UNIVERSITY OF LONDON
IMPERIAL COLLEGE OF SCIENCE, TECHNOLOGY AND MEDICINE

EXAMINATIONS 2003

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

Tuesday 6 May 2003, 10:00
Duration: 120 minutes

Answer THREE questions

Paper contains 4 questions
Calculators not required

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

1 Consider and answer questions on the following scheme for authorised but anonymous identification of wireless mobile devices connecting to a wireless infrastructure (e.g. Imperial College). The scheme has a *registration protocol* where a mobile device (A) obtains an authorised-anonymous id (ID) from the wireless infrastructure's central authority (T). The mobile device needs to authenticate at this stage also. Once an anonymous ID is obtained the mobile device can send packets via any wireless infrastructure access point (B) using a *connection protocol.*

a Registration Protocol (H is a cryptographic hash function, e.g. SHA or MD5)

Step0:	A↔T:	Authenticate A to T
Step1	A:	Generate r0 and r1
Step2	A→T:	$c0 = E_T(r0) \times H(r1)$ plus authentication data
Step3	T:	Check A is an authorised device
Step4	T→A:	$c1 = D_T(c0)$
Step5	A:	ID = c1 with r0 removed
Step6	A:	Check ID

What is being returned in Step4? How is r0 removed from c1 in Step 5? What is the value of the ID? How is the ID checked in Step6? What makes ID anonymous? Suggest an authentication protocol for step0. Discuss what properties r0 and r1 should have. Why is r1 hashed in Step2?

b Connection Protocol

Step7	A→B:	$c0 = E_T(r1, ID)$
Step8	B→T:	c0
Step9	T:	Check c0
Step10	T→B:	$c1 = E_{BT}(r1, ID)$
Step11	B:	Check c1
Step12	B→A:	Ack
Step13	A→B:	Packet1 = (Msg1 , H(Msg1, 1, r1))
Step14	B:	Check Packet1
	...	
Step15	A→B:	PacketK = (MsgK , H(MsgK, K, r1))
Step16	B:	Check PacketK
	...	

How does T check c0 in Step9? How does B check c1 in step 11? How does B check packets e.g. in Step16? Why is r1 sent in step 7 and hashed in the message sending steps e.g. 13 and 15?

(Continued)

c The scheme also has a protocol that allows a new anonymous ID to be generated from an existing ID without an authentication step. This protocol starts:

Re-Registration Protocol

Step1 A: Generate s0 and s1 and Session Key K_{AT}

Step2 A→T: $e0 = E_T(\, r1,\ ID,\ E_T(s0) \times H(s1),\ K_{AT}\,)$

Explain in detail how this re-registration protocol might proceed.

d One problem with the protocol is that a mobile device with an anonymous ID can access the wireless infrastructure forever. How can a revocation mechanism be added to the scheme?

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

2a Outline how a meet-in-the-middle attack works.

b Show that the DES key consisting of all 0-bits and the DES key consisting of all 1-bits are both weak keys. What are the other two weak keys?

c Consider the following shell command invoked on a UNIX system:

```
( date ; ps guax ) | md5_hash
```

where **`ps guax`** lists all information about all processes on the system. Comment on whether this command produces acceptable pseudorandom data?

d It is often said that breaking RSA is equivalent to factoring the modulus n. Show that it is not necessary to factor n in order to determine the private key d from the modulus n and the public key e.

e Show that RSA is not secure against a chosen ciphertext attack. In particular show how we can decrypt a given ciphertext X. Hint: first encrypt some plaintext P using the public key.

f A trusted server *Trent* produces session keys for users *Alice* and *Bob* as follows:

Alice user has two private keys d_{aa} and d_{at} which are derived from *Alice*'s original RSA private key d_a. d_{aa} is only known to Alice, d_{at} is only known to the *Trent*. d_a is destroyed after deriving the two private keys. *Alice*'s public key e_a is available to everyone.

Bob has similarly produced keys d_{bb}, d_{bt} and e_b.

When *Alice* wishes to communicate with *Bob*, she sends a message to *Trent* asking for a session key. *Trent* replies with a message to *Alice* that only *Alice* can read, and a message to *Bob* that only *Bob* can read.

For the above scheme work out how the two private keys are related, what messages are sent by *Trent*, and how *Alice* and *Bob* determine the session key from the message they receive.

