Q1.

a) Ethical Scenario:

As an information security officer at a government agency, you hand sensitive information critical to national security. The agency has recently implemented a new information system to enhance efficiency in processing and storing classified data. As part of your responsibilities, you discover a potential vulnerability in the system that could be exploited by external actors, posing a significant threat to the confidentiality and integrity of the classified information. However, disclosing this vulnerability to the system developers and initiating the necessary updates would require temporarily shutting down the system. This shutdown, even if brief, could disrupt ongoing intelligence operations and potentially compromise vital national security initiatives. On the other hand, failing to address the vulnerability could lead to unauthorized access and potential leaks of sensitive information. As the information security officer, you face a challenging ethical dilemma:

1. Do you immediately report the vulnerability and advocate for the system shutdown, prioritizing the security of the classified information?
2. Do you withhold information about the vulnerability temporarily, allowing ongoing operations to continue while working with the development team to address the issue without shutting down the system?
3. Do you assess the situation further, considering the potential impact of the vulnerability and the feasibility of addressing it without a system shutdown, before deciding on a course of action?

Answer the following for this scenario based on ACM code of conduct clauses:

i. State ACM clauses that support your decision 1) if you withhold information, 2) report immediately, and 3) take more time for further analysis. Also, explain your selection for each of these decisions. [3]
ii. What you will do when facing this dilemma as the information security officer? [1]

Format answers of both parts as per the below template.

List of clauses related to Q1 a(1) Immediate release	**List of clauses related to Q1 a(2) Withhold information**	**List of clauses related to Q1 a(3) Assess situation further**
• 1.1, 1.2, 1.3 • 2.1, 2.5, 2.6 • 3.3, 3.4	• 1.1, 1.2, 1.6 • 2.1, 2.6 • 3.4	• 1.1, 1.2, 1.3 • 2.2, 2.5 • 3.4
To avoid harm, maintain honesty and trustworthiness, and fulfill professional responsibilities. This approach ensures a swift response to potential threats to national security by protection of sensitive information.	When considering the broader context and principles of minimizing harm, ensuring fairness, and achieving effectiveness in addressing vulnerabilities. However, should be made with careful consideration of potential risks and impacts.	When emphasizing careful consideration, transparency, and the balancing of potential impacts. While not explicitly stated, the ACM Code of Conduct encourages thoughtful and informed decision-making, especially in complex situations where security concerns need to be balanced with operational needs.
Single explanation about what you will do in this situation (5-6 lines). **Immediate reporting and advocacy for system shutdown:** to safeguard classified information and perform the duty to avoid harm. OR **Simultaneously assess the situation further:** by evaluating the impact and will make a strategy to address the vulnerability without a system shutdown. This will help minimize disruption to ongoing intelligence operations while ensuring the security of classified information. Key goals are: • Addressing vulnerability as soon as possible while remain operational with minimal risk. • Transparency, honesty, and a commitment to the highest quality/effectiveness in decision-making process. • Keeping stakeholders, including the development team, in communication loop to collaboratively address the issue.		

b) Legal Scenarios:

Leo Snow is a skilled cybersecurity expert with deeply rooted hatred towards a political figure. Determined to create confusion, he coordinates a disinformation campaign. He starts by gaining unauthorized access to a critical infrastructure information system by breaching the security protocols of a government database containing secret information. He then manipulates authentic documents related to national security, injecting small but misleading details to frame the political figure for spying. In addition, he releases deepfake videos on various online platforms to show the political figure's involvement in unethical and criminal activities. He also employs spamming techniques to disseminate manipulated content across social media channels, resulting in the rapid spread of false information and causing widespread panic and public outcry.

Answer the following question for the scenario:

i. Identify FOUR legal issues as stated in the Prevention of Electronic Crime Act 2016. [2]

Unauthorized access to critical infrastructure information system (Section 6):
- Leo Snow gains unauthorized access to a critical infrastructure information system.
- Penalty: Imprisonment up to three years, a fine up to one million rupees, or both.

Unauthorized copying or transmission of critical infrastructure data (Section 7):
- Leo Snow manipulates authentic documents related to national security and transmits them.
- Penalty: Imprisonment up to five years, a fine up to five million rupees, or both.

