# Computers and Network Security

dr. Katerina Mitrokotsa

August 12th, 2008

**Instructions:** Questions should be answered in English. Each question carries equal marks (20%). You should answer all five questions. The final grade will be the sum of the points divided by 10. Points will be rounded to the nearest half point.

You have 2 hours and 45 minutes to complete this exam. Please read all questions carefully before attempting them.

1. (a) How would you encrypt passwords in a password file to avoid dictionary attacks. Motivate your answer. *(3 points)*

   (b) RSA is a public (asymmetric) key cryptographic scheme. On what computational infeasibility does the security of RSA depend? *(2 points)*

   (c) What is perfect forward secrecy and why is it important of secure communication? *(3 points)*

   (d) Why is Double DES not significantly more secure than single DES? *(4 points)*

   (e) Pseudo random number generators (PRNG) are commonly used in both software and hardware. What is a pseudo random number (rather than a true random number). What are the limitations of pseudorandom number generators? *(3 points)*

   (f) Describe two approaches that can be used in order to prevent denial of service attacks. *(5 points)*

2. (a) i. Outline the operation of Lamport's Hash password scheme. Use diagram(s) in your answer. *(5 points)*

   ii. Is Lamport's Hash vulnerable to an attack? If so write down the attack. *(5 points)*

   (b) Consider the following protocol:

$$\begin{array}{lcl} A \rightarrow B & : & A, \{g^a modp\}_{K_A} \\ B \rightarrow A & : & \{g^b modp\}_{K_B} \\ A \rightarrow B & : & \{message\}_{g^{ab} modp} \end{array}$$

   Where $a$ is a random value generated by $A$, $b$is a random value generated by $b$, $K_A$ is $A$'s public key and $K_B$ is $B$'s public key while $g$ and $p$ are random values shared between $A$ and $B$.

   i. Is this protocol vulnerable to replay attacks? If yes under which circumstances? Describe the attack. *(5 points)*

   ii. Describe a revised version of this protocol that address this attack. *(5 points)*

3. (a) Which of the following six authentication protocols are vulnerable to a *reflection attack*? If so, write down the attack. If not, explain why the reflection attack fails. $N_A$ and $N_B$ are nonces. *(10 points)*

$$\begin{array}{lcl} A \rightarrow B & : & A, N_A \\ B \rightarrow A & : & N_B, \{N_A\}_{K_{AB}} \\ A \rightarrow B & : & \{N_B\}_{K_{AB}} \end{array} \qquad \begin{array}{lcl} A \rightarrow B & : & A, \{N_A\}_{K_{AB}} \\ B \rightarrow A & : & N_B, \{N_A + 1\}_{K_{AB}} \\ A \rightarrow B & : & \{N_B\}_{K_{AB}} \end{array}$$

$$\begin{array}{lcl} A \rightarrow B & : & A, N_A \\ B \rightarrow A & : & N_B, \{N_A + 1\}_{K_{AB}} \\ A \rightarrow B & : & \{N_B\}_{K_{AB}} \end{array} \qquad \begin{array}{lcl} A \rightarrow B & : & A, \{N_A\}_{K_{AB}} \\ B \rightarrow A & : & \{N_B\}_{K_{AB}}, \{N_A + 1\}_{K_{AB}} \\ A \rightarrow B & : & \{N_B + 1\}_{K_{AB}} \end{array}$$

$$\begin{array}{lcl} A \rightarrow B & : & A, N_A \\ B \rightarrow A & : & N_B, \{N_A\}_{K_{AB}} \\ A \rightarrow B & : & \{N_B\}_{(K_{AB}+1)} \end{array} \qquad \begin{array}{lcl} A \rightarrow B & : & A, \{N_A\}_{K_{AB}} \\ B \rightarrow A & : & \{N_B, N_A + 1\}_{K_{AB}} \\ A \rightarrow B & : & \{N_B + 1\}_{K_{AB}} \end{array}$$

(b) Kerberos is a distributed authentication system originally designed to secure campus facilities at MIT.

i. Outline (using a diagram) how Kerberos (version 4) works. *(5 points)*

ii. Realms were extended in Kerberos version 5.

A. What problem do they address? *(2 points)*

B. Briefly explain how they function. *(3 points)*

4. (a) For what security reasons are messages compressed after signing and not before signing in PGP? *(3 points)*

(b) Which trust model is followed in PGP? Outline how this trust model works. *(4 points)*

(c) How is revocation performed in PGP? What is its disadvantage? *(2 points)*

(d) What are the main differences between the X.509 and the PGP trust models? *(6 points)*

(e) What are cross certificates and what are certificate chains? *(5 points)*

5. (a) i. Briefly explain how a packet filtering firewall operates. *(4 points)*

ii. Give one advantage of using stateful instead of stateless firewalls. *(2 points)*

(b) Give two advantages of using SSH instead of SSL/TLS. *(5 points)*

(c) i. What are the main differences between discretionary and mandatory access control? *(3 points)*

ii. Explain how protection rings can be used to implement an access control policy. *(6 points)*

(d) i. What is a covert channel? *(2 points)*

ii. List two different types of covert channels. *(2 points)*