UNIVERSITY OF LONDON
IMPERIAL COLLEGE OF SCIENCE, TECHNOLOGY AND MEDICINE

EXAMINATIONS 2001

MEng Honours Degree in Information Systems Engineering Part IV
MSci Honours Degree in Mathematics and Computer Science Part IV
MEng Honours Degrees in Computing Part IV
MSc 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 Associateship of the City and Guilds of London Institute
This paper is also taken for the relevant examinations for the Associateship of the Royal College of Science

PAPER C430=I4.14

NETWORK SECURITY

Thursday 3 May 2001, 10:00
Duration: 120 minutes

Answer THREE questions

Paper contains 4 questions
Calculators not required

1a For DES and other block ciphers:

(i) What is the purpose of the Initialisation Vector (IV)?

(ii) Explain whether it is necessary for the IV to be a random number?

(iii) Explain why the IV need not to be secret.

(iv) Explain why the integrity of the IV needs to be protected.

(v) Explain why for OFB mode, the IV needs to be unique for each message.

(vi) How might we pad the last plaintext block in order in order to cope with messages that are not an exact multiple of the block size?

b Assuming that encryption is used without integrity, give 4 examples of how an attacker might be able to usefully manipulate DES ciphertext without detection

c Although plaintext messages are concealed by CBC chaining, very long messages will still have patterns. Apply the birthday paradox to predict after how many blocks of a very long message, identical blocks will occur.

d Consider the following variant of CBC mode. For a plaintext block P_i , the corresponding ciphertext block C_i is produced with the following encryption method:

$$C_i = E_k (P_i \textbf{ xor } P_{i-1} \textbf{ xor } C_{i-1})$$

For this variant mode:

i) Derive the decryption method.

ii) Draw diagrams for both the encryption and decryptions methods.

iii) Comment on the result of an adversary swapping two adjacent ciphertext blocks.

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

2 In this question you are asked to consider a 3-message protocol that enables Alice to confidentially send a message P to Bob without any advance exchange of keys. The protocol assumes the existence of an encryption algorithm with the following commutative property:

$$E_{K1}(E_{K2}(P)) = E_{K2}(E_{K1}(P))$$

In the following messages, Alice's key is A; Bob's key is B. A is only known to Alice and B is only known to Bob. The first two messages of the protocol are:

Alice→Bob: $C1 = E_A(P)$

Bob→Alice: $C2 = E_B(C1)$

a Deduce the third message necessary to complete the protocol and explain how the protocol works. Remember that A is only known to Alice, and B is only known to Bob.

b The three message protocol above can be adapted to use an asymmetric key encryption/decryption algorithm similar to RSA. For the adapted protocol, encryption is performed using $C=P^E \bmod N$; decryption with $P = C^D \bmod N$, where N is a large prime for which N–1 has a large prime factor, and $E*D=1 \bmod (N-1)$.

Explain how this adapted protocol works. Remember that Alice's encryption and decryption keys are only known to her, while Bob's are only known to him.

What "hard" problem would an eavesdropper Eve have to solve in order to recover P?

c One time pads are commutative but will not work with the protocol above. Explain how an eavesdropper Eve, can recover the message P, if one-time pads are used for the protocol you completed in part a.

d Perform a man-in-the-middle attack on the protocol in part a. Assume that the man-in-the-middle is called Max and that his key is M.

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

3 For this question you are asked to consider the firewall set-up of a company called Doc, that employs a **screened subnet architecture**. The bastion host has a *web server* and an *ftp server* for Internet users, as well as *web* and *ftp proxies* for company users.

The ruleset for the internal packet filter router (that connecting the internal network to the perimeter network on which the bastion host resides) is:

Rule	Dir.	Source Address	Dest. Address	Source Port	Dest. Port	TCP Flags	Action
S1	In	DocNet	*	*	*		Deny
S2	Out	#DocNet	*	*	*		Deny
H1	Out	DocNet	Bastion	>1023	4488		Allow
H2	In	Bastion	DocNet	4888	>1023	ACK	Allow
F1	Out	DocNet	Bastion	>1023	4421		Allow
F2	In	Bastion	DocNet	4421	>1023	ACK	Allow
F3	In	Bastion	DocNet	*	6000-6020		Deny
F4	In	Bastion	DocNet	>1023	>1023		Allow
F5	Out	DocNet	Bastion	>1023	>1023	ACK	Allow
X	*	*	*	*	*		Deny

The ports used above are: 21 (FTP), 4488 (HTTP Proxy), 4421(FTP Proxy), and 6000-6020 (Server ports) and

DocNet defines the company's internal subnet (e.g. 234.121.12.*)

#DocNet defines any address *not* in the company's subnet range.

Bastion is the company's bastion host (e.g. 234.121.13.99). Note: the bastion host's IP address is on the company's perimeter subnet.

* means ANY

Rules are applied top-down. The first match causes the corresponding action to be taken. Directions are listed relative to the site (In=Inbound, Out=Outbound).

a For this ruleset explain the purpose of each of the rules. Identify and discuss any rules that could be improved, and any additional rules that should be included.

b Tabulate the corresponding ruleset for the external packet router (that connecting the perimeter network to the outside world) and explain the purpose of each rule, or group of rules. Assume that the company's Web server runs on port 80, and the company's Ftp server runs on ports 21 and 20. State any additional assumptions that you make.

The two parts carry, respectively, 40% and 60% of the marks.

4 For this question you are asked to write some of the security policies that might be relevant for an online auction company called **Awk.com**. **Awk.com** allows users to buy and sell most goods online. Sellers can post details of their goods on **Awk.com**'s web pages, and interested buyers can bid for the goods.

For parts a) and b) below, discuss the policies that are desired, but do not discuss how those policies would be implemented (mechanisms). Do explain the rationale for your choices however and use examples where appropriate.

a For each of the following discuss what policies the users (buyers/sellers) of the system might want with respect to:

i) Security i.e. Confidentiality, Authentication, Integrity and Availability

ii) Privacy

iii) Fairness of auction

iv) Behaviour of other users

v) Payments

b For each of the following discuss what policies **Awk.com** might want from the system with respect to:

i) Security i.e. Confidentiality, Authentication, Integrity and Availability

ii) Identification of users

iii Monitoring behaviour of users

iv) Performance

v) Backups

The two parts carry, respectively, 50% and 50% of the marks.