Question Paper

Exam Date & Time: 06-Dec-2023 (02:30 PM - 05:30 PM)

MANIPAL ACADEMY OF HIGHER EDUCATION

FIFTH SEMESTER B.TECH. DEGREE EXAMINATIONS - NOVEMBER / DECEMBER 2023
SUBJECT: ICT 3156- CYBER SECURITY

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

Answer all the questions.

Any data not provided may be suitably assumed.

1A)	Preserving confidentiality, integrity, and availability of data is a restatement of the concern over interruption, interception, modification, and fabrication. How do the first three concepts relate to the last four? That is, is any of the four equivalent to one or more of the three? Is one of the three encompassed by one or more of the four?	(5)
1B)	With the help of a diagram, map and explain the types of controls/countermeasures with the kinds of threat and the security properties that it (control) protects.	(3)
1C)	Apply your understanding of how Method-Opportunity-Motive factors determine feasibility of attack?	(2)
2A)	Analyze the process of trust establishment within an organization through a chain of verification, its application to cryptographic key exchange, and the method's correlation to the distribution and authentication of public keys for secure communication. How this hierarchical trust model ensures the authenticity of public keys while considering its advantages and potential limitations within an organizational structure.	(5)
2B)	In public key cryptography, how does the use of two keys effectively reduce the key management problem compared to symmetric encryption? Explain the practical implications of this approach in terms of key proliferation and user convenience.	(3)
2C)	Evaluate the relative strengths and weaknesses of AES (Advanced Encryption System) compared to the DES (Data Encryption Standard) algorithm.	(2)
3A)	Malicious web contents are root cause for the various attacks on the web. Analyze the relevance and applicability of five such web contents. Provide examples of their significance in the context of current security challenges.	(5)
3B)	Compare ethical hacking Tools with their usage in operation	(3)
3C)	Classify distinct categories of harm caused by DNS poisoning and Session hijacking.	(2)
4A)	Explain the intricate structure of a layered operating system, providing a comprehensive breakdown of the sequential stages that characterize the loading process? Unravel the inherent complexity within the layers, offering an in-depth exploration of their interplay. Furthermore, articulate a meticulous step-by-step progression, outlining the systematic and staged manner in which the operating system undergoes loading.	(5)
4B)	Consider a digital signature system that uses a public key cryptosystem, such as RSA or DSA. The system works as follows: i) The sender generates a digital signature for the message using their private key. ii) The sender sends the message and the digital signature to the receiver. iii) The receiver verifies the digital signature using the sender's public key. Suppose that an attacker has access to a large number of message-signature pairs from the system. The attacker uses this information to train a machine learning model to generate fake	(3)

digital signatures. The attacker can then use these fake digital signatures to sign and send malicious messages that appear to be from legitimate users.
Explain how can the digital signature system be modified to protect against this attack by providing detailed analysis?

4C) Analyse the following smishing message and identify the key elements that make it effective: (2)

Sender: [Bank Name]
Message:

[Customer Name],

Your account has been suspended due to suspicious activity. To verify your identity and reactivate your account, please reply to this message with your full name, date of birth, and Social Security number.

Thank you for your cooperation.

[Bank Name] Security Team

5A) Cyberterrorism is considered by some defence analysts to be a larger threat than traditional terrorism. Justify this statement with real time example. What do you understand by Cyberterrorism? Explain the cyber threats which India is vulnerable to and bring out the state of the country's preparedness to deal with the same. (5)

5B) A company is developing a new facial recognition technology that can be used to identify and track individuals in real time. The company claims that the technology can be used to improve public safety by preventing crime and terrorism. However, there are also concerns about the potential for the technology to be misused to track and monitor individuals without their consent. (3)

Analyse the ethical and legal implications of the company's new facial recognition technology. Consider the following questions:

Explain potential benefits and risks of the technology?
How can the technology be used to improve public safety without violating individual privacy?
What laws and regulations should be in place to govern the use of facial recognition technology?

5C) Analyse the role of Risk Analysis in cybersecurity and delve into its complexities. Identify three key factors that contribute to the challenges of conducting a thorough cyber risk analysis. (2)

-----End-----