Interference with critical infrastructure information system or data (Section 8):
- Leo Snow interferes with the critical infrastructure information system by manipulating documents.
- Penalty: Imprisonment up to seven years, a fine up to ten million rupees, or both.

Cyber terrorism (Section 10):
- Leo Snow commits offenses under Sections 6, 7, and 8 with the intent to create fear, panic, or insecurity in the government or public.
- Penalty: Imprisonment up to fourteen years, a fine up to fifty million rupees, or both.

Spamming (Section 25):
- Leo Snow employs spamming techniques to disseminate manipulated content.
- Penalty: Imprisonment up to three months, a fine up to five million rupees, or both.

Offences against dignity of a natural person (Section 20):
- Leo Snow intentionally exhibits or transmits false information about the political figure.
- Penalty: Imprisonment up to three years, a fine up to one million rupees, or both.

Malicious code (Section 23):
- Leo Snow uses malicious code in deepfake videos with the intent to cause harm.
- Penalty: Imprisonment up to two years, a fine up to one million rupees, or both.

Cyber stalking (Section 24):
- Leo Snow follows, monitors, and contacts the political figure with the intent to coerce or harass.
- Penalty: Imprisonment up to three years, a fine up to one million rupees, or both (potentially five years if the victim is a minor).

ii. Name victims entities (other than Leo and the political figure) because of various security violations. [2]

- Government Database: Victim of Unauthorized Access (Section 6):
- Critical Infrastructure Information System: Victim of Unauthorized Access (Section 6):
- Public and Society: Potential Victims of Cyber Terrorism (Section 10):
- Potential Victims of Spamming (Section 25):
- Identity Information Owners: Potential Victims of Unauthorized Use of Identity Information (Section 16):
- Individuals in Deepfake Videos: Potential Victims of Offences Against Modesty of a Natural Person and Minor (Section 21):

iii. Identify TWO key law enforcement challenges in this scenario. Write 3-4 lines detailing each. [2]

- Determining the **true identity of Leo Snow** might be challenging due to the use of sophisticated techniques to conceal his identity online. -

- Investigating cybercrimes involving unauthorized access, manipulation of critical infrastructure, and creation of deepfake videos **requires specialized technical expertise**.

- Investigating cybercrimes often involves accessing and analyzing personal and sensitive data, **raising concerns about privacy and compliance with data protection laws**.

- Addressing the global impact of disinformation campaigns, such as the one orchestrated by Leo Snow, **requires coordinated efforts across multiple jurisdictions**.

- **Coordinating with social media platforms** to combat the spread of manipulated content and disinformation poses a challenge for law enforcement.

- **Encouraging public awareness about cybersecurity threats** and disinformation, and fostering a culture of reporting suspicious activities, is a continual challenge.

- **Legislative frameworks may struggle to keep pace with rapidly evolving technologies**, making it challenging to prosecute emerging cybercrimes effectively.

Question 2: Analyze each of the following brief scenarios and suggest possible solutions along with a detailed explanation of any one solution. Format your answer as per the given template.

a) A series of information security incidents took place in a **recently established** medium-sized company. The management is concerned about the security of information systems including sensitive customer data.

Possible solutions: 1. Perform InfoSec risk assessment (due to medium size). 2. Vulnerability assessments related to network devices and application and cloud usage (services + vendor) 3. Employee training and Use of Encryption tools and techniques to safeguard Infosec assets.
Explanation of one solution: (3-4 lines) While vulnerability assessments, employee training, and encryption are integral components of a comprehensive security strategy, a risk assessment provides the foundational understanding necessary to tailor these measures to the specific needs and risks of the organization. It acts as a roadmap for effective and resource-efficient security measures, making it a critical first step in the security improvement process. →Identify and classify information assets. Evaluate and prioritize potential risks and threats. Assess the vulnerabilities and likelihood of exploitation. Develop a risk treatment plan to mitigate identified risks. Establish a continuous risk monitoring process.

b) Several research institutions are collaborating on a groundbreaking project that involves the exchange and analysis of research data. They need to **exchange data over multiple networks** including the Internet and it contains proprietary algorithms, experimental results, and confidential information critical to the success of the project.

