UNIVERSITY OF GHANA

B.SC COMPUTER SCIENCE, SECOND SEMESTER EXAMINATIONS: 2014/2015

CSIT204: INFORMATION SECURITY (3 Credits)

INSTRUCTION:

*ANSWER **ALL** QUESTIONS IN SECTION A. ANSWER QUESTION **41** AND ANY OTHER TWO FROM SECTION B.*

TIME ALLOWED:

THREE (3) HOURS

SECTION A

Answer ALL the Questions in this Section: Each Question Carries 1 Mark [40 Marks]

1. The C.I.A. triad signifies

   A. Confidentiality, Integrity and Authentication

   B. Control, Integrity and Authentication

   C. Control, Integrity and Availability

   D. confidentiality, integrity, availability

2. When an employee transfers within an organization,

   A. the employee must undergo a new security review.

   B. the old system IDs must be disabled.

   C. all access permission should be reviewed.

   D. the employee must turn in all access devices

3. Which of the followings is an example of simple substitution algorithm?

   A. RSA

   B. DES

   C. Caesar cipher

   D. Blowfish

4. The practice of embedding a message in a document, image, video or sound recording so that its very existence is hidden is called?

   A. Anonymity.
   C. Shielding.
   B. Steganography.
   D. Data diddling.

5. The likelihood of a threat source taking advantage of vulnerability is referred to as…

   A. Vulnerability
   C. Risk
   B. Threat
   D. Exposure

6. An instance of being exposed to losses is referred to as …….

   A. Vulnerably
   C. Risk
   B. Threat
   D. Exposure

7. Risk analysis allows you to do all of the following except:

   A. Quantify the impact of potential risks and the cost of a countermeasure
   B. Create an economic balance between the impact of a risk
   C. Provides a cost/benefit comparison
   D. Prevent risk

8. A cipher that scrambles letters into different positions is referred to as what?

   A. Substitution
   C. Running key
   B. Stream
   D. Transposition

9. Cryptography does not concern itself with:

   A. Availability
   C. Integrity
   B. Authenticity
   D. Confidentiality

10. Which of the following includes the definition of procedures for emergency response?

   A. Operations Planning
   C. Business Continuity Planning
   B. Disaster Recovery Planning
   D. Backup Planning

11. The percentage of loss a realized threat could have on a certain asset is known as

A. Single loss expectancy (SLE)
B. Annualized rate of occurrence (ARO)
C. Exposure factor (EF)
D. Asset value (AV)

12. The estimated frequency a threat will occur within a year is known as the:

A. Single loss expectancy (SLE)
B. Annualized rate of occurrence (ARO)
C. Exposure factor (EF)
D. Asset value (AV)

13. Which of the following does a digital signature provide?

A. It provides the ability to encrypt an individual's confidential data.
B. It ensures an individual's privacy.
C. It identifies the source and verifies the integrity of data.
D. It provides a framework for law and procedures.

14. Which type of attack is based on the probability of two different messages using the same hash function producing a common message digest?

A. Statistical attack
B. Differential cryptanalysis
C. Differential linear cryptanalysis
D. Birthday attack

15. Which network topology offers the highest reliability and availability?

A. Bus
B. Star
C. Ring
D. Mesh

16. Which of the following is the correct calculation?

A. Asset value (%) x exposure factor (%) = single loss expectancy (%)
B. Asset value ($) x exposure factor (%) = single loss expectancy ($)
C. Asset value (%) x exposure factor ($) = single loss expectancy ($)
D. Asset value ($) x exposure factor ($) = single loss expectancy ($)

17. As an information systems security professional, what is the highest amount would you recommend to a corporation to invest annually on a countermeasure for protecting their assets valued at $1 million from a potential threat that has an annualized rate of occurrence (ARO) of once every two years and an exposure factor (EF) of 10% :

    A. $100,000.
    C. $500,000.
    B. $20,000.
    D. $50,000.

18. A risk is the likelihood of a threat source taking advantage of a vulnerability to an information system. Risks left over after implementing safeguards is known as:

    A. Leftover risks.
    C. Remaining risks.
    B. Residual risks.
    D. Exposures

19. The SETA program consists of three elements. These are

    A. Security Education, Security Policy Development, and Security Awareness.
    C. Security Education, Security Training, and Security Awareness.
    B. Security Education, Security Training and Risk Management
    D. Risk Management, Information Protection, and Security Awareness

20. Which type of law encompasses family law, commercial law, and labor law, and regulates the relationship between individuals and organizations?

    A. Private Law
    C. Public Law
    B. Commercial Law
    D. Civil Law

21. In a typical information security program, what is the primary responsibility of information (data) owner?

    A. Ensure the validity and accuracy of data.
    C. Monitor and audit system users.
    B. Determine the information sensitivity or classification level.
    D. Ensure availability of data.

