Batch - 1

__/__/____

Name - Akshat Negi
SapID - 500106533

Assignment - I T Data Security.

Section - A

Q1. Define data security. How do data security threats differ from vulnerabilities? Provide examples to support your explanation.

Ans 1. Data Security refers to the practices and technologies used to protect digital data from unauthorized access, corruption, or theft. It includes mechanisms like encryption, access controls, and regular audits to ensure the confidentiality, integrity and availability of data. It is crucial for protecting sensitive information such as personal data, financial records and intellectual property.
Threats and vulnerabilities are different concepts in cybersecurity:

- Threats are external or internal actions/events that could lead to data compromise. For example, malware attacks, phishing emails, or insider threats.
- Vulnerabilities are weaknesses or flaws in systems that can be exploited by threats. These include software bugs, misconfigured systems, or weak passwords.

Example:
A threat like SQL injection can exploit a vulnerability in a poorly coded database query. This leads to unauthorized data access or manipulation.

__/__/__

Q2. List and explain three types of cryptographic techniques and discuss how they mitigate threats in data security.

Ans2. Cryptographic techniques are critical for securing sensitive data and ensuring safe communication. Below are three major types:

1) Symmetric Key Cryptography:

- Uses a single key for both encryption and decryption.
- Example: Advanced Encryption Standard (AES).
- Mitigation: Prevents unauthorized access to sensitive information by requiring the key for decryption. Ideal for encrypting large amount of data, such as stored files.

2) Asymmetric Key Cryptography:

- Employs a pair of keys: a public key for encryption and a private key for decryption.
- Example: RSA (Rivest-Shamir-Adleman).
- Mitigation: Ensures secures & communication between parties who have never met, such as during HTTPS transactions.

3) Hashing:

- Converts input data into a fixed-length string (Hash).
- Example: SHA-256 (Secure Hash Algorithm).

__/__/____

- Mitigation: Protects data integrity by making it computationally infeasible to reverse or alter data without detection.

These techniques collectively address data breaches, unauthorized access and data tampering.

Q3. Discuss the importance of privacy laws and regulations in ensuring organizational safety. Provide examples of key laws such as GDRP or & CCPA.

Ans3. Privacy laws and regulations are essential for ensuring organizational handle personal data responsibly. They protect consumer rights, enhance trust, and reduce the risk of breaches or legal actions. Key benifits include:

- Data Governance: Regulations require organizations to implement strong data goverance practices.
- Consumer Confidence: By ensuring data security, organizations built trust with their users.
- Compliance and Penalties: Laws impose hefty penalties for non-compliance, encouraging better practices.

Examples:

- GDPR: (General Data Protection Regulation): Implemented in the EU, GDRP mandates organizations to obtain explicit user concent before processing personal data. It also grants user the right to request data deletion ("right to be forgotten").
- CCPA (California Consumer Privacy Act): Grants California residents the right to know what data is collected, opt-out of data sales and request data,

deletion.

In conclusion, these regulations play a vital role in fostering accountability and ensuring that businesses prioritize privacy and security.

Q4. Explain the concept of control volume and control mass in the context of cybersecurity frameworks. Why are they significant in defining security perimeters?

Ans4. In cybersecurity, control volume and control mass are conceptual models to define the scope of protection:

- Control Volume: Focuses on securing data flows and monitoring activity within a defined boundary. For example: protecting data packets traveling through a network firewall.
- Control Mass: Focuses on securing assets such as servers, devices or databases.

Significance in Cybersecurity Frameworks:

1. Improved Security: Defining these boundaries ensures targeted implementation of security measures, such as network monitoring and intrusion detection.
2. Granularity: Allows organizations to apply different security policies for distinct systems or zones.
3. Better Risk Management: Ensures that critical systems and sensitive data are prioritized in protection strategies.

For example: implementing control volume involves using intrusion detection systems (IDS) to monitor inbound/outbound traffic, while control mass might involve encryption of stored files.

Q5. Discuss the role of third-party technologies like identity management systems (IMS) or cloud access security brokers (CASB) in ensuring secure cloud operations.

Ans5. Third party technologies like Identity Management Systems (IMS) and Cloud Access Security Brokers (CASB) play crucial roles in securing cloud environments.

- Identity Management Systems (IMS): These systems are responsible for managing user identities and controlling access to resources in cloud environments. They ensure that only authorized users can access sensitive data and systems by enforcing policies like multi-factor authentication (MFA), role-based access control (RBAC) and single sign-on (SSO). IMS helps mitigate unauthorized access and insider threats by providing centralized user management. Example: A company uses an IMS to manage employee access to cloud storage, ensures that only users in certain roles can access specific documents.

- Cloud Access Security Brokers (CASB): CASBs act as intermediaries between users and cloud service providers, offering visibility and control

__/__/____

over cloud usage. They help monitor and enforce security policies for data protection, compliance and threat detection. CASBs can prevent data breaches, ensure compliance with regulations like GDPR and mitigate risks associated with shadow IT.

Example: A CASB can prevent users from uploading sensitive files to unapproved cloud platforms and enforce encryption for data in transit.

Together, IMS and CASB strengthen the security of cloud-based systems, ensuring that access to sensitive resources is managed effectively and that security policies are consistently enforced.

Section - B

Q6. Describe the evolution of data protection techniques, such as encryption, tokenization and secure multiparty computation. How have these adapted to modern threats?

