**CSC 321 SPECIAL EXAM REVISION**

**QUESTION ONE (COMPULSORY) [30 MARKS]**

**a) Discuss the reasons why security of a computer can never be absolute. [1 mark]**

**1. Evolving Threat Landscape:** Threats to computer systems constantly evolve as attackers develop new techniques and exploit vulnerabilities.

**2. Human Factor**: Human error, negligence, or malicious insider actions can compromise security measures.

**3. Complexity of Systems**: Modern computer systems are complex and interconnected, making it difficult to anticipate and mitigate all possible vulnerabilities.

**4. Resource Limitations:** Limited resources, such as time, budget, and expertise, constrain the implementation of comprehensive security measures.

**5. Zero-Day Vulnerabilities:** Unknown vulnerabilities or "zero-day" exploits can be exploited by attackers before security patches or updates are developed and deployed.

**b) Briefly explain the three main goals of information system security. [6 mark]**

**1. Confidentiality:** Ensuring that sensitive information is accessible only to authorized individuals or entities.

**2. Integrity:** Maintaining the accuracy and reliability of data and systems by preventing unauthorized modification or deletion.

**3. Availability**: Ensuring that information and resources are available and accessible to authorized users when needed, while mitigating disruptions and denial-of-service attacks.

**c) Explain how the following general types of threats affects computer system.**

**[6 marks]**

1. **Spoofing**

Spoofing involves masquerading as a trusted entity to gain unauthorized access or deceive users. This threat affects computer systems by undermining the authenticity of communication, leading to unauthorized access, data theft, or manipulation.

1. **Non-repudiation**

Non-repudiation ensures that parties cannot deny their actions or transactions. Its absence can lead to disputes over the validity of transactions, compromising the integrity and trustworthiness of the system.

**Denial of service**

Denial of service attacks disrupt legitimate access to resources or services by overwhelming the target system with a high volume of requests or malicious traffic. This threat affects computer systems by causing service downtime, loss of productivity, and reputational damage.

**d) An encryption scheme is unconditionally secure and computationally secure. Discuss**

**[4 Marks**

An encryption scheme that is unconditionally secure provides absolute protection against decryption, even with unlimited computational resources. However, such schemes are theoretical and often impractical due to key size requirements. On the other hand, a computationally secure encryption scheme is practical and provides security against decryption by any feasible computational means within a reasonable time frame, typically based on the computational complexity of mathematical problems like factoring large numbers or discrete logarithms.

**e) Passwords have been successfully providing security for computer systems for a long time. Discuss problems with passwords and discuss ways of improving passwords**

- **Brute Force Attacks:** Automated attempts to guess passwords by trying different combinations.

- **Social Engineering:** Manipulating individuals into revealing passwords through deception.

- **Password Reuse:** Using the same password across multiple accounts, increasing the risk if one account is compromised.

- **Weak Passwords:** Short, common, or easily guessable passwords.

**Ways to improve passwords include:**

- **Complexity Requirements:** Requiring a combination of uppercase, lowercase, numbers, and special characters.

- **Length Requirements:** Requiring longer passwords to increase complexity and resistance to brute force attacks.

- **Multi-Factor Authentication**: Adding an additional layer of security by requiring something the user knows (password) and something they have (e.g., a token or smartphone).

- **Password Managers:** Encouraging the use of password managers to generate and store complex, unique passwords for each account.

**f) Define the following terms.**

**[5 Marks**

1. **Computer security**

Computer Security: The protection of computer systems and data from unauthorized access, use, disclosure, disruption, modification, or destruction.

1. **Threat**

Threat: Any potential danger or risk to computer systems or data that could exploit vulnerabilities and cause harm.

1. **Vulnerability**

Weaknesses or flaws in computer systems or processes that could be exploited by threats to compromise the confidentiality, integrity, or availability of data or systems.

**g) What is intrusion detection?**

Intrusion detection is the process of monitoring and analyzing network or system activities for signs of unauthorized access, malicious activities, or security policy violations. It involves identifying abnormal patterns or behaviors that may indicate a security breach and triggering alerts or automated responses to mitigate the threat.

**QUESTION TWO [20 MARKS]**

**a) Your company is engaged in confidential negotiations with another company. In what ways could rivals use sniffing to get this commercially sensitive data? For each way say what you could do to minimize the risk.**

**[8 Marks]**

**1. Packet Sniffing:** Rivals could deploy packet sniffers to capture network traffic containing the confidential negotiations.

