Student Number							

Surname	Given Name/s

Examination Paper

SEMESTER: FIRST SEMESTER EXAMINATIONS 2010

UNIT: INB255 SECURITY - THEORY 1

DURATION OF EXAMINATION: **PERUSAL:** 10 MINUTES
WORKING: 2 HOURS

EXAMINATION MATERIAL SUPPLIED BY THE UNIVERSITY:

EXAMINATION BOOKLETS - FIVE (5) PER STUDENT

EXAMINATION MATERIAL SUPPLIED BY THE STUDENT:

NIL, EXCEPT FOR WRITING IMPLEMENTS

INSTRUCTIONS TO STUDENTS:

Students are prohibited from having mobile phones or any other device capable of communicating information (either verbal or written) *in their possession during the examination*

NOTES MAY BE MADE <u>ONLY</u> ON THE EXAMINATION PAPER DURING PERUSAL TIME

ALL FIVE (5) QUESTIONS ARE TO BE ATTEMPTED

ATTEMPT EACH QUESTION IN A SEPARATE EXAMINATION BOOKLET

ALL QUESTIONS ARE OF EQUAL VALUE

<u>THIS EXAMINATION PAPER MUST NOT BE REMOVED FROM THE EXAMINATION ROOM</u>

QUESTION 1 [12 Marks]

(a) Many phishing attacks begin with a spam email claiming to be from a legitimate organisation, such as a bank, asking users to follow a link in the email to a site which requests personal information. A recent study of the responses of bank customers to phishing emails found that only 0.000564% of bank customers actually click on the link in a phishing email and, of those customers who do click on the link, approximately 45% will divulge their personal credentials to the phishing site. Despite the very small response rate to these emails, phishing is regarded as a serious information security problem.

(i) The traditional information security goals or services are often represented by the acronym **CIA**. Give the name *and* a clear explanation of the security goal the phishing scenario relates to.

(2 Marks)

(ii) Clearly explain the difference between a **vulnerability** in an information system and a **threat**. To illustrate your answer, *in addition to your explanation*, give an example of each related to the bank phishing email scenario described above.

(3 Marks)

(iii) Given the very low response rate to a phishing email, explain why this is regarded as a serious information security problem.

(1 Mark)

(b) The information security standard **AS27001:2006** is the specification for information security management systems, and uses a Plan-Do-Check-Act process model for setting up and managing an ISMS. Briefly explain the purpose of the **Do** phase of the PDCA model, and the steps involved in this phase.

(3 Marks)

(c) Section 5.4 of **AS31000:2009** deals with Risk Assessment. This comprises the following three steps of the risk management process: *Risk identification*, *Risk analysis* and *Risk evaluation*.

(i) Explain the process involved in performing the *Risk Identification* step.

(1 Mark)

(ii) Explain how information from studies, such as the phishing email 'link clicking' statistics given above, can be used in the *Risk Analysis* step.

(1 Mark)

(iii) Information used in risk analysis may be either *quantitative* or *qualitative*. Explain the difference between quantitative and qualitative expressions for likelihood.

(1 Mark)

QUESTION 2 [12 Marks]

(a) The *one-time pad* is a binary additive stream cipher. This is the only known *provably secure* cipher. However, it is not widely used. Clearly explain the restrictions that limit the use of the one-time pad.

(2 Marks)

(b) Electronic Code Book (ECB) is a mode of operation defined for any **block** cipher. With the aid of a clearly labelled diagram, explain how *encryption* is performed in ECB mode.

(2 Marks)

(c) Hash functions are often used for providing security services related to integrity. Consider the case where Alice sends both a message, M, and the SHA-1 hash of the message, $H(M)$, to Bob. Bob can compute $H(M')$, the hash of the received message M', and compare it to the received hash, $H(M)$. If $H(M) = H'M')$, what assurance does Bob have about the received message M'?

(2 Marks)

(d) The Diffie-Hellman key exchange is to be used to establish a shared secret key between Alice and Bob. Alice and Bob have agreed to use the prime $p = 13$ and base value $g = 2$.

(i) Copy and complete the following table to show that

$$g^1 \bmod 13, g^2 \bmod 13, \ldots, g^{12} \bmod 13,$$

give all the values $\{1, 2, \ldots, 12\}$.

i	1	2	3	4	5	6	7	8	9	10	11	12
$g^i \bmod p$	2	4			6			9	5	10	7	1

(1 Mark)

(ii) If Alice chooses the random value $a = 4$, what value does Alice send to Bob?

(1 Mark)

(iii) If Alice then receives the value 4 from Bob, what is the value of the shared secret key?

(1 Mark)

(e) Clearly explain the major *advantage* asymmetric ciphers have over symmetric ciphers with respect to key distribution.

(2 Marks)

(f) Clearly explain why applications using symmetric ciphers can not provide non-repudiation.