Possible solutions: 1. Encryption tools and techniques: Data Encryption, Secure FTP 2. Network segmentation and VPNs 3. Access controls including MFA and Incident Response Plan.
Explanation of one solution: (3-4 lines) Network segmentation (inculuding use of VPN) provides a robust foundation for securing the collaborative project by isolating sensitive research data and critical systems. It enhances control over access, limiting unauthorized entry, while VPNs ensure secure and encrypted communication over the Internet, mitigating the risk of data interception. This strategy addresses both data protection and secure communication aspects efficiently.

c) The government is modernizing its election infrastructure to conduct secure and tamper-proof elections by a robust mechanism to **validate each voter** during electronic online voting.

Possible solutions: 1. Biometric Authentication and Multi-Factor Authentication 2. End-to-End Encryption: 3. ~~Block-chain Technology~~
Explanation of one solution: (3-4 lines) Biometric Authentication and Multi-Factor Authentication (MFA). This combination provides a robust approach to voter validation by uniquely identifying individuals through biometrics and adding an extra layer of security with MFA. Together, these measures strengthen the election infrastructure's security and safeguard the integrity of the electronic voting process.

d) A pharmaceutical research lab is equipped with state-of-the-art equipment, highly sensitive data, and proprietary research findings. The management wants **real-time security** to safeguard intellectual property and prevent unauthorized access.

Possible solutions: 1. Intrusion detection and Intrusioin prevention systems (IDS+IPS): 2. Access Controls and Role-Based Permissions: 3. Regular Security Audits and Penetration Testing:
Explanation of one solution: (3-4 lines) Access Controls and Role-Based Permissions strict implementation based on job roles, the pharmaceutical research lab can ensure that only authorized personnel have access to sensitive data and proprietary findings. This approach directly addresses the need for real-time security by preventing unauthorized access, minimizing the risk of data breaches, and maintaining control over intellectual property. While intrusion detection and prevention systems and regular security audits are important, robust access controls form a foundational layer of protection for sensitive research environments.

e) A manufacturing plant producing electronics relies on an interconnected network to control automated manufacturing processes, monitor equipment, and manage sensitive intellectual property. Recent incidents of **unauthorized access to various servers and bandwidth consumption by outward traffic** raise concerns about potential cyber threats.

Possible solutions: 1. Intrusion Detection and Prevention Systems (IDS+IPS): 2. Employee Training and Awareness: 3. Regular Security Audits, Penetration Testing, Incident response plan and Backups:
Explanation of one solution: (3-4 lines) Regular security audits, penetration testing, an incident response plan, and data backups addresses the breadth of potential cyber threats. Proactive assessments and a robust incident response capability are crucial for identifying vulnerabilities, responding to incidents swiftly, and ensuring business continuity through effective backups.

Question 3:

a) List four types of firewalls and their main characteristics. Discuss a practical scenario where each of these types is used.

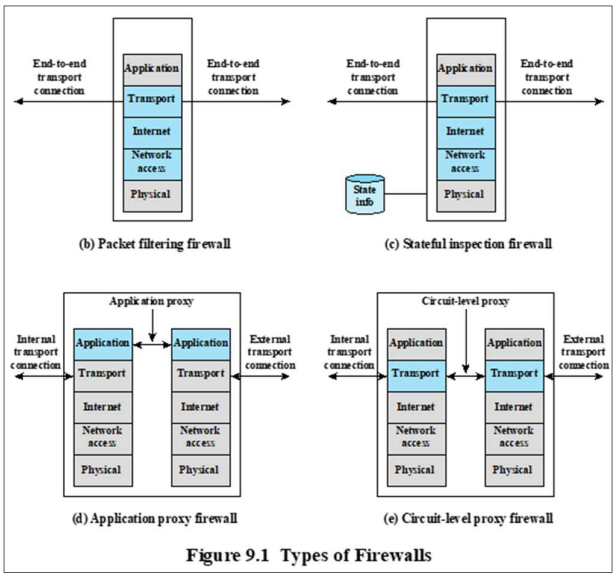


Figure 9.1 Types of Firewalls

List:

