Calculator may be used in this examination but must not be used to store text. Calculators with the ability to store text should have their memories deleted prior to the examination.

UNIVERSITY OF BIRMINGHAM

School of Computer Science

Final Year – Degree of MEng with Honours
Computer Science/Software Engineering

Final Year – Joint Degree of MSci
Mathematics and Computer Science

Degree of MSc
Advanced Computer Science
Computer Security
Intelligent Systems Engineering
Internet Software Systems
Natural Computation

Undergraduate Occasional
Computer Science/Software Engineering
Electronic and Electrical Engineering

06 17417

Computer Security

Summer Examinations 2008
Time Allowed: 1 ½ hours

[Answer THREE out of Four Question]

[Marks indicated on this paper add up to 102%. The final mark will be capped at 100%.]
[Answer 3 out of 4 questions]

1. [Authentication]

A bank customer uses internet banking to make payments.

(a) Explain the mechanisms used to correctly authenticate:
   (i) the customer to the bank. [9%]
   (ii) the bank to the customer. [9%]

(b) Could a network intermediary (such as the customer's internet service provider) obtain the customer's authentication credentials during the login? Explain your answers. [8%]

(c) Could malware on the customer's computer obtain the customer's authentication credentials during the login? Explain your answers. [8%]

2. [Key agreement]

(a) Explain the terms confidentiality and integrity. [11%]

Alice and Bob each have a public/private key pair (PK_A, SK_A) and (PK_B, SK_B). You can assume that Alice knows Bob's public key and Bob knows Alice's public key. We use the notation Enc_K(m) for the encryption of m by the key K, Sign_K(m) for the signature of m with the key K, and H(m) for the secure hash of m. Alice wants to send some large files to Bob over a public network, in such a way as to guarantee confidentiality and integrity.

(b) Suppose that, for each file f, Alice sends to Bob the message: Enc_{PK_B}(f, Sign_{SK_A}(H(f))). Briefly explain whether this guarantees confidentiality and integrity. Is it efficient for use on a mobile device with low computational power? [6%, 5%]

(c) Suppose instead that Alice and Bob want to use a symmetric session key K_{AB} to encrypt the files. They first need to agree the session key. Suppose that the protocol stipulates that Bob chooses the key K_{AB} and sends to Alice the message Enc_{PK_A}(K_{AB}). Then, for each file f, Alice sends to Bob the message Enc_{K_{AB}}(f). Does this protocol guarantee confidentiality and integrity? Explain your answer. [12%]

-2- Turn over
The following protocol, described in lectures, is designed to enable an appropriately equipped computer to provide unforgeable guarantees about the application software it is running. The protocol relies on the computer hardware having a public/private key pair, \( PK_H \) and \( SK_H \), and firmware to run the protocol. (In trusted computing, the hardware keys are called the endorsement key, and the device that stores them is called the TPM.)

**Attestation protocol**
- When an application \( A \) is started, it first generates a new public/private key pair \( PK_A \) and \( SK_A \), called the *attestation identity key* (AIK). The application requests the hardware to certify its public key. The certificate \( C_A = \text{Sign}_{SK_H}(PK_A, #A) \) returned by the hardware includes a hash \( #A \) of the executable \( A \).
- When the application wants to attest its validity to a remote server, it sends the certificate \((PK_H, C_A)\) to the server. The server checks:
  - The signatures are valid, and \( PK_H \) has not been revoked.
  - The application hash embedded in \( C_A \) is on the server's list of applications it trusts.
- The application now authenticates itself by proving knowledge of \( SK_A \). For example, the application and the server can run a key exchange to generate a session key.

(a) Suppose a television broadcasting company wants to implement a "view again" service on its website which allows users to play video content, but prevents them from recording it or copying it. Can this protocol help them? Explain your answer. [11%]

(b) Suppose Microsoft wants to write a new generation of web browser, called “Internet Explorer Ultimate”, which is immune from attacks from viruses and buffer overflows. Can this protocol help them? Explain your answer. [11%]

(c) This protocol (which is not part of the Trusted Computing Group specification) has been criticised because it could compromise the privacy of users. Explain why this is so. Briefly explain how protocols which have been adopted by the Trusted Computing Group have addressed this privacy concern. [12%]
4. [Secure hash functions]

(a) What is a secure hash function? [11%]

(b) SHA1 is a 160-bit (or 20-byte) secure hash function. Assume that it is perfectly secure. What is the probability that, if I take a random message M and compute its hash value, I will get the result

2e ae 70 47 5c 2d 90 ce 07 d0 84 53 ce 27 bc a8 fb 35 3d f1

(c) A software company uses the following method to distribute software to its clients.

- it puts the software on an insecure web server
- the client downloads the software and computes an SHA1 hash of the downloaded file. She then telephones the software company, and reads out the first two bytes of the SHA1 20-byte hash (that would be 2e ae in the example above). Again, we assume that SHA1 is perfectly secure.
- If the bytes read out agree with the company's record of the hash value, the client accepts the software as securely transmitted.

Estimate the difficulty an attacker would have to create malware which, when downloaded in this way, would result in a hash value in which the first two bytes are correct. Since SHA1 is considered secure, the attacker can only use brute force. Your answer should be an estimate of the computation time required by the attacker. You can make any reasonable assumptions about the computation power of the attacker and the time to compute the hash of a file, but you should state those assumptions. [12%]