Office Use Only

Monash University

Semester One Examination Period 20XX

Faculty Of Information Technology
Sample Exam Paper

EXAM CODES: **FIT3031**

TITLE OF PAPER: **Information & Network Security**

EXAM DURATION: 3 hours writing time

READING TIME: 10 minutes

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

☐ Berwick	☐ Clayton	☑ Malaysia	☐ Off Campus Learning	☐ Open Learning
☑ Caulfield	☐ Gippsland	☐ Peninsula	☐ Enhancement Studies	☑ Sth Africa
☐ Pharmacy	☐ Other (specify)			

During an exam, you must not have in your possession, a book, notes, paper, electronic device/s, calculator, pencil case, mobile phone or other material/item which has not been authorised for the exam or specifically permitted as noted below. Any material or item on your desk, chair or person will be deemed to be in your possession. You are reminded that possession of unauthorised materials in an exam is a discipline offence under Monash Statute 4.1.

No examination papers are to be removed from the room.

AUTHORISED MATERIALS

CALCULATORS	☐ **YES**	☑ **NO**
OPEN BOOK	☐ **YES**	☑ **NO**
SPECIFICALLY PERMITTED ITEMS	☐ **YES**	☑ **NO**

INSTRUCTIONS

1. PART-B-There are **SEVEN** questions, please answer **ALL** of them.
2. PART-A-MCQs, T/F & SHORT-ANSWERS.
3. Write on one side of the paper only.
4. Total marks - 100. This exam contributes 60% to your result for this unit.

Answer the following questions:

1.

a. Explain any two examples of security violations that can be experienced in the transmission of information over the network. For each example given, name the type of security service that applies to such violations.

b. There are two major concerns with regards to **where** to implement the security mechanisms designed to combat security violations. Briefly explain these two concerns.

(8+5=13 marks)

Sample Solution:

a)

– **A** transmits a sensitive file to **B** that must be protected from disclosure. **C**, not authorized to read the file, monitors the transmission and captures the file during transmission. (data confidentiality) 3 marks

– **D** intercepts a message during transmission, changes the content and transmits to **F** as if it originated from **E.** (Integrity/ Authentication) 2 marks

– A message is sent from a customer to a stockbroker with instructions of transactions. Subsequently, the investments lose value and the customer denies sending the message (non-repudiation) 3marks

b)

– The physical placement of security mechanisms in the network is very important. This has to do with taking a decision about where on the network these mechanisms are needed and where on the network they will be best implemented to prevent attacks/security violations. 3marks

– The logical placement of the security mechanism is also important. This has to do with taking a decision about what layer on the TCP/IP architecture a security mechanism should be placed. 2marks

2.

a. Suppose Bob chooses n=35 as his RSA modulus and chooses e=7 as his public key exponent so that his public key (n, e) = (7, 35). Calculate his private key exponent d.

b. In asymmetric encryption, a sender can deny his public key and a hacker can create a false key to impersonate someone. Explain how it can be ensured that the public key belongs to the entity that it claims it belongs to.

c. Explain why sending **m** + **MD5 (m),** which denotes message **m** concatenated with its digest, does not guarantee message integrity for **m**. What can you do make it secure?

(7+7+6=20 marks)

Solution:

a) n=5x7=35,

So, p=5 and q =7

Hence, ø(N)= (5-1)(7-1)=24.

The private key exponent, d should satisfy: de mod ø(N)=1

dx7mod24=1

dx7/24 should give a remainder of 1, thus d=7.

Private key = (7, 35). 7 marks

b) A trusted body is required to certify public key. The trusted body is the Certification Authority (CA) which certifies the public key of any user.

- user A generates his/her public key and submits to CA for certification
- CA determines identity and background of A
- CA appends time stamp to public key, generates hash code and encrypts with CA's private key.
  - This constitutes the signature of CA
  - hash code ensure that public key is unaltered
- Signed public key of A is now available for presentation
- Any one equipped with CA's public key can authenticate A's authenticity

7 marks

c) An intruder may intercept m, change its content and compute MD5 on the new content. The receiver will not be able to detect that such modification has happened. However, if the digest is computed from the message m and a secret key k (shared between sender and receiver), no third party without the key k would be able to re-compute a valid digest on changed message. The sender will send the following**: m + MD5(m, k)**

6 marks

3.

a. What hash function is used in PGP and what is the length of the message digest? What is the use of detached signature supported by PGP?

b. Why does PGP generate a signature before applying compression?

