Tribhuvan University

Faculty of Humanities & Social Sciences

OFFICE OF THE DEAN

2021

Bachelor in Computer Applications

Course Title: Information Security
Code No: CACS459
Semester: VIII

Here are the **detailed answers with explanations and examples** for all the **Information Security questions** from the **2021 BCA exam**:

Group B

(Attempt any SIX questions) [6×5 = 30]

---

2. What is Information Security? List and briefly define fundamental security design principles. [1+4]

Definition of Information Security:

Information Security (InfoSec) is the practice of **protecting information** from unauthorized access, modification, disclosure, and destruction. It ensures the **CIA triad**:

- **Confidentiality:** Prevents unauthorized access to sensitive information.
- **Integrity:** Ensures data is accurate and cannot be modified without authorization.
- **Availability:** Ensures that information and resources are available when needed.

Fundamental Security Design Principles:

1. **Least Privilege:** Users should have **only** the necessary access rights to perform their tasks. Example: A junior employee in a company should not have access to financial records.
2. **Defense in Depth:** Security should be implemented in multiple layers, so if one fails, another can protect the system. Example: Using a firewall, antivirus, and encryption together.
3. **Fail-Safe Defaults:** Systems should deny access by default unless explicitly allowed. Example: A database that blocks all incoming connections unless permitted.

4. **Separation of Duties:** Critical tasks should be divided among multiple people to prevent fraud. Example: One employee approves transactions while another processes them.
5. **Open Design:** Security mechanisms should be based on well-tested cryptographic techniques instead of secrecy. Example: Open-source encryption protocols like AES and RSA.

---

3. Explain HMAC with its objectives. [1+4]

HMAC (Hash-based Message Authentication Code):

HMAC is a **cryptographic function** that ensures **data integrity and authentication** by combining a cryptographic **hash function (like SHA-256) and a secret key**.

Objectives of HMAC:

1. **Data Integrity:** Ensures that the message has not been **tampered with** during transmission.
    - Example: If someone modifies an online transaction, HMAC will detect the change.
2. **Authentication:** Verifies that the message is sent by an **authorized sender**.
    - Example: A bank uses HMAC to verify that an online transaction request is genuine.
3. **Resistance to Replay Attacks:** Prevents attackers from **reusing valid authentication codes** to resend fake messages.
    - Example: HMAC prevents hackers from resubmitting an old payment request.
4. **Keyed Hashing:** Uses a **secret key** to make it more secure than regular hashing.
    - Example: Even if an attacker knows the hash function, they cannot verify messages without the secret key.

---

4. What are the vulnerabilities of passwords? Explain different strategies used for the selection of effective passwords. [5]

Vulnerabilities of Passwords:

1. **Weak Passwords:** Easily guessable passwords like "123456" or "password" are insecure.
2. **Brute Force Attacks:** Hackers try multiple password combinations until they guess the right one.

3. **Phishing Attacks:** Users are tricked into revealing their passwords via fake emails or websites.
4. **Password Reuse:** Using the same password across multiple platforms increases risk.
5. **Shoulder Surfing:** Attackers observe users entering their passwords in public places.

Strategies for Effective Password Selection:

1. **Use Long & Complex Passwords:** Include uppercase, lowercase, numbers, and symbols.
    - Example: "aB!9@3xY$7K" is more secure than "password123".
2. **Enable Multi-Factor Authentication (MFA):** Adds an extra layer of security.
    - Example: Logging in requires both a password and a verification code sent to a mobile device.
3. **Avoid Dictionary Words:** Prevents dictionary attacks.
    - Example: Instead of "Sunflower123", use "S@1nF!o$wer7"
4. **Regularly Update Passwords:** Changes should be made periodically.
    - Example: Changing your online banking password every 3 months.
5. **Use a Password Manager:** Helps generate and store strong passwords securely.

---

5. Define access right. Explain the concept of trust framework. [2+3]

Access Right:

Access rights determine **who can access what resources** within a system. It defines **permissions** such as read, write, execute, or delete for users and groups.

- Example: A student may have "read" access to study materials, but only an admin can "edit" them.

Trust Framework:

A **trust framework** is a set of **rules and policies** that govern **identity verification, authentication, and data sharing** within an organization.
It consists of:

1. **Identity Providers (IdPs):** Entities that verify user identities (e.g., Google, Facebook Login).
2. **Service Providers (SPs):** Applications requiring authentication (e.g., Banking apps).

3. **Authentication Protocols:** Secure communication methods like **OAuth, SAML, and OpenID Connect**.

---

6. Describe honeypot with the types of honeypots that may be deployed. [1+4]

Honeypot:

A **honeypot** is a **decoy system** designed to **attract cyber attackers** and study their behavior.

Types of Honeypots:

1. **Low-Interaction Honeypots:** Simulate only basic services to capture attack attempts.
    - Example: A fake login page to track brute-force attacks.
2. **High-Interaction Honeypots:** Provide real operating system environments for deeper analysis.
    - Example: A fully functional web server that logs hacker activities.
3. **Pure Honeypots:** Fully operational production systems used for in-depth analysis.
4. **Client Honeypots:** Detect attacks targeting **client-side applications** like web browsers.

---

7. How can you say that Intrusion Detection System is the backbone of Information Security? Justify along with its categories. [5]

Intrusion Detection System (IDS) as a Backbone of InfoSec:

An **IDS** is essential for detecting **unauthorized access, malware, and network intrusions** in real-time.

