Two hours

UNIVERSITY OF MANCHESTER
SCHOOL OF COMPUTER SCIENCE

Cryptography and Network Security

Date: Tuesday 1st June 2010
Time: 09.45 – 11.45

Please answer any THREE questions from the five provided.

This is a CLOSED book examination

The use of electronic calculators is NOT permitted.
1. Given the RSA, a well-known public-key cryptosystem, AES (Advanced Encryption Standard), a symmetric cryptosystem, and $H(x)$, a cryptographic hash function (e.g. SHA-1), answer the following questions.

a) Contrast the two different cryptosystems with regard to their respective strengths and limitations. (4 marks)

b) You are given two large primes, $p$ and $q$. Explain how the RSA public and private keys are generated, and give the equations if necessary. Also give the equation to encrypt a message $M$ (assuming $M$ is shorter than the product $p \times q$) to achieve confidentiality using the RSA cryptosystem, and the equation to decrypt the ciphertext to obtain the plaintext. (6 marks)

c) If you are asked to send a very large message to Bob, propose an efficient method by which confidentiality and authenticity of the message can be assured. State any assumptions if necessary. (6 marks)

d) Name two desirable properties that hash function $H(X)$ must possess in order to guarantee the security of the authenticity service, and say why these properties are necessary. (4 marks)

2. Alice is going to send a signed email to Bob. To allow Bob to verify her signature on the email, Alice will need to acquire a X.509 public-key certificate from a certification authority (CA) remotely via a communication network. Assuming that the key generation task is performed by Alice, answer the following questions.

a) What is a public-key certificate? Outline the mandatory fields of an X.509v3 certificate. (4 marks)

b) Design a certificate acquisition protocol by which Alice could submit her public key to a CA, and obtain an X.509 certificate for the public key from the CA. You should give a step-by-step description of the protocol, including any verification that is respectively performed by Alice and CA. (6 marks)

c) Identify two security threats in this certificate acquisition process, and explain how the protocol described in (b) addresses these threats. (4 marks)

d) Outline ALL the necessary verifications that ought to be performed by Bob when he receives the signed email from Alice in order to be assured of the authenticity of the email. (6 marks)
3. Kerberos is an important system that supports authentication in distributed environments.

a) Outline the main properties of the Kerberos system. (4 marks)

b) Describe the Kerberos 4 protocol, and identify two applications of this protocol. (6 marks)

c) 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. (4 marks)

d) Extend the Kerberos 4 protocol to allow a client $C$ in a realm $A$ to access a server in another realm $B$. Explain why $C$ needs to acquire a ticket from the ticket-granting server in $A$ and then another ticket from the ticket-granting server in $B$. (6 marks)

4. You are asked to implement a new IEEE802.11 WLAN (Wireless Local Area Network) for a company with 100 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) Which mode of IEEE802.11 WLAN operations is more appropriate for this WLAN and wired network integration? Justify your answer. (2 marks)

b) 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)

c) Describe key features of the IEEE 802.1x authentication standard, and outline the benefits of having these key features. (6 marks)

d) Wired Equivalent Privacy (WEP) is the original 802.11 Security proposal, whereas WAP2 (Wireless Protected Access) is the full implementation of IEEE 802.11i proposal (which is the WLAN Security Standard). Use a table to contrast these two security proposals in terms of key sizes, key management methods, and security services that they each support. You should also highlight how the security services are provided. (6 marks)
5. There are a number of approaches to securing Web traffics. Internet Protocol Security (i.e. IP security, or IPSec) and Secure Socket Layer (SSL) are two such approaches. Answer the following questions.

a) Contrast IPSec and SSL with respect to the security services that they each provide and their scope of applicability. (4 marks)

b) What protocols does SSL comprise? Outline the functions or services provided by each of the SSL protocols. (8 marks)

c) Describe two session-key establishment methods supported in SSL. In your description, you should also comment on how entity authentication and key freshness properties are ensured in these methods. (8 marks)