A18866

THIS IS NOT AN OPEN-BOOK EXAMINATION
– CANDIDATES MAY NOT CONSULT ANY
REFERENCE MATERIAL DURING THE
SITTING

Calculators may be used in this examination
provided they are not capable of being used to
store alphabetical information other than
hexadecimal numbers.

THE UNIVERSITY OF BIRMINGHAM

Degree of MSc

Advanced Computer Science
Natural Computation
Internet Software Systems

Degree of MEng with Honours

Computer Science/Software Engineering. Final Examination

Degree of MSci with Honours

Mathematics and Computer Science. Final Examination

Undergraduate Occasional

Computer Science/Software Engineering
Mathematics

06 17417

Computer Security

Saturday 14th May 2005 0930 hrs – 1130 hrs

[Answer ALL Questions]
1. Alice wishes to download software from the Internet and install it on her computer.

   (a) What is a sandbox? How can sandboxes contribute to the security of downloading and running software from the Internet? [10%]

   (b) What are MD5 hashes? How can they contribute to the security of downloading and running software from the Internet? [10%]

   (c) What are digital signatures? How can they contribute to the security of downloading and running software from the Internet? [10%]

   Your answers should carefully distinguish the purpose of each of the three mechanisms under construction.

2. The TV show Big Sister invites its audience to vote each week on which of up to six contestants should be evicted from Big Sister House. The vote is carried out on the Internet.

   Big Sister aims to collect 20 million legitimate votes each week. It is known that many people would like to pervert the election, for commercial reasons.

   (a) Propose an appropriate system for Big Sister. Your proposal should describe the system. It should say what messages are sent between the user’s computer and the server; and describe what security mechanisms you recommended to be included. [10%]

   (b) List some attacks which you believe your system will resist. [10%]

   (c) List some attacks your system is vulnerable to. [10%]
3. A bank wishes to commission a system which will allow users connecting to the bank by the internet to biometrically authenticate themselves in order to instruct payments from their account.

A consultancy proposes the following scheme to the bank:

- Users wishing to register for the scheme will present themselves at their branch. The bank will take a scan of their fingerprint ("enrolment"), and will issue them with an off-the-shelf USB computer mouse equipped with a fingerprint scanner such as the one shown in the picture. It will also issue them with the bank’s client software.

- At home, when Alice wishes to authenticate, she plugs in the mouse and launches the client software. The software asks her to enter her account number and the payment instructions, and to place her finger on the mouse. It then encrypts the account number, the instruction, and the fingerprint scan with the public key of the bank and sends them to the bank.

- The bank compares the received fingerprint scan with the one presented at enrolment time for that account. Assume that this process of comparison is robust and reliable. If the received fingerprint and the enrolled fingerprint match, the bank accepts the instruction and carries it out. The scheme is illustrated in the figure.
(a) Explain how this scheme may be defeated, so that another user Bob could get the bank to accept his instructions about Alice’s account. [10%]

To improve the scheme, the consultancy proposes the following modifications.

- The mouse will be manufactured with a public/private key pair, in such a way that:
  - the private key is embedded inside the mouse and cannot be extracted; all records of it are destroyed at the time of manufacture.
  - the mouse can sign messages it emits with its private key.
- At authentication time, the bank sends a nonce to Alice’s mouse. The mouse pairs the fingerprint scan and the nonce and signs them. The client software pairs this signed message with the account number and the payment instruction and encrypts them with the bank’s public key and sends that encrypted message to the bank.
- The bank checks the signed message, and checks the fingerprint scan. It accepts the instruction if these checks succeed.

The improved scheme is illustrated below:

(b) Will this scheme work? Explain your answer. [10%]
4. Write at most one page about ONE of the following ((a) OR (b) OR (c)).

(a) What is the purpose of Shor’s algorithm for quantum computers? What is its significance for the field of computer security?

(b) “Linux is more secure than Windows”. Fact or fiction?

(c) What methods do music copyright holders have at their disposal to prevent unauthorised distribution of their music? Will any of these succeed in the long run?

[20%]