Avinashilingam Institute for Home Science and Higher Education for Women
(Deemed to be University) Coimbatore-641043.

Master's Degree Examination – November 2018
III Semester

Class : II PG **Time: 3 hours**
Major : MBA-IT Organisation Administration **Max. Marks: 60**

17MBMC21S Functional Specialisation II.P.I Information Security and Audit Control

Part A **10 x 1/2 = 5**
Choose the correct answer

1. _____ is a weakness which allows an attacker to reduce a system's information assurance.

   a. Security b. Vulnerability c. Eavesdropping d. Spoofing

2. _____ is the act of surreptitiously listening to a private conversation, typically between hosts on a network.

   a. Firewall b. Cryptography c. Tampering d. Eavesdropping

3. ____ is placeholder information associated with a single use of a program that can handle multiple concurrent users.

   a. Treats b. Network c. Hacking d. Attacks

4. A predetermined attack against a computer system, computer data, programs and other information is called as_____

   a. Cyber crime b. Cyber Terrorism c. Ethical Hacking d. Security issues

5. A possibility of suffering from loss in software development process is called _____

   a. Security risk b. Cyber risk c. Software risk c. Hardware risk

6. _____ is designed to provide strong authentication for client/server applications by using secret-key cryptography.

   a. Kerberos b. Pass code c. Public key d. Private key

7. The COBIT was first released in the year _____

   a. 1994 b. 1995 c. 1996 d. 1997

8. _____ is associated with the process of converting ordinary plain text into unintelligible text and vice-a-versa.

   a. Encryption b. Authentication c. Trojan d. Cryptography

9. _____ is the use of a computer to do something improper or illegal

   a.Computer abuse b. Computer hanging c. Computer forensics d. All the above

10. _____ are the moral guidelines that govern the use of computers and information systems

    a. Computer system b. Computer ethics

    c. Computer networking d. Computer technology

PART – B (5*4=20)

Answer ALL the following
Each answer should not exceed 200 Words or one page

11.a. What are the characteristics of information? Explain

(OR)

11.b. Write short notes on SDLC

12.a. What are the business needs for information security? Explain

(OR)

12.b. What are the causes of Cyber terrorism? Explain

13.a. Briefly explain the need for risk management in security analysis

(OR)

13.b. What are the risk control strategies in risk management of security analysis? Explain

14.a. What are the uses of Cryptography? Explain

(OR)

14.b. What are the biometric identification techniques? Explain

15.a. Briefly explain the various legal issues involved in information security system

(OR)

15.b. Write short notes on "The Self Hack Audit"

PART – C (5*7=35)

Answer the following
Each answer should not exceed 600 words or three pages

(Q 20 is Compulsory)

16.a.Describe the various security model components

(OR)

16.b. How to assess the security of computer systems? Explain

17.a. What are the reasons for software attacks? How to overcome such software attacks? Explain

(OR)

17.b. Discuss in details about various types of network security issues.

18.a. How to identify and assess the risk in security analysis? Explain

(OR)

18.b. Enumerate the procedure involved in implementing Kerberos in distributed systems

19.a. What are the policy standards for information security? Explain

(OR)

19.b. What are the methods of computer abuse? How to detect computer abuse? Explain

20.a. **Compulsory Question:**
Hacktivists (hacker activists) have threatened mass disruptions at major events to publicize or bring attention to their causes. Days before the opening ceremony at the London 2012 Summer Olympic Games, British security services warned Olympics authorities about the threat of a cyber attack on the stadium's power supply. Hacktivists have also threatened to hack into traffic control systems At major events, such as the 2014 FIFA World Cup, using vulnerabilities in traffic control systems that were recently published in two separate studies. The studies revealed that traffic control systems could be disrupted or rendered inoperable. One researcher used a remote -control drone and cheap programmable hardware to launch an attack on a traffic system and sent fake data to sensors –small wireless vehicle detection devices embedded in the ground

that transmit information about automobile location and movement. Traffic could be impacted if the sensors were wirelessly linked to traffic lights. The other research team showed that it was possible to break into the wireless communications of another system's traffic controllers because there were no passwords in use and no encryption used in the transmissions. Terrorists could exploit traffic control system vulnerabilities to direct traffic toward (or restrict it to) a planned attack location. While the products detailed in the studies are deployed primarily in the U.S., about 200,000 of the sensors in one system are in use worldwide –such as the UK , France, and Australia. Experts believe that many traffic infrastructure devices created by various vendors have similar security properties due to a lack of security consciousness in the traffic control systems field.

Questions:

a. How to increase the security of the traffic control system?
b. How to detect fake data sent to sensors of traffic control system?
c. Is it possible to block non-essential traffic information system?
d. Why sensors were wirelessly linked to traffic lights?
e. List out the traffic infrastructure devices used in the traffic control systems field.

***