1. Packet Filtering Firewall.
2. Stateful Inspection Firewalls.
3. Application-Level Gateway.
4. Circuit-Level Gateway.

Main characteristics:

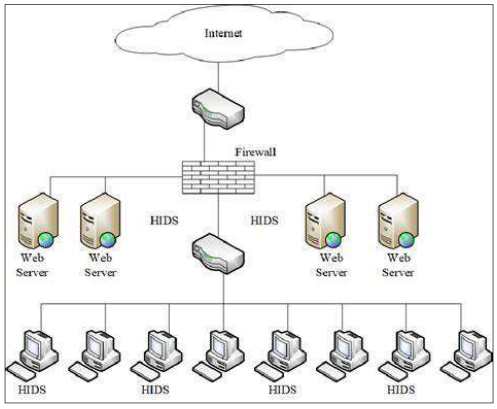
Packet Filtering Firewalls operate at the network layer (Layer 3) of the OSI model and make decisions (forward or discard) based on predefined rules for individual packets. They examine header information, such as source and destination IP addresses, ports, and protocols, to determine whether to allow or block the passage of packets. These firewalls are typically stateless (see stateful below). Packet filtering firewalls provide a fundamental level of network security by controlling traffic based on specified criteria. **Scenario**: Restricting incoming traffic on a router to allow only specific port numbers (e.g., HTTP on port 80) to protect a web server from unauthorized access.

Stateful Inspection Firewalls. Stateful Inspection Firewalls, also known as dynamic packet filtering firewalls, monitor the state of active connections by creating a directory of outbound TCP connections. There is an entry for each currently established connection. The packet filter will now allow incoming traffic to high-numbered ports only for those packets that fit the profile of one of the entries in this directory. Some stateful firewalls also keep track of TCP sequence numbers to prevent attacks that depend on the sequence number, such as session hijacking. Some even inspect limited amounts of application data for some well-known protocols such as FTP, IM, and SIPS commands, to identify and track related connections. **Scenario**: Allowing outbound data transmission only if it corresponds to a previously established and valid incoming connection, preventing unauthorized access through dynamically opened ports.

Application-Level Gateway. The Application-Level Gateway (ALG) operates at the application layer of the OSI model and provides deep packet inspection for specific protocols, such as FTP, SIP, or H.323. It understands the application-specific traffic, allowing it to make intelligent decisions based on the content and context of the data. ALGs often feature protocol-specific security mechanisms, enhancing overall network security by effectively managing and filtering application-layer traffic. **Scenario**: Permitting or denying specific applications, such as instant messaging or peer-to-peer file sharing, based on application-layer protocol analysis to control and secure user activities.

Circuit-Level Gateway. A Circuit-Level Gateway operates at the session layer of the OSI model, facilitating the creation of secure connections between internal and external networks. It does not inspect the content of data packets but instead validates the overall session, making it particularly efficient for handling protocols like TCP. A circuit-level gateway does not permit an end-to-end TCP connection; rather, the gateway sets up two TCP connections, one between itself and a TCP user on an inner host and one between itself and a TCP user on an outside host. Once the two connections are established, the gateway typically relays TCP segments from one connection to the other without examining the contents. **Scenario**: Establishing secure virtual private network (VPN) connections between remote users and the internal network by validating sessions and managing connection handshakes for encrypted communication.

b) Intrusion Detection is one of the key features of any IS strategy. Discuss with the help of a diagram basic architecture of Host based IDS and Network IDS.



IDSs are often classified based on the source and type of data analyzed, as:

a) Host-based IDS (HIDS): Monitors the characteristics of a single host and the events occurring within that host, such as process identifiers and the system calls they make, for evidence of suspicious activity.

b) Network-based IDS (NIDS): Monitors network traffic for particular network segments or devices and analyzes network, transport, and application protocols to identify suspicious activity.

