UNIVERSITY OF JOHANNESBURG

FACULTY OF SCIENCE

ACADEMY OF COMPUTER SCIENCE AND SOFTWARE ENGINEERING

MODULE:	**IT08X47/IT8X298** INFORMATION SECURITY
CAMPUS:	**APK**
ASSESSMENT:	**EXAM JUNE 2021.**

DATE	JUNE 2021	**SESSION**	Morning
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 or other sources.
6. You are **NOT** allowed to assist or gain assistance from anyone else.

QUESTION 1 (The need for security) [20]

You have been employed as the Information Security (IS) Engineer at the Utopian National Medical Aid Scheme (UMAS). The Utopian government is in the process of providing national medical aid for all its citizens. (20)

One of your first tasks as the IS Engineer is to produce a document that clearly highlights five of the most common IS threats a typical general practitioner (GP) will have. The identification of the five threats can only use the information provided in this question. At least one control must be described for each threat that the GP can implement that will address the threat. The control MUST be realistic to the size of and capability of a typical GP.

The typical GP in Utopia has the following IT infrastructure:

- One or two reception computers that stores and manage patient information.
- One or two tablet devices used by GPs in their consultation rooms to look up symptoms.
- The computers are typically connecting to the Internet through an ADSL router with built-in firewall.
- Receptionists use the computers for email and basic Internet browsing.
- In most cases, computers and tablet computers use wireless connections, using a shared password for the WiFi network.
- Backups of patient information are normally done on removable USB devices taken home by the GP at the end of each day.

Your document must contain the following:

- **Describe** five typical threats applicable to the average GP in Utopia.
- For each threat, highlight **why** the threat was identified.
- For each threat, **describe** one control the GP (*or IT service provider of the GP*) can implement that will address the threat. The control must be applicable for such a small enterprise.

Marks are awarded as follow:

- Describing five threats. One mark per threat. (5)
- Describing why each one is a threat. (5)
- Control of threat. Two marks per control (10).

Threats may include:

- Physical theft of backed up media.
- Malware delivered through email or other means.
- Phishing attacks.
- Physical theft of tablet devices.
- Fires or floods caused by sprinkler systems.
- Shared password on the WiFi network may be leaked, and must be complex or changed.
- Anything that makes sense, given the scenario.

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.

QUESTION 2 (Information Security Planning) [16]

2.1 The UMAS are gearing up for a major IT project that will automate the processing of medical aid claims from GPs. You have been asked to ensure that information security management in UMAS follow best practice. You are thinking of using either Cobit or ISO 27002 as a guideline. (10)

Compare Cobit against ISO 27002 and state which one you would select as best practice and **why** you have made that decision.

(Four marks per best practice, based on relevant facts) (4 x 2)

(Two marks stating why a specific best-practice was used) (2)

Cobit:

- Used primarily to audit IT controls.
- Most widely used best practice for IT governance.
- Cobit consists of 37 processes divided in 2 domains. (Management and Governance)
- Two of the processes (AP013 and DSS05) specifically relates to security

ISO 27002

- Code of Practice for Information Security.
- Created first as a British Std with other organisations such as BP for IS.
- Accepted by many countries as a national standard.
- Was first BS7799, then ISO 17799, then ISO 27002.
- Cannot specifically be certified for ISO 27002 but can be certified for ISO 27001.

Either can be used. ISO has a much stronger focus on ISM where Cobit has much stronger focus on IT. It all depends on the organisation's existing IT maturity.

2.2 A comprehensive IS awareness and training program is one of the requirements for the new IT project. Write a brief memo that describes how you will implement both IS *training* and *awareness* for UMAS. The memo must address the following aspects for the awareness portion as well as the training portion: (6)

- Which employees will be targeted.
- What format it will take.
- How employees will be tested to determine if they understood the training and awareness.

Targeted:

Awareness: Typically all employees

Training: Those employees that may be working in the IT department or key positions with the systems

Format:

Awareness: Any realistic awarenss mechanism. This can include, videos and newsletters.

Training: Form of lectures, workshops etc.

Testing:

Awareness: Small test with true or false, multiple choice.

Training: Demonstrating problem solving

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

One of the General Practitioners (GPs) contacted you after you visit them. They are considering using a cloud-based booking system to handle their daily patient appointments. Reception staff must be able to manage the appointments, while the doctors only need to see bookings for them. They are concerned about the risks that such a system may have. (15)

By specifically referring to the 5 Information Security services covered in ISO 7498/2, what controls will you recommend they implement?

Marks are awarded as follow:

- Describing the 5 IS services of ISO 7498/2. (5)
- Describing one or more controls per IS service relevant to the scenario. (10)

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

Identification and Authentication:

- Users must use some form of identification and authentication.
- Since it will be cloud based, multi-factor authentication is recommended.

Authorisation:

- Groups will be used to ensure that reception staff may create, modify, and delete appointments.
- Doctors can be put in a special group to ensure they only see appointments assigned to them.

Integrity:

- The network protocol must ensure only authorised users can modify the appointments.
- The network protocol must ensure that network traffic cannot be modified by a third party.