(6+6 = 12 marks)

Sample Solution:

(a) SHA-1 160 bit message length. 1 mark

A detached signature is useful in several contexts. A user may wish to maintain a separate signature log of all messages sent or received. A detached signature of an executable program can detect subsequent virus infection. Finally, detached signatures can be used when more than one party must sign a document, such as a legal contract. Each person's signature is independent and therefore is applied only to the document. Otherwise, signatures would have to be nested, with the second signer signing both the document and the first signature, and so on.

5 marks

(b)

- The sender needs to store only the uncompressed message and the signature for future verification
  - Otherwise, compressed message needs to be store as well
- There are different compression algorithms and different versions of the same algorithm
  - If compression is done after encryption, all PGP implementation must use the same version of the same algorithm
- It strengthen the security as cryptanalysis on compressed message is more difficult

6 marks -> 2 marks for each point

4.

a. In relation to IPSec, answer the following:

i. Explain how IPSec can prevent a replay attack.

ii. Explain the difference between transport and tunnel mode operation of IPSec? When is it suitable to use each of the above modes of operation?

b.

i. Explain SSL protocol?

ii. Explain what is HTTPS? & iii. Explain SSH protocol?

(4+(5+3)+2+4=18 marks)

Sample Solution

(i) A replay attack is one in which an attacker obtains a copy of an authenticated packet and later transmits it to the intended destination. The receipt of duplicate, authenticated IP packets may disrupt service in some way or may have some other undesired consequence.

2 marks

The sequence number field in AH or ESP header associated with a particular SA is not duplicated. When a packet with duplicated sequence number with same SA is received, it is discarded. 2 marks

(ii) Transport mode provides protection primarily for upper-layer protocols. That is, transport mode protection extends to the payload of an IP packet.
Transport mode is meant to be used between two fixed hosts, or to put it another way, when the VPN endpoints are the final destinations of the traffic in the VPN. In particular, transport mode cannot be used to connect two networks or a network and a host. 4 marks

Tunnel mode provides protection to the entire IP packet.
The typical use of tunnel mode is to connect either two networks or a host and a network: for example, a remote office network to a home office network. It is more flexible than transport mode, but this flexibility comes at the expense of increased bandwidth requirements. 4marks

(b) **(i)** *SSL provides security services between TCP and applications that use TCP*

2 marks

(ii) *HTTPS (HTTP over SSL) refers to the combination of HTTP and SSL to implement secure communication between a Web browser and a Web server. 2 marks*

iii. SSH provides secure, remote logon and other secure client/server facilities 2 marks

5.

a. What security areas are addressed by IEEE 802.11i? Briefly describe the four IEEE 802.11i phases of operation.

b. WAP end-to-end security has a security gap in between. Describe 2 possible solutions to solving this problem?

c. What is the difference between an SSL connection and an SSL session?

.

d. Describe services that are provided by the SSL Record Protocol.

((2+4)+4+4+4=18 marks)

(a) Ans: IEEE 802.11i addresses four main security areas: authentication, key management, data confidentiality & data integrity. 2 marks

Discovery: An AP uses messages called Beacons and Probe Responses to advertise its IEEE 802.11i security policy. The STA uses these to identify an AP for a WLAN with which it wishes to communicate. The STA associates with the AP, which it uses to select the cipher suite and authentication mechanism when the Beacons and Probe Responses present a choice.
Authentication: During this phase, the STA and AS prove their identities to each other. The AP blocks non-authentication traffic between the STA and AS until the authentication transaction is successful. The AP does not participate in the authentication transaction other than forwarding traffic between the STA and AS.
Key generation and distribution: The AP and the STA perform several operations that cause cryptographic keys to be generated and placed on the AP and the STA. Frames are exchanged between the AP and STA only
Protected data transfer: Frames are exchanged between the STA and the end station through the AP. As denoted by the shading and the encryption module icon, secure data transfer occurs between the STA and the AP only; security is not provided end-to-end.
Connection termination: The AP and STA exchange frames. During this phase, the secure connection is torn down and the connection is restored to the original state. 4 marks

(b) Ans: The first approach (Figure 6.20a) is to make use of TLS between client and server. A secure TLS session is set up between the endpoints. The WAP gateway acts as a TCP-level gateway and splices together two TCP connections to carry the traffic between the endpoints. However, the TCP user data field (TLS records) remains encrypted as it passes through the gateway and so end-to-end security is maintained.

