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

Question Paper Code : 80330

M.C.A. DEGREE EXAMINATION, AUGUST 2015

Elective

DMC 1977 – INFORMATION SECURITY

(Regulation 2009)

Time : Three hours Maximum : 100 marks

Answer ALL questions.

PART A — (10 × 2 = 20 marks)

1. If the C.I.A. triangle is incomplete why is it so commonly used in security?

2. Differentiate between attack and threat.

3. Write the expression to calculate the single loss expectancy.

4. Differentiate between Quantatitive with Qualitative Risk Control Practices.

5. State the uses of VISA International model.

6. When is the DR plan used?

7. What is RADIUS? What advantage does it have over TACACS?

8. State the functions of Port Scanners.

9. Find the 'n' and $\phi(n)$ value in RSA if P = 7 and Q = 17.

10. List any four physical security devices.

PART B — (5 × 16 = 80 marks)

11. (a) (i) Identify the six components of an information system. Which are most directly affected by the study of computer security? Illustrate with an example. (8)

(ii) Why is the top-down approach to information security superior to the bottom-up approach? (8)

Or

(b) (i) Has the implementation of networking technology created more or less risk for businesses that use information technology? Why? Explain. (8)

(ii) What is intellectual Property (IP)? Is it afforded the same protection in every country of the world? What laws currently protect it in the United States and Europe? (8)

12. (a) (i) Discuss in detail about the strategies used for controlling the risk. (8)

(ii) Explain the different planning approaches to mitigate the risk. (8)

Or

(b) (i) How is an incident response plan different from a disaster recovery plan? (8)

(ii) What is risk appetite? Explain why risk appetite varies from organization to organization. (8)

13. (a) Design the ISO 17799 for an automobile organization. (16)

Or

(b) (i) What is contingency planning'? How is it different from routine management planning? What are the components of contingency planning? (8)

(ii) Discuss the elements of a business impact analysis. (8)

14. (a) (i) Describe how the various types of firewalls interact with the network traffic at various levels of the OSI model. (8)

(ii) How does a false positive alarm differ from a false negative one? From a security perspective, which is least desirable? (8)

Or

(b) (i) How does a network-based IDPS differ from a host-based IDPS? (8)

(ii) Discuss in detail about any two tools used for scanning and analyzing the assert. (8)

15. (a) (i) Which security protocols are predominantly used in Web-based electronic commerce? (8)

(ii) List and describe the four categories of locks. In which situation is each type of lock preferred? (8)

Or

(b) (i) What is a work breakdown structure (WBS)? Is it the only way to organize a project plan'? Explain. (8)

(ii) List and describe the options available for the location of the information security functions within the organization. Discuss the advantages and disadvantages of each option. (8)

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

Question Paper Code : 22332

M.C.A. DEGREE EXAMINATION, FEBRUARY/MARCH 2015.

ELECTIVE

DMC 1977 — INFORMATION SECURITY

(Regulations 2009)

Time : Three hours Maximum : 100 marks

Answer ALL questions.

PART A — (10 × 2 = 20 marks)

1. Write the four important functions performed by Information security for an organization.

2. List out the various components of an information system.

3. Define risk management.

4. Describe residual risk with figure.

5. What are the NIST documents which can assist in the design of a security framework?

6. Prepare a list for security education and training programs and see which category has the most examples. Which do you think would be more cost-effective in terms of both time and money?

