Monash University
Semester Two Examination Period
2003
School Of Information Management and Systems

TITLE OF PAPER: Information System Security (IMS3110)

EXAM DURATION: 2 hours

READING TIME: 10 minutes

THIS PAPER IS FOR STUDENTS STUDYING AT: (tick where applicable)

☐ Berwick  ☐ Clayton  ☐ Malaysia  ☐ Distributed Learning  ☐ Open Learning
☒ Caulfield  ☐ Gippsland  ☐ Peninsula  ☐ Enhancement Studies  ☐ Sth Africa
☐ Other (specify)

Candidates are reminded that they should have no material on their desks unless its use has been specifically permitted by the following instructions.

AUTHORISED MATERIALS

CALCULATORS ☐ YES  ☒ NO
OPEN BOOK ☐ YES  ☒ NO
SPECIFICALLY PERMITTED ITEMS ☐ YES  ☒ NO

MARK ALLOCATION:

PART A – Compulsory Question 50 marks
PART B – Short answer questions 40 marks (10 marks each)
PART C – Terminology 10 marks (2 marks each)
TOTAL 100 marks

WEIGHTING 60 %

Candidates must complete this section if required to answer in this paper

STUDENT ID __ __ __ __ __ __ __ __ DESK NUMBER __ __ __ __
SURNAME ...........................................................................SIGNATURE..............................................
OTHER NAMES (in full) .................................................................................................................................
There are numerous benefits to businesses when conducting business over the Internet. However since the Internet was only designed to offer ease of communication, security risks are a very real concern (Merkow & Breithaupt, 2000).

a) Describe the possible negative consequences to an organisation that suffers a major security breach to a core information system. 10 marks

b) To establish a secure information system, a security conscious organisation should adopt a security framework. Describe a security framework with which you are familiar, and discuss how it provides the base for information system security. 20 marks

c) OCTAVE is a risk based strategic assessment and planning technique, specifically designed for IS security. Describe how this technique can support the information system framework you described in b). (You may present this technique in diagrammatical form to support your answer – however this on its own will not be sufficient to gain full marks). 20 marks

PART B SHORT ANSWER 40 marks

Answer any FOUR from the following questions:

1. Provide at least five reasons why security threats and breaches to security systems have been increasing over the last 20 years. 10 marks

2. When a threat impacts on an information system, a well organised and integrated access control system should be in place to lessen the damage to the information system. In a clearly labelled diagrammatic representation, display the ‘control relational model’. 10 marks

3. To identify potential exposure areas or vulnerabilities in a system, Fisher applied a process called the “data control life cycle”. Describe this process. 10 marks

4. When developing a security policy, and to provide the basis for certification, a six phase development model has been promoted by the International Standard For Writing And Implementing Security Policies (ISO17799). Describe this development model and include a diagram showing how these phases link. 10 marks

5. Implementing a security system is often considered to be a “burden” on the current information systems. Describe the nature of this burden? 10 marks

6. According to a survey of IT managers conducted by Gartner Dataquest in 2000, more than 60 percent of businesses did not have a “basic” disaster recovery plan. In light of these findings, discuss the possible reasons why the majority of organisations do not have disaster recovery plans in place. 10 marks

7. Recently, a new virus, W32 Blaster Worm, compromised information systems of numerous Australian Universities and organisations, indiscriminately affecting many PC’s. Describe the procedures Monash University IT staff employed to mitigate against this breach in their information systems. 10 marks

8. Gartner (2003) state that, ‘Passwords and PINs remain the standard user authentication solutions, both on the Internet and for applications within a system. However, they are
considered to be quite vulnerable. Discuss the types of password management an organisation can adopt to reduce their vulnerability.


10. The term “Annual Loss Expectancy (ALE)” refers to a process used to support risk management. Describe what is meant by this term.

PART C DEFINITIONS

Explain the meaning of any FIVE of the following terms:

i Steganography
ii Trapdoors (backdoors)
iii Vulnerabilities
iv Virus
v Distributed Denial of Service (DDoS) Attack
vi Secure Sockets Layer (SSL)
vii Trojan Horse
viii Firewalls
ix Crash Kit
x Non-repudiation