BRAINWARE UNIVERSITY

Term End Examination 2023
Programme – B.Tech.(CSE)-2019
Course Name – Security and Privacy of Data
Course Code - PEC801A
(Semester VIII)

Full Marks : 60 **Time : 2:30 Hours**

[The figure in the margin indicates full marks. Candidates are required to give their answers in their own words as far as practicable.]

Group-A

(Multiple Choice Type Question) 1 x 15=15

1. *Choose the correct alternative from the following :*

(i) Predict the limitation of the Digital Signature Algorithm (DSA):

a) It is slower than other digital signature mechanisms
b) It is less secure than other digital signature mechanisms
c) It requires a longer key size compared to other digital signature mechanisms
d) None of the above

(ii) Identify the type of attack that involves tricking a user into disclosing sensitive information:

a) DDoS attack
b) SQL injection
c) Social engineering
d) Sniffing

(iii) Choose the type of attack that involves gaining access to a system by pretending to be a legitimate user:

a) Social engineering
b) DDoS attack
c) SQL injection
d) Cross-site scripting

(iv) State that the Confidentiality is the protection of:

a) Data integrity
b) System availability
c) Data privacy
d) System performance

(v) Identify that Integrity is concerned with:

a) The availability of information
b) The accuracy and completeness of information
c) The protection of information from unauthorized access
d) The destruction of information

(vi) Predict the potential impact of a successful spear-phishing attack on an organization:

a) Improved employee productivity
b) Increased network speed
c) Loss of sensitive data
d) Improved customer satisfaction

(vii) Identify which of the following is not an example of an access control mechanism:

a) Usernames and passwords
b) Biometric authentication

c) Firewalls
d) Encryption

(viii) Choose the encryption mode that is the fastest to encrypt data:

a) Electronic Codebook (ECB)
b) Cipher Block Chaining (CBC)
c) Cipher Feedback (CFB)
d) Output Feedback (OFB)

(ix) Identifywhich of the following principles ensures that data remains accurate, complete, and consistent?

a) Confidentiality
b) Integrity
c) Availability
d) Availability

(x) Identify which of the following visualizations accurately represents the relationship between confidentiality, integrity, and availability?

a) A Venn diagram where each concept is represented by a circle, and the circles overlap in the center to show that all three concepts are interrelated.
b) A bar graph where each concept is represented by a different color, and the height of the bar represents the importance of each concept.
c) A pie chart where each concept is represented by a slice, and the size of the slice represents the amount of resources allocated to each concept.
d) A flowchart where each concept is represented by a different shape, and the arrows show the relationships between the concepts.

(xi) Cite the concept that refers to ensuring that data is accessible and usable only by authorized parties:

a) Confidentiality
b) Integrity
c) Availability
d) Authentication

(xii) Choose the digital signature mechanism that uses elliptic curve cryptography:

a) RSA
b) ElGamal
c) ECDSA
d) None of the above

(xiii) Trace the concept that involves keeping track of who has accessed or modified data:

a) Confidentiality
b) Integrity
c) Availability
d) Accountability

(xiv) Trace the concept that involves ensuring that data is not subject to unauthorized modification or deletion:

a) Confidentiality
b) Integrity
c) Availability
d) Backup

(xv) Identify the property of a hashing algorithm that makes it suitable for ensuring message integrity:

a) Collision resistance
b) Key distribution
c) Public key encryption
d) Symmetric key length

Group-B

(Short Answer Type Questions) 3 x 5=15

2. Apply digital signature mechanisms using public key cryptosystems. (3)
3. State the similarities and differences between confidentiality and integrity in the context of information security. (3)
4. Define the concept of data confidentiality and state how it can be ensured in an organization. (3)
5. Show how the following message would be encrypted using the Caesar cipher with a shift of 3: "HELLO WORLD". (3)
6. Classify encryption systems based on their key length. (3)

OR

Analyze the limitations of using symmetric key cryptography in securing large data. (3)

Group-C

(Long Answer Type Questions) 5 x 6=30

7. Explain the difference between symmetric and asymmetric key cryptography, and compare their strengths and limitations in the context of secure communication and data storage. (5)
8. Examine the use of hybrid encryption systems in securing large data sets, and evaluate the strengths and limitations of this approach. (5)
9. Distinguish between a Firewall and an IDS, and evaluate the strengths and weaknesses of each in protecting a computer network. (5)
10. Evaluate the effectiveness of a Firewall in preventing unauthorized access to a computer network, and justify the need for additional protection mechanisms such as an IDS and an IPS. (5)
11. Analyze all types of data protection strategies in security with example (5)
12. Express the importance of packet filtering in a firewall and provide examples of types of packets that should be filtered out. (5)

OR

Write a report on the common threats faced by computer networks and suggest strategies for mitigating these threats using firewall, IDS, and IPS. (5)

****