Categories of IDS:

1. **Network-Based IDS (NIDS):** Monitors entire network traffic.
    - Example: Detects DoS attacks by analyzing traffic spikes.
2. **Host-Based IDS (HIDS):** Installed on computers to track system activities.
    - Example: Alerts administrators about unauthorized file changes.
3. **Signature-Based IDS:** Detects attacks based on **predefined attack patterns**.
    - Example: Identifies known malware signatures.
4. **Anomaly-Based IDS:** Uses AI to detect **unusual behavior**.

---

8. Explain the terms SSL, TSL, and handshake protocol. [5]

SSL (Secure Sockets Layer):

A cryptographic protocol that ensures **encrypted communication** between a web server and a browser.

TLS (Transport Layer Security):

An upgraded version of SSL with **stronger encryption** and **better security**.

Handshake Protocol:

Establishes a **secure connection** between two communicating parties by:

1. Verifying identities.
2. Exchanging encryption keys.
3. Starting secure communication.

- Example: When visiting https://www.google.com, your browser uses TLS to encrypt data.

Group C

(Attempt any TWO questions) [2×10 = 20]

---

9. Define the terms threats and attacks in terms of Information Security. Explain different types of security threats in detail.

Threats in Information Security:

A **threat** is any potential danger that can cause harm to an organization's **data, systems, or networks**. Threats can be **intentional (hackers, malware)** or **unintentional (accidental deletion, system failure)**.

Attacks in Information Security:

An **attack** is an actual attempt to **exploit vulnerabilities** in a system to **steal, modify, or destroy data**.

Types of Security Threats:

1. **Malware (Malicious Software):** Software designed to harm systems.
    - Example: Viruses, worms, trojans, ransomware.
2. **Phishing Attacks:** Attackers send fake emails to trick users into revealing sensitive information.
    - Example: A fake email from a "bank" asking for your password.

3. **Denial-of-Service (DoS) Attack:** Attackers overload a system with traffic, making it unavailable.
    - Example: A website crash due to a massive influx of fake requests.
4. **Man-in-the-Middle (MITM) Attack:** Hackers intercept communication between two parties.
    - Example: A hacker spying on a bank transaction using an unsecured Wi-Fi connection.
5. **SQL Injection:** Injecting malicious SQL commands into a database to extract sensitive information.
    - Example: Entering ' OR '1'='1' -- in a login field to bypass authentication.
6. **Insider Threats:** Employees misusing their access to steal or manipulate data.
    - Example: A disgruntled employee leaking confidential files.
7. **Zero-Day Attacks:** Exploiting unknown vulnerabilities before a fix is available.
    - Example: Hackers finding and using a bug in newly released software.

---

10. What is a cryptosystem? Explain the concepts of Vigenere and Rail Fence Ciphers in detail. [2+8]

Definition of Cryptosystem:

A **cryptosystem** is a set of cryptographic **algorithms, protocols, and keys** used for **secure communication and data protection**. It includes:

- **Plaintext:** Original message.
- **Ciphertext:** Encrypted message.
- **Encryption Algorithm:** Converts plaintext to ciphertext.
- **Decryption Algorithm:** Converts ciphertext back to plaintext.
- **Key:** A secret value used in encryption and decryption.

Vigenère Cipher:

A **polyalphabetic substitution cipher** that uses a **keyword** to encrypt messages.

Encryption Formula:

$C_i = (P_i + K_i) \mod 26$

Where **C** = Ciphertext, **P** = Plaintext, **K** = Key

Example:

- **Plaintext:** HELLO
- **Key:** KEY

- **Encryption:**
    - H + K → R
    - E + E → I
    - L + Y → J
    - L + K → V
    - O + E → S
- **Ciphertext: RIJVS**

Rail Fence Cipher:

A **transposition cipher** that rearranges letters into a rail-like pattern.

Example (3-rail system):

- **Plaintext:** ATTACKATDAWN
- **Rail Pattern:**

A C D W

T A K T A A

T A N

- **Ciphertext: ACDWTKTAATAN**

This makes decryption **more complex** for attackers without knowing the rail pattern.

---

11. What is a security audit? What is its importance? Explain the security auditing architecture in detail. [2+2+6]

Definition of Security Audit:

A **security audit** is a systematic evaluation of an **organization's security policies, processes, and controls** to ensure compliance and identify vulnerabilities.

Importance of Security Audits:

1. **Identifies Weaknesses:** Helps find vulnerabilities before attackers do.
2. **Ensures Compliance:** Meets industry standards (ISO 27001, GDPR).
3. **Prevents Data Breaches:** Strengthens defenses against cyber threats.
4. **Enhances Trust:** Clients and partners feel secure knowing the system is regularly audited.

Security Auditing Architecture:

1. **Audit Planning:**
    - Define objectives, scope, and audit policies.
2. **Data Collection:**
    - Gather logs, network traffic, and system access records.
3. **Analysis & Evaluation:**
    - Identify **security gaps** and detect anomalies.
4. **Reporting:**
    - Create an **audit report** with recommendations.
5. **Remediation:**
    - Implement security fixes and policy updates.
6. **Continuous Monitoring:**
    - Regular audits ensure **ongoing security compliance**.
