PAPER CODE NO.	EXAMINER : Peter McBurney
COMP515	DEPARTMENT : Computer Science Tel. No. 794 6760

THE UNIVERSITY
of LIVERPOOL

MAY 2004 EXAMINATIONS

Degree of Master of Science

TECHNOLOGIES FOR E-COMMERCE

TIME ALLOWED: Two and a half Hours

INSTRUCTIONS TO CANDIDATES

Answer any four questions.

Each question is worth 25 marks.

If you attempt to answer more than the required number of questions, the marks awarded for the excess questions will be discarded (starting with your lowest mark).

Electronic calculators are not permitted.

THE UNIVERSITY
of LIVERPOOL

QUESTION 1

(a) HTTP lacks state. What does this mean? **4 marks**

HTTP has no record of the history of requests, or of their success or failure. So one client may make the same request repeatedly.

(b) List two advantages and two disadvantages of HTTP's being stateless. **4 marks**

Advantages:
A user may access web-pages in any order
Content may be replicated on multiple servers
Low resource overheads

Disadvantages:
Unable to manage commitments to action
Allows servers to be subject to malicious repeated requests
Unable to deal with multi-step transactions
Cannot easily customize response to client

(c) Briefly describe three methods for overcoming HTTP's lack of state. **6 marks**

Require users to submit relevant information each time they request a URL.
Have the GET and POST commands include values of state variables with each request.
Store values of state variables on the client machine (in the form of cookies).
Store values of state variables on the server, and access this with session variables.

(d) When would you advise an e-commerce programmer to use session variables? Why? **6 marks**

It is advisable to use session variables when:
It is necessary to track state for client-server interactions.
It is necessary to track state for all clients, even those with old browsers or those disabling cookies.
It is necessary to prevent clients inserting their own values in state variables (as they may do with embedded state variables and cookies).
Likely client numbers do not result in resource limitations on the server (since client information is stored on the server, not on the client).

(e) What is the semantic web? How does it differ from the original World-Wide-Web? What are its advantages and disadvantages? **5 marks**

The semantic web has web-pages with machine-readable content. The original WWW involved pages created by humans to be read by humans; the current WWW involves mostly pages created by machines, and read by humans; the semantic web will involve mostly pages created by machines and mostly read by machines. Main advantage is machine readability, and hence the creation of capability for automated interactions. Main disadvantage is the bottleneck of annotation of web-content.

QUESTION 2

(a) Draw a diagram to show how a CORBA client and server are connected through an Object Request Broker, showing stubs and skeletons. **3 marks**

See below

(b) The Internet is a best-effort communications medium. Explain what problems this creates for communications. **5 marks**

Packets may be lost, they may be delayed, they may be corrupted in transit, they may arrive out of order, there may be network congestion or flow problems, network entities may go off-line without warning and without backup, etc.

(c) Explain how the TCP protocol seeks to overcome these problems. **6 marks**

TCP features include:
A handshake for session set up;
Use of ACKS from the sender to verify that individual packets have arrived.
Use of cumulative ACKS to verify that packets arrive in order.
Pipelining
Congestion Control;
Flow control.

(d) Suppose you are tasked with the design of an Internet application, and you can use either the TCP protocol or the UDP protocol in your application. What factors would you consider in choosing between them? **6 marks**

Factors such as:
Is the application time-critical?
Must packets arrive in sequence?
Is loss of some packets acceptable?
Is flow control required?
Is network congestion a concern?

(e) Explain why voice-over-Internet applications typically use the UDP protocol. What are the performance consequences of this choice, both for the application and for the Internet as a whole?

5 marks

Voice-communications can tolerate the loss or out-of-order delivery of some packets, so use of UDP is not deleterious. Moreover, avoiding Internet congestion and flow control mechanisms contained in TCP is useful, so VOIP applications typically use UDP. The performance consequences are:
For the application a potential loss of sound quality;
For the Internet possible network congestion.

QUESTION 3

(a) Using the FIPA ACL performatives, list a dialogue between a single potential seller and multiple potential buyers engaged in an auction using an open-cry English protocol. **5 marks**

inform(seller: all: English auction start)
cfp(seller: all: proposals to buy item A at price above threshold)
propose(bidder 1: all: buy-at-price-1)
propose(bidder 2: all: buy-at-price-2), etc
cfp(seller: all: proposals to buy item A at price above price-k)
propose(bidder 1: all: buy-at-price-1)
propose(bidder 2: all: buy-at-price-2), etc

cfp(seller: all: proposals to buy item A at price above price-m) :accept-proposal(seller: all: proposal from bidder-d)
reject-proposal(seller: all: proposals not from bidder-d)
request(seller: bidder-d: please complete the transaction).