7. Illustrate mantraps.

8. Describe the different ways in which smoke detectors are operating.

9. Define steganography. What is the importance in using Steganography tools?

10. List out the internal control strategies with respect to personal security.

PART B — (5 × 16 = 80 marks)

11. (a) What are the approaches used for information security? Explain in detail the System development life cycle. (16)

Or

(b) Explain the legal, ethical and professional issues related to information security. (16)

12. (a) Illustrate in detail risk control strategies. (16)

Or

(b) What are the components of Risk management? Explain each in detail. (16)

13. (a) Describe in detail the designing of new security architecture. (16)

Or

(b) (i) Define security blueprint. Explain the necessity of the security framework. (4)

(ii) Describe with figure the continuity strategies needed for information security. (12)

14. (a) Define firewall. What are its different types? Explain the working of each in detail. (16)

Or

(b) Write a note on the following

(i) Honey pots, Honey nets (4)

(ii) Padded cell systems (4)

(iii) Trap and trace systems (4)

(iv) Actine intrusion prevention. (4)

15. (a) Explain with example the various classical encryption schemes. (16)

Or

(b) (i) Perform the encryption and decryption using RSA algorithm for the following data.

P=7, Q=11, e=17, m=8. (8)

(ii) Discuss any three cryptographic tools and their significance in information security. (8)

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

Question Paper Code : 96330

M.C.A. DEGREE EXAMINATION, FEBRUARY/MARCH 2014.

Elective

DMC 1977 — INFORMATION SECURITY

(Regulations 2009)

Time : Three hours Maximum : 100 marks

Answer ALL questions.

PART A — (10 × 2 = 20 marks)

1. "Internetwork security is both fascinating and complex" - Justify the statement.

2. Identify the six components of an information system.

3. List the general categories of unethical and illegal behavior.

4. What are the threats to Information security?

5. Define security policy.

6. Mention the drawbacks of ISO 17799/B5 7799.

7. Define the padded cell in Honey Pot.

8. What are the detection methods used by IDS?

9. Define the two types of locks.

10. What are the controls used in secure facility?

PART B — (5 × 16 = 80 marks)

11. (a) Explain why a successful information security program is responsible for both an organization's general management and IT management. (16)

Or

(b) How the same phases used in the traditional SDLC can be adapted to support the implementation of an information security project? Give the detailed analysis. (16)

12. (a) What is risk management? Why is the identification of risks, by listing their assets and their vulnerabilities, so important to the risk management process? (16)

Or

(b) (i) Explain the process of vulnerability identification and assessment for different threats faced by an information security system. (10)

(ii) What value does an automated asset inventory system have for the risk identification process? (6)

13. (a) Describe what an information security blueprint is, identify its major components, and explain how it supports the information security program. (16)

Or

(b) Explain the major steps in Contingency Planning. (16)

14. (a) What is the significance of audit records in intrusion detection? Explain the various fields of an audit record. (16)

Or

(b) (i) Taking your own packet filtering rule set, explain the working packet-filtering router. (8)

(ii) "One way to secure against Trojan horse attacks is the use of a secure, trusted OS". Explain. (8)

15. (a) Alice and Bob wish to share private messages, where each of them of two separate keys generated. What kind of strategy would you suggest to ensure confidentiality, key management and authentication for the conversation between Alice and Bob? Explain the strategy and also highlight the design issues related to the strategy proposed. (16)

Or

(b) Explain clearly with relevant illustration how authentication is addressed in PGP. (16)

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

Question Paper Code : 86330

M.C.A. DEGREE EXAMINATION, AUGUST 2013.

Elective

DMC 1977 — INFORMATION SECURITY

(Regulation 2009)

Time : Three hours Maximum : 100 marks

Answer ALL questions.

PART A — (10 × 2 = 20 marks)

1. Explain the basic components of information security.
2. Differentiate between laws and ethics.
3. List some of the asset attributes.
4. What value does an automated asset inventory system have for the risk identification process?
5. Define ISO 17799/BS 7799 standards and their drawbacks.
6. What are the three types of security policies?
7. What are the measures that may be used for intrusion detection?
8. How firewalls are categorized by processing mode?
9. List few applications of steganography.
10. List some of the drawbacks in electronic monitoring.

PART B — (5 × 16 = 80 marks)

11. (a) Enumerate the phases of security systems development life cycle.

Or

(b) "Information security is a major concern for the software industry today as the number of internal threats is nearly 80%" – Discuss on the statement, highlighting the various security attacks.

