Two hours

Special instructions:
e.g. On-Line Examination: This paper will be taken on-line and this is the paper format which will be available as a back-up

UNIVERSITY OF MANCHESTER
SCHOOL OF COMPUTER SCIENCE

Computer Networks

Thursday 22nd January 2011

Time: 14:00 – 16:00

Marker's feedback version

Marking Scheme Included

Please answer any THREE Questions from the FOUR questions provided.

Use a SEPARATE answerbook for each SECTION.

Marks will be awarded for reasoning and method as well as being correct.

The use of electronic calculators is permitted provided they are not programmable and do not store text.

Section A

Answer *two* of the four questions

This text appears only in the marking scheme version

1. Security

> **Marker's feedback**
> This environment, together with the `fb` class option, can be used to produce a version of your paper that also includes post-marking feedback

a) In relation to network security, give a brief definition for each of the following terms:

i) Authentication (1 mark)

> **Model Answer:** Authentication is the mechanism of making somebody believe that you are who you say you are. The `answer` command takes two arguments, the first being a brief answer and the second a description of the way marks are allocated. **N.B.** The `answer` macro is only for short, unformatted answers only. For anything that requires the use of an included environment, eg program listing or table, use the `mkscheme` or `mkscheme*` environments, see below.
> **Distribution of Marks:** 1 Mark for any reasonable answer.

ii) Confidentiality (1 mark)

> **Model Answer:** Confidentiality is a property of a piece of information that prevents it from being distributed on facebook or so.
> **Distribution of Marks:** 1 Mark for any reasonable answer.

iii) Integrity (1 mark)

iv) Digital signature (2 marks)

b) Sue wants to send a file to John. As she is concerned that someone might tamper with the contents of the file, she wants to protect it so that John is confident that he receives the same contents as Sue sent. John has recently been receiving viruses hidden within what appear to be valid files. Therefore, he will only use the file from Sue if he has proof that it does come from Sue.

By using network security techniques, design a mechanism that allows Sue to send her file to John such that John can be sure that it comes from Sue and that its contents have not been modified. Sue already has a public-private key pair for which John has a validated copy of the public key. You should describe how your mechanism works and include a diagram to illustrate your answer. (6 marks)

c) Describe what the man-in-the-middle attack is and illustrate why it is possible. (5 marks)

d) Describe why digital certificates can reduce the possibility of a man-in-the-middle attack, and any limitations that digital certificates may have that prevent them from completely avoiding this attack. (4 marks)

2. a) In the context of web servers, what is a cookie and why is it used? (3 marks)

   b) Outline how a web application would fetch a webpage containing multiple objects using version 1.0 (non-persistent) of the HTTP protocol. (2 marks)

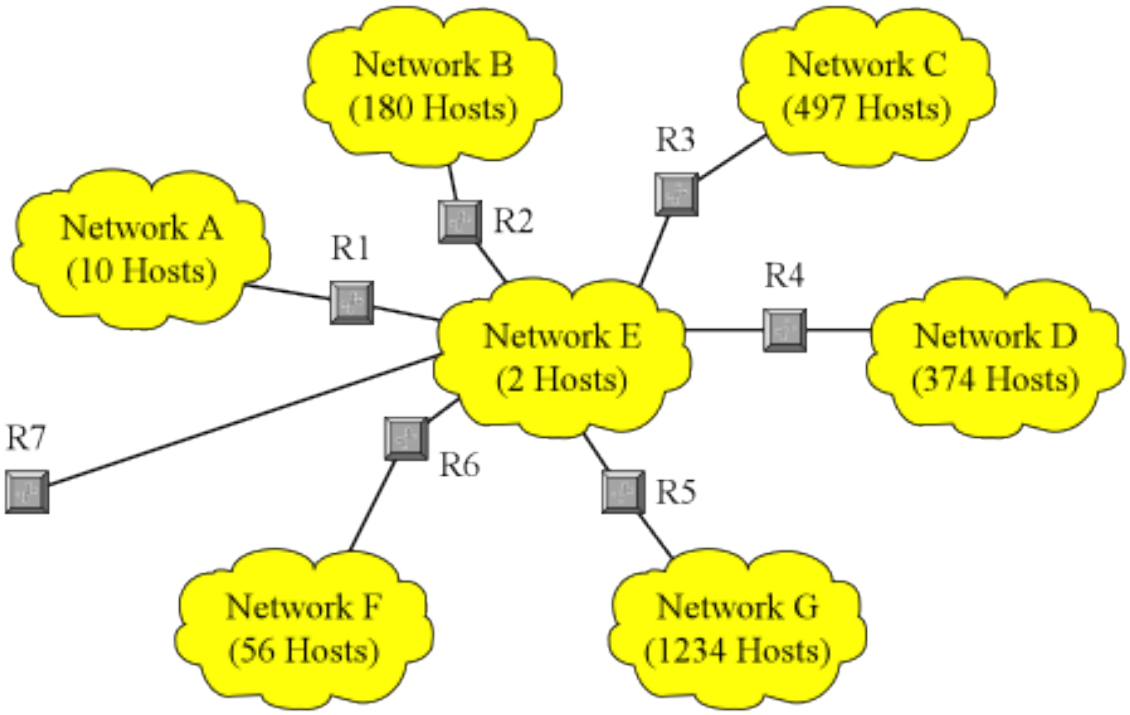
> **Model answer and marking scheme for Q2b**
> This is a way of interpolating longer solutions that are too complex for the `\answer` macro
> **Distribution of Marks:** 1 mark for this and 1 mark for that

