2910326 Computer security

Examiner's report: Zone B

General remarks

Many candidates performed well in this examination. In fact the examiners feel that although each question contained some unseen and applied material, the paper did not fully test the more able candidates. In next year's examination paper, candidates should therefore expect a larger quantity of unseen and harder question parts.

Some candidates lost marks through writing out entire sections from the subject guide. Candidates needed to apply theory and show a good understanding of the subject in order to gain high marks.

The following are comments on each of the examination questions. Please refer to the Zone A Examiner's report for comments on the two coursework assignments.

Question 1 (Password systems and access control)

This question was quite well done. Most candidates realised that Walter's password policy was much too strict and that as a consequence staff would be unable to remember their passwords. Thus the staff may resort to writing their passwords down, recycling their passwords or using very obvious passwords, all of which would be detrimental to the security of the system.

A more suitable password policy should have included rules on password length (between 6 and 9 characters is an acceptable length), frequency of password changes (every 3–6 months is generally sufficient) and composition of passwords (for example that the password must be an alphanumeric mix). The policy may also include rules such as 'users should not base their passwords on dictionary words' or 'the user must change the default password'. Note that candidates were required to write a password policy for the users of the system. Therefore system rules such as limiting log-in attempts were not appropriate in answer to this question. Some candidates simply wrote out sections from the subject guide here without attempting to relate their answers to the question.

Most candidates were able to interpret the graph given in part b). However some gave access control matrices and others over-complicated the question assigning particular rights such as read and write to subjects. The question asked simply for an access control list. Thus S_1: O_2, O_3, O_4 etc. is sufficient. The graph shown is not a lattice since it contains several butterfly shapes. For example both S_1 and S_2 are connected to both O_2 and O_3. Therefore it is not clear whether S_1 or S_2 is dominant and there is no least upper bound.

Question 2 (Symmetric cryptosystems, Needham-Schroeder and Key Escrow)

Few candidates who chose to answer this question scored high marks. For part ai) commercially available symmetric key cryptosystems include Rindjael (AES), Triple-DES, Blowfish, IDEA and RC5. Many candidates named DES which is now considered insecure due to its small keysize and so would not be used commercially. Likewise Caesars cipher and the substitution cipher are not commercial cryptosystems.

Alice will need 11 different keys to communicate with 11 different people using a symmetric key cryptosystem since each pair of users will require a different key. In total there are 12 users and each must share a key with the 11 other users. Thus there are (12*11)/2 = 66 different keys in total.

Most candidates were able to describe the Needham-Schroeder protocol and how it can be used to exchange keys between Alice and another user of the symmetric key cryptosystem.

For part b) the majority of candidates knew the purpose of a key escrow protocol but had difficulty in describing the *3 of 3* protocol for part i) and implementing the *2 of 3* protocol for part iii). Only the most able candidates could set up the correct simultaneous equations ($4=5a + k \bmod 43$ and $12 = 39a + k \bmod 43$) and therefore find the value of k (in this question $k=18$)

Question 3 (Algorithm for Modular Exponentiation and RSA)

This question was answered by nearly all candidates and was a wise choice in most cases. The majority of candidates were able to give the pseudocode for computing $x^n \bmod m$. However, few were able to show that the complexity of the algorithm is $O(b(n^3))$. This is because the repeat loop in the algorithm is performed $b(n)$ times where $b(n)$ is the binary size of n. Each execution of the loop requires one or two multiplications and so is of order $O(b(n^2))$. Hence the entire algorithm has computational complexity of $b(n)*b(n^2)=O(b(n^3))$.

Nearly all candidates were able to describe the RSA public key cryptosystem as this was straightforward bookwork. Those who had correctly described the algorithm for modular exponentiation in part a) were generally able to use it to calculate $m=526^7 \bmod 703$ for part bii).

Question 4 (Discrete Logarithm Problem, Diffie-Hellman, El-Gamal, X509)

This question was chosen by approximately half the candidates and was generally answered very well. Most were able to state the discrete logarithm problem although many forgot to say that the modulus p must be a prime number. Most were also able to describe the Diffie-Hellman key exchange protocol and use the given keys to illustrate their answer. Diffie-Hellman is vulnerable to a man-in-the-middle attack because an attacker Charles can intercept the communications between Alice and Bob and replace them with his own, pretending to Alice that he is Bob and to Bob that he is Alice.

El Gamal is a public key cryptosystem based on the discrete logarithm problem and most candidates were able to correctly describe its key generation protocol. Some wasted time by also giving the encryption and decryption protocols.

Describing the X.509 protocol is straightforward bookwork and most candidates were able to answer part e) with little difficulty.

Question 5 (PGP)

This question was chosen by many candidates, probably because the first part was a standard bookwork question. Most candidates answered part a) well but answers to part b) were not so good.

Most candidates could describe the PGP protocol for exchanging an encrypted signed message. However, some just wrote sections straight from the subject guide demonstrating little understanding. Very few candidates answered the question in part b,ii) stating instead features such as e-mail compatibility and segmentation. The question asks which of the security features listed in part a) are provided by PGP. These are confidentiality, integrity, non-repudiation and authentication.

Part iii) was bookwork and was answered well by those candidates who had revised PGP. This was obviously not a good choice of question for candidates who do not have a good understanding of the PGP protocol.