COMP61421

Two hours

UNIVERSITY OF MANCHESTER
SCHOOL OF COMPUTER SCIENCE

Cyber Security

Date: Thursday 28th January 2016

Time: 09:45 - 11:45

Please answer any THREE Questions from the FOUR Questions provided

---

This is a CLOSED book examination

The use of electronic calculators is NOT permitted

[PTO]

1. Kerberos is an authentication protocol designed to allow nodes communicating over an insecure network to prove their identities in a secure manner. Answer the following questions

   a) Explain what a ticket is and what a ticket granting ticket is. (4 marks)

   b) Explain what security attacks Kerberos protocol messages are most vulnerable to and what protection measures the Kerberos protocol design has taken to thwart the attacks. (4 marks)

   c) Describe Kerberos v4 (version 4) protocol. (6 marks)

   d) Extend the Kerberos v4 protocol to allow a client *C* in a realm *A* to access a service in realm *B*. You should clearly describe your protocol extension and explain why your extended protocol could support this controlled access of services provided by another realm. (6 marks)

2. Wired Equivalent Privacy (WEP) is the original 802.11 security proposal, whereas WPA2 (Wireless Protected Access) is the full implementation of IEEE 802.11i proposal (which is the WLAN Security Standard). IEEE 802.11i uses AES (Advanced Encryption Standard) based CCM (Counter-Mode/Cipher-Block-Chaining Message-Authentication-Code) protocol to achieve message confidentiality and integrity. Answer the following questions.

   a) The following is the WEP authentication protocol used to authenticate a mobile user (*U*) when *U* makes a request to access a wireless access point (*AP*). The protocol contains four steps:

   Step_1. U->AP: I am U and would like to access your AP
   Step_2. AP->U: n
   Step_3. U->AP: n⊕RC4(WKey)
   Step_4. AP->U: grant (or reject)

   Where, '*A->B: M*' denotes *A* sends *B* a message, *M*, '*n*' is a random number and it serves as a challenge here, '⊕' is exclusive-or (i.e. *xor*) operator, *WKey* is a secret shared between *U* and *AP*, and *RC4* is a stream cipher.

   Explain if this protocol is secure. If yes, give your justifications. If not, fix the problem to make the protocol secure. (6 marks)

   b) Describe key features of the IEEE802.1x authentication standard, and outline the benefits of having these key features. (6 marks)

   c) Use a table to contrast the two security proposals (WEP and WAP2), in terms of key size, key management method, and security services that they each support. You should also indicate (where appropriate) how the security services are provided in these proposals. (8 marks)

3. An access control system should ensure that every access to a system and its resources be controlled and that all and only authorized accesses can take place. There are a number of ways (referred to as access control mechanisms or models) that can be used to implement an access control system. These are Discretionary Access Control (DAC), Mandatory Access Control (MAC) and Role-based Access Control (RBAC) models. DAC can further be classified into Access Control Matrix, Access Control List (ACL) and Capability, etc. Answer the following questions.

   a) Explain the main differences among the three access control models: DAC, MAC and RBAC. (6 marks)

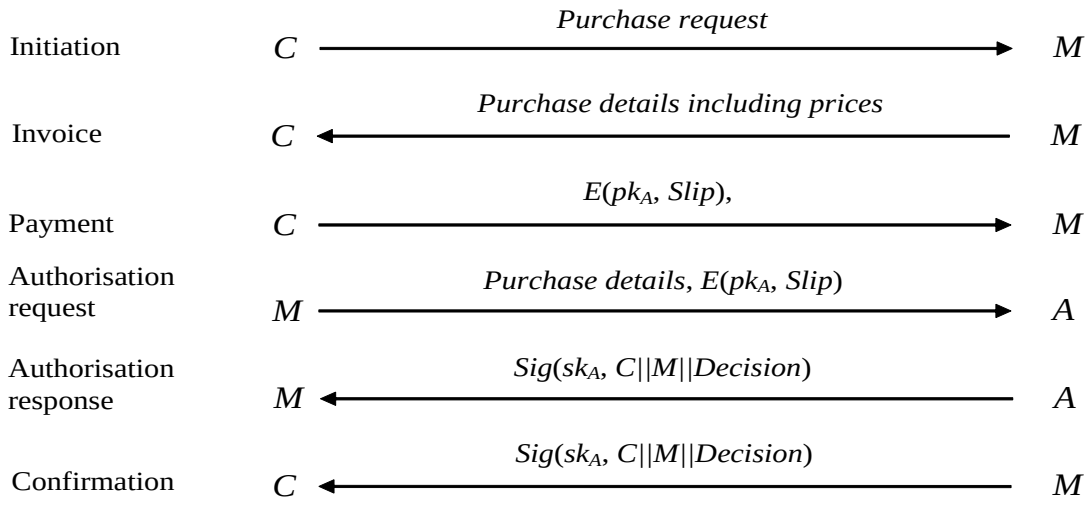
   b) You have been asked to design an access control system for a company, called ABC Ltd. The company has three sale staff. Two of them are senior staff, S={S1, S2}, and the third one is junior staff, J={J1}. The objects to be protected are four file directories, Dir-1, Dir-2, Dir-3 and Dir-4. The access requirement (i.e. policy) is: the two senior staff have read and write access to Dir-1 and Dir-2 and execute right to Dir-4. The junior staff has read access to Dir-1 and read and write access to Dir-3.

      Draw respective Access Control Matrix, ACL and Capability tables to illustrate how the above access control requirement are expressed using these models. (6 marks)

   c) Contrast the ACL and Capability models, 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. (8 marks)

[PTO]

4. The following gives a credit card based e-payment protocol:



Here, *C*, *M* and *A* represent a customer, a merchant and an acquirer (i.e. the merchant's bank), respectively. pk_A and sk_A are *A*'s public and private keys, *E*(*pk*, *x*) denotes the encryption of *x* with key *pk*, *Sig*(*sk*, *x*) denotes *x* signed with key *sk* (i.e. *Sig*(*sk*, *x*) = *x* || *E*(*sk*, *H*(*x*))), *H*(x) is cryptographic hash function, *x*||*y* is the concatenation of data items *x* and *y*, and *Slip* = {the description of goods to purchase, prices to pay, *C*'s credit card number}, *Decision* = *yes* or *no*.

a) Discuss in general terms two security threats to credit card based electronic payment. (4 marks)

b) Discuss whether or not the above protocol can prevent each of the two security threats described in (a) above. (6 marks)

c) Customer *C* wants to purchase electronic goods from merchant *M*, and wishes to have a fair trade in the sense that either *C* receives the goods and *M* receives the payment, or neither of them gets anything from the other. Extend the above protocol to achieve this fair trade, stating any assumptions you make, and justify how the extended protocol can achieve the fairness. (10 marks)

END OF EXAMINATION