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 7 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.
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 VASCOL 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 VASCOL:

- VASCOL uses an Internet-facing web page that service providers use.
- Service providers use usernames and passwords to identify and authenticate themselves to the system.
- VASCOL 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 VASCOL 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 VASCOL system has never been tested against OWASP Top 10 vulnerabilities.

Your document must contain the following:

- **Describe** four typical threats applicable to VASCOL 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)

Deviations in quality of service. Only UT is used, which means that if UT is down, then no service can be provided.

Trespass. It may be possible for attackers to attack service provider login details.

Technical hardware failures. The server hardware is 7 years old and not under warranty anymore.

Software attacks. Man in the middle attacks may be possible to get access to information. Information may be changed to change delivery addresses, thus stealing the actual vaccines.

Technical Software Failures. Since it is a web site, it may be susceptible to

Threats should be real-world threats. This can include many things such as Phishing attacks, Password re-use, man-in-the-middle attacks, denial-of-service attacks etc.

The categories that students can choose from is:

- Compromises to intellectual property
- Deviations in equality of service
- Espionage or trespass
- Forces of nature
- Human error or failure
- Information extortion
- Sabotage or vandalism
- Software attacks
- Technical hardware failures or errors
- Technical software failures or errors
- Technological obsolescence
- Theft

The justification of threat must answer the question "Why" is the threat a problem.

The control of the threat can be a general control that can be implemented. It must specifically apply to the threat.

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.

Two marks per item:

a) Threat agent: VaccineFree. They are the party that attacked UNV
b) Subject. Virtual machine used by the attacker
c) Object. The database or database server.
d) Vulnerability. The firewall, with incorrectly configured port.

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)

Enterprise IS Policy

Executive level document. Sets the responsibilities and penalties and disciplinary actions.

Should be included in the RFQ. EIS Policy must be approved by the board.

Issue-specific security policy

Addresses specific areas of technology. Requires frequent updates. Contains statements on the organisation's position on a specific issue.

Must be included in the RFQ, since it defines the organisation's position and require the board to approve.

System-specific security policy

Acts as standard or procedures when configuring or maintaining a system. Provides managerial guidance or technical guidance.

My or may not be included in the RFQ, but most of these policies apply to a system specifically which is normally part of the IT department's responsibilities. Not normally part of the responsibility of the board.

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

It became apparent that the VASCOL 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 VASCOL 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)

The student should list the five information security services.
For each service the following aspects could be considered.

Identification and Authentication:

- Before any connection is established.
- There must be positive identification

- There may multiple factors of identification and authentication.

Authorisation:

- Levels of access may depend on the level of identification and authentication
- The system can apply access control or capability list structures.

Integrity:

- Data sent over the network must be signed or contain a message digest.
-

Confidentiality:

- There must be some level of assurance that data can only be accessed between two parties.
- This can be established using encryption during transmission and at rest.

Non-repudiation:

- Transactions must be linked to specific nodes.
- Nodes should not have the ability to deny performing a transaction in the future.
- Even after verification occurred, any transaction must be linked to a specific node. This ensures that nodes cannot deny

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*.

Section 1: Many requirements may be listed here. They may include:

- Withstand man-in-the-middle attacks.
- Ensure perfect forward secrecy.
- The integrity of messages must be assured.
- All messages must be confidential.
- System must ensure non-repudiation.
- Other requirements, such as positive identification and authentication and authorisation, may also be given.

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. (25)

- Structured approach. (3)
- Clearly describing and highlighting different security keys. (4)
- Describing the implementation details. (18)
- Man-in-the-middle attack: HMAC that is signed by the sender to verify integrity and authentication.

- Ensure perfect forward secrecy: Solution must make use of Ephemeral keys, using Diffie-Hellman
- Integrity of message: Each message must have a MAC (Key with the message).
- Confidentiality: Student should try and use symmetric key encryption for confidentiality, but half marks may be given for asymmetric key encryption.
- Non-repudiation: Must make use of PKI and messages must be digitally signed.

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

Section 3: Three IS risks

- Evaluation, must identify and discuss three risks.
- Depending on the requirements, these may be things such as perfect-forward secrecy, man-in-the-middle attacks, centralised storage of public keys etc.

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`

WXRY

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***

MRORU

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

Size:
The smaller the key the less effort it is to brute force attack.

Distribution:
Both the sender and receiver needs the same key. The question is always how the key should be distributed between the two parties, that can guarantee the confidentiality of the key.

Derivation:
If a key is derived from a short or simple password, then an attacker can also derive the key, if they know the parameters.

TOTAL PAPER **[100]**