(b) Draw a Message Sequence Chart to show the sequence of FIPA ACL utterances for an open-cry Dutch auction protocol. **5 marks**

see attached

(c) A brewing company called *Global Beers* approaches you to build them an extranet to manage their relationships with their suppliers. Their suppliers fall into three categories: agricultural producers of hops; manufacturers of bottles and kegs; and manufacturers of brewing machinery. Global Beers wants to have on-line auctions, so that suppliers in each category have to compete with each other to sell their products or services to Global Beers. What objectives should Global Beers have for such auctions, and why? Given these objectives, what type of auction(s) would you recommend, and why? **10 marks**

Note that in this case suppliers win an auction if they offer the lowest price.

Possible objectives for Global Beers:
Reduce costs of supply through use of competitive auctions (cost minimization)
Improve speed and efficiency of supplier-selection process
Ensure fairness and transparency of auction procedures
Increase range of suppliers by use of open procedures.

The following are probably not objectives for Global Beers:
Eliminate winner's curse
Ensure bidders bid honestly.

What types of auction? The following would be a reasonable argument:

Open-cry auctions are likely to yield lower prices to Global Beers than sealed bid auctions, since bidders see each other's valuations. Second-price auctions would eliminate the winner's curse, but this is not a concern to Global Beers. Thus, I would recommend ascending or descending open-cry auctions.
Of these two, there may be an argument that one is preferable to the other, although this difference may disappear with repeated auctions. If Global Beers starts with an initial price and allows bidders to cry out lower prices (strictly an English auction, although descending), then the final price is likely to be better for Global Beers than if Global Beers start with an initial floor price and raises it incrementally, allowing bidders to shout "Accept" when it reaches a level they are happy with (strictly speaking a Dutch auction, although ascending).

(d) What advantages and disadvantages can you see in the use of the FIPA ACL for the conduct of electronic auctions? **5 marks**

Advantages:
FIPA ACL is a standard, so likely many users.
Language has been designed with contractual negotiations and auctions in mind.
Simple syntax.

Disadvantages:
Semantics requires sincerity (not appropriate for auctions).
Semantics cannot be verified.

QUESTION 4

(a) Consider a double auction market for wholesale electricity with potential buyers making bids, and potential sellers making asks in successive rounds. Suppose in round 1 the following bids were made:

- Buyer 1 bids for 200 units at £6 per unit.
- Buyer 2 bids for 100 units at £10 per unit.
- Buyer 3 bids for 200 units at £3 per unit.

Suppose in the same round the following asks were made:

- Seller 1 asks for £4 per unit for 25 units.
- Seller 2 asks for £10 per unit for 200 units.
- Seller 3 asks for £8 per unit for 350 units.

Suppose the managers of this marketplace are investigating different clearing algorithms. Show which buyers and which sellers are matched with which, and the resulting transaction prices and quantities, under each of the following algorithms:

Algorithm 1: Buyers and sellers are matched pairwise: highest bid buyer paired with lowest-ask seller, and then next-highest buyer with next lowest seller, and so on. The transaction price for each pair is equal to the average of the bid and ask price spread, and the transaction quantity for each pair equal to the minimum of the bid and ask amounts.

Matches as follows:
Buyer 2 with Seller 1: Price = £7, units = 25.
Buyer 1 with Seller 3: Price = £7, units = 200.
Buyer 3 with Seller 2: Price = £6.50, units = 200.

3 marks

Algorithm 2: As for Algorithm 1, except that after each transaction, any units offered by the seller and not sold to the paired buyer, are then sold to the next buyer.

3 marks

Matches as follows:
Buyer 2 with Seller 1: Price = £7, units = 25.
Buyer 1 with Seller 3: Price = £7, units = 200.
Buyer 3 with Seller 3: Price = £6.50, units = 150.
Buyer 3 with Seller 2: Price = £6.50, units = 50.

For the remainder of this question, assume that two participants are engaged in an interaction using the monotonic concession protocol (MCP), which proceeds through a number of rounds.

(b) How does an interaction using the MCP begin? **1 mark**

One party proposes a deal.

(c) What utterances can each participant make at each round of this protocol? **3 marks**

At each round, the participant whose turn it is can:
Accept the most recent proposal from the other party
Make a counter-proposal
, or Withdraw from the interaction.

(d) Under what circumstances does the interaction end? **4 marks**

When one of the following events occurs:
One party accepts a deal proposed by the other.
One party withdraws from the interaction.

(e) Describe with a diagram how you could represent this interaction using Javaspaces (or Tuple spaces)? What Javaspace (or Tuplespace or Linda) commands would correspond to each possible utterance? **6 marks**

The basic idea is that proposed deals by one party are represented by insertions into the shared tuple space, and these are accepted by the other party withdrawing from the space.

