Two Hours

UNIVERSITY OF MANCHESTER
SCHOOL OF COMPUTER SCIENCE

M.Sc. in Advanced Computer Science

Computer Security

Wednesday 23rd January 2008
Time: 09:45 - 11:45

Please answer any THREE Questions from the FIVE questions provided

This is a CLOSED book examination

The use of electronic calculators is NOT permitted.
1. Alice works for ABC Ltd. She regularly works from home, and needs to transfer data between her home computer and her boss, Bob’s, computer (Bob’s computer is connected to the corporate network of ABC Ltd - please refer to the Figure). Alice’s home computer and the ABC’s corporate network are connected via the Internet. The data to be transferred is largely confidential information and needs confidentiality and integrity protection. Alice has been advised to use Diffie-Hellman key exchange protocol to derive a shared key for the needed security protections. But Alice is concerned about the man-in-the-middle attack. Another suggestion is for Alice to choose IPSec software to provide the required security protection. Answer the following questions.

a) Explain what the man-in-the-middle attack is, and suggest one measure that can be used to counter this attack. (6 marks)

b) Name the IPSec component that can be used to provide confidentiality and integrity security services, and explain how the two security services are provided by the chosen component. (8 marks)

c) Which mode would you suggest Alice to use, Tunnel mode or Transport mode? Justify your suggestion by outlining pros and cons of each mode. (6 marks)
2. Authentication, confidentiality, and integrity are three characteristics of secure communication. A networked system may be subject to threats to these characteristics by attackers who exploit vulnerabilities in the networked system. In order to prevent attacks we implement controls or security services.

Suppose that $KU_A$ and $KR_A$ are the public and private keys of a party $A$ respectively, that $KU_B$ and $KR_B$ are those of a party $B$, and that each of $A$ and $B$ can use any cryptosystems.

a) If $A$ wants to send a very long message to $B$, suggest an encryption method by which only $B$ can decrypt the message and the encryption/decryption processes are the most efficient. (6 marks)

b) Can $A$ encrypt a message so that anyone receiving the message will be assured that the message is indeed sent from $A$ (i.e. authenticity protection)? If yes, give your method; and if not, explain why not. (6 marks)

c) Prior to communication, parties $A$ and $B$ must have each other’s digital certificates. Explain what a digital certificate is, what security assurance it provides, and what verifications the recipient of the certificate should perform upon its receipt. (8 marks)

3. Cryptosystems can be classified into symmetrical (conventional) and asymmetrical (public-key) ones. For example, DES (Data Encryption Standard) and AES (Advanced Encryption Standard) are symmetrical cryptosystems whereas RSA is an asymmetrical cryptosystem.

a) State one advantage and one disadvantage of symmetrical cryptosystems over asymmetrical cryptosystems. (4 marks)

b) Give the key size and plaintext block size of DES, and give the key size(s) and plaintext block size of RSA. (6 marks)

c) What is the main concern for symmetrical key distribution and what is the main concern for public key distribution? Design a protocol for symmetrical key distribution without any assistance of a public-key cryptosystem. (10 marks)
4. In a Computer Science School, there is an administrator (A), three lecturers (L1, L2 and L3) and the Head of School (H). Three documents concerning the School are StaffSalary.doc, Timetable.doc and Marks.doc.

H has permission to read all of the documents and also has write access to StaffSalary.doc. The administrator, A, has read and write access to Timetable.doc and read access to StaffSalary.doc. The lecturers each have read access to Timetable.doc and read and write access to Marks.doc.

a) List the subjects, objects and operations, which will be used in the access control table. (5 marks)

b) Draw an Access Control List (ACL) table to express the access control policy as detailed above. (5 marks)

c) Contrast the following two types of access control mechanisms, Access Control List and Capability, in terms of (i) ease of making an authorisation decision during execution; (ii) ease of adding access for a new subject; (iii) ease of deleting access by a subject; and (iv) ease of creating a new object to which all subjects by default have access to. Justify your answers to the questions. (10 marks)

5. Upon a risk analysis on a company's site network, some threats are identified. These include threats from malicious code (i.e. virus, worms and Trojan horse) and threats from denial of service (DoS) attacks. To address these threats, an administrator in the company, Bob, has suggested using a firewall to control the access of the site network from the Internet.

a) Contrast the three types of malicious code, virus, worms and Trojan horse. (6 marks)

b) There are three types of firewalls to choose from: packet filtering firewalls, stateful packet inspection firewalls, and application gateways. Describe the working mechanisms of the three types of firewalls. (6 marks)

c) Do you think the use of firewalls is an effective countermeasure to these threats? You should justify your answer. (8 marks)

END OF EXAMINATION