Two hours

UNIVERSITY OF MANCHESTER
SCHOOL OF COMPUTER SCIENCE

Computer and Network Security

Date: Wednesday 23rd January 2013
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. SSL (Secure Socket Layer) is widely used to counter threats to Web security. Answer the following questions.
   (a) What protocols does SSL comprise? Outline the functions or services provided by each of the SSL protocols. (6 marks)
   (b) Describe in detail, how, in SSL, server and client authentications are achieved. (6 marks)
   (c) For each of these threats to Web security, brute-force attack, replay attack, man-in-the-middle attack and password sniffing, describe how each attack is performed and how each attack is countered by a particular feature of SSL. (8 marks)

2. The Kerberos authentication system supports client-server authentication in distributed environments. Answer the following questions.
   (a) Describe the Kerberos 4 protocol. (5 marks)
   (b) Describe the role of the authenticator used in the Kerberos protocol, and explain why an authenticator is NOT required when a client requests a ticket-granting ticket from an authentication server. (5 marks)
   (c) Outline three properties of the Kerberos solution to ensure the level of security in achieving client authentication. (6 marks)
   (d) Explain how to extend the Kerberos 4 protocol to allow a client $C$ in a realm $A$ to access a service server in another realm $B$. (4 marks)

[PTO]
3. You are asked to implement a new IEEE802.11 WLAN (Wireless Local Area Network) for a small business with 10 computer users. The company has already got a wired network facility and it is required that this WLAN should be integrated with the existing wired network facility.

   (a) Identify three security threats that are introduced as the result of this wireless network installation and integration, and outline security services that are required to address these threats.

   (6 marks)

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

   (6 marks)

   (c) Wired Equivalent Privacy (WEP) is the original 802.11 Security proposal, whereas WPA2 (Wireless Protected Access) is the full implementation of the IEEE 802.11i WLAN Security Standard. Outline four weaknesses in the WEP security designs, and explain how these weaknesses are rectified in WPA2.

   (8 marks)

4. Confidentiality, integrity and authentication 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.

Assuming that the two communicators, Alice and Bob, have never met before and they do not trust each other, and that each of Alice and Bob can use any of the cryptosystems and cryptographic hash functions. Now Alice wants to send a very large message to Bob. Answer the following questions (in your following protocol design, you should clearly indicate any assumptions used and the operations performed by each of the communicators).

   (a) Design a protocol by which Alice can send this message to Bob and only Bob can decrypt the message and the encryption/decryption processes are the most efficient.

   (6 marks)

   (b) Design a protocol by which Alice can send the message to anyone, and anyone receiving the message can be assured that the message is not a replay of a previously sent message and it is indeed from Alice.

   (6 marks)

   (c) Design a protocol by which Alice can send the message to Bob. The protocol design should satisfy the following requirements: message confidentiality, origin authentication, integrity and freshness are protected during transmission, the protocol is the most efficient in terms of communication cost and Bob is less vulnerable to DoS (Denial of Service) attacks. In your design, you should clearly justify how each stated design requirement is satisfied.

   (8 marks)

END OF EXAMINATION