UNIVERSITY OF LONDON
IMPERIAL COLLEGE OF SCIENCE, TECHNOLOGY AND MEDICINE

EXAMINATIONS 2003

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

Monday 12 May 2003, 10:00
Duration: 120 minutes

Answer THREE questions

Paper contains 4 questions
Calculators not required

1 A hotel air-cooling system has a microcomputer for every room connected to a central operator's workstation via a network. Each room has a temperature sensor and a local control panel with a switch to enable/disable the room air-cooler and a dial to set the desired temperature. The current state (cooler on/off and local temperature) of every room is indicated on the operator's display. The room controller sends state information every 30 seconds to the operator. The operator has a display to indicate status information for all rooms in the hotel.

A Java RMI object invocation system is used for implementation. Use the following interface specification:

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

public interface iSensor extends Remote {
        public int sensread ( ) throws RemoteException;  } // read temperature

public interface iDial extends Remote {
        public int dialread ( ) throws RemoteException;  }  // read temperature dial

public interface iSwitch extends Remote {
        public boolean getswitch ( ) throws RemoteException;  }  // true = enabled

public interface iCooler extends Remote {
        public void setcooler ( boolean cmd ) throws RemoteException;  }
        //true = on, false = off

public interface iOperator extends Remote {
       public void  report  (int  temp, boolean coolerOn, string roomNumber)
              throws RemoteException; }
```

a Produce a diagram indicating all the objects needed to model the cooling system and show named *operation invocations* between objects (only a single room system plus the operator need be shown).

b Give the Java class for the *room-controller* as a client, which is created with a parameter indicating room number. Use a URL of the form rmi://roomNumber/objectName for binding to local objects.

c Give the Java class for the *operator* as a remote object i.e. a server. Assume that a procedure which uses normal Java I/O to write to the display is available

```
update (int  temp, boolean coolerOn, int room)
```

Implementations for the remote objects Sensor, Dial, Switch and Cooler are not needed. Strict Java syntax is not required but your solution should indicate what is needed for implementing remote objects, remote reference registration, binding and security, and holding room state information in the operator etc.

The three parts carry, respectively, 20%, 40% and 40% of the marks.

2a Explain the difference between *Maybe (best efforts)* and *At-most-once call* semantics for a remote operation invocation.

b Assume a library procedure of the form:

```
Result = RequestReply (DestIPAddr, DestIPPort, P1, P2, P3 ...Pn, Reply)
Result = OK, Fail (no-reply), ParametersTooLong
```

It takes the parameters P1 ... Pn packs them into a message which is sends using the Universal Datagram Protocol transport protocol (UDP) to the remote host whose IP address is DestIPAddr on port number DestIPPort.

At the remote side a process listens on the destination IP port to receive requests, executes a program using the parameters
P1 ... Pn and then generates a reply parameter, also sent back using the UDP service.

Assume the size of the parameters P1 .. Pn are limited to fit into a single UDP packet and the run-time system which implements this request-reply call supports *at-most-once* semantics.

i) What additional information will the run-time system have to add to the request and reply UDP messages?

ii) Outline the functions that have to be performed by the run-time systems at both the client and server side in order to support at-most-once semantics. Your solution must explain how to initialise and deal with sequence numbers, time-outs, retransmissions etc, but assume the server only receives requests from a single client.

The two parts carry, respectively, 25% and 75% of the marks.

3a Compare a Management Domain with a distributed file system directory. How can a domain be used to represent the rights of a person within the system?

b What is a management role and why is it needed? With an aid of a diagram, briefly explain how it can it be implemented using domains and policies?

c Company A has a file system with 2 types of files – temporary files which can be deleted at any time and production files which are considered permanent. All staff can read all files between 09.00 and 18.00, and programmers can write temporary files between 09.00 and 18.00. There is a FileSys manager agent which receives an event LowCapacity when the file system free space becomes < 5%, and deletes all temporary files (ignore errors due to open files). Assume file objects support the operations read, write, delete and use the following notation for policies.

```
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  <action> ;
        when < constraints>;
}
```

i) Indicate, by means of a diagram the set of domains required to implement the above scenario. Indicate policies as named arrows from subject to target.

ii) Specify the required authorisation and obligation policies using the above notation.

The three parts carry, respectively, 20%, 30%, 50% of the marks.

4a Briefly describe, with the aid of a diagram, the Bell-LaPadula security model for military security. Give the conditions for both reading and writing target objects

b A firm of accountants has 2 branches in the UK with 20 employees at one branch and 10 at the other. Each branch has a server holding client data. They want to allow all employees access to both servers via the internet. A new systems programmer suggest that a solution would be to hold the user passwords on both servers and to manually distribute an encryption key to each workstation and server. Users can then login to either server, using ordinary login but sending the user's password encrypted with the key held on each workstation. The server can decrypt the password and check its validity against the passwords which are stored in a file on the server, encrypted with the same key

i) Discuss the security risks in the above design

ii) Describe a suitable centralised authentication service protocol, *optimised for the small size of the firm*, which can be installed at the larger branch to serve the firm of accountants. Use the format Kxy{M} for encryption of a message M using a key known to X and Y. Your solution must describe the messages exchanges, and the reasons for each item in the message.

The two parts carry, respectively, 30% and 60% of the marks.