2023 EXAMINATIONS

Part II

COMPUTING AND COMMUNICATIONS – On-line Assessment

Available Time **[2.5 Hours]**

Recommended Completion Time **[2 Hours]**

SCC.363 Security and Risk

Candidates are asked to answer ***THREE*** *questions from* ***FOUR****; each question is worth a total of 20 marks.*

Question 1

Consider the following Python3 code listing using the RSA implementation from cryptography.io.

```
…
private_key = rsa.generate_private_key(
        public_exponent=65537,
        key_size=2048)

public_key = private_key.public_key()

message = b"a"*256

ciphertext = public_key.encrypt(
        message,
        padding.OAEP(mgf=padding.MGF1(algorithm=hashes.SHA256()),
        algorithm=hashes.SHA256(),
        label=None))
…
```

Listing 1 - Example code using RSA

1.a Explain in detail the issue in Listing 1 and how it can be fixed.

[6 marks]

1.b Provide three (3) role-based policies supported by the RBAC$_1$ model. Explain the policies and express them using the element sets and relations supported by the RBAC$_1$ model (USERS, ROLES, PRMS, PA, etc.)

[6 marks]

1.c You are a network security engineer in a company offering email and file transfer services. Using the TCP/IP model as a reference, explain how you can protect these services e.g., against phishing attacks for the email, control the type of files uploaded/downloaded in the file transfer service.

[4 marks]

1.d Consider a web application interfacing with a relational database management system (RDBMS) at its backend. The web application provides login functionalities. Authorisation is based on role-based policies. All data is stored in the RDBMS. Provide a threat model using a tree structure to explore ways of an attacker gaining access to sensitive data in the RDBMS. Note that each parent node of your tree should have no more than two child nodes, and the maximum depth of your tree should be 4. Also describe separately what the threat model is depicting.

[4 marks]

[20 Total Marks]

Question 2

Consider the following Python3 code listing using the RSA implementation from cryptography.io.

```
…
private_key = rsa.generate_private_key(
        public_exponent=65537,
        key_size=2048)

public_key = private_key.public_key()

message = b"example"

ciphertext = public_key.encrypt(
        message,
        padding.OAEP(mgf=padding.MGF1(algorithm=hashes.SHA256()),
        algorithm=hashes.SHA256(),
        label=None))

words = {"This", "is", "an", "example"}
bValue = False

for word in words:
        ciphertext_BF = public_key.encrypt(
            word.encode(),
            padding.OAEP(mgf=padding.MGF1(algorithm=hashes.SHA256()),
            algorithm=hashes.SHA256(),
            label=None))
        if ciphertext == ciphertext_BF:
            bValue = True

print(bValue)
```

Listing 2 – Example code using RSA

2.a What is the value of `bValue` at the end of Listing 2 and why? Explain your answer in detail.

[4 marks]

2.b Elaborate on the main similarities/differences between hash-based message authentication codes and digital signatures.

[4 marks]

2.c Convert RBAC$_2$ policies to ABAC policies. This requires describing two (02) RBAC$_2$ policies using the element sets and relations supported by the RBAC$_2$ model (USERS, ROLES, PRMS, PA, etc.) and convert them into ABAC policies using appropriate attributes and other elements supported by ABAC.

[6 marks]

2.d You are a network security engineer, asked to protect a web application available over a VPN. The requirements include data integrity and confidentiality, consistency in network performance and protection against man-in-the-middle attacks. Explain what protocols you will use and why using as a reference the OSI model.

[6 marks]

[Total 20 Marks]

Question 3

3.a Risk assessment is a key element of risk management. It has three parts, risk identification, risk analysis, and risk evaluation. In particular, risk evaluation is the process of comparing the results of risk analysis with certain risk criteria to determine whether the risk is acceptable, leading to a decision about risk treatment.

i. Describe the risk criteria used in the process advocated by the CISSP and provide its formula.