Host Intrusion Detection System (HIDS). A HIDS is a security mechanism designed to monitor and analyze the internal activities of a single host, such as a computer or server. It operates by examining system logs and file integrity, detecting anomalous behavior or potential security breaches. HIDS focuses on identifying suspicious activities within the host environment, providing real-time alerts and aiding in the rapid response to security incidents.

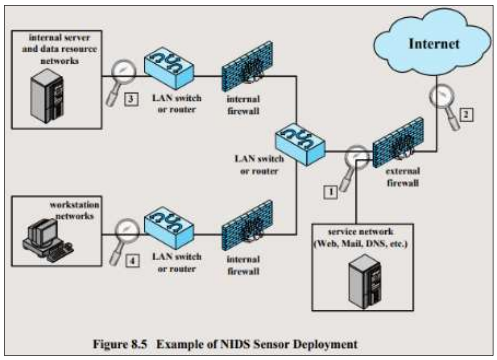


Figure 8.5 Example of NIDS Sensor Deployment

Network Intrusion Detection System (NIDS). A NIDS is a security solution designed to monitor and analyze network traffic for signs of malicious activities or unauthorized access. It is concerned with the entire network system. It operates by inspecting packets traversing the network and compares them against predefined signatures or behavioral patterns. NIDS identifies and alerts on potential security threats, enabling timely response to mitigate risks. Main characteristics include real-time monitoring, signature-based detection, and the ability to analyze network traffic patterns for anomalies.

c) Illustrate with the help of a diagram how the digital immune system is implemented and executed in an active network environment.

A Digital Immune System combines various security components to proactively detect, respond to, and mitigate cybersecurity threats in an active network environment. Following are the key components of a Digital Immune System:

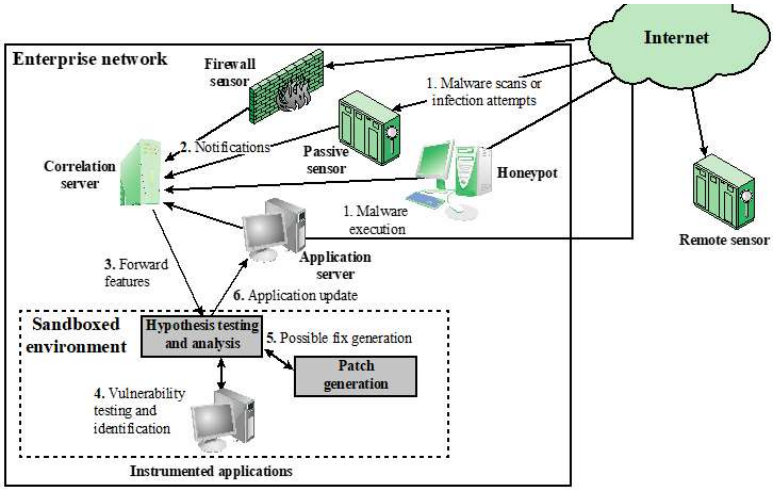


Figure 9.5 Placement of Malware Monitors (adapted from [SIDI05])

- Intrusion Detection System (IDS): **Function**: Monitors network or system activities for suspicious behavior or known attack patterns. **Role**: Provides early detection of potential threats and abnormal activities.
- Intrusion Prevention System (IPS): **Function**: Analyzes and takes action to block or prevent detected malicious activities. **Role**: Acts as a proactive defense mechanism by actively preventing identified threats from causing harm.
- Sandbox Environment: **Function**: Isolates and analyzes suspicious files or code in a controlled environment to identify potential threats. **Role**: Enhances threat detection by analyzing files in a secure environment, preventing potential damage to the actual network.
- Correlation Server: **Function**: Aggregates and analyzes data from various security sources to identify complex threats and patterns. **Role**: Provides a comprehensive view of the security landscape by correlating information from different sources, enabling more accurate threat detection.
- Honeypot: Function: Mimics a vulnerable system to attract and trap attackers, allowing security teams to study their tactics and methods. Role: Acts as a decoy to divert and identify potential threats while providing valuable insights into attackers' techniques.
- Sensors: Function: Collects data and monitors network or system activities. Role: Distributed sensors enhance the coverage of threat detection across the network, providing real-time data for analysis.
- Security Information and Event Management (SIEM): Function: Collects, stores, and analyzes log data from various network devices and applications. Role: Enables centralized monitoring, analysis, and reporting of security events, facilitating effective incident response.
- Incident Response System: Function: Provides a structured approach to address and mitigate security incidents. Role: Ensures a coordinated and timely response to security events, minimizing the impact of incidents.

