules are executed and can accommodate hundreds of users (as compared to only 100 users with the two tier architecture) by providing functions such as queuing, application execution, and database staging.

Question 2

a) Explain the following terms as used in computer networks performance evaluation:

I. Bandwidth [2 Marks]

The bandwidth of a communication link refers to the number of bits per second that can be transmitted on the link.

II. Latency [2 Marks]

Latency corresponds to how
long it takes a message to travel from one end of a network to the other.

Latency corresponds to how long it takes a message to travel from one end of a network to the other.

Latency = Propagation + Transmit + Queue

III. Network throughput [2 Marks]

Throughput or network throughput is the average rate of successful message delivery over a communication channel. The throughput is usually measured in bits per second (bit/s or bps), and sometimes in data packets per second or data packets per time slot.

b) Consider a transcontinental channel with RTT (two way latency) of 100 milliseconds. Calculate the total throughput (bandwidth) of the channel if it is able to hold 2.25 megabits. [3 marks]

2.25Mb/50ms

c) Describe any three network topologies used in LANs [6 Marks]

Network topology defines the structure of the network. It falls into two categories: Physical and Logical topology. Physical topology is the actual layout of the wire or media. The physical topologies used in Local Area Networks (LAN) include:

Ring topology, which connects one host to the next and the last host to the first. This creates a physical ring of cable.

A mesh topology is implemented to provide as much protection as possible from interruption of service. each host has its own connections to all other hosts.

Star topology, which connects all cables to a central point of concentration.

The **Line topology** connects one host to the next and the last host doesn't connect to the first. This creates a physical line of cable.

A tree (hierarchical) topology is similar to an extended star. However, instead of linking the hubs and/or switches together, the system is linked to a computer that controls the traffic on the topology.

Bus topology, which uses a single backbone cable that is terminated at both ends. All the hosts connect directly to this backbone.

The **logical topology** of a network is how the hosts communicate across the medium. The two most common types of logical topologies are **broadcast** and **token passing**.

Broadcast topology simply means that each host sends its data to all other hosts on the network medium. There is no order that the stations must follow to use the network.

Token passing which controls network access by passing an electronic token sequentially to each host. When a host receives the token, that host can send data on the network. If the host has no data to send, it passes the token to the next host and the process repeats itself.

d) Distinguish between private and public networks; and explain advantages and disadvantages of using a public network with respect to network performance. [5 marks]

A private network is one in which all devices on the network and all links between those devices are used and administratively controlled by a single organization.

A ***public network*** is one where network connectivity and resources are shared by many different administrative units. Typically no one company using the network has control over every piece of the network.

Advantage:

- Public networks enable organizations to take advantage of **economies of scale**, as it’s often the case that Wide Area Network links that handle a large amount of traffic aren’t much more expensive than slower WAN links. With the cost of a faster link split among multiple organizations, users can enjoy faster network speeds at lower cost than would be possible on a private network.
- They allow organizations to basically **time-share connectivity**, and not pay for a line when they’re not using it.

Disadvantage

- Reduced amount of control over data and host security.
- Less control over bandwidth than do private networks. (reduced speeds)

Question 3

a) Write short notes on the following wireless protocols:

i. 802.11a [2 marks]

802.11a supports bandwidth up to 54 Mbps and signals in a regulated frequency spectrum around 5 GHz. This higher frequency compared to 802.11b shortens the range of 802.11a networks. The higher frequency also means 802.11a signals have more difficulty penetrating walls and other obstructions.

Advantages: fast maximum speed; regulated frequencies prevent signal interference from other devices

Disadvantages - highest cost; shorter range signal that is more easily obstructed

ii. 802.11b [2 marks]

802.11b supports bandwidth up to 11 Mbps, comparable to traditional Ethernet. 802.11b uses the same unregulated radio signaling frequency (2.4 GHz) as the original 802.11 standard.

Advantages: lowest cost; signal range is good and not easily obstructed

Disadvantages: slowest maximum speed; home appliances may interfere on the unregulated frequency band

iii. 802.11g [2 marks]

802.11g supports bandwidth up to 54 Mbps, and it uses the 2.4 Ghz frequency for greater range. 802.11g is backwards compatible with 802.11b, meaning that 802.11g access points will work with 802.11b wireless network adapters and vice versa.

