UNIVERSITY OF LONDON
IMPERIAL COLLEGE OF SCIENCE, TECHNOLOGY AND MEDICINE

EXAMINATIONS 2004

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
PhD
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

NETWORK SECURITY

Thursday 13 May 2004, 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 With the aid of a diagram outline the overall structure of AES *encryption.*

b What changes are needed to the structure of *decryption* in AES to make AES decryption have the same structure as AES encryption. Give justifications for the changes.

c i) In AES, why was encryption efficiency considered more important than decryption efficiency?

ii) Why might AES decryption be slower than AES encryption on 8-bit processors? How can AES decryption on 8-bit processors be speeded up?

iii) In the MixColumns transformation, coefficients have one of the small values: {00}, {01}, {02}, or {03}. The coefficient {00} implies no processing; for each of the other three coefficients, what computation is used?

iv) Why is the first and the last transformation of AES an AddRoundKey transformation?

d Using AES's polynomial arithmetic, work out the product (•) of the two polynomials $(x^7 + x^6 + 1)$ and $(x^2 + x)$ modulo $m(x) = x^8 + x^4 + x^3 + x + 1$, giving your answer both as a polynomial and as a hexadecimal value.

e Provide a definition for the **xtime** operation and then use **xtime** to form the product of the polynomials given in part d.

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

2a Consider the following protocol used by student Alice (A) to send courseworks to lecturer Bob (B).

Alice's long-term public-private key-pair is (KUA, KRA), while Bob's is (KUB, KRB). Alice creates a short-term public-private key-pair (KUX, KRX) and then sends the following messages to Bob:

Msg0: A→B: $ID_A, ID_B, E_{KRA}(KUX, ID_A, ID_{B,}\ T_{A0})$

Msg1: A→B: $ID_A, ID_B, E_{KUB}(1, E_{KRX}(CW1, T_{A1}))$

Msg2: A→B: $ID_A, ID_B, E_{KUB}(2, E_{KRX}(CW2, T_{A2}))$

...

T_{A0}, T_{A1}, T_{A2} are timestamps.

i) Explain how this protocol works, and comment on whether Bob can consider Alice as responsible for the courseworks received in messages 1, 2, etc.

ii) Show how another student, Max, can attack the protocol to obtain credit for Alice's coursework.

iii) Show how the short-term private key KRX can be used to prevent your attack in part (ii).

b Three cryptographers are having dinner around a table. The restaurant owner tells them that their dinner has been paid for, anonymously, either by one of them, or by the NSA (National Security Agency). One of the cryptographers is unhappy with having his meal paid for by the NSA, so they decide to find out whether it is the NSA who has paid, or one of them, without exposing which one of them it is. They devise the following protocol:

1. Each diner flips a coin and shows it to his left neighbour, i.e. each diner will see the outcome of two coin flips: his own and his right neighbour's.

2. Each diner then announces whether the outcomes of the two coin flips that they have seen are the "*Same*". If the diner is the payer, however, he lies (i.e. he says the opposite).

For this protocol show that:

i) an odd number of "*Same*" announcements means that the NSA is paying, while an even number means that one of the diners is paying.

ii) a non-payer cannot tell which of the other two is the payer, if the NSA is not paying.

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

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

3a Briefly describe the *screened subnet* firewall architecture. Indicate in which cases it would be used and what configuration you would typically expect the various components to have.

b The FTP protocol can operate in *passive* mode in which the control connection is established in the same way but the data connection is established differently. Instead of informing the server of the port allocated for the data connection the client notifies the server that it wishes to use passive mode. The server then dynamically allocates a port of its own in the application port range and informs the client of the port number. A TCP data connection is then opened by the client from its dynamically created data port to the server's data port.

i) Discuss the advantages and disadvantages of the passive mode of operation over the normal mode and identify the situations in which it should be used.

ii) A packet filtering router separates an Internal network (denoted *IntNet*) from the Outside network (denoted *OutNet*). Give the rules necessary to configure the packet filtering router to allow internal clients to access outside FTP servers in passive mode, and to provide access to outside clients to an internal FTP server (denoted *host1*) also in passive mode. The rules should be given in the format below and you should explain what each rule achieves. Assume the direction can be *in, out* or *any* (both directions) where *in* denotes incoming external traffic.

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

c RockingStone is a music magazine which allows its reporters to browse the web and use the ICQ protocol in order to interact with fans. ICQ is a conferencing protocol which allows users to send messages to each other through the *icq.com* server and to establish direct connections with each other to chat or to exchange files. ICQ clients communicate via UDP with the server (which runs on port 4000) and via TCP (on ports > 1024 only) with the server and with other clients. The UDP exchange with the server is established first and then used to exchange the port numbers for the TCP connections to the server, which are initiated by the clients. These connections are then used to exchange messages with other users and to establish direct client to client TCP connections. RockingStone's network is separated from the Outside network by a packet filtering router.

i) Give a configuration for the packet filtering router in the same format as for question b) above.

ii) Discuss the security implications of the use of ICQ and propose recommendations to improve the security of the network.

The three parts a, b and c carry, respectively, 15%, 40%, 45% of the marks.

4a X.509, PGP and SPKI/SDSI differ in their use and meaning of identity (i.e., the name identifying an entity). For each one of them, briefly discuss how they deal with identity and list their respective advantages and disadvantages.

Your answer will need to take into account considerations such as:

- Is the name unique? How is uniqueness guaranteed?
- Who assigns the name and on what basis?
- What meaning does the name have for the recipient of a certificate and does the identified entity correspond to the person the recipient thinks? (Consider a certificate issued for Michael Jackson – the software engineer, not the singer).

Give your answer to the questions above in bullet point form.

b i) Why do you think IBM's Trust Policy Language (TPL) is called a *Trust* Policy Language?

ii) Consider the following TPL policies expressed in English:

- "Users that have partner certificates signed by *self* are placed in the group partners."
- "A partner certificate signed by a member of the partners group is needed to be a member of the department group."

Explain how these can be implemented in SPKI/SDSI and give the specification of the certificates. Explain clearly the notation you have used.

c List the advantages and disadvantages of a cascaded delegation framework for access control such as the one used in SPKI/SDSI.

d A set of game players form a community which functions according to the following rules:

- Every player has a computer which can run both game servers and clients.
- *Advanced* players are allowed to start new games on any computers
- A player is recognised as *advanced* by all community players when he is recognised to be *advanced* by at least 3 *advanced* players or 10 *beginners.*
- A player can join the community as a *beginner* when introduced by any 3 existing community players.
- Beginners can join any games while they are in progress.

Briefly explain how you would implement authentication and access control for the system described above. List the advantages and disadvantages of your proposal and highlight any relationships to frameworks studied during the course.

The four parts carry, respectively, 30%, 25%, 20%, 25% of the marks.