

2010 Paper 4 Question 7

Introduction to Security

- (a) Briefly explain the following terms, and for each give **one** example of a technique that implements it:
- (i) secure commitment; [2 marks]
 - (ii) mandatory access control policy; [2 marks]
 - (iii) perfect secrecy; [2 marks]
 - (iv) message authentication code. [2 marks]
- (b) You have been hired by CustomWidgets Ltd to secure the web interface to a legacy system. This system is complex, its source code has been lost, and you have been unable to find a precise definition of allowable input values. You have been asked to write input validation procedures, that will identify values which are suspected to be malicious, and flag them for later manual inspection. For each of these input fields, explain **one** validation procedure you could perform, and justify why it is appropriate:
- (i) the name of a file in a particular directory on the server; [3 marks]
 - (ii) a parameter that you believe will be used on a command-line; [3 marks]
 - (iii) a string that will be loaded into memory and parsed. [3 marks]
- (c) For **one** of the validation procedures you gave in part (b), discuss how a sophisticated attacker could circumvent detection. [3 marks]