COMP38411

Two hours

UNIVERSITY OF MANCHESTER
SCHOOL OF COMPUTER SCIENCE

Cryptography and Network Security

Date: Friday 22nd January 2016

Time: 14:00 - 16:00

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. Alice and Bob have access to both symmetric and asymmetric (i.e. public-key) ciphers, such as DES (Data Encryption Standard), AES (Advanced Encryption Standard) and RSA (a public-key cipher). Alice is to send Bob a highly important and sensitive email message, M. Before the transmission, Alice encrypts M using a symmetric key, Ks, and encrypts Ks using Bob's RSA public key, PKb. This transmission can be expressed using the following communication protocol:

   A->B: E(M, Ks)||E(Ks, PKb),

   where 'A->B' denotes A sends a message to B. 'E(M, Ks)' denotes the encryption of M using Ks. 'E(Ks, PKb)' denotes the encryption of Ks using PKb. 'a||b' denotes concatenation of a and b.

   Answer the following questions.

   a) Draw an attack tree, where the goal of the attack is to read M. The tree should at least have TEN leaf nodes, each capturing a unique security attack, and the attacks will lead to unauthorised access of message M. The names of the attacks you identify and how the attacks are mounted should be clearly outlined.

   (10 marks)

   b) For each identified attack, explain a preventive countermeasure.

   (10 marks)

2. IPSec is a collection of mechanisms and protocols that provide key management, authentication, confidentiality, integrity and anti-replay protections at the IP (Internet Protocol) layer.

   a) Explain why a Security Association (SA) is needed, and with the help of a diagram, show how an SA is established between two parties.

   (8 marks)

   b) Describe the purposes of the Tunnel and Transport modes of IPSec, and use diagrams to illustrate the IPv4 packet format used by ESP (Encapsulating Security Payload) for each of the Tunnel and Transport modes. In your diagrams, you should clearly indicate the scope of security protections afforded by the ESP protocol.

   (7 marks)

   c) Use an example to explain why the two IPSec modes may need to be combined to protect a data flow, and describe how to combine the two modes in your example.

   (5 marks)

[PTO]

3. Cryptosystems are very important for network security.

   a) Describe two application scenarios, one showing that RSA is more suitable for the scenario than AES (Advanced Encryption Standard), and the other that AES is more suitable than RSA. Justify your answer.

   (4 marks)

   b) Describe how to apply RSA to generate and verify a digital signature on a message, M. Give proper mathematical equations, and discuss how the signature assures the integrity and origin authentication of the message.

   (8 marks)

   c) What is a digital certificate? Name two applications (each with a different security requirement) for which a digital certificate may be needed, and explain how the security requirements are met. Name three checks (or verifications) that ought to be performed by the recipient of a digital certificate.

   (8 marks)

4. Suppose the following is *Bob*'s entry in the password file of a Unix Server, *Alice*.

Bob: 14mo31bmRY0Yg: 12:31:Bob Smith: /home/bsmith:/bin/csh	Password file on server

   Answer the following questions.

   a) Describe the user authentication process used in Unix, i.e. the process by which the Server, *Alice,* authenticates the user, *Bob*. In your description, you should also outline the input required by the authentication method.

   (6 marks)

   b) Name three measures taken by the Unix authentication system to protect users' passwords.

   (6 marks)

   c) Is the Unix authentication system secure against a replay attack? If so, explain how the attack is prevented. If not, suggest an authentication method that is secure against the replay attack. In your suggestion, you should also highlight measures you need to take to ensure the security of your suggested method.

   (8 marks)

END OF EXAMINATION