UNIVERSITY OF LONDON
IMPERIAL COLLEGE OF SCIENCE, TECHNOLOGY AND MEDICINE

EXAMINATIONS 1999

MEng Honours Degrees in Computing Part IV
MEng Honours Degree in Information Systems Engineering Part IV
MSci Honours Degree in Mathematics and Computer Science Part IV
MSc Degree in Advanced Computing
for Internal Students of the Imperial College of Science, Technology and Medicine

This paper is also taken for the relevant examinations for the
Diploma of Membership of Imperial College
Associateship of the City and Guilds of London Institute
Associateship of the Royal College of Science

PAPER 4.30 / I 4.14

NETWORK SECURITY

Wednesday, May 5th 1999, 10.00 – 12.00

Answer THREE questions

For admin. only:
paper contains 4 questions

1a Outline how the following cryptanalytic attacks work:

i) Cipher-text only

ii) Known-plaintext

iii) Chosen-plaintext

b Define the term *unconditionally secure.* Is a one-time pad unconditionally secure? Explain.

c What is a *man-in-the-middle* attack?

d Define the function used in Diffie-Hellman Key Exchange and then prove that Diffie-Hellman Key Exchange is vulnerable to a man-in-the-middle attack.

The four parts carry, respectively, 30%, 20%, 10% and 40% of the marks.

2 Consider the following protocol for client-server authentication and key exchange where Bob is the server and Alice the client:

	From	**Message**	**To**
Message 1	Alice	From: Alice **Only: AliceBob** AliceN: 66	Bob
Message 2	Bob	**Only: AliceBob** AliceN: 66+1 BobN: 77	Alice
Message 3	Alice	**Only: AliceBob** BobN: 77+1	Bob
Message 4	Bob	**Only: AliceBob** SessionK: -1	Alice

a For this protocol outline the purpose of each message and describe how the protocol works.

b The protocol is vulnerable to an attack similar to that possible with the Needham-Schroeder protocol. What is the attack and how can it be prevented in this protocol?

c Finally simplify the protocol in order to remove redundancies and reduce the amount of encryption used while preserving the security of the protocol. Explain why your simplifications are possible.

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

3a Describe how the following firewall components operate:

i) a circuit-level gateway?

ii) an application-level gateway?

b A school is considering installing a firewall into it's computer network. For each of the following firewall controls describe the control and give an example of the control that the teachers at the school would appreciate:

i) service control

ii) direction control

iii) user control

iv) behaviour control

c Which of the following four internet security policies: *paranoid, permissive, promiscuous* or *prudent*, would be most appropriate for a school to adopt for its firewall. Define the policy you select and explain why it would be the best choice.

d Tunnelling refers to the practice of encapsulating all the messages of one protocol within another protocol. Comment on the implications of this practice for firewall protection.

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

4a You are asked to design an applet programming language for use on the internet. List four features that you would incorporate in your language design to ensure safe execution. Explain your choice of features.

b For your applet programming language list four restrictions that an applet execution environment, such as a web browser, should enforce when executing untrusted applets that attempt to access local resources. Explain your restrictions.

c Java applets can carry out denial-of-service attacks. Describe four such attacks. What facilitates could be incorporated into a web-browser to lessen the likelihood of Java denial-of-service attacks?

d "*Jumping the Firewall*" is an example of an early Java-based attack. Describe the attack and explain whether or not the attack exploits a weakness in the Java security model.

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

End of paper