[2 marks]

ii. An organization ran a security scan recently and found that several devices had significant vulnerabilities. These devices have been used to support the organization's major businesses over the past three years and have a huge amount of confidential data stored in them. The initial setup of the devices was a big financial and technical investment and it took one year to have all the necessary components installed to be able to support the organization's full businesses. These devices and data are key intellectual properties of the organization and are making a substantial profit each year. Based on the above description, which type of risk treatment do you think is most appropriate and why?

[4 marks]

iii. The organization above performed a one-shot thorough risk analysis and placed proper security controls accordingly. However, after a short while, they found that some of the above devices still got attacked. Please provide potential reasons for this from the following three aspects: (1) limitation of one-shot security controls (hint: think about the Plan Do Check Act cycle); (2) residual risk and incident management; (3) the phenomenon of moral hazard.

[4 mark]

3.b Cyber threat intelligence (CTI) is related to state threat intelligence, but has its own featu res.

i. Briefly state which features of CTI make it more difficult than state threat intelligence.

[3 marks]

ii. Identify major drawbacks of the intelligence cycle model and discuss how the intelligence funnel model addresses these drawbacks.

[3 marks]

3.c In economics, lock-in makes a customer dependent on a vendor.
i. Use an example to describe the concept of lock-in cost.

[2 marks]

ii. Briefly explain why the effect of technology lock-in may harm security of a product.

[2 marks]

[Total 20 marks]

Question 4

4.a.i Assume that X, Y and Z are three independent discrete random variables. Their distributions are provided by the following three tables. Find the standard deviation of the random variable 2X+5Y+3Z.

x_i	2	5	7	11	15	16	20	22	23
$P(X=x_i)$	0.10	0.05	0.15	0.18	0.11	0.16	0.05	0.14	0.06

y_i	-3	0	5	7	10
$P(Y=y_i)$	0.16	0.25	0.30	0.18	0.11

z_i	-8	-6	-5	-4	-3	-2	-1
$P(Z=z_i)$	0.02	0.02	0.16	0.15	0.20	0.22	0.23

[3 marks]

4.a.ii For the problem of 4.a.i, find the probability that Y+Z is within the interval [-5, 2].

[2 marks]

4.b During an analysis of machines on a network, it is found that 30% of them are infected with a worm, 60% infected with a virus, and 20% infected with both. This result is used to test the performance of a new screening procedure. Now it is known that, for the machines that are infected by at least one attack, the new procedure correctly returns ‘positive’ 70% of time, and for the machines that are not infected by either attack, the procedure incorrectly returns ‘positive’ 15% of the time. Find the probability that a machine is affected by at least one attack given that the machine is tested positive.

[5 marks]

4.c A company is to run in parallel three types of procedures, P1, P2 and P3, for the purpose of vulnerability test. Each type of the procedures has its own effectiveness level, computational overhead, and cost. To derive an optimal strategy, the company aims to minimize the total computational overhead subject to the following constraints: (1) the total effectiveness level must be no less than 15000; (ii) the total cost must be no greater than 10000; (3) the number of P1 must be no less than 6; (4) the number of P2 must be no greater than 10. The effectiveness level, computational overhead, and cost for each type of the procedures are given in the table below.

Question 4 continues on next page…

Question 4 continued.

	P1	P2	P3
Effectiveness level	1500	800	3200
Computational overhead	2200	600	2500
Cost	300	650	540

i. Formulate the above problem as a linear program and express it in the following canonical form

$$\begin{aligned} \max_{x} \quad & c^T x \\ \text{s.t.} \quad & Ax \le b. \end{aligned}$$

Identify the parameters c, A, and b, but do not solve the problem.

[4 marks]

ii. Consider the following three potential strategies: (1) P1 = 7, P2=2, P3=0; (2) P1=6, P2=8, P3=0; (3) P1=8, P2=3, P3=1. By only evaluating the objective function and the constraints of your formulated linear program over these three strategies, determine whether each of these three strategies is possible to be the optimal solution and explain the reasons. Again, do not solve the problem.

[4 marks]

4.d Briefly state the disadvantages of the simple random sampling method, and how the systematic sampling method and the stratified sampling method can mitigate one or more of these disadvantages.

[2 marks]

[Total 20 marks]

--- End of Paper ---