- To minimize this risk, encryption techniques such as Transport Layer Security (TLS) or Virtual Private Networks (VPNs) can be used to encrypt the data being transmitted, making it unreadable to anyone intercepting the traffic.

**2. Man-in-the-Middle (MITM) Attacks:** Attackers could position themselves between the communicating parties and intercept the data as it passes through.

- Implementing secure communication protocols and using digital certificates for authentication can help mitigate the risk of MITM attacks.

**3. Unauthorized Network Access:** Rivals could gain unauthorized access to the network infrastructure and deploy sniffing tools to capture data.

- Implementing strong network access controls, such as firewalls, intrusion detection systems, and access control lists, can help prevent unauthorized access to the network.

**4. Insider Threats**: Malicious insiders within the company or network could conduct sniffing attacks to leak confidential information.

- Implementing strict access controls, conducting regular security audits, and educating employees about the importance of data confidentiality can help mitigate the risk of insider threats.

**b) An Operating system (sometimes abbreviated as "OS") is the program that, after being initially loaded into the computer by a boot program, manages all the other programs in a computer. The other programs and I/O accessibility, it means that the OS can form first line defense in your computer.**

**Giving examples, discuss the following security provided by computer operating systems.**

**[8 Marks]**

1. **Discretionary access control (DAC)**

DAC allows users to control access permissions to their own resources. Examples include file system permissions in Windows and Unix-like operating systems, where users can set access permissions for files and directories.

1. **Mandatory access control (MAC)**

MAC enforces access controls based on security labels assigned to subjects and objects. An example is SELinux (Security-Enhanced Linux), where access decisions are based on security policies defined by system administrators, regardless of user settings.

**(iii)Role-based access control (RBAC)**

Role-Based Access Control (RBAC)\*\*: RBAC restricts access based on the roles that users hold within an organization. Examples include Active Directory in Windows environments and RBAC frameworks in Unix-like systems, where users are assigned roles with specific permissions.

**c.) Some people say security is inconvenient. From your own perspective discuss why this statement may be true. [4 Marks]**

- **Complexity:** Implementing and managing security measures often involves complex configurations and procedures that can be time-consuming and difficult to understand.

- **Restrictions:** Security measures, such as strong passwords, encryption, and access controls, can impose restrictions on users, making it more challenging to access and share information.

- **Additional Steps:** Security measures may require users to take additional steps, such as authentication processes or encryption/decryption procedures, which can slow down workflow and productivity.

- **Learning Curve:** Users may need to learn new security practices and technologies, which can be daunting and time-consuming.

- **False Positives:** Security measures may sometimes flag legitimate activities as security threats, leading to frustration and inconvenience for users.

**QUESTION THREE [20 MARKS]**

**a) With the aid of examples differentiate between a passive and active attack. [4 Marks]**

- **Passive Attack**: In a passive attack, the attacker eavesdrops on communication between two parties without altering the data. The goal is to gather information surreptitiously. For example, intercepting unencrypted network traffic to capture sensitive data, such as usernames and passwords.

- **Active Attack:** In an active attack, the attacker manipulates or alters data during transmission between two parties. The goal is to disrupt or modify the communication. For example, a man-in-the-middle attack where the attacker intercepts and modifies messages between a client and a server to impersonate one of the parties and steal sensitive information.

**b) Within the context of any application-to-application communication, there are some specific securities requirements including… Briefly explain them**

**(i) Authentication**

Authentication ensures that parties involved in communication are who they claim to be. This can be addressed through methods such as:

- Username and password authentication

- Two-factor authentication

- Public key infrastructure (PKI) for digital signatures and certificates

1. **Confidentially**

Confidentiality ensures that data exchanged between parties is protected from unauthorized access. This can be addressed through methods such as:

- Encryption techniques (e.g., AES, RSA) to scramble data so that only authorized parties can decrypt it

- Virtual Private Networks (VPNs) to create secure, encrypted tunnels for data transmission

**(iii)Integrity**

Integrity ensures that data remains unchanged and unaltered during transmission. This can be addressed through methods such as:

- **Hash functions** to generate checksums or hashes of data, which can be compared at the receiving end to verify integrity

- Message authentication codes (MACs) to create a cryptographic checksum that is appended to the message to detect tampering

**c) Explain three main models used to evaluate security of computer systems.**

**(4 Marks]**

**1. Bell-LaPadula Model:** This model focuses on confidentiality and access control, defining rules based on security levels (e.g., top secret, secret, confidential) and access permissions (e.g., read, write).