The combination of these components forms a comprehensive Digital Immune System, creating a resilient and proactive defense against a wide range of cyber threats in an active network environment.

Question 4: Write **3-4 lines** answers to the following: *Note: 0.5 wt. bonus if you attempt all parts **neatly** on **two-facing pages** of the answer sheet.*

a) How and why public key vulnerable to an attack? Explain the design principles of your solution.
Mark distribution: 100% marks if both How and Why are answered with public key certificate mentioned.
A public key is accessible to everybody in by definition in asymmetric encryption. E.g. on the web page or as a signature in an unencrypted email message etc. An attacker can forge his/her key and thus get a message instead of the actual owner. A public key certificate issued by a 3rd party verifies the owner of the public key is known. The receiver therefore verifies the public key with the certificate authority.

b) Recall our coverage of malicious software (malware). Specify how you would approach stopping the spread of and cleaning the systems already affected by malware.
Mark distribution: detect propagation mechanism + scan payload signature (No marks for non-technical answers like antivirus)
Malware code needs to be studied (e.g. by running it in a sandbox) to determine its propagation mechanism (how it attaches or uses network API to replicate itself) and payload (how it infects the file or other portion of the OS/hardware). This information can be used to stop propagation (e.g. closing a particular port at the firewall) and/or clean already affected files.

c) Define an inference channel. Now draw a labeled diagram to show how it works.
Mark distribution: Correct description OR diagram
The information transfer path by which unauthorized data is obtained, using authorized access to a database, is referred to as an inference channel. Inference is the process of performing authorized queries and deducing unauthorized information from the legitimate responses received.

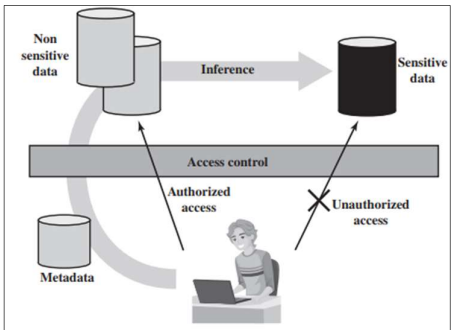
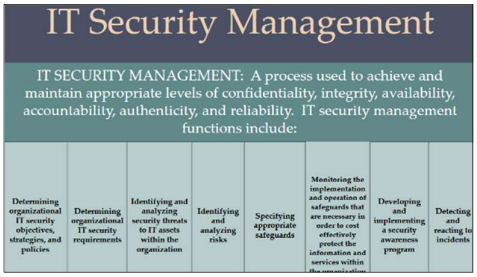


Figure 5.7 **Indirect Information Access via Inference Channel**

d) Explain key steps of the IT security management process that ensures Information security in large organizations.
Mark distribution: 100% (all points), 50% and 25%
i) determining the organization's IT security objectives, strategies, and policies. ii) performing an IT security risk assessment that analyzes security threats to IT assets within the organization, and determines the resulting risks. iii) selecting suitable controls to cost-effectively protect the organization's IT assets. iv) writing plans and procedures to effectively implement the selected controls. v) implementing the selected controls, including the provision of a security awareness and training program. vi) monitoring the operation, and maintaining the effectiveness, of the selected controls. vii) detecting and reacting to incidents.



e) How is cryptanalysis different from brute force attack? How do you approach brute force attack on the DES cipher?
Marks distribution: Cryptanalysis=1, Brute force=1, DES=2
Cryptanalysis uses knowledge and previous code-breaking skills of an experienced cryptographer, whereas, in the brute force approach a hacker tries all or carefully selected subset of keys to break the cipher using a known message. DES uses a 54-bit key so trying 2^{54} keys (theoretically half the keyspace i.e. 2^{27}) will break the DES cipher.

----------(X)----------