Advantages: - fast maximum speed; signal range is good and not easily obstructed

Disadvantages: - costs more than 802.11b; appliances may interfere on the unregulated signal frequency

b) Explain the following terms in Mobile IP addressing.

i. Home address [2 Marks]

The “normal”, permanent IP address assigned to the mobile node. This is the address used by the device on its home network, and the one to which datagrams intended for the mobile node are always sent.

ii. Care-of address [2 Marks]

A secondary, temporary address used by a mobile node while it is 'traveling” away from its home network. It is a normal 32-bit IP address in most respects, but is used only by

Mobile IP for forwarding IP datagrams and foradministrative functions. Higher layers never use it, nor do regular IP devices when creating datagrams.

c) Discuss the difference between a circuit switched network and a packet switched network. [2 marks]

Circuit-switched is a type of network in which a physical path is obtained for and dedicated to a single connection between two end-points in the network for the duration of the connection.

Packet-switched describes the type of network in which relatively small units of data called packets are routed through a network based on the destination address contained within each packet

d) Distinguish between thin client architecture and full client architecture as applied in client – server computing for mobile environments. [4 marks]

A thin client can refer to either a software program or to an actual computer that relies heavily on another computer to do most of its work. A thin client is part of a network, and the client software or computer acts as an interface, while the network server computer does all the real work.

The thin client architecture offloads most application logic and functionality from clients to stationary servers. In the thin client architecture, applications in stationary servers are usually mobile-aware and optimized for mobile client devices.

The full client architecture emulates server functions on the client devices and, therefore, is able to minimize the uncertainty of connectivity and communications. Mobile clients must be able to use networks with rather unpleasant characteristics

A full client architecture can be used to effectively support the disconnected or weakly connected clients. Compared to a thin client architecture, the full client architecture is at the other extreme of the range of extended client-server model. The full client architecture supports the emulation of functions of servers at the client host so that applications can be executed without fully connecting to remote servers.

e) Weak connectivity and resource constrains greatly affect delivery of server data and maintenance of client – server data consistency. Explain any two data access strategies in mobile information system. [4 marks]

➨ The range is delimited by two extremes.

1) At one extreme, adaptation is entirely the responsibility of individual applications. This approach, called **laisse-faire adaptation, avoids the need for system support.**

2) The other extreme, called **application-transparent adaptation**, places the entire responsibility for adaptation on the system.

   ➨ A typical case of this approach is to use proxies to perform adaptation on behalf of applications.

➨ Between these two extremes lies a spectrum of possibilities that are referred to as application-aware adaptation.

Question 4

a) Explain the difference between authorization and authentication with regards to computer network security [1 Marks]

Authentication deals with the question of whether you are actually communicating with a specific process. Authorization is concerned with what that process is permitted to do. For example, a client process contacts a file server and says: I am Scott's process and I want to delete the file cookbook.old. From the file server's point of view, two questions must be answered:

1. Is this actually Scott's process (authentication)?

2. Is Scott allowed to delete cookbook.old (authorization)?

b) Explain the difference between secret key algorithms and public key algorithms. [4 Marks]

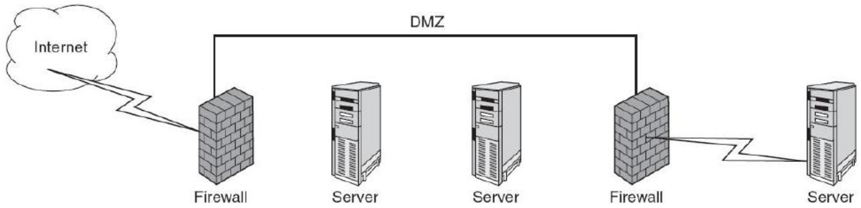
Public key encryption algorithms are based on the premise that each sender and recipient has a private key, known only to him/her and a public key, which can be known by anyone. Each encryption/decryption process requires at least one public key and one private key.

Private Key encryption also referred to as conventional, single-key or symmetric encryption requires all parties that are communicating to share a common key.

c) Describe how proxy based firewalls differ from filter based firewalls [4 Marks]

Check note. (ability to filter based on feature and certain sections of web page)

d) Using a diagram explain the effect of a demilitarized zone to the security of a network. [2 marks]



This is a network segment located between two firewalls as shown. This is used as a buffer zone to keep the internal network safe from the outside world while offering services that are useful outside of the internal network without allowing the entire network to be available to Internet users.

DMZ contains devices that need Internet access: Web, DNS, and e-mail servers. These servers all have to be hardened to keep them from being attacked by malicious users.

e) Describe the three basic internal security threats in computer networks [6 Marks]

Internal users inappropriately accessing information to which they should not have access, such as payroll records, accounting records, or software development information

Internal users accessing other users' files to which they should not have access

Internal users impersonating other users and causing mischief, such as sending e-mails under another person's name

Internal users accessing systems to carry out criminal activities, such as embezzling funds

Internal users compromising the security of the network, such as by accidentally (or deliberately) introducing viruses to the network

Internal users "sniffing" packets on the network to discover user accounts and passwords

f) Write short notes about the following threats:

i. Trojan horse [1 Marks]

A Trojan horse is a program that purports to do something interesting or useful and then performs malicious actions in the background while the user is interacting with the main program.

ii. Worm [1 Marks]

A worm is a program that propagates by sending copies of itself to other computers, which run the worm and then send copies to other computers.