22. Which choice below is an accurate statement about standards?

A. Standards are the high-level statements made by senior management in support of information systems security.

B. Standards are the first element created in an effective security policy program.

C. Standards are used to describe how policies will be implemented within an organization.

D. Standards are senior management's directives to create a computer security program.

23. A SOCKS firewall implementation can be classified as which type of firewall?

A. Stateless filtering

B. Stateful filtering

C. Circuit-level

D. Application-level

24. Which of the following is a "Class A" fire?

A. Halon

B. Electrical

C. Common combustibles

D. Liquid

25. Which of the following statement is most accurate of digital signature?

A. It allows the recipient of data to prove the source and integrity of data.

B. It can be used as a signature system and a cryptosystem.

C. It is a method used to encrypt confidential data.

D. It is the art of transferring handwritten signature to electronic media.

26. Who is generally responsible for computer system security?

A. everyone in the organization.

B. corporate management.

C. the corporate security staff.

D. everyone with computer access

27. Privacy laws generally include which of the following provisions:

A. Individuals have the right to remove data that they do not wish disclosed.

B. Government agencies must ensure that their data is accurate.

C. Government agencies must provide access to all other government agencies.

D. Government agencies may not use data for a purpose other than that for which it was initially collected.

28. Differentiate between a computer virus and a worm.
29. What is intellectual property?
30. Explain “Dumpster Diving” with respect to Information Security.
31. How does Disaster Recovery Plan differ from Business Recovery Plan?
32. Differentiate between Digital Certificates from Digital Signatures.
33. Explain the Clean Desk Policy.
34. Data categorization must be comprehensive and mutually exclusive. Explain these concepts.
35. Explain Redundancy with respect to Design of Security Architecture.
36. What is meant by security perimeter?
37. How is DMZ different from Firewall?
38. What is meant by Link Encryption?
39. Differentiate Steganography from Encryption.
40. An attack in which the attacker eavesdrops on the victim’s session and uses statistical analysis of patterns and inter-keystroke timings to discern sensitive session information is referred to as …….

SECTION B

Answer Question 1 and any other two questions this section [50 Marks]

41. a. Charlie Moody called the meeting to order. The conference room was full of developers, systems analysts, and IT managers, as well as staff and management from sales and other departments.

“All right everyone, let’s get started. Welcome to the kick-off meeting of our new project team, the Sequential Label and Supply Information Security Task Force. We’re here today to talk about our objectives and to review the initial work plan.”

"Why is my department here?" asked the manager of sales. "Isn't security a problem for the IT department?"

Charlie explained, "Well, we used to think so, but we've come to realize that information security is about managing the risk of using information, which involves almost everyone in the company. In order to make our systems more secure, we need the participation of representatives from all departments."

Charlie continued, "I hope everyone read the packets we sent out last week describing the legal requirements we face in our industry and the background articles on threats and attacks. Today we'll begin the process of identifying and classifying all of the information technology risks that face our organization. This includes everything from fires and floods that could disrupt our business to hackers who might try to steal or destroy our data. Once we identify and classify the risks facing our assets, we can discuss how to reduce or eliminate these risks by establishing controls. Which controls we actually apply will depend on the costs and benefits of each control."

"Wow, Charlie!" said Amy Windahl from the back of the room. "I'm sure we need to do it— I was hit by the last attack, just as everyone here was—but we have hundreds of systems."

"It's more like thousands," said Charlie. "That's why we have so many people on this team, and why the team includes members of every department."

Charlie continued, "Okay, everyone, please open your packets and take out the project plan with the work list showing teams, tasks, and schedules. Any questions before we start reviewing the work plan?"

As Charlie wrapped up the meeting, he ticked off a few key reminders for everyone involved in the asset identification project.

"Okay, everyone, before we finish, please remember that you should try to make your asset lists complete, but be sure to focus your attention on the more valuable assets first. Also, remember that we evaluate our assets based on business impact to profitability first, and then economic cost of replacement. Make sure you check with me about any questions that come up. We will schedule our next meeting in two weeks, so please have your draft inventories ready."

[Culled from Principles of Information Security, 4th Edition]

i. Did Charlie effectively organize the work before the meeting? Why or why not? Make a list of three important issues you think should be covered by the work plan. For each issue, provide a short explanation. [10marks]

ii. Do you think Charlie's response to the Sales Manager's question was adequate? Explain your stand point. [4marks]

iii. Do you think Charlie's suggestion of focusing on valuable assets and profitable assets in the last paragraph is justified? How would you identify such assets? [10 marks]

b. An Information asset K has a value score of 120 and has two vulnerabilities: Vulnerability 2 has a likelihood of 0.5 with a current control that addresses 20 percent of its risk; vulnerability 3 has a likelihood of 0.2 with no current controls. Your estimate indicates that assumptions and data are 80 percent accurate. Determine the risk of Asset K. [6marks]

42. a. With a clear sketch, explain the components of the System Development Life Cycle. [9 marks]

b. With Suitable examples, explain the characteristics of Information. [6marks]

43. a. Analyze the levels of control of the security architecture design process. [8 marks]

b. With suitable examples, explain the Plan-Do-Check-Act cycle of the ISMS [7marks]

44. a. Write Short notes on the physical security plans to detect and respond to fires and fire hazards. [5marks]

b. Explain the following briefly with examples:

i. Substitution Cipher [6marks]

ii. Transposition Cipher [4marks]