UNIVERSITY OF JOHANNESBURG

FACULTY OF SCIENCE

ACADEMY OF COMPUTER SCIENCE AND SOFTWARE ENGINEERING

MODULE: **IT08X47/IT8X298**
INFORMATION SECURITY

CAMPUS: **APK**

EXAM: **MAY 2019**

DATE 21 MAY 2019 **SESSION** 08:30 – 10:30

INTERNAL EXAMINER Mr. J du Toit

EXTERNAL EXAMINER Prof L Futcher

DURATION 2 Hours **MARKS** 100

Please read the following instructions carefully:

1. Write clearly and legibly.
2. Answer all questions.
3. This paper consists of 4 pages

QUESTION 1 (Digital Signatures, Confidentiality and Non-Repudiation) [30]

You are a systems designer for the Utopian Information Exchange (UIE). The UIE makes use of an Internet based messaging application. Your responsibility is to design a process that will describe how each message in the system is encrypted using a unique key for each message. You can assume that each person using the system has a set of public and private keys. Public keys are publicly available to anyone using the system and is stored in a tamper resistant area.

The following security features are required:
a) The process must be able to withstand a man-in-the-middle attack.
b) The process must assure perfect forward secrecy.
c) The integrity of messages must be assured.

Discuss the process involved when a sender(S) would like to send a message to a receiver(R). Your discussion should describe all the steps ***up to*** the point where secure keys are established between the sender(S) and receiver(R) to ensure that symmetric key encryption can be used for normal message encryption. You ***do not*** have to describe how the established secure keys are used to encrypt the normal message between the sender and the receiver.
Start the discussion by naming each of the keys mentioned in the process.

Marks are awarded for:
Structure, neatness and logic approach (3).
Naming the keys (5).
Process explanation (22).

QUESTION 2 (Digital Identities) [20]

2.1	**Discuss** how a browser determines if a web site's certificate should be trusted when it uses an HTTPS connection.	(10)
2.2	**List** two advantages and two disadvantages when storing public keys in a central repository.	(8)
2.3	You just found out that a copy has been made of your web server's certificate. **Briefly describe** if this is a cause for concern.	(2)

QUESTION 3 (IDPS and other tools) [12]

3.1 You need to decide to invest in either a signature based or anomaly-based intrusion detection system. **Compare** a signature based IDPS against an anomaly-based IDPS. (6)

3.2 Figure 1 describes the basic architecture of a multi-regional company. In your answer sheet, clearly **indicate** two locations where you will deploy network IDPS and **motivate** why. (6)

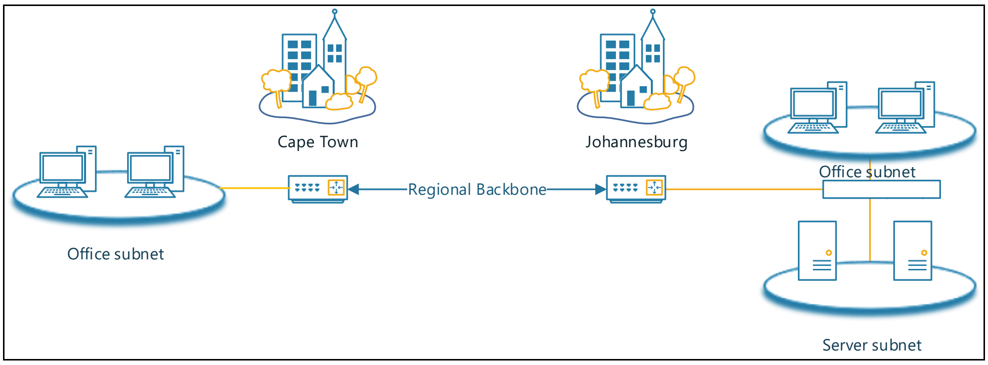

Figure 1: Network diagram

QUESTION 4 (Confidentiality) [10]

4.1 Given the following clear text alphabet and polyalphabetic substitution cipher. **Write** the cipher text for the word: ***LIMP*** (2)

Clear Text	ABCDEFGHIJKLMNOPQRSTUVWXYZ
Substitution cipher 1:	DEFGHIJKLMNOPQRSTUVWXYZABC
Substitution cipher 2:	GHIJKLMNOPQRSTUVWXYZABCDEF
Substitution cipher 3:	JKLMNOPQRSTUVWXYZABCDEFGHI
Substitution cipher 4:	MNOPQRSTUVWXYZABCDEFGHIJKL

4.2 **Write** the cipher text when a permutation cipher is applied to the following clear text given the following permutation key. (2)
Permutation key: **1 -> 2; 2 -> 5; 3 -> 1; 4 -> 3; 5 -> 4**
Clear text: ***BLAZE***

4.3 **Discuss** three problems with keys used in symmetric encryption (6)

QUESTION 5 (Threats and attacks) [10]

5.1 **Describe** two different types of password cracking techniques. (4)

5.2 You are assisting in designing the security of a new WiFi network at your office. **Describe** two communication interception techniques attackers can use on a WiFi network. (4)

5.3 **Motivate** which technique for choosing a password is better: (2)

1.) A ten-character password with at least one uppercase, one lowercase, one number and one special character.
2.) A five-word passphrase.

QUESTION 6 (Multi-Dimensional Aspects of Information Security and Policies) [8]

6.1 **Name** and provide a **motivation** for each of the three dimensions that intersect in the McCumber cube for the following Information Security control: A policy that governs the encryption of data when it is sent to third parties. (6)

6.2 **Name** the type of information security policy that ***ISO27002*** can help create in an organisation. (2)

QUESTION 7 (Access Control and Firewalls) [10]

7.1 **List** the permissions that the following ***subjects*** have on the following ***objects*** in a Biba integrity model. Assuming a classification of Important is higher than Untrusted. (4)

Subjects:

- {Excel, Important}
- {Internet Browser, Untrusted}

Objects:

- {Exam Marks, Important}
- {GOT_S7E5, Untrusted}

List the permissions in the following syntax:
[Subject – Permissions – Object]

7.2 **Discuss** the role of a DMZ in a firewall architecture. In your discussion mention the network level access to and from the DMZ as well as the type of services normally found in a DMZ (4)

7.3 A friend of yours are considering buying an ADSL router with content filter capabilities. **Describe** to your friend the role of content filters in an ADSL router. (2)

TOTAL PAPER **[100]**