Reg. No. : | | | | | | | | | | | | |

Question Paper Code : 10509

M.E./M.Tech. DEGREE EXAMINATIONS, APRIL/MAY 2019.

Second Semester

Computer Science and Engineering

CP 5291 – SECURITY PRACTICES

(Common to M.E. Mobile and Pervasive Computing/M.E. Software Engineering)

(Regulation 2017)

Time : Three hours Maximum : 100 marks

Answer ALL questions.

PART A — (10 × 2 = 20 marks)

1. Define Cryptography.
2. How intrusion detection system works?
3. How security is ensured in wireless network?
4. What is meant by Internet Security?
5. State policy driven system management.
6. List the information security essentials for IT managers.
7. Define cyber forensics and how it is different from cyber crime?
8. Write the purpose of key establishment protocols.
9. List out the privacy enhancing technologies.
10. What is meant by Risk Management?

PART B — (5 × 13 = 65 marks)

11. (a) Explain briefly about Fault tolerance and Resilience in cloud computing environments.

Or

(b) Discuss in detail about the security issues in web application and web services.

12. (a) Explain the architecture of wireless network security with its applications.

Or

(b) Explain how secure communication is ensured in optical network security systems.

13. (a) Describe in detail about the importance of identity and user management system.

Or

(b) Explain the methodologies used in intrusion detection and prevention system.

14. (a) Write short notes on :

(i) Security e-Discovery (6)

(ii) Satellite Encryption. (7)

Or

(b) Explain the various authentication protocols used in computer fraud detection and cyber forensics.

15. (a) Describe the security and privacy principles to be followed in environment monitoring system.

Or

(b) Explain briefly about Storage Area Network security devices with its applications.

PART C — (1 × 15 = 15 marks)

16. (a) The assistant manager (the complainant) with the fraud control unit of a large business process outsourcing (BPO) organization filed a complaint alleging that two of its employees had conspired with a credit card holder to manipulate the credit limit and as a result cheated the company of INR 0.72 million. The BPO facility had about 350 employees. Their primary function was to issue the bank's credit cards as well as attend to customer and merchant queries. Each employee was assigned to a specific task and was only allowed to access the computer system for that specific task. The employees were not allowed to make any changes in the credit-card holder's account unless they received specific approvals. Each of the employees was given a unique individual password. In case they entered an incorrect password three consecutive times then their password would get blocked and they would be issued a temporary password. The company suspected that its employees conspired with the son (holding an add-on card) of one of the credit card holders. The modus

operandi suspected by the client is as follows. The BPO employee deliberately keyed in the wrong password three consecutive times (so that his password would get blocked) and obtained a temporary password to access the computer system. He manually reversed the transactions of the card so that it appeared that payment for the transaction has taken place. The suspect also changed the credit card holder's address so that the statement of account would never be delivered to the primary card holder.

For the above given forensic case, Identify the problem, security issues, investigation team and investigation strategy, evidences and preventive measure for future.

Or

(b) Discuss in detail about the various types of attacks occur in LAN, Intranet and Internet, and also write the procedure to mitigate those attacks.
