UNIVERSITY OF LONDON
IMPERIAL COLLEGE OF SCIENCE, TECHNOLOGY AND MEDICINE

EXAMINATIONS 2002

MEng Honours Degree in Electrical Engineering Part IV
MSc in Computing for Industry
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

Friday 3 May 2002, 14:30
Duration: 120 minutes

*Answer THREE questions*

Paper contains 4 questions
Calculators not required

***Section A** (Use a separate answer book for this Section)*

1a Show that DES decryption can be done by applying the DES encryption algorithm to the ciphertext with the subkey schedule applied in reverse.

b Let $C = E_K(P)$ represent the DES encryption of plaintext block P. Show that if we complement the plaintext block P and the key K, then the ciphertext C is also complemented i.e. $\overline{C} = E_{\overline{K}}(\overline{P})$ where $\overline{x}$ denotes the bitwise complement of $x$.

c For ECB, CBC, CFB and OFB modes, comment on the effect of a single-bit error in the received ciphertext, i.e. how much of the "decrypted" plaintext will be affected?

d Using CBC Mode, Alice encrypts a sequence of plaintext blocks $P_1,...,P_n$ using key K and initialisation vector $IV$ and obtains ciphertext blocks $C_1,...,C_n$. She defines the last ciphertext block $C_n$ to be her Message Authentication Code (MAC).

Meanwhile using CFB Mode, Bob encrypts the same sequence of plaintext blocks $P_1,...,P_n$ using the same key K and the same initialisation vector $IV$ and obtains ciphertext blocks $D_1,...,D_n$. Bob encrypts the last ciphertext block to obtain his MAC i.e. his MAC is $E_K(D_n)$.

Show that Alice's MAC and Bob's MAC are the same.

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

© University of London 2002

2 The Mobile Network (TMN) adopts the following protocol for generating a session key between two mobile phones Alice and Bob (Trent is TMN's trusted server):

| | **From** | **Message** | **To** |
|---|---|---|---|
| Message 1:<br>$A \to T$: B, $E_T(\textit{random}_A)$ | Alice | Callee: Bob<br>**Only: Trent**<br>RandA: −66 | Trent |
| Message 2:<br>$T \to B$: A | Trent | Caller: Alice | Bob |
| Message 3:<br>$B \to T$: A, $E_T(\textit{key}_B)$ | Bob | Caller: Alice<br>**Only: Trent**<br>KeyB: −77 | Trent |
| Message 4:<br>$T \to A$: B, $\textit{random}_A$ **xor** $\textit{key}_B$ | Trent | Callee: Bob<br>Pad: −66 **xor** −77 | Alice |

Alice and Bob now communicate securely use the session key $\textit{key}_B$

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

b Show how an adversary Max (a suitably modified phone!) can successfully intercept a call from Alice to Bob and masquerade as Bob.

c Show how two adversaries Max and Nat can acquire the session key used by Alice and Bob and use it to eavesdrop on their call. *Hint*: Make a concurrent call with Trent.

d TMN modify Trent to reject new session keys that are duplicates of previously used session keys. Assuming RSA is used for encrypting messages sent to Trent, show how our two adversaries Max and Nat can still acquire the session key used by Alice and Bob. *Hint*: Use the properties of modular multiplication.

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

© University of London 2002

***Section B*** *(Use a separate answer book for this Section)*

3a Explain how a key can be securely split into 3 parts and give 2 different uses for this technique in key management.

b The following protocol is used by two entities A and B to exchange a message M and establish a session key $K_S$ using a Key Distribution Centre (KDC).

| | |
|---|---|
| A → KDC: | $A, B, N_A, E_A(K_S)$ |
| KDC → A: | $E_A(N_A), E_B(K_S)$ |
| A → B: | $A, E_{KS}(M), E_B(K_S)$ |

Where:

$E_A$ and $E_B$ denote encryption with the keys of A and B respectively, which the KDC knows,

$K_S$ denotes the shared session key between A and B and

$E_{KS}$ denotes encryption with the shared session key.

$N_A$ denotes a random number or nonce generated by A

i) Demonstrate how using a replay attack, a man in the middle known to the KDC, can decrypt the message M.

ii) Propose a modification to the protocol to counter this attack.

iii) This protocol is used by the head of Arkadia's secret services to arrange meeting points with her spies. Shortly after Arkadia's secret services have been infiltrated by a double agent, all its spies are captured. Explain how, without relying on the previous attack, this is possible and propose a modification to the protocol to counter this possibility.

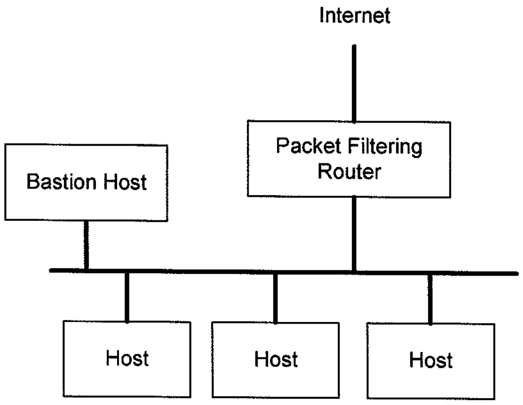
c A small company uses Pretty Good Privacy (PGP) to ensure the confidentiality and authenticity of internal communication. The company's policy states that all employees must be approved by both the Director of Human Resources (DRH) and the Chief Technology Officer (CTO). Explain how the PGP public ring and configuration can be setup for all employees and how messages would be kept confidential.

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

4a i) Describe how packet filtering is performed, for example by a packet filtering router.

ii) Some protocols, such as FTP, perform dynamic "call-back" connections from the server. Explain why this introduces a risk and what packet filtering rules can be used to reduce it.

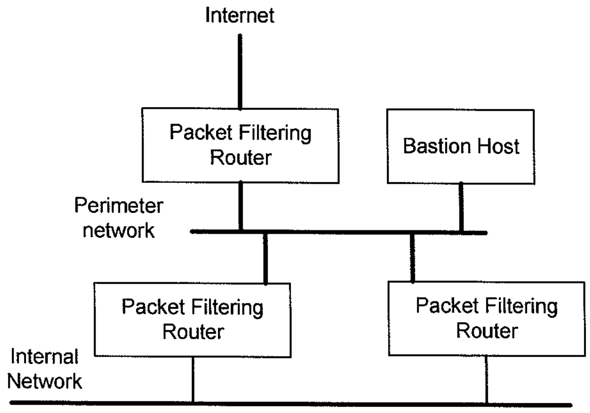
b A company called DoC uses the firewall set-up below. The bastion host has a *web server* (port 80), an *SMTP server* (port 25), an *FTP server* (port 21) as well as an *FTP proxy* (port 4421) and an *HTTP proxy* (port 4488). Company users can access outside information only through the proxies on the bastion host.



Give a possible set of rules for the packet filtering router in the format below, and explain what each rule does. Assume the direction of the traffic can be *in*, *out,* or *any* (both directions).

| Rule Number | Direction | Source Address | Source Port | Dest. Address | Dest. Port | TCP Flags | Action |
|---|---|---|---|---|---|---|---|

c A company uses the firewall set-up below.



i) Explain why a company would use the set-up above with two internal packet filtering routers (the ones connecting the internal network to the perimeter network).

ii) If the perimeter network is compromised and the internal packet filtering routers are poorly configured this set-up may lead to information leakage. Explain why this can occur and give the firewall rules necessary to avoid it.

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