Ans 6. The evolution of data protection techniques has been driven by the need to protect data against increasingly sophisticated cyber threats. Key advancements include:

- Encryption: Initially used for basic data protection, encryption has evolved from simple substitution ciphers to complex algorithms like AES (Advanced Encryption Standard). Modern encryption techniques ensure data confidentiality both in transit and at rest. With the rise of cloud computing and data breaches, encryption has become essential for protecting sensitive data, even when it is outside the organization's direct control.
- Tokenization: Tokenization replaces sensitive data with unique identifiers or "tokens," which are meaningless outside the context of the system. This approach helps protect data in payment systems and prevents exposure of sensitive information during transactions.

Modern Adaptions: In the context of cloud services, tokenization allows sensitive customer data to be stored securely while enabling analytics and business operations with anonymized data.

__/__/____

- Secure Multiparty Computation (SMC): SMC allows multiple parties to compute a result based on their private data without revealing their individual inputs. This technique is used for privacy-preserving computations and collaborations across untrusted environments.
Modern Adaptation: SMC is being used in industries like healthcare and finance for collaborative analysis of sensitive data, ensuring compliance with regulations like GDRP while maintaining privacy.

These techniques have adapted to modern threats by enabling data protection in distributed, cloud based environments and ensuring that sensitive information remains secure even in scenarios involving multiple parties or third party systems.

Q7. With examples, explain and analyze techniques used to counter threats in web applications, such as SQL Injection, XSS and CSRF.

Ans 7. Web applications are often targeted by attackers exploiting common vulnerabilities. Here are some techniques used to counter these threats:

- SQL Injection (SQLi): SQL injection occurs when attackers insert malicious SQL code into an application's input fields to manipulate the database.

__/__/____

Countermeasures:

- Prepared Statements / Parameterized Queries: These ensure that SQL queries are not directly constructed from user input, preventing code injection.
- Input Validation: Ensuring only expected data types are entered in user inputs reduces the chance of malicious code.

Example: Using Prepared Statement in Java prevents SQL injection by seperating the query structure from the user input.

- Cross-Site Scripting (XSS): XSS occurs when an attacker injects malicious scripts into web pages viewed by other users, typically through input fields or URLs.

Countermeasures:

- Output Encoding: Encoding output ensures that any injected scripts are rendered as text, not executable code.
- Content Security Policy (CSP): A CSP restricts the sources from which scripts can be loaded, prevented the execution of unauthorized scripts.

Example: Escaping special characters like < and > when displaying user input helps prevent XSS attacks.

- Cross-Site Request Forgery (CSRF): CSRF exploits the trust a site has in the user's browser, causing the user to unknowingly perform actions on a web application.

Countermeasures:

- Anti-CSRF Tokens: These unique tokens are added

to requests, and only valid tokens are accepted, ensuring requests originate from authenticated users.

- Same Site Cookies: This cookie attribute prevents the browser from sending cookies along with cross-site requests.

Example: Implementing CSRF tokens in forms ensures that every request made to the server is legitimate and not initiated by an attacker.

These techniques when combined, significantly reduce the risk of common attacks, making web applications more secure and resilient against exploitation.

Q8.

Sol. Given: $p = 7 \quad q = 11 \quad e = 3$

message $M = 15$

$$n = p \times q$$
$$= 7 \times 11$$
$$= 77$$

$$\phi(n) = (p-1) \times (q-1)$$
$$= 6 \times 10$$
$$= 60$$

$$3 \times d \equiv 1 \bmod 60 \quad 3 \times d \bmod 60 = 1$$

Using Euclidean Algorithm

GCD of 3 and 60 = 3

$d = 47$

__/__/____

$M = 5$

Encryption =

$C = M^e \bmod n$

$= 5^3 \bmod 77$

$= 125 \bmod 77$

$= 48 \rightarrow$ Encrypted text

Decryption =

$C = C^d \bmod n$

$= 48^{47} \bmod 77$

$= 5 \rightarrow$ Decrypted text

Q9.

Sol. Given: $P = 17$ $g = 3$

Party A's key = 5

Party B's key = 7

$A = g^a \bmod p$

$= 3^5 \bmod 17$

$= 243 \bmod 17$

$= 15$

$B = g^b \bmod p$

$= 3^7 \bmod 17$

$= 2187 \bmod 17$

$= 12$

Shared Secret Key

A's key

$S_A = 12^5 \bmod 17$

$= 248832 \bmod 17$

$= 6$

B's key

$S_B = 15^7 \bmod 17$

$= 6$

∴ Shared Secret Key = 6

Q10.

Sol. ECC

Curve Equation $= y^2 = x^3 + 5x + 7$

ECC Equation $= y^2 = x^3 + 5x + 7 \bmod 19$

$P = (6,3)$

$Q = (10,2)$

1) 2P

$$\lambda = \frac{3x^2 + a}{2y_1} \bmod p$$

$P = (6,3)$

$p = 19$

$$\lambda = \frac{3(6)^2 + 5}{2(3)} \bmod 19$$

$$= \frac{113}{6} \bmod 19$$

We need to compute the modular inverse of 6 modulo 19

$$\lambda = \frac{113 \times 16}{1} \bmod 19$$

$= 1808 \bmod 19$

$= 17$

New coordinates for 2P

$x_3 = \lambda^2 - 2x_1 \bmod p = (17)^2 - 2(6) \bmod 19$

$= 289 - 12 \bmod 19$

$277 \bmod 19 = 12$

$y_3 = \lambda(x_1 - x_3) - y_1 \bmod p$

$= 17(6-12) - 3 \bmod 19 = 7$ Thus, $(12,7) = 2P$