One way they spread is by attaching to e-mails along with a message that entices the recipients to open the attachment. The attachment contains the worm, which then sends out copies of itself to other people defined in the user's e-mail address book, without the user knowing that this is happening.

iii. Virus [1 Marks]

A computer virus is a program that spreads by infecting other files with a copy of itself. Files that can be infected by viruses include program files (.COM, .EXE, and .DLL) and document files for applications that support macro languages sophisticated enough to allow virus behavior (Microsoft Word and Excel are common targets of macro-based viruses).

Question 5

a) Differentiate between server-side program and client-side programs [2 Marks]

Server side program refers to the operations that are performed by the server in a client- server relationship in a computer network. Typically, a server is a computer program, such as a web server, that runs on the remote server, reachable from a user's local computer or workstation.

Client side means that the action take place on the user's (client's) computer. Client – side scripting generally refers to the class of computer programs on the web that are executed at client side

b) With reference to Mobile Data Access describe the concepts of server-push and client-pull highlighting typical application scenarios [4 Marks]

The data access strategies in a mobile information system can be characterized by delivery modes, data organizations, and consistency requirements, etc. The mode for server data delivery can be server-push, client-pull, or hybrid.

The server-push delivery is initiated by server functions that push data from the server to the clients. (E.g. from broadcast massages from mobile telephone operators also consider server in stock market and weather appplications sending data to clients who simply view but can't request)

The client-pull delivery is initiated by client functions which send requests to a server and "pull" data from the server in order to provide data to locally running applications. (E.g. real estate's application requesting for data from database server)

The hybrid delivery uses both server-push and client- pull delivery.

c) Distinguish between error detection and error correction [4 Marks]

Error detection just identifies that a bit (or bits) has been received in error.

Error correction corrects errors at a far-end receiver.

Both require a certain amount of redundancy to carry out the respective function. Redundancy, in this context, means those added bits or symbols that carry out no other function than as an aid in the error-detection or error-correction process.

One of the earliest methods of error detection was the parity check. With the 7-bit ASCII code, a bit was added for parity, making it an 8-bit code. This is character parity. It is also referred to as vertical redundancy checking (VRC).

A checksum is a simple error-detection scheme whereby each message is accompanied by a value based on the number of bits in the message. The receiving device then applies the same formula to the message and checks to make sure the value is the same. If the value matches, it is assumed that the complete transmission was received. If not, the receiver can assume that the message has somehow become corrupt.

d) Explain thin client architecture and full client architecture [4 marks]

A thin client can refer to either a software program or to an actual computer that relies heavily on another computer to do most of its work. A thin client is part of a network, and the client software or computer acts as an interface, while the network server computer does all the real work.

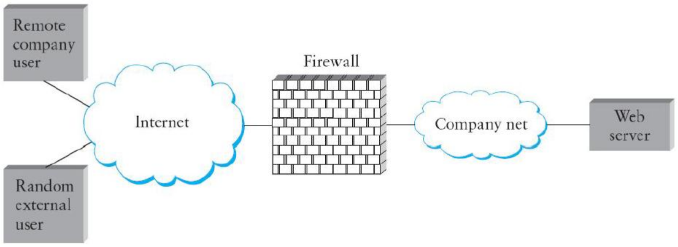
The thin client architecture offloads most application logic and functionality from clients to stationary servers. In the thin client architecture, applications in stationary servers are usually mobile-aware and optimized for mobile client devices.

The full client architecture emulates server functions on the client devices and, therefore, is able to minimize the uncertainty of connectivity and communications. Mobile clients must be able to use networks with rather unpleasant characteristics

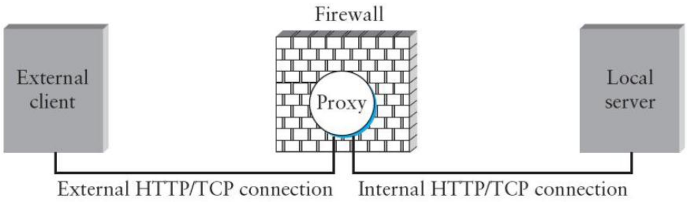
A full client architecture can be used to effectively support the disconnected or weakly connected clients. Compared to a thin client architecture, the full client architecture is at the other extreme of the range of extended client-server model. The full client architecture supports the emulation of functions of servers at the client host so that applications can be executed without fully connecting to remote servers.

e) Describe how proxy based firewalls differ from filter based firewalls [4 Marks]

Filter-based firewalls are the simplest and most widely deployed type of firewall. They are configured with a table of addresses that characterize the packets they will, and will not, forward. each entry in the table is a 4-tuple: It gives the IP address and TCP (or UDP) port number for both the source and destination.



