UNIVERSITY OF JOHANNESBURG

FACULTY OF SCIENCE

ACADEMY OF COMPUTER SCIENCE AND SOFTWARE ENGINEERING

MODULE:	**IT08X47/IT8X298**
	INFORMATION SECURITY
CAMPUS:	**APK**
ASSESSMENT:	**EXAM - SSA. JULY 2021**

DATE	JULY 2021	**SESSION**	Normal
INTERNAL EXAMINER		Dr J du Toit	
EXTERNAL EXAMINER		Dr R Serfontein	
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
4. This is an open book assessment. You may consult your notes and textbook during the assessment.
5. You are **NOT** allowed to copy from any notes or write anything directly from the notes.
6. You are **NOT** allowed to assist or gain assistance from anyone else.

QUESTION 1 (The need for security) **[23]**

1.1 The Utopian National Vaccine (UNV) management group employed you as an Information Security Engineer. UNV is responsible for deploying much-needed vaccines to the citizen of Utopia. UNV will use an extensive network of service providers to ensure the successful vaccination of each citizen. (17)

UNV manages the communication between themselves and each service provider through a national Vaccine management system called VACSOL. Service providers use VACSOL for primarily two purposes. Service providers place orders for vaccines using the system. Service providers update patient records with vaccination status after the vaccine has been administered. Service providers also have the option to update profile information such as operating hours and delivery addresses.

One of your first tasks as the IS Engineer is to produce a document that clearly highlights four of the most common IS threats UNV may experience. The identification of the four threats can only use the information provided in this question. At least one control must be described for each threat that UNV can implement to address the threat. The control MUST be realistic to the information provided below.

Information regarding VACSOL:

- VACSOL uses an Internet-facing web page that service providers use.
- Service providers use usernames and passwords to identify and authenticate themselves to the system.
- VACSOL is installed and running on server hardware that is seven (7) years old. The warranty for most of the hardware has already expired.
- UNV makes use of Utopian Telecoms as their Internet connectivity provider.
- Service providers can administer vaccines 24-hours a day, which requires a high level of availability of the VACSOL system.
- Patient information does not seem to have any apparent value. However, the vaccines have a resale value of nearly double the market value on the black market.
- The VACSOL system has never been tested for any web vulnerabilities.

Your document must contain the following:

- **Describe** four typical threats applicable to VACSOL and UNV.
- For each threat, highlight **why** the threat was identified.
- For each threat, **describe** one control UNV can implement that will address the threat.

Marks are awarded as follow:

- Describing four threats. One mark per threat. (4)
- Describing why each one is a threat. (4)
- Control of threat. Two marks per control. (8)
- Readability and neatness. (1)

./1.2 Continued on the next page

1.2 UNV experienced an information security attack a week after you joined. A forensic investigation identified the following facts: (6)

- Patient records stored on the UNV database was leaked to the Internet.
- A hacktivist group called VaccineFree was identified as the attacker.
- VaccineFree got access to the database of patient records through an incorrectly configured firewall port.
- The access logs on the firewall show that the attack was launched from a device with an IP address belonging to a temporary virtual machine.

Given the above scenario, identify each of the following Information Security aspects and provide a reason why the item was identified.

a) Threat agent.
b) Subject.
c) Object.
d) Vulnerability.

QUESTION 2 (Information Security Planning) **[12]**

After the attack on UNV, the Chief Information Security Officer started a project to review information security policies for which the board and top management is responsible. (12)

You have been asked to help determine the scope of the project. For each of the different types of policies, argue whether the type of policy should be included in the project's scope.

Marks are awarded as follow:

- Listing of the three types of IS policies. One mark per policy type. (3)
- A brief description of each policy type. One marks per policy type. (3)
- The argument of whether the policy type should be included in the scope. Two marks per policy type (6)

QUESTION 3 (The five information security services) **[15]**

It became apparent that the VACSOL system was not initially as secure as it could have been. A few cases have been identified where unauthorised access to the system caused the delivery addresses of the vaccines to be modified. The vaccines were delivered to the incorrect addresses, which caused those batches to be stolen. (15)

A project to improve the overall security of VACSOL has been launched. Write a set of requirements that address each of the five Information Security services in ISO 7498/2.

Marks are awarded as follow:

- Listing and providing a basic description of the 5 IS services (5)
- Clearly describe how the Information Security service will be implemented for this project (10)

QUESTION 4 (Digital Signatures, Confidentiality and Non-Repudiation) **[40]**

The UNV would like to implement and design a system that will allow messages to be sent and received between UNV and the vaccination sites. It is your responsibility as the IS Engineer for UNV to define the security requirements and define a process that will describe how the system will implement the requirements. The focus of the requirements should be on integrity, confidentiality and non-repudiation.

4.1 Start writing a design specification document. The design specification document must highlight and specify the various security requirements that the system should adhere to. (6)

Describe at least three security requirements, with the focus on *integrity*, *confidentiality* and *non-repudiation*.

4.2 Describe in detail how the system will both establish secure communication channels and transmit and receive messages securely to comply with the requirements established in 4.1. Marks are awarded as follow: (25)

- Using a structured approach in the answer. (3)
- Clearly describing and highlighting different security keys. (4)
- Describing the implementation details. (18)

4.3 Critically evaluate the design and identify and discuss three high-level risks that the implementation and requirements did not address. (9)

QUESTION 5 (Confidentiality) **[10]**

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

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

5.2 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: ***RUMOR***

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

TOTAL PAPER **[100]**