Two Hours

UNIVERSITY OF MANCHESTER
SCHOOL OF COMPUTER SCIENCE

M.Sc. in Advanced Computer Science

Computer Security

Wednesday 21st January 2009

Time: 14:00 – 16:00

Please answer any THREE Questions from the FIVE questions provided

The use of electronic calculators is NOT permitted.
1. IPSec is a collection of mechanisms and protocols that provide key management, authentication, confidentiality, message integrity, and replay detection at the IP (Internet Protocol) layer. Answer the following questions.

   a) Explain what a Security Association (SA) is, and, with the help of a diagram, describe how an SA is established between two routers at run-time. (8 marks)

   b) Contrast tunnel and transport modes of working, and use diagrams to illustrate the scope of the protection in each mode. (6 marks)

   c) The Encapsulating Security Payload (ESP) protocol, one of the two IPSec traffic security protocols, provides confidentiality and integrity protections, and replay detection, to IP packets. Outline the outbound and inbound packet processing performed by the protocol. (6 marks)

2. 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. (3 marks)

   b) Assuming that a message $M$ of 1024-bits long is to be encrypted using the DES cryptosystem, and the key used is $K$. Which of the following modes of encryption, the ECB (Electronic Codebook) mode, or the CBC (Cipher Block Chaining) mode, should be used? Justify your answer. (5 marks)

   c) Given two large primes, $p$ and $q$, and a cryptographic hash function $H(x)$, explain how the RSA public and private keys are generated, and give the necessary equations. Also describe how a digital signature on $M$ is generated and how the signature is verified. (8 marks)

   d) Name three desirable properties that the hash function $H(x)$ must possess in order to guarantee the security of the signature scheme, and say why these properties are necessary. (4 marks)
3. Discretionary Access Control (DAC) is a type of access control used to govern the ability of subjects to access objects. You have been asked to design an access control system for a company, called AndrewBob Ltd, using DAC. The company has six staff. Two of them are senior managers, S={S1, S2}, and the rest are junior staff, J={J1, J2, J3, J4}. In addition, the company has one Chief Executive, E. The objects to be protected are three file directories, StaffSalary, PurchaseRecord and SaleRecord.

The Executive has permissions to read all of the directories and also has write access to StaffSalary. The two senior managers have read and write access to PurchaseRecord and SaleRecord and read access to StaffSalary. The junior staff each has read access to PurchaseRecord and read and write access to SaleRecord.

a) List the subjects, objects and operations, which will be used in the access control table. (3 marks)

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

c) Contrast the following three types of access control mechanisms, Access Control List, Capability, and Directory Access, 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. (12 marks)

4. A risk assessment on a company’s computer system has identified a number of threats. The threats include those from malicious code as well as those from unintentional software flaws. Answer the following questions.

a) Contrast these types of malicious code:
   i) Internet worms,
   ii) Trojan horses,
   iii) polymorphic viruses. (6 marks)

b) Name two detection measures against malicious code, and comment on their strengths and limitations. (4 marks)

c) Describe how a buffer overflow vulnerability (an unintentional implementation flaw in programming) could be exploited to cause more serious harm than program crash or core-dump. Your description should include clear explanation of what a buffer overflow is, and what serious damages it may cause to computer systems. (6 marks)

d) Name 4 principles for designing secure software systems. (4 marks)
5. A personal health monitor worn by a patient transmits collected health data through wireless communication to a software system \( P \) running on a trusted network host in the vicinity of the patient’s location, to produce the patient’s health monitoring reports. Another software system \( G \) operating on a networked computer or a mobile device such as PDA (Personal Digital Assistant) used by the patient’s GP (or doctor) can request the latest health monitoring report from the patient’s system \( P \) to allow the GP to check the report and take necessary actions when needed.

a) Identify two security threats to the communications between the two software systems \( P \) and \( G \) mentioned above, and explain the consequences that could be caused by each of the identified threats. (6 marks)

b) Design an efficient communication protocol to allow only system \( G \) to request and read the patient’s health monitoring reports from system \( P \) with the assurance of confidentiality, authenticity and integrity, where both symmetric and asymmetric (or public-key) cryptosystems including secure hash functions are available for the protocol design. State any assumptions you use for the design, and explain how the designed protocol operates. (10 marks)

c) Explain how the protocol produced in (b) can prevent each of the two security threats identified in (a). (4 marks)