A proxy is a process that sits between a client process and a server process. To the client, the proxy appears to be the server; in a sense, the proxy is standing in for the server. To the server, the proxy appears to be the client. the firewall dynamically decides what packets to forward and what packets to drop, with the policy embodied in the application-specific proxy.



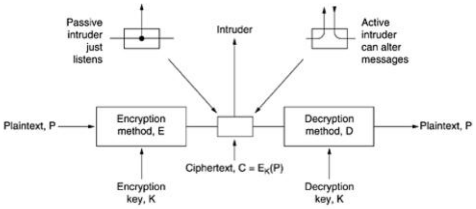
f) Write short notes on the term parity check [2 Marks]

A parity check ensures that when data is transmitted from one device to another or stored locally, there is a means to recover lost transactions. Parity checks are used during data transmission to detect errors caused by interference or noise.

When data is transmitted, each character is encoded as a 7-bit binary number. Then an eighth bit is added to make a byte. This bit is called a parity bit. Technically this is described as an (8, 7) error-checking code. A system can use either even or odd parity. In even parity, the value of the parity bit is set such that the total number of 1s in the data is even.

Question 6

a) With use of diagram, explain the five major parts in a basic encryption model [6 Marks]



b) Describe two types of intruders that can affect data privacy and or integrity [2 Marks]

Sometimes we only have passive intruder (just listen to message)

Active intruders can also can also record messages, play them back later, inject their own messages, or modify legitimate messages before they get to the receiver (active intruder)

c) Explain the two methods of breaking private encryption [2 Marks]

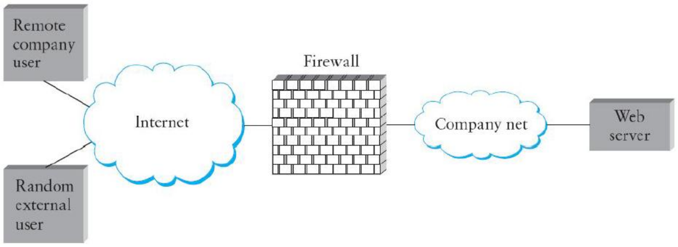
Brute force is just as it sounds; using a method (computer) to find all possible combinations and eventually determine the plaintext message.

Cryptanalysis is a form of attack that attacks the characteristics of the algorithm to deduce a specific plaintext or the key used. One would then be able to figure out the plaintext for all past and future messages that continue to use this compromised setup.

d) Write notes about the following firewalls

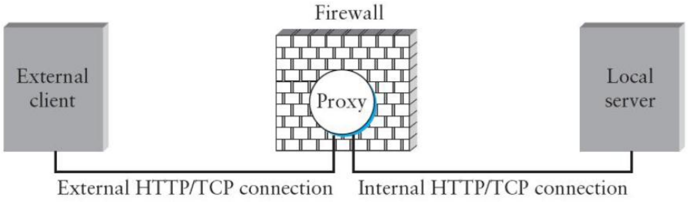
a Filter-Based firewall [2 marks]

Filter-based firewalls are the simplest and most widely deployed type of firewall. They are configured with a table of addresses that characterize the packets they will, and will not, forward. each entry in the table is a 4-tuple: It gives the IP address and TCP (or UDP) port number for both the source and destination.



b Proxy-Based firewall [4 marks]

A proxy is a process that sits between a client process and a server process. To the client, the proxy appears to be the server; in a sense, the proxy is standing in for the server. To the server, the proxy appears to be the client. the firewall dynamically decides what packets to forward and what packets to drop, with the policy embodied in the application-specific proxy.



e) TLS security technology automatically encrypts e-mail messages between servers thereby reducing the risk of snooping, interception, and alteration. Explain the two layers that make up Transport Layer Security (TLS) protocol [4 Marks]

TLS is composed of two layers: the TLS Record Protocol and the TLS Handshake Protocol.

The TLS Record Protocol provides connection security with some encryption method such as the Data Encryption Standard (DES).

The TLS Handshake Protocol allows the server and client to authenticate each other and to negotiate an encryption algorithm and cryptographic keys before data is exchanged.