Question Paper

Exam Date & Time: 01-Dec-2022 (09:00 AM - 12:00 PM)

MANIPAL ACADEMY OF HIGHER EDUCATION

MANIPAL INSTITUTE OF TECHNOLOGY, MANIPAL
FIFTH SEMESTER B.TECH END SEMESTER EXAMINATIONS, NOV/DEC 2022

CYBER SECURITY [ICT 3156]

Marks: 50 **Duration: 180 mins.**

A

Answer all the questions.

Instructions to Candidates: Answer ALL questions Missing data may be suitably assumed

1)		Give an overview of Data Encryption Standard (DES) algorithm and distinguish between various forms of DES algorithms	(5)
	A)		
	B)	Why computer crime is hard to prosecute? Explain	(3)
	C)	Suppose a department has determined that some users have gained unauthorized access to the computing system. Managers analyzed that this risk has 10% likelihood of occurrence per year with an estimated $5,00,000 cost to reconstruct the correct data. One approach to addressing this problem is to install a more secure data access control program which costs $30000. Calculate the annual savings, if any, with this approach	(2)
2)		Consider a person's buying a sculpture that costs $100. The buyer takes out five $20 bills, carefully counts them in front of the seller, and lays them on the table. Then the seller turns around to write a receipt. While the seller's back is turned, the buyer takes back one $20 bill. When the seller turns around, the buyer hands over the stack of bills, takes the receipt, and leaves with the sculpture. Explain the type of programming flaw relevant to this scenario with its security implications and counter measures	(5)
	A)		
	B)	In virtual memory, the user's program does not know what true memory addresses it uses. List the advantages for the operating system by this hiding of true memory addresses	(3)
	C)	Distinguish between vulnerability, threat, control, and risk. How do you classify controls?	(2)
3)		Specify the good design reasons for isolating security functions in a security kernel. What are the basic interactions monitored by Trusted Computing Base (TCB)? Explain	(5)
	A)		
	B)	Banking and other financial transactions are ordinarily protected in transit by an encrypted session, using a protocol named SSL or HTTPS. Whether these protocols completely secure transactions from man-in-the-browser attack? Justify your answer	(3)
	C)	Compare various types of firewalls	(2)
4)		Illustrate types of injection attacks with suitable examples	(5)
	A)		
	B)	One means of limiting the effect of an untrusted program is confinement: controlling what processes	(3)

have access to the untrusted program and what access the program has to other processes and data. Explain how confinement would apply to a program that computes the sum of the integers 1 to 10

C) Explain a security plan model with its appropriate content that can help security management task (2)

5) In an encryption employed in a network, data portion of the communication was secured for confidentiality. However, the addressing data were exposed. Thus, someone monitoring traffic between points A and B would know the volume of traffic communicated. Is there any technique to secure both addressing data and data portion during transit? Justify your answer (5)

A)

B) Suppose Alice and Bob have Rivest-Shamir-Adelman (RSA) public keys in a file on a server. They communicate regularly using authenticated, confidential messages. Eve wants to read the messages but is unable to crack the RSA private keys of Alice and Bob. However, she is able to break into the server and alter the file containing Alice's and Bob's public keys. How should Eve alter that file so that she can read confidential messages sent between Alice and Bob, and forge messages from either? (3)

C) How does browser encryption protect data during transmission? Describe the protocols related to the browser encryption (2)

-----End-----