Thus, the match between utterances, tuple-space and Linda commands would be:
Propose(deal) == write(deal) == out(deal)
Accept(deal) == take(deal) == in(deal)

There is no direct match for the Withdraw utterance, except perhaps if the proposer were to use the command take(deal) *to remove all his previously-inserted tuples, i.e., all his prior* write(deal) *utterances.*

(f) What factors are important in assessing an interaction protocol? **5 marks**

Factors such as:
Expressiveness.
Does the protocol facilitate resolution (the reaching of agreement)?
Simplicity of syntax?
Computational simplicity?
Is there an agreed semantics?

QUESTION 5

(a) A company called *Global Beers* wants you to develop a distributed electronic application for them, incorporating all their current business activities and systems. About which aspects of the distributed system would you need to make design decisions? What criteria would you use to assess the resulting system? **9 marks**

Full marks awarded for having most of the following items. Proportional marks for having items pro rata.

Decisions required concerning:
What elements to include in the distributed system (e.g. clients, servers, specialist servers, databases, peripherals, etc).
Their physical location.
Logical connections between them.
Physical connections between them.
Which protocols and design languages will be used by the elements?
What security measures will be taken?
What provisions for redundancy will be made?
How will operational performance be optimized?

Criteria for assessment:
Effectiveness
Manageability
Information Coherence
Optimal Performance
Extensibility
Scalability
Fault Tolerance
Security
Resistance to lawsuits.

(b) *Global Beers* wants a sub-system of the overall system to enable their customers to purchase beer and wines over the Internet. Draw a diagram to show the main components of such a sub-system.

6 marks

See attached

(c) The company wants all visitors to its web-site to fill in a form with their name, postal address and other details, with this form submitted to the company's server. From there, Global Beers will then store this information in a company database, which they can analyze for marketing purposes.

(i) Global Beers also wants to sell their database of customer names and addresses to other companies. What must Global Beers do first for this to be legal in Britain? **2 marks**

They must first get the permission of each customer on the list.

(ii) Further, Global Beers asks you to develop a cookie which will track all the other web-sites visited subsequently by each client who browses their site. Is this possible with HTTP? Why or why not? **3 marks**

No, this is not possible. Cookies are not enabled to do this.

(e) What is a legacy system? Why would they be important in an application such as the online alcohol purchase system planned by Global Beers? **5 marks**

A legacy system is a operational computer system in an organization which is predates the proposed new system. In the case of Global Beers, such systems might include billing and accounting systems, stock-control and inventory systems, and marketing data warehouses. Any online purchasing system would need to interact with these, to a greater or lesser extent. Hence, the designers of the new system need to take into account the legacy systems in place when building the new system.

QUESTION 6

The following questions concern various versions of an authentication protocol, called **AP** (Authentication Protocol). The versions are labelled *APv1, APv2,* etc.

(a) In *APv1*, the sender of a message, say Alice, can authenticate herself to the receiver, say Bob, by sending the message *"I am Alice"*. What is the flaw in *APv1* as an authentication protocol? **2 marks**

Anyone could impersonate Alice.

(b) To overcome the flaw in *APv1*, a modification to the protocol is made. In this version, *APv2*, the sender Alice also sends her IP address. What is the flaw in *APv2* as an authentication protocol? **2 marks**

Anyone could impersonate Alice, since they could insert her IP address in the appropriate field of packets sent to Bob.

(c) In *APv3*, Alice and Bob agree a special word beforehand, and then whenever they communicate, Alice also sends this special word with her message. What is the flaw in *APv3* as an authentication protocol? **3 marks**

Anyone could eavesdrop on Alice's communications, and thus obtain the special word.

(d) In *APv4*, protocol *APv3* is modified to use a sequence of nonces and a symmetric key algorithm. Explain how *APv4* would work. **3 marks**

Each nonce is a special word which is only used once. The first nonce is encrypted using the symmetric key algorithm and sent with the first message between Alice and Bob. The next nonce is then used for the next message between the two, and so on.

(e) What is the major practical problem in implementing protocol *APv4*? What solutions exist to this problem? **6 marks**

Distribution of the nonces and the symmetric key to both Alice and Bob. Solutions include:
Use of trusted third-parties to generate keys.
Use of asymmetric-key system to distribute symmetric keys.
Couriers, phone calls, faxes and snail mail.

(f) In *APv5*, protocol *APv4* is modified to allow an asymmetric key algorithm. Explain how *APv5* would work. **4 marks**

The protocol could begin with Alice sending a message to say that she is Alice. Bob could then send her a nonce word. Then she would encrypt it using her private key. Bob would then decrypt it using her public key. Provided her private key had not been stolen, Bob's decryption using her public key would guarantee to him that the message he received from Alice was in fact from her.

(g) What factors would be important in choosing between *APv4* and *APv5*? **5 marks**

The extent to which the the authentication will involve many parties, or just one.
The extent to which the authentication process will need to be undertaken multiple times, or just once.
The extent to which alternative means of delivery of keys is possible, e.g., via face-to-face meetings, or courier delivery.
The size and importance of the transactions for which authentication is required.