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 alphabetic 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

06 17417
Computer Security

Tuesday 9th May 2006  0930 hrs – 1100 hrs

[Answer any THREE Questions]
1. Hash functions
   (a) What are the properties of a secure hash function? [11%]

   (b) A company wishes to use a 128-bit secure hash function \( h \) so that clients who
download its software can then telephone the company to verify the hash of the
downloaded file. The company is concerned to find that collisions have recently
been discovered for \( h \), although no one has succeeded in reversing \( h \) for a
particular hash value. Advise them on the security of the proposed scheme. [11%]

   (c) Another company needs a hash function which returns a variable number of bits
(instead of 128 bits, as in the case of MD5, for example), with the requirement
that the more bits they obtain, the more secure the hash is. One of their
programmers proposes the following function:

   \[
   \text{INPUT: } M = \text{message to be hashed; } n = \text{length of hash required}
   \]

   \[
   \text{result} = "";
   \]

   while (result.length()<n)
   \[
   \text{result += MD5(result+MD5(M))}
   \]

   return result truncated to n bits

   Advise the company on whether this will suit their requirement. [11%]

2. Malware
   (a) Alice, Bob, Carol and Dave run Windows on their broadband networked
computers. Alice has a firewall (F), a virus detector (V), and regularly downloads
updates and patches to her software (U). Bob has F and V but not U; Carol has
V,U but not F, and Dave has F,U but not V. Explain an attack
   (i) on Bob which wouldn't work so easily on Alice
   (ii) on Carol which wouldn't work so easily on Alice
   (iii) on Dave which wouldn't work so easily on Alice
   (iv) on Alice

   [11%]

   (b) Present the three most convincing arguments you know of supporting the view
that current versions of GNU/Linux are more secure than current versions of
Windows. Are these arguments valid? [11%]

   (c) "Trusted computing will mean an end to viruses and worms." Explain the meaning
of this claim. Discuss its validity. [11%]
3. Key certificates

(a) What is a certificate authority? Explain a scenario in which they are useful. [9%]

(b) What is the web of trust model in PGP? [8%]

(c) Alice receives an email, apparently signed using a PGP private key by Bob. She does not know Bob's public key, but she knows and has signed the public keys of Carol and Dave. Dave has signed the keys of Alice, Bob and Eve. Eve has signed Carol's and Dave's keys. Alice has "complete trust" in Dave, and "part trust" in Carol and Eve. Should Alice accept the signature on Bob's email? Explain your answer, specifying any assumptions you make about PGP. [8%]

(d) Sally has gone to the police with an email she says is from Richard, in which he threatens to kill her. Richard denies writing the email, even though it is signed with his PGP key, and plenty of Richard's friends have digitally signed Richard's key certificate confirming that it is indeed his PGP key. The police consult you in order to find out whether it can be proved beyond reasonable doubt that Richard wrote the email. Advise them. [8%]
4. Fair exchange protocols

(a) Alice and Bob are on opposite sides of the world. They have agreed that she will send Bob a digital photograph of her performing in "The Fairy Queen" when she was eight years old, provided he sends her digital recording of him playing Bach's Prelude in C major. Each party wants to ensure that the other one keeps his or her side of the bargain. Offer them advice on how to proceed which is appropriate to the situation described. You should state any reasonable assumptions you make about the scenario.

Note: The Alice and Bob of this question are different from the Alice and Bob in other questions.

(b) Carol wants to sign a message M and send it to Dave, but she wants to obtain a receipt from him. Using the ideas of optimistic fair exchange, they proceed as follows. Assume that Carol has registered with a trusted third party which is capable of converting Carol's signature on a promise of any text T to Carol's signature on the text T itself. First, Carol sends a signed promise of M to Dave. Next, he sends her the receipt for M. Then, she sends him the signed text M.

1. Carol \( \xrightarrow{\text{sign promise } M, \text{ Carol}} \) Dave
2. Dave \( \xrightarrow{\text{sign receipt } M, \text{ Dave}} \) Carol
3. Carol \( \xrightarrow{\text{sign } M, \text{ Carol}} \) Dave

If Dave does not receive message 3, he can present messages 1 and 2 to the trusted third party, which will convert message 1 into Carol's signature on M and send it to Dave, and send message 2 to Carol.

The purpose of this protocol is to guarantee fair exchange.

(i) What is fair exchange? [6%]

(ii) Does the protocol guarantee fair exchange? Explain your answer. [8%]

(iii) Does this protocol guarantee timeliness for each participant? [8%]

Note: The Carol and Dave of this question are different from the Carol and Dave in other questions.
5. Electronic voting

(a) Explain the meaning of the properties eligibility, privacy, and fairness in the context of electronic voting protocols. [12%]

(b) Explain why blind signatures are useful in electronic voting protocols. [9%]

(c) Agents A0, A2, ..., A(k-1) want to elect a leader. Assume that A0,...,A(k-1) is the set of eligible voters, and that (for each i) Ai and A(i+1) know each other's public key reliably. In this question, the operations + and - on indices are interpreted modulo k. To cast her vote, Ai does the following:

(i) She invents a nonce ni, signs it, encrypts it with A(i+1)'s public key, and sends it to A(i+1).

(ii) She decrypts and verifies the signature on the nonce n(i-1) she receives from A(i-1), and sets pi to be the bitwise XOR of n(i-1) and ni.

(iii) She then puts the pair (pi,vi) on an anonymous bulletin board, where vi is her vote.

Assume that the bulletin board can be read and written by anybody, but no one can remove messages from it. Any agent can verify the votes and compute the winner. To do this he checks that k pairs have been written to the bulletin board, and that p1 XOR p2 XOR p3 XOR ... XOR p(k-1) = 0, and then computes the winner from v1, v2, ..., v(k-1). Which of the three properties mentioned above hold for this system? Explain your answer, clarifying any reasonable additional assumptions you need to make. [12%]