IMPERIAL COLLEGE OF SCIENCE, TECHNOLOGY AND MEDICINE

EXAMINATIONS 2017

BEng Honours Degree in Electronic and Information Engineering Part II
MEng Honours Degree in Electronic and Information Engineering Part II
MEng Honours Degree in Mathematics and Computer Science Part III
MSc in Computing Science
for Internal Students of the Imperial College of Science, Technology and Medicine

This paper is also taken for the relevant examinations for the Associateship of the City and Guilds of London Institute

PAPER C527

COMPUTER NETWORKS AND DISTRIBUTED SYSTEMS

Monday 8 May 2017, 10:00
Duration: 120 minutes

Answer THREE questions

Paper contains 4 questions
Calculators required

Section A (Use a separate answer book for this Section)

1 a A workstation uses Cristian's algorithm for clock synchronisation in order to synchronise with a time server. The times at which the messages are sent $(T0)$ and received $(T1)$ are outlined below.

T0	T1
17:43:04.220	17:43.04.234
17:43:04:250	17:43:04.262
17:43:04:274	17:43:04.307

Assuming the server takes less than $2ms$ to reply to any message, explain what correction should be applied to the clock.

b A European wide high speed rail control system has a dedicated time server receiving the Coordinated Universal Time (UTC) from satellites with an accuracy of $10ms$ and a set of operator workstations.

Trains have a maximum speed of $360Km/h$ and receive UTC from an onboard GPS receiver with an accuracy of $10ms$. Each train communicates its position to the workstations, which incurs a $10ms$ delay. Assume the workstation is synchronised with the time server within $5ms$. Give the inaccuracy of the position of the train as given by a workstation due to propagation delay and time synchronisation.

c Assume that the interactions between trains and workstations in part b) above use Java RMI. Consider the case of trains on a single track reporting their position to workstation $wks.rail.com$. The workstation maintains the position of all the trains, and ensures that a minimum separation distance (MSD) of $8.2Km$ is maintained between them (assume trains are travelling in the same direction).

Trains report their position every $20s$. When receiving a position report from a train the workstation returns $false$ if its distance to any other train is less than the MSD. Additionally, the workstation warns the other trains that are too close (i.e., below the MSD) via an RMI invocation. Assume the interfaces to be as follows:

For the *Workstation*:

```
1 public interface IReport extends Remote {
2   boolean reportPosition(int TrainId, float position);
3 }
```

For the *Train*:

```
1 public interface INotify {
2     void notifyWarning();
3 }
```

Additionally, assume that the following local function exists and allows a train to retrieve its position, which it can report to the workstation.

```
1
2       public static float getConvertCurrentPosition()
```

Scheduling a task to be performed every x seconds in a new thread can be done in Java with the following code:

```
1  Timer t = new Timer( );
2
3  t.scheduleAtFixedRate(new TimerTask() {
4
5      @Override
6      public void run() {
7          // code to be executed
8      }, 1000,20000);
9
10 }
```

i) Give the Java RMI Implementation for the *Train* class

ii) Give the Java RMI Implementation for the *Workstation* class

Strict Java syntax is not required but your solution should indicate what is needed for instantiating remote objects, remote reference registration, binding, security and appropriate exception handling. State clearly any additional assumptions that you make.

The three parts carry, respectively, 20%, 20%, and 60% of the marks.

2a The following protocol has been proposed for two parties Alice A and Bob B to interact across the Internet using a trusted server S that has shared keys with all the parties. The protocol uses symmetric cryptography. K_{XY} denotes a symmetric key known only to X and Y. T_X denotes a timestamp generated by X.

$$\text{Message 1} \quad A \longrightarrow S: \quad A, \{T_A, B, K_{AB}\}_{K_{AS}}$$
$$\text{Message 2} \quad S \longrightarrow B: \quad \{T_S, A, K_{AB}\}_{K_{BS}}$$

i) Explain what each message achieves and what the protocol as a whole achieves.

ii) Propose a modification of the protocol to achieve mutual authentication in two additional messages.

b List the similarities and differences between a Kerberos Authentication Server and a Certification Authority as encountered in Public Key Infrastructures. Discuss the context in which each is more appropriate to use and consider the cases of users interacting across administrative domains.

c An organisation allows its users to browse the web and use the Flack application for messaging and file exchange. Flack is a conferencing protocol which allows users to send messages to each other through the *flack.com* server and to establish direct connections with each other to exchange files. Flack clients communicate via UDP with the server (which runs on port 4000) and via TCP (on ports > 1024) with the server and with other clients. The UDP exchange with the server is established first and then used to exchange the port numbers for the TCP connections to the server, which are initiated by the clients. These TCP connections are then used to exchange messages with other clients and to establish direct client to client TCP connections for file transfer. The organisation's network is separated from the outside network by a packet filtering router (PFR).

i) Give a configuration for the PFR in the following format.

Rule No.	Protocol	Dir.	Source Address	Src. Port	Dest. Address	Dest. Port	TCP Flags	Action

ii) Discuss the security implications of using Flack and propose recommendations to improve the security of the network.

The three parts carry, respectively, 20%, 20%, and 60% of the marks.

Section B (Use a separate answer book for this Section)

3 Consider the following scenario: You are a network administrator tasked with setting up new computer laboratories in your company. You are given the class C network *216.0.0.0*. You decide to divide it and use the network *216.0.0.128* with subnet mask *255.255.255.192* for the first computer laboratory. Please answer the following questions and explain all your answers:

a What network classes exist, how do they differ, and how can you find out what network class *216.0.0.0* is by just examining the address.

b What is the total number of hosts you could address using the whole class C network if you decided not to divide it into any subnets?

c Given the class C network and subnet mask above, how many subnets do you have available and how many hosts per subnet are addressable?

d What is the range of IP addresses you can assign to hosts in the first computer laboratory and what is the broadcast address of this subnet if one exists?

e What are the private internet address ranges that are available, in case you need more IP addresses than you were given? What are the limitations of private addresses and discuss any mechanisms that can overcome these limitations.

f You decide to use DHCP to configure the IP addresses of the computers dynamically. What does DHCP stand for, what else could you use it for, and how does DHCP dynamically configure a computer with an IP address?

The six parts carry, respectively, 20%, 10%, 10%, 15%, 25%, and 20% of the marks.

4 a Consider the example where host A sends 5000 bytes of data to host B over an uncongested link using TCP. Draw a TCP sequence diagram that shows the connection establishment, data transmission, and connection release. Include all relevant TCP flags, fields, and data sizes for every TCP segment in the diagram.

Take the following additional information into account: (a) Host A never sends more than 2000 bytes of data in one TCP segment, and (b) Host B has a buffer of 9000 bytes, which is not emptied throughout the lifetime of the whole transmission.

b Explain what TDM, FDM and CDMA are, how each of them works, and what has to be considered if they are to be deployed.

c What is the Address Resolution Protocol (ARP) used for, why is it needed, and how does it work?

d Draw the OSI Reference Model and TCP/IP Model next to each other in a way that clearly shows how the layers of one model are represented in the other. Also, for each of the 3 lowest layers, list at least 2 services that they provide.

The four parts carry, respectively, 25%, 30%, 25%, and 20% of the marks.