Network Security

dr. Thomas B. Quillinan
dr. Bruno Crispo

August 21st, 2007

Instructions: Questions should be answered in English. Each Question carries equal marks (10 points). Attempt all 10 questions. The final grade will be the sum of the points divided by 10. Grades will be rounded to the nearest half point. For grading purposes, 5.5 will be rounded to a 6. You have 2 hours and 45 minutes to complete this exam. Please read each question carefully before attempting it.

1. (a) i. What is a Message Authentication Code (MAC)? *(1 points)*
   ii. What is non-repudiation? *(1 points)*
   iii. Why can a MAC not be used to achieve non-repudiation? *(2 points)*
   iv. If you cannot use a MAC, what would you use to enforce non-repudiation? Explain your answer. *(2 points)*

   (b) A programmer uses DES-CBC mode to provide integrity when encrypting messages with shared key K, as follows:

   $$\{Message :: OK\}_K$$

   Explain why a programmer may think that this provides integrity and suggest why such an implementation does not operate as expected. *(4 points)*

2. Consider the following security protocol:

   $$\begin{array}{lcl} A \rightarrow B & : & \{N_A, A\}_{K_B} \\ B \rightarrow A & : & \{N_A, N_B, B\}_{K_A} \\ A \rightarrow B & : & \{N_B\}_{K_B} \end{array}$$

   Where N_A and N_B are nonces.

   (a) What is a nonce? *(2 points)*
   (b) The exchanged nonces N_A and N_B can be used to generate a session key. How can this be achieved? *(4 points)*
   (c) Is this protocol vulnerable to an attack? Motivate your answer. *(4 points)*

3. ElGamal is a so called randomized public key encryption (RPK) algorithm, that is, encrypting the same plaintext message twice results in two different ciphertexts.

   (a) Is this property desirable or not? Motivate your answer. *(2 points)*
   (b) How can a classical public key algorithm be modified in such a way that it also becomes a RPK algorithm? *(4 points)*
   (c) What is entrophy and why is it important? *(4 points)*

4. (a) What is a covert channel? (*2 points*)
   (b) List two different types of covert channels. (*2 points*)
   (c) Give an example of one of these types of covert channels and explain how it can be abused. (*6 points*)

5. (a) Typically, does a VPN use asymmetric, symmetric or both types of cryptography? Explain your answer. (*4 points*)
   (b) Explain how the use of IPSec could *reduce* the possibility of *detecting* viruses. (*6 points*)

6. (a) For what security reasons are messages compressed after signing and not before signing in PGP? (*3 points*)
   (b) SSL allows for certificate chains.
      i. What problem do these chains solve? (*1 points*)
      ii. Explain how such certificate chains operate. (*2 points*)
   (c) Give two advantages and two disadvantages of using SSL instead of IPSec. (*4 points*)

7. (a) How are permissions granted to users in the Role Based Access Control (RBAC) model? (*4 points*)
   (b) Give an example of a separation of duties policy. Why are they used? (*2 points*)
   (c) How would you implement a separation of duties policy in KeyNote? Give an example of such a KeyNote policy. (*4 points*)

8. Certificate revocation is considered to be a hard problem in computer security. Several revocation mechanisms have been developed towards addressing this problem.
   (a) If there is a revocation mechanism, why do certificates need an expiration date? (*3 points*)
   (b) What are delta CRLs? Why are they used? (*3 points*)
   (c) Briefly outline the operation of the On-Line Revocation Scheme (OLRS). (*4 points*)

9. Access Control Lists (ACL) and Capabilities provide different appoaches to implementing the Access Control Matrix.
   (a) Using a simple example, explain the access control matrix. (*2 points*)
   (b) Compare and contrast ACLs and Capabilities. (*4 points*)
   (c) What is a reference monitor? (*2 points*)
   (d) What are the two main properties guaranteed by the Bell-LaPadula model? (*2 points*)

10. Kerberos is a distributed authentication system originally designed to secure campus facilities at MIT.
   (a) Outline (using a diagram) how Kerberos (version 4) works. (*4 points*)
   (b) What is "single sign-on", and how does Kerberos provide it? (*2 points*)
   (c) Realms were introduced in Kerberos version 5.
      i. What problem do they address? (*2 points*)
      ii. Briefly explain how they function. (*2 points*)