UNIVERSITY OF LONDON
IMPERIAL COLLEGE OF SCIENCE, TECHNOLOGY AND MEDICINE

EXAMINATIONS 2001

BEng Honours Degree in Computing Part III
BEng Honours Degree in Information Systems Engineering Part III
MEng Honours Degree in Information Systems Engineering Part III
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 C335=I3.14

DISTRIBUTED SYSTEMS

Friday 4 May 2001, 10:00
Duration: 120 minutes

Answer THREE questions

Paper contains 4 questions
Calculators not required

1 A building security system has a controller for every room with integrated switch and display. Each room also has a motion detector. The switch can be used to enable or disable alarms being generated from the local motion detector. The display indicates *disabled*, *enabled* or *alarm* condition. Each room-controller communicates with the motion detector and a centralised operator via a network. The current state of every room is indicated on the operator's display. The operator has a keyboard to enter room numbers and commands to clear an alarm for a particular room. The room-controller sends state information every 5 seconds to the operator, and receives a return value to indicate whether an alarm condition has been cleared.

a Assuming a Java RMI object invocation system for implementation, produce a diagram indicating all the objects needed to model this security system and the operation invocations between objects (only a single room system plus the operator need be shown). Assume that normal Java input-output is used by the room-controller to interact with its switch and display and by the operator to interact with its keyboard and display. Use the following interface specification.

```
package securitySystem;
import java.rmi.*;

public interface MotionDetector extends Remote {
      public boolean detect ( ); } // assume detect resets motion detector

public interface iOperator extends Remote {
      public boolean report (int room, int status); // true response clears alarm

int disabled = 0; enabled =1; alarm = 2; // status values
```

b Give a *pseudocode* outline for the *room-controller* as a client, which is created with a parameter indicating room number, and the *operator* as a server. Strict Java syntax is not required.

The two parts carry, respectively, 20%, 80% of the marks.

2a Describe the *transport* protocol needed to implement the following *synchronous* message interaction primitives and cater for timeouts. Assume error-free message transmission.

Send (port, t, message) – sends message to port and blocks, up to t seconds, waiting for it to be received.
Receive (port, msg) – blocks the receiver until a message is available on port, then it is received into variable msg.

b *Briefly* explain the functions performed by both client and server for an RPC binding to take place.

c *Briefly* discuss the system failures and communication error conditions that a reliable RPC mechanism would have to consider. Mention what the underlying system can do about each failure.

The three parts carry, respectively, 25%, 30 and 45% of the marks.

3a Define the terms *domain*, *authorisation policy* and *obligation policy*.

b A company runs an internal video database server. All staff are permitted to perform the actions list on the server to list all videos, start (video) and stop (video) to view videos between 14:00 and 18:00. Production staff can perform the actions insert (video) or delete (video) on the database between the hours 09:00 and 14:00. When a video is started the database server generates an event start and an event stop when the video is stopped. Both these events have the IP address of the viewer's workstation as a parameter. A bandwidth manager receives these events and reserves 2 Mbit/s bandwidth for the workstation on the internal routers, provided the total reserved bandwidth is always < 80 Mbit/s.

Assume an object bw with 3 operations, which can be invoked by the bandwidth manager:

bw.add (n) adds n to the reserved bandwidth
bw.subtract (n) subtracts n from the reserved bandwidth
bw.total ( ) returns the total reserved bandwidth

Indicate, by means of a diagram, the set of domains required for the above scenario and specify the two authorisation and two obligation policies required, using the following notation:

```
auth+ policy_name {
        subject <subjectdomain>; target <target domain>;
        action <actionlist>; when < constraints>;
}

 oblig policy_name {
        on <eventname (event_parameters)>;
        subject <subjectdomain>; target <target domain>;
        do  <action1>  -> <action2> ->..;   // sequence of actions
        when < constraints>;
}
```

The two parts carry, respectively, 15%, 85% of the marks.

4 The department wishes to implement a system whereby all assessed work is submitted by email. Students send coursework by email to a central office server which acknowledges receipt and forwards the coursework to the relevant lecturer who also acknowledges receipt to the office.

There is no need for encryption of the coursework.

Using the notation below, describe a protocol between a student S, central office O, and lecturer L to give non-repudiation of submission and delivery. Explain how your protocol works, how it supports non-repudiation and justify the need for each field in a message.

L	lecturer name
S	student name
cwid	course work identifier (course and coursework number)
cw	actual coursework
H(cw)	hash digest of coursework
Tx	timestamp generated by X
Kxy	a secret key known to X and Y
Kso{m}	indicates encryption of a message m with a key known to S and O
Klo{m}	indicates encryption of a message m with a key known to L and O.

Assume the central office is trusted; each student and lecturer has a secret key known only to themselves and the central office; and the office does not hold coursework after sending it to a lecturer.