> **Marker's feedback**
> This environment can be used to produce a version of your paper that also includes post-marking feedback

   c) Explain the issues that arise from the use of version 1.0 of the HTTP protocol, how version 1.1 (persistent) of the protocol addresses these, and any issues associated with the use of version 1.1 of the HTTP protocol. (6 marks)

   d) Show how the TCP uses acknowledgements, timeouts and sequence numbers to make the transmission of data between the distributed parts of an application appear reliable when an acknowledgement packet is lost. (4 marks)

   e) The following picture shows the structure of the network being used by an organisation. The Internet authorities have allocated this organisation the block of network addresses 195.123.0.0-195.123.x.0. By using the Classless Inter-Domain Routing (CIDR), decide how these addresses should be allocated within the organisation, and what netmasks should be used, to allow all of the organisation's hosts to be fully connected to the Internet. (5 marks)


Network B
(180 Hosts)
Network C
(497 Hosts)
R3
Network A
(10 Hosts)
R2
R1
R4
Network E
(2 Hosts)
Network D
(374 Hosts)
R7
R6
R5
Network F
(56 Hosts)
Network G
(1234 Hosts)

[Next page →]

Section B

3. a) Assume you are using a 1024x768 pixel video source with 24 bits for each pixel's colour. Explain why video data must be compressed for transmission to a typical home network through an ADSL link operating at 8Mbps? (2 marks)

   b) If the network delays for sending the video from part 3 b) above to a home video player is on average 100ms. Explain why a much larger delay is necessary before playing the data? (3 marks)

   c) A number of families are watching different videos delivered interactively in real-time from a single streaming server over the Internet to their homes.

   Draw a diagram to show a possible network architecture for this scenario. (5 marks)

   Using your diagram as an example, explain why a simple client + server architecture might struggle to support this application over the Internet. (2 marks)

   How are content suppliers solving the network congestion problems caused by using a simple client + server architecture? (5 marks)

   d) One of the families in 3. c) above, decides to skip a section of the video they have already seen and click a "jump forward 30 minutes" button on their home system.

   List what the multi-media streaming system needs to do in order to react to this request? (3 marks)

Model answer and marking scheme for Q3

Non-interpolated solution and marking scheme, possibly using the parts and subparts environments.

a) Video data is . . .

b) The delay is caused . . .

c) Picture goes here

d) The streaming system . . .

4. a) What are the most important differences between a wired network medium and a wireless one? (6 marks)

   b) How is space multiplexing enforced for local terrestrial broadcast wireless stations such as BBC Radio Manchester (on 95.1MHz) and Key 103 (on 103MHz)? (2 marks)

   c) How is space multiplexing enforced when using wireless local area networking standards such as IEEE 802.11 and Bluetooth? (2 marks)

   d) Why is Ethernet not run directly over a wireless medium?

   IEEE 802.11 provides an Ethernet like service over wireless. How does IEEE 802.11 do this? (4 marks)

Model answer and marking scheme for Q4d
Code is not appropriate for this answer, these are just a couple of examples of how you might include sections of code, without using the standard verbatim environment, which is not suitable for this context. **Environments like this can not be used within an argument of the `answer` command**

```
1     // code using fancyvrb package
2     // line numbers and frame lines optional
3    while (true)
4        do
5            stuff // this is a comment
6            more stuff
7        done
```

```
# code using listings package
while (true)
     do
          stuff // this is a comment
          more stuff
     done
```

Distribution of Marks: 1 mark for this and 1 mark for that

   e) What do both Ethernet and IEEE 802.11 do before re-transmitting data lost due to a collision? Why? (4 marks)

f) Why do all Ethernet standards for all supported types of wired media specify a strict maximum wire length? (2 marks)

Section C

This section is multiple choice

5. What is the answer to this question?

   A. This
   B. That
   C. The other
   D. None of the above

   B

6. What is the answer to this question?

   A. This
   B. That
   C. The other
   D. None of the above

   C

7. What is the answer to this question?

   A. This
   B. That
   C. The other
   D. None of the above

   A

8. What is the answer to this question?

   A. This
   B. That
   C. The other
   D. None of the above

   D