12. (a) What is risk management? Why is the identification of risks by listing their assets and their vulnerabilities so important to the risk management process? Explain.

Or

(b) Identify the existing conceptual frameworks for evaluating risk controls and formulate a cost benefit analysis.

13. (a) What is an information security blueprint? Identify its major components and explain how it supports the information security program.

Or

(b) Explain VISA international security model in detail.

14. (a) With neat diagrams highlight the differences between screened host firewall single homed bastion and screened host firewall dual homed bastion.

Or

(b) How scanning and analysis tools are useful in enforcing information security? Explain the different types of the scanning and analysis tools.

15. (a) With suitable sketches, explain the working of DES algorithm.

Or

(b) What is the contribution of phil Zimmerman towards creation of PGP? Also explain reasons for the popularity of PGP.

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

Question Paper Code : 86330

M.C.A. DEGREE EXAMINATION, FEBRUARY/MARCH 2013.

Elective

DMC 1977 — INFORMATION SECURITY

(Regulation 2009)

Time : Three hours Maximum : 100 marks

Answer ALL questions.

PART A — (10 × 2 = 20 marks)

1. What are the characteristics of information?

2. What is the need for security?

3. What is risk management?

4. What are the types of access controls?

5. Define policy.

6. What are the advantages of VISA international security model?

7. Define firewall.

8. What do you mean by intrusion detection system?

9. What is cryptoanalysis?

10. What are major sources of physical loss?

PART B — (5 × 16 = 80 marks)

11. (a) (i) Describe the NSTISSC security model. (8)

(ii) Explain the various phases of security SDLC. (8)

Or

(b) (i) Discuss the components of an information systems. (8)

(ii) Describe the various categories of threats to information. (8)

12. (a) (i) Explain the risk identification process in detail. (8)

(ii) Elaborate on risk assessment and the documentation of its results. (8)

Or

(b) (i) Describe the asset identification and valuation with example. (8)

(ii) Explain the risk controlling strategies in detail. (8)

13. (a) (i) Explain the different types information security policies. (8)

(ii) Explain the features of NIST security model. (8)

Or

(b) (i) Explain briefly about the ISO 17799/BS7799 model. List its limitations. (8)

(ii) Describe the components used in design of security architecture. (8)

14. (a) (i) Discuss the various generations of firewalls. (8)

(ii) Explain the different types of intrusion detection system. (8)

Or

(b) (i) Explain the different types of firewall systems in detail. (8)

(ii) Explain how scanning and analysis tools are useful in enforcing information security. (8)

15. (a) (i) Explain the components of cryptology. (8)

(ii) Describe the various methods of power management and conditioning. (8)

Or

(b) (i) Describe the various access control devices. (8)

(ii) Discuss the security considerations for nonemployees. (8)

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

Question Paper Code : 76514

M.C.A. DEGREE EXAMINATION, AUGUST 2012.

Elective

DMC 1635 — INFORMATION SECURITY

(Regulation 2007)

Time : Three hours Maximum : 100 marks

Answer ALL questions.

PART A — (10 × 2 = 20 marks)

1. Distinguish between direct attacks and indirect attacks.

2. What is the best method for preventing an illegal or unethical activity? Mention the three conditions that should be present in order to apply this method.

3. Information asset "X" has a value score of 100 and has two vulnerabilities : Vulnerability 1 has a likelihood of 0.5 with a current control that addresses 50% of its risk; Vulnerability 2 has a likelihood of 0.1 with no current controls. Assume that assumptions and data are 80% accurate. ***Calculate the ranked list of risk ratings for the two vulnerabilities.***

4. What is risk management?

5. Mention the limitations of Intrusion Detection Systems (IDS).

6. How does remote journaling differ from electronic vaulting?

7. What are the three types of VPN technologies defined by VPNC?

8. What is a port scanner?

9. Encrypt the text "***CHANGE IN PLAN MEET ME AT DAWN***" using Caesar cipher.

10. Enumerate the functions of a Chief Information Security Officer (CISO).

PART B — (5 × 16 = 80 marks)

