2021 EXAMINATIONS

Part II

COMPUTING AND COMMUNICATIONS – On-line Assessment

Available Time	**[23 Hours]**
Recommended Completion Time	**[3 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

1.a Assume the following asymmetric cryptosystem that can be used to exchange a key between two parties *A* and *B*.

Step 1: *A* and *B* share a prime number *q* and an integer *α.*

Step 2: *A* generates a private key PR_A and computes a public key $PU_A = a^{PR_A} \; mod \; q$

Step 3: *B* generates a private key PR_B and computes a public key $PU_B = a^{PR_B} \; mod \; q$

PR_A and PR_B are kept private since these are the private keys of *A* and *B,* respectively, and PU_A and PU_B can be sent away. Both participants can compute the same key K as follows:

Step 4: B sends PU_B *to A* and *A* computes the key as follows: $K = (PU_B)^{PR_A} \; mod \; q$, and

Step 5: A sends PU_A to *B* and *B* computes the key as follows: $K = (PU_A)^{PR_B} \; mod \; q$.

i. Identify a type of attack that the above cryptosystem is insecure against and explain why it is vulnerable to such an attack.

[2 marks]

ii. Describe at a high-level how your identified attack may be deployed, i.e. explain the sequence of actions; the mathematical proof is not required.

[4 marks]

iii. How could you overcome this vulnerability?

[2 marks]

1.b Answer the following questions:

i. Let f(x) = (2*x^3 + 1) mod 5 where x$\in$ [1, 9]. Explain if function f(x) is weak collision resistant by providing an example.

[3 marks]

ii. Let *m* = 01010010 be an 8-bit message. Considering the application of a ‘perfect encryption scheme’ (one-time pad), define an appropriate key and calculate the ciphertext of *m*.

[3 marks]

1.c IPSec is a network protocol suite used in Virtual Private Networks (VPNs).

i. Explain what level of security is offered by the transport and tunnel modes, respectively.

[2 marks]

Question 1 continues on next page…

Question 1 continued.

ii. When would you select to use the transport and tunnel modes, respectively?

[2 marks]

iii. IPSec supports the use of both the Authentications Header (AH) protocol and the Encapsulation Security Payload (ESP) protocol. What is offered when both are enabled and what may a disadvantage of using both?

[2 marks]

[Total 20 marks]

Question 2

2.a A relational database management system (RDBMS) is a database management system based on the relational model.

i. What type of an access control model should be supported by such a system and why?

[2 marks]

ii. Provide two example policies.

[2 marks]

2.b Consider the following code in the C programming language

```
#include <stdio.h>

int main() {

       int index;

       char s[8];

       index = 16;

       s[index] = 0;

       return 0;

}
```

i. Explain what vulnerability may be exploited in the above code and why is that possible in C?

[4 marks]

ii. Considering an equivalent code in Java or C#, explain if the above vulnerability would exist too and why?

[2 marks]

2.c Considering the following access control matrix, list two *capabilities,* and two *access control lists*.

		files				
		Login	less	nslookup	visudo	chrome
users	root	rwx	rwx	rwx		
	alice	x	x	x	x	x
	bob	x	x	x	x	x

r: Read; w: Write; x: eXecute

[4 marks]

Question 2 continues on next page…

Question 2 continued.

2.d Assume a role-based access control model (RBAC).

i. Explain what type of constraints may be supported by RBAC

[2 marks]

ii. Define and draw an appropriate role hierarchy that may be applicable in an academic institute (e.g. university).

[4 marks]

[Total 20 marks]

Question 3

3.a The term **Threat** is used in two main ways within cybersecurity two different types of assessment or analysis.

i. Provide the **two** main definitions of threat.

[2 marks]

ii. Explain why the key difference.

[2 marks]

iii. In the context of a Threat Actor explain the following terms with examples; ***Inhibitors, amplifiers, catalysts***.

[3 marks]

3.b Explain in your own words the relationship between Cyber Threat Intelligence and Risk Management.

[3 marks]

3.c The Intelligence Cycle has five main phases; ***Processing, Collection, Analysis, Planning, D issemination*** *(not listed in order)****.*** Explain the purpose of each phase and identify the correct sequencing.

[6 marks]

3.d Outline the **two** key criticisms of the Intelligence Cycle.

[4 marks]

[Total 20 marks]

Question 4

4.a In Security assessments both Quantitative and Qualitative analytical techniques are used

i. Provide a definition for each class of technique.

[2 marks]

ii. You need to survey a series of experts to obtain data to use in a stochastic model for the impact of a new zero-day attack. Identify which analytical technique you would use and explain your answer.

[3 marks]

4.b Risk Assessment is a fundamental process of risk management

i. Provide a definition for this process including its key constituent parts.

[4 marks]

ii. Provide an example of a risk assessment against a system of your choice covering TWO risks with example Annual Loss Expectancies for any given one-year period.

[2 marks]

4.c Once risks are understood the Risk Treatment phase is used to modify those risks

i. Define the 4 types of potential treatment.

[2 marks]

ii. Explain the term **Residual Risk**.

[1 mark]

4.d. You have a database essential to the operation of your business. It is on an older operating system that cannot be upgraded as the database service is no longer supported by the manufacturer. Both the operating system and the database service have well-known vulnerabilities which are not being patched by the vendors. There is a development process in place but the new system is 12 months from the operation. As such this has been identified as a very high risk for your business.

i. Which risk treatment would you apply and why?

[2 marks]

ii. At a high level explain identify what you would do as part of your risk treatment.

[4 marks]

[Total 20 marks]

--- End of Paper ---