**2. Biba Integrity Model:** This model emphasizes integrity and prevents data from being modified by unauthorized users. It defines rules based on integrity levels (e.g., low, medium, high) and access permissions (e.g., read, write).

**3. Clark-Wilson Model:** This model focuses on integrity and emphasizes separation of duties and controlled access to data. It uses well-formed transaction rules to ensure that data is accessed and modified according to predefined constraints.

**d) Security policy is a very paramount component of any information system in an organization, list two personnel involved in design and formulation of security policies in an organization and state their roles.**

**[4 Marks]**

**1. Chief Information Security Officer (CISO**): The CISO is responsible for overseeing the organization's overall information security strategy and policies. Their role involves identifying security risks, implementing security measures, and ensuring compliance with regulations and industry standards.

**2. Security Policy Administrator:** The security policy administrator is responsible for developing, documenting, and enforcing security policies within the organization. Their role involves creating guidelines, procedures, and standards for information security, as well as ensuring that employees are aware of and adhere to these policies.

**QUESTION FOUR [20 MARKS]**

**a) Access control can be a policy, software or a hardware device which is used to allow or deny access to a resource. Discuss any three access control methods.**

**[9 Marks]**

**1. Discretionary Access Control (DAC):** DAC allows owners of resources to control access to those resources based on the identity and permissions of users and groups. Owners can grant or revoke access privileges at their discretion. For example, in Unix-like operating systems, file permissions (read, write, execute) are set by the file owner and can be modified using commands like chmod.

**2. Role-Based Access Control (RBAC):** RBAC assigns permissions to users based on their roles within an organization. Users are granted access based on their job functions or responsibilities, rather than their individual identities. For example, in a healthcare organization, doctors may have access to patient records, while receptionists may only have access to appointment scheduling systems.

**3. Mandatory Access Control (MAC):** MAC enforces access controls based on security labels assigned to subjects (users, processes) and objects (files, resources). Access decisions are determined by a central authority, typically based on security policies. For example, SELinux (Security-Enhanced Linux) enforces MAC policies by assigning security labels to files and processes and defining rules for access based on those labels.

**b) What is penetration testing? Discuss why it is important. [6 Marks]**

Penetration testing is a method of assessing the security of computer systems, networks, or applications by simulating real-world attacks. It involves authorized, controlled attempts to exploit vulnerabilities in a system to identify weaknesses and assess the effectiveness of existing security measures. Penetration testing is important for several reasons:

- **Identifying Vulnerabilities:** Penetration testing helps identify vulnerabilities and weaknesses in systems before they can be exploited by malicious attackers. This allows organizations to proactively address security issues and prevent potential breaches.

- **Assessing Security Posture:** Penetration testing provides insights into the overall security posture of an organization's systems, networks, and applications. It helps organizations understand their risk exposure and prioritize security investments and resources.

- **Compliance Requirements:** Many regulatory standards and compliance frameworks require organizations to perform regular penetration testing as part of their security assessment and audit processes. Compliance with these requirements helps organizations avoid fines, penalties, and reputational damage.

- **Improving Incident Response:** Penetration testing helps organizations improve their incident response capabilities by identifying potential attack vectors and weaknesses that could be exploited during a security incident. This allows organizations to develop and test incident response plans and procedures more effectively.

**c) Explain the following types of malicious software.**

**[5 Marks]**

1. **Trojans**

Trojans are malicious software programs that appear to be legitimate but perform unauthorized actions when executed. They often disguise themselves as benign or useful software to trick users into installing them. Once installed, Trojans can perform various malicious activities, such as stealing sensitive information, creating backdoors for remote access, or launching denial-of-service attacks.

1. **Logic bombs**

Logic bombs are pieces of code that are inserted into software systems to execute a malicious action when certain conditions are met. These conditions could be a specific date, time, or event triggered by the attacker. Once activated, logic bombs can perform destructive actions, such as deleting files, corrupting data, or disrupting system operations.

1. **Virus**

Viruses are self-replicating malicious programs that infect other files or systems by attaching themselves to host files or exploiting vulnerabilities. They can spread through various means, such as email attachments, infected websites, or removable storage devices. Once activated, viruses can modify, corrupt, or delete files, steal sensitive information, or disrupt system operations.