11. (a) (i) Compare and contrast SDLC with SecSDLC. (8)

(ii) What is meant by an attack? How does it differ from vulnerability and briefly explain about back doors, Brute Force attacks, DoS and DDoS? (8)

Or

(b) (i) List the ten commandments of computer ethics and explain about Association of Computing Machinery. (8)

(ii) Define threat. List the general categories of threats with examples and explain about any two types of threats. (8)

12. (a) (i) Explain about G-P information classification scheme that helped companies to achieve confidentiality and integrity of information. (8)

(ii) Give a brief description about Access Controls. (8)

Or

(b) (i) Give a brief summary about the four basic Risk Control strategies. (8)

(ii) Give a brief account about Cost Benefit Analysis. (8)

13. (a) Explain in detail about Incident Response Planning. (16)

Or

(b) (i) Enumerate the key technology components of an Information Security Architecture. (8)

(ii) Briefly explain about NIST models. (8)

14. (a) (i) How can a firewall be categorized based on its processing mode? (8)

(ii) Write short note on Packet Sniffers, Honey pots and Honey nets. (8)

Or

(b) Explain in detail about Network based IDS and Host based IDS. (16)

15. (a) (i) Give a brief account about some of the important employment policies and practices. (8)

(ii) List the controls used for enforcing physical security and explain about any four physical security controls. (8)

Or

(b) The values of public key and private key are (N, E) = (33, 3) and (N, D) = (33, 7). Use RSA algorithm to encrypt the word ***"TECHNOLOGY"*** and also show how the Word can be decrypted from its encrypted form. (16)

———————

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

Question Paper Code : 87530

M.C.A. DEGREE EXAMINATION, FEBRUARY 2012.

Elective

DMC 1977– INFORMATION SECURITY

(Regulation 2009)

Time : Three hours Maximum : 100 marks

Answer ALL questions.

PART A — (10 × 2 = 20 marks)

1. Name three of the four functions that information security performs for an organization.

2. What are the various types of malware? How does it differ from viruses?

3. What are the three categories of unethical or illegal behaviour?

4. How will you determine the overall lost potential per risk (ALE)?

5. How will you express the residual risk?

6. Name two problems associated with benchmarking.

7. Mention the components of the sphere of security.

8. When does an incident become disaster?

9. What is the role of Proxy server in the information security?

10. What is DMZ? Mention its role in security architecture.

PART B — (5 × 16 = 80 marks)

11. (a) (i) Draw the major steps involved in contingency planning. (4)

(ii) Name the primary functions of IRP, DRP and BCP. (4)

(iii) What are the five testing strategies in the IR plan? Give a brief description of each. (8)

Or

(b) Explain the phases in Sec DLC model. Discuss briefly about salient steps which makes security development life cycle model unique from the software development life cycle model.

12. (a) Discuss each of the major types of attack used against controlled system. Among the major attack which are more common attacks in your organization. State the reason.

Or

(b) Explain the methods to assess and control the risk.

13. (a) Once the project team for information security development has created the ranked vulnerability worksheet, the team must choose one of four basic strategies to control the risks that result from these vulnerabilities. What are the four strategies?

Or

(b) As you might expect, the U.S. military classification scheme has a more complex categorization system than required by most corporations. Briefly describe each of the levels of classification.

14. (a) (i) Which are the most common implementations of firewall architecture? Write short notes on each implementation. (10)

(ii) Explain the factors that need to be considered while you configure the firewall for your organization. (6)

Or

(b) (i) What is RADIUS? What advantage does it have over TACACS? (6)

(ii) Describe about the Intrusion Detection System (IDS) and their approaches in protecting network and host information assets. (10)

15. (a) (i) Explain the protocols used to provide secured communication. (8)

(ii) Write a short notes on Public Key Infrastructure (PKI).

Or

(b) What are the four issues that can be addressed when considering access control devices? Give two examples of each area of authentication.

———————