Confidentiality:

- Data on the back-end storage must only be available to members of the practice.
- Encryption at rest can be used to ensure that even the cloud provider cannot read the data.
- Network traffic must be encrypted to ensure confidentiality of information.

Non-repudiation:

- The system may be built to ensure it audits all transactions.
- Transaction logs must be available to authorised users.
- Admin rights to staff accounts must be limited to a special accounts.

QUESTION 4 (Digital Signatures, Confidentiality and Non-Repudiation) [34]

UMAS is ready to start developing and designing its automated medical aid processing system.
General Practitioners (GPs) will use the new system to submit claims on behalf of patients

The first version of the messaging system makes use of a centralised system that stores public keys.

4.1 **Describe** how the system can use *Forward Public Key Encryption* (only) to ensure a claim is kept confidential when a GP submits it. (4)

Keys:

- UMAS Private Key (PrivR)

- UMAS Public Key (PubR)

Process:

The following activities happen:

- GP generates a message (M)
- GP encrypts M using PubR ES = E(M)PubR
- UMAS decrypts ES using PrivR exposing M.

4.2 **Describe** how the system can use *Inverse Public Key Encryption* (only) to ensure the non-repudiation of messages sent from the GP to UMAS. (4)

Keys:

- GP Private Key (PrivS)
- GP Public Key (PubS)

Process:

The following activities happen:

- GP generates a message (M)
- GP encrypts M using PrivS ES = E(M)PrivS
- UMAS decrypts ES using PubS exposing M.
- Because PubS was used to decrypt the message, the message is guaranteed to be sent by GP.

4.3 The Managing Director of UMAS heard about Inverse Public Key Encryption and would like to ensure confidentiality. (2)

What would you say to the MD regarding his request?

IPKE does not guarantee confidentiality. Anyone can decrypt the message since the public key is in the public domain.

4.4 **Discuss** the problem that Envelope Public Key Encryption has with regards to perfect forward secrecy. (4)

If we consider that the messages may be recorded.

And UMAS and GPs private keys may be compromised in the future, then

We can decrypt all these messages, past, current, and future.

4.5 **Describe** how the process in 4.2 (Inverse Public Key Encryption) can be changed to be more processing efficient. (8)

The GP creates a message M.

GP creates a digital signature (DS) of M. This is done by

(2) DS = E(H(M))PrivS (1) Mark for the hashing (1) Mark for the encrypting

DS and M is sent to UMAS

UMAS verifies the signature by:

(1) UMAS creates a hash of M. H’(M)

(1) UMAS decrypts E(H(M))PrivS using PubS.

(1) This generates H(M)

(1) UMAS verifies H(M) = H'(M)

(1) If they match UMAS is assured that M came from GP and (1) that it has not been tampered with.

4.6 UMAS would like to enhance the message system to use Diffie-Hellman to establish ephemeral keys. **Describe** how the Diffie-Hellman process generates two ephemeral keys on two devices. The description should describe each variable or component and the process that eventually creates an ephemeral key on the one unit and the other unit. (12)

Public Components:

(1) n = very big prime number (At least 2048 bits)

(1) g = generator (This is a prime number less than n)

UMAS

(1) UMAS generates a secret number a

(1) UMAS generates a public number using formula

(1) g^a mod n = N

(1) UMAS generates k using formula

(1) M^a mod n = k

GP

(1) GP generates a secret number b

(1) GP generates a public number using formula:

(1)g^b mod n = M

(1) GP generates k using formula

(1) N^b mod n = k

QUESTION 5 (Digital Identities) [15]

The implementation of the claims system was a success, but the UMAS would like to plan and upgrade the claims system to use digital identities.

5.1 **Discuss** two IS reasons why UMAS may have decided to consider using digital identities from a Certificate Authority, instead of continuing to use the centralised storage of digital identities? (4)

(2) The centralised storage is a central point of failure, which can result in the whole system from functioning.

(2) Compromising the security in the central storage, may allow attackers to create false identities, compromising the integrity of information.

5.2 **Describe** the process that would allow UMAS to get a digital identity from a Certificate Authority. (6)

(1) UMAS submits their public key and personal information to a Certificate Authority.

(1) The CA verifies the personal information of UMAS

(1) The CA creates a CTDI = (public key + personal information)

(1) The CA hashes the CTDI. H(CTDI)

(1) The CA encrypts H(CTDI) using PrivCA. E(H(CTDI))PrivCA.

(1) The CA returns UMAS's DI = (E(H(CTDI))PrivCA, CTDI)

5.3 One of the general practitioners (GPs) signed an email using their private key. The GP attached an X.509v3 certificate in the email. (5)

Statement: You are assured that the message was sent by the GP.

Discuss the validity of the above statement.

(One or Two marks per argument)

The question is whether we can trust if the certificate really belongs to the GP.

- If the certificate has been signed by a trusted CA and
- we can verify the digital signature in the certificate AND
- if the certificate is valid and
- contains the clear text information about our colleague then we can trust.
- If there is a problem with the CA that signed the certificate OR
- if the clear text information in the certificate indicates that the certificate does not belong to our colleague then we cannot assume that the message was sent by our colleague

TOTAL PAPER **[100]**