(1 Mark)

QUESTION 3 [12 Marks]

(a) The Bell-La Padula (BLP) security model is a formal model of a computer security policy, which provides access control based on object classifications and subject clearances.

(i) Give an example of a security level heirarchy suitable for use in a BLP model.

(ii) Explain what is meant by *domination* with respect to your security level heirarchy.

(iii) Explain the purpose of the star (*) property of the BLP model, and briefly descibe the property.

(3 Marks)

(b) A large advertising company handles advertising campaigns for a number of different clients, including the two toy manufacturers *Trixie* and *Topsy*, and the two biscuit manufacturers *Crispy* and *Crumbles*. Information related to these four companies is contained in a total of ten different objects, as follows:

Trixie:	Object 1, Object 2, Object 3	*Crispy:*	Object 6, Object 7, Object 8
Topsy:	Object 4, Object 5	*Crumbles:*	Object 9, Object 10

A Brewer-Nash Chinese Wall security model has been implemented. The ith row of the access permission matrix N is shown below.

Object number	1	2	3	4	5	6	7	8	9	10
Subject i	f	t	f	f	f	f	f	f	f	f

Based on this information, which of the following access requests by Subject i would be granted? Justify your response by referring to the security properties of the model.

(i) Read only access to Object 5.

(ii) Simultaneous read access to Object 3 and write access to Object 6.

(3 Marks)

(c) During the Policy Enforcement Phase of access control implementation, *identification* and *authentication* of users is performed.

(i) Clearly explain why authentication is required.

(ii) Explain what is meant by the phrase *'single factor authentication'*.

(iii) Explain why monitoring of access should be performed during the Policy Enforcement Phase.

(3 Marks)

(d) Reusable passwords are commonly used to authenticate users. The passwords may be randomly generated or user selected. List three *disadvantages* associated with the use of user selected reusable passwords.

(3 Marks)

QUESTION 4 [12 Marks]

(a) In public key cryptography, when an attacker replaces a public key (say Alice's public key) with a different key whose private key is known to the attacker, this is known as *spoofing*.

(i) Explain how the spoofing problem can result in a failure of confidentiality when public key encryption is used.

(1 Mark)

(ii) Clearly explain how digital certificates can provide a solution to the spoofing problem.

(1 Mark)

(iii) When verifying a digital certificate, what assumptions must be made in order to trust the contents of the digital certificate?

(2 Marks)

(b) Hierachical and browser models are two widely used types of architecture for public key infrastructure (PKI). Explain two (2) major *disadvantages* of the *browser* model compared to the *heirarchical* model.

(2 Marks)

(c) Clause 14 of **AS27002:2006** deals with business continuity management. Describe three of the items recommended in **AS27002:2006** for consideration when developing and implementing business continuity plans.

(3 Marks)

(d) In a recent incident, a traveller accessed their airline's online flight check-in system using their personal booking number and flight number. When they entered this information the personal information of two other airline passengers was shown on the screen. The information included the other passengers' full names and contact telephone numbers, email addresses and their flight itineraries.

(i) Organizations in Australia must comply with relevant federal and state legislation. Which legislative Act is applicable in this situation? Explain your answer.

(2 Marks)

(ii) Explain how the information contained in the exposed records could be used by criminals to perform identity theft.

(1 Mark)

QUESTION 5 **[12 Marks]**

(a) A network communications protocol known as HTTP Authentication can be performed as either *Basic* or *Digest* Authentication.

(i) Clearly explain the major security problem associated with the use of *Basic Authentication* over an insecure channel.

(1 Mark)

(ii) When used over an insecure channel, *Digest authentication* does not have the same security problem. Explain the mechanism used in digest authentication to provide protection.

(2 Marks)

(b) TLS is a commonly used network communications protocol.

(i) For either the OSI or TCP/IP model, at which layer is this protocol performed?

(1 Mark)

(ii) When using the TLS Handshake protocol, the server sends the client a certificate. Clearly explain what the client uses the certificate for, and why this is required.

(2 Marks)

(c) A *firewall* is used to restrict access between a protected network and other sets of networks. Packet filters are often used in this role. Briefly describe:

(i) how a *simple packet filter* operates;

(ii) how a *stateful packet filter* operates;

(iii) a method of attack that will be detected by a stateful packet filter but not a simple packet filter.

(3 Marks)

(d) Intrusion detection systems (IDS) are automated systems that detect suspicious events. An IDS can be either *host-based* or *network-based.* Briefly describe the operation of a *host-based* IDS.

(1 Mark)

(e) Detection methods used by IDS are normally considered to be either *misuse-based* or *anomaly-based.*

(i) Briefly explain the operation of *misuse-based* detection methods.

(ii) Explain a major weakness of *misuse-based* IDS.

(2 Marks)

END OF PAPER