Another possible approach is shown in Figure 6.20b. Here we assume that the WAP gateway acts as a simple Internet router. In this case, end-to-end security can be provided at the IP level using IPsec 4 marks

Ans: Connection: A connection is a transport (in the OSI layering model definition) that provides a suitable type of service. For SSL, such connections are peer-to-peer relationships. The connections are transient. Every connection is associated with one session. Session: An SSL session is an association between a client and a server. Sessions are created by the Handshake Protocol. Sessions define a set of cryptographic security parameters, which can be shared among multiple connections. Sessions are used to avoid the expensive negotiation of new security parameters for each connection. 4 marks

(b) The following services are provided

Ans: Confidentiality: The Handshake Protocol defines a shared secret key that is used for conventional encryption of SSL payloads. Message Integrity: The Handshake Protocol also defines a shared secret key that is used to form a message authentication code (MAC). The method used for these are:

- **Fragmentation** - fragments the data in manageable block size (16KB or less)
- **Compression** – optional, must be lossless, SSLv3 (TLS) does not specify any compression algorithm

- **Integrity protection -** compute MAC on the compressed data using SHA-1,MD; uses a shared secret key negotiated in handshake protocol
- **Encryption -** compressed message and MAC are encrypted using symmetric encryption algorithm; Algorithm permitted: IDEA, RC2, RC4, DES, 3DES, Fortezza
- **Append SSL record header**

4 marks

6.

a. List and briefly define three classes of intruders.

b. Having an Intrusion Detection System (IDS) in a network is crucial for ensuring security. What are the benefits that can be provided by an intrusion detection system?

c. What are the characteristics of stealth and polymorphic viruses that make them difficult to detect? Name two advanced antivirus techniques.

d. Firewalls are a viewed as a means to protect internal networks from external networks. In relation to this, explain the following:

(i) List three design goals for a firewall.

(ii) What is a DMZ network and what types of systems would you expect to find on such networks?

(iii) What is the difference between an external and internal firewall?

(3+3+(4+1)+3+3+2=19 marks)

(a) ANS: Masquerader: An individual who is not authorized to use the computer and who penetrates a system's access controls to exploit a legitimate user's account.
Misfeasor: A legitimate user who accesses data, programs, or resources for which such access is not authorized, or who is authorized for such access but misuses his or her privileges.
Clandestine user: An individual who seizes supervisory control of the system and uses this control to evade auditing and access controls or to suppress audit collection. 3 marks

(b) **ANS:** **1.** If an intrusion is detected quickly enough, the intruder can be identified and ejected from the system before any damage is done or any data are compromised. Even if the detection is not sufficiently timely to preempt the intruder, the sooner that the intrusion is detected, the less the amount of damage and the more quickly that recovery can be achieved.
2. An effective intrusion detection system can serve as a deterrent, so acting to prevent intrusions.
3. Intrusion detection enables the collection of information about intrusion techniques that can be used to strengthen the intrusion prevention facility.

3 marks

(c) Stealth virus: a) explicitly designed to hide from virus scanning programs; b)actively hides any change it has made to the hard disk; c)The virus takes over system functions that are used in reading files or system sectors.

2 marks

Polymorphic virus: a) mutates with every infection, making "signature" detection impossible appearance and size changes; b) difficult to detect by scanning as each copy looks different; c) needs more than one method of viral detection.

2 marks

Two advance anti-virus techniques: a) Generic Decryption; b) Digital Immune System 1 mark

(d) (i) **1.** All traffic from inside to outside, and vice versa, must pass through the firewall. This is achieved by physically blocking all access to the local network except via the firewall. Various configurations are possible, as explained later in this section. **2.** Only authorized traffic, as defined by the local security policy, will be allowed to pass. Various types of firewalls are used, which implement various types of security policies, as explained later in this section. **3.** The firewall itself is immune to penetration. This implies that use of a trusted system with a secure operating system. 3 marks

(ii) Between internal and external firewalls are one or more networked devices in a region referred to as a DMZ (demilitarized zone) network. Systems that are externally accessible but need some protections are usually located on DMZ networks. Typically, the systems in the DMZ require or foster external connectivity, such as a corporate Web site, an e-mail server, or a DNS (domain name system) server. 3 marks

(iii) An **external firewall** is placed at the edge of a local or enterprise network, just inside the boundary router that connects to the Internet or some wide area network (WAN). One or more **internal firewalls** protect the bulk of the enterprise network. 2 marks