Two hours

UNIVERSITY OF MANCHESTER
SCHOOL OF COMPUTER SCIENCE

Cryptography and Network Security

Date: Tuesday 20th January 2015
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. Alice and Bob have access to both symmetric and asymmetric (i.e. public-key) ciphers, such as AES (Advanced Encryption Standard, a symmetric block cipher), RSA (a public-key cipher) and SHA-256 (a cryptographic hash function). Alice is to send Bob a highly important and sensitive email message, M. Answer the following questions.

a) Outline the criteria for the design of a secure symmetric block cipher and explain how these criteria are satisfied in the design of AES. In answering this question, you should highlight the transformation steps used in an AES encryption process and how these transformation steps serve the design criteria you have outlined.

(8 marks)

b) Explain how the RSA public and private keys are generated, and give the necessary equations. Also give the equation to encrypt $M$ (assuming $M$ is a very short message) to achieve confidentiality using RSA, and the equation to decrypt the ciphertext to obtain the plaintext.

(6 marks)

c) In addition to the data confidentiality requirement, Bob also requires that, once the message is sent, Alice cannot falsely deny that she has actually sent the message. Here we assume that the message size is large. Design and clearly describe a method to satisfy the security requirements specified by Bob. In addition, the method should be efficient and resilient against DoS attacks on the recipient, i.e. Bob. Justify your design.

(6 marks)
2. Internet Protocol Security (IPSec) is a suite of protocols for securing IP (Internet Protocol) packets sent between two communication entities. IPSec operations can largely be classified into two stages: a pre data transfer stage and data transfer stage. Assuming that \( I \) (Initiator) and \( R \) (Responder) are two communication entities. Answer the following questions.

a) With the use of a diagram, explain what operations the two entities, \( I \) and \( R \), need to perform in the pre data transfer stage, and how these operations are carried out.

(6 marks)

b) The Diffie-Hellman (DH) algorithm is supported in IPSec. Describe the algorithm, and explain what vulnerability this algorithm has and how the vulnerability can be prevented in IPSec.

(8 marks)

c) Assume \( Cert_I \) is \( I \)'s X.509 certificate and \( Cert_R \) is \( R \)'s X.509 certificate and the certification hierarchy used is given in the diagram below. Describe what verifications the Initiator, \( I \), should perform to verify the validity of \( Cert_R \). Also, give the mandatory fields of an X.509 certificate.

(6 marks)
3. Assume that ‘read another user’s email (without authorisation)’ is the goal of the attack here. Identify any possible avenues (i.e. actions and possible methods) the attacker may take to successfully accomplish this attack.

   a) Draw a threat tree clearly highlighting the possible avenues you have identified. (10 marks)

   b) For each avenue identified, explain a preventive countermeasure. (10 marks)

4. Assume that A and B are two parties who wish to communicate over the Internet. Also assume that $K_{UA}$ and $K_{RA}$ are the public and private keys of a party A, respectively, $K_{UB}$ and $K_{RB}$ are those of a party B, and each of A and B can use any cryptosystems. Answer the following questions.

   a) There is a remark saying that: “Authentication is the most important security requirement for any distributed computer system”. Do you agree with this remark? Justify your answer. (4 marks)

   b) Now suppose that the two parties, A and B, wish to establish a secure session, and they use the following authentication protocol to authenticate each other. Here $ra$ and $rb$ are random numbers picked by A and B, respectively; $i \rightarrow j : M$ means that party $i$ sends a message $M$ to party $j$; $x||y$ means the concatenation of $x$ and $y$; $E_K()$ means encryption using $K$.

      $\text{Step}_1$: A $\rightarrow$ B: $E_{K_{RA}}(ra||B||A)$
      $\text{Step}_2$: B $\rightarrow$ A: $ra||E_{K_{RB}}(rb||A||B)$
      $\text{Step}_3$: A $\rightarrow$ B: $rb$

   Identify a security flaw in this protocol, and suggest a solution to fix the flaw. Clearly state any assumption(s) that you may use. (6 marks)

   c) Redesign an authentication protocol using a symmetric cryptosystem. The protocol should support mutual authentication and should be the most efficient, in terms of both computational and communication costs. You should also identify any potential threats or attacks on the symmetric key based authentication protocol and explain any countermeasures that you use to thwart such threats. (10 marks)

END OF EXAMINATION