1. **Spyware**

Spyware is malicious software designed to secretly monitor and collect information about a user's activities without their consent. It can track keystrokes, capture screenshots, record web browsing habits, and collect personal or sensitive information. Spyware often operates stealthily in the background, making it difficult for users to detect and remove.

**QUESTION FIVE [20 MARKS]**

1. **A company is interested venturing into e-commerce in order to grow their market share. They have heard about the many risks and pitfalls inherent in this and have approached your security consulting firm for advice. Highlight five key threats the organization may face from attackers. [5 Marks]**

**1. Data Breaches:** Attackers may attempt to steal sensitive customer information, such as credit card numbers, personal details, or transaction records, through hacking, phishing, or malware attacks.

**2. Payment Fraud:** Attackers may exploit vulnerabilities in payment systems or conduct fraudulent transactions using stolen credit card information, leading to financial losses and reputational damage.

**3. Distributed Denial of Service (DDoS) Attacks:** Attackers may overwhelm the organization's e-commerce website or infrastructure with a flood of traffic, disrupting service availability and causing downtime for legitimate users.

**4. Phishing Attacks:** Attackers may use deceptive emails, fake websites, or social engineering techniques to trick customers or employees into disclosing sensitive information or credentials, which can be used for identity theft or further attacks.

**5. Website Defacement or Manipulation:** Attackers may deface the organization's website, inject malicious code, or manipulate content to spread misinformation, discredit the organization, or exploit visitors.

1. **What are five measures you would suggest the organization employ to counter these possible attacks? [5 Marks]**
2. **Implement Strong Encryption: Use** encryption protocols such as TLS (Transport Layer Security) to secure data transmission between customers and the e-commerce website, ensuring confidentiality and integrity of sensitive information.

**2. Deploy Multi-Factor Authentication (MFA):** Require customers and employees to authenticate using multiple factors such as passwords, biometrics, or one-time passcodes to enhance account security and prevent unauthorized access.

**3. Regular Security Patching**: Keep software, plugins, and systems up to date with the latest security patches and updates to mitigate vulnerabilities that attackers may exploit for unauthorized access or malware infections.

**4. Implement Web Application Firewalls (WAF): Deploy** WAF solutions to monitor and filter incoming web traffic, blocking malicious requests, SQL injections, cross-site scripting (XSS), and other common web application attacks.

**5. Employee Training and Awareness**: Provide regular training and awareness programs to educate employees and customers about cybersecurity best practices, phishing awareness, and how to recognize and respond to security threats effectively.

**c) Why are security audits and penetration testing done? Who would you recommend to do**

**this? Why?**

Security audits and penetration testing are conducted to assess the effectiveness of an organization's security controls, policies, and procedures, and to identify vulnerabilities and weaknesses in its systems, networks, and applications. Security audits provide a systematic review of security measures and compliance with regulations and standards, while penetration testing simulates real-world attacks to identify exploitable vulnerabilities.

I would recommend hiring specialized cybersecurity firms or consultants with expertise in security audits and penetration testing to perform these assessments. These firms typically have experienced security professionals with in-depth knowledge of attack techniques, tools, and methodologies, and can provide unbiased assessments and recommendations tailored to the organization's specific needs and risk profile.

**d) Briefly discuss several types of protection provided by firewalls. [5 Marks]**

**1. Packet Filtering:** Firewalls examine incoming and outgoing network packets based on predefined rules (such as IP addresses, ports, and protocols) and block or allow them accordingly to prevent unauthorized access and network attacks.

**2. Stateful Inspection:** Firewalls maintain state information about active connections and analyze the context of network traffic to make more informed decisions about allowing or blocking packets, enhancing security and performance.

**3. Application Layer Filtering:** Firewalls can inspect and filter traffic at the application layer (Layer 7 of the OSI model), allowing administrators to enforce more granular control over specific applications, protocols, or services to prevent application-level attacks and data leakage.

**4. Proxy Services:** Firewalls can act as proxies for outgoing connections, intercepting and inspecting traffic before forwarding it to the destination, allowing for content filtering, malware detection, and policy enforcement.

**5. Virtual Private Network (VPN) Support:** Firewalls can provide VPN services to establish secure encrypted tunnels for remote access or site-to-site communication, ensuring confidentiality and integrity of data transmitted over public networks.