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

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

3a Explain briefly how application-level gateways help towards maintaining the confidentiality and integrity of the network they protect. Why are application-level proxies harder to compromise than the applications or servers which they proxy?

b PONY is a music records production company which needs to secure its network. PONY wishes to allow its customers to:

- access its web site (on port 80), in order to browse their catalogue,
- download music files from an ftp server (port 21)
- play RealAudio files from a RealAudio server (on port 7070). RealAudio by default uses a system where a TCP connection initiated by the client is used for session control while the data is transferred using UDP. This provides better performance. However, it is possible to configure RealAudio to restrict UDP to use only ports in the range 6970-7170 or to use only the TCP connection (i.e. data transfer also occurs on the TCP connection).

PONY company users are not permitted to access external networks.

After investigating various options PONY decides to employ a *screened subnet* firewall architecture with two bastion hosts in the perimeter network (the network segment between the inner and the outer packet filtering routers). One bastion host (B1) is dedicated to the web server and the other (B2) is dedicated to the ftp server and the RealAudio server.

Assuming that the Real Audio server is used in its default configuration, give a possible set of rules for configuring the outer packet filtering router, which separates the perimeter network from the external networks. The rules should be given in the format below and you must briefly explain what each rule does. Assume the direction of the traffic can be *in*, *out*, or *any* (both directions) where *in* denotes incoming external traffic.

Denote the internal network of PONY as PONYnet and the perimeter network as PONYperim.

Rule Number	Protocol	Direction	Source Address	Source Port	Dest. Address	Dest. Port	TCP Flags	Action

c The employees of the PONY company described in question b) have convinced their management to allow them to access external web sites and to play RealAudio files stored on external servers. To permit this, PONY has installed a real audio proxy on B2 (port 4721) and an http proxy on B1 (port 4488).

i) Discuss how the RealAudio proxy should be configured with respect to connections to external servers and to connections with company users assuming that they are configured separately. You must discuss their security implications and choose the configuration which would be most appropriate.

ii) Specify the additional rules needed for the outer packet filtering router.

iii) Specify the rules needed on the internal packet filtering router to allow company users to access external web servers and play external RealAudio files.

The three parts a, b &c carry, respectively, 10%, 50%, 40% of the marks.

4a i) Explain what a certificate (as used in PGP and X.509) is and list 5 fields that you would expect to find in a certificate.

ii) Explain what is meant by a certification authority hierarchy in X.509 and what steps need to be taken to verify a certificate. Use a diagram to illustrate your answer.

iii) Briefly explain how *trust* is handled differently in PGP and X.509.

b i) In an X.509 certificate, the *name* of the person to whom the certificate is issued is written in hierarchical form. For example, John Smith, may have the name: `/C=UK/O=Imperial College/OU= Registry/CN=John Smith` where C=country, O=organization, OU= Organisational Unit, CN=Common Name. John A. Smith and John B. Smith are both working in Registry at Imperial College. Each goes to a different certification authority, shows his employment contract and is issued with a certificate. The two certificates may however have the same name. Briefly discuss how this could be avoided.

ii) PGP has no prescribed format for the *name* included in the certificate. Usually, an email address is used but email addresses change frequently. Discuss what problems this creates and suggest how to address them.

c In more general terms a certificate can be thought of as a signed statement (*assertion).* Thus, we could generalise a certification framework to issue assertions about whether a user has been successfully authenticated, whether a user has been permitted to access a resource (e.g., file), or assertions about the attributes of a user. For example, the British Medical Association could assert that a person is a qualified Medical Doctor, London Hope Hospital could assert that a person is employed with the rank of consultant, or a login server could assert that a user has been authenticated successfully.

i) List three main contributions that a framework which permits the generation, distribution and verification of assertions would bring to current Internet security systems and give examples for each.

ii) Which information would you expect to find in an assertion?

iii) How should attributes about whose values assertions are made be defined and identified?

iv) Who is permitted to issue assertions and how can an entity being presented with an assertion know that the issuer should be trusted to issue that assertion?

v) How should revocation be handled for authentication assertions, attribute assertions and authorisation (permission) assertions?

vi) Indicate the steps necessary to verify an assertion about the attributes of a person.

The three parts carry, respectively, 35%, 30%, 35% of the marks.