CS 7349
Data and Network Security
Quiz #1

Name: Bingying Liang
ID: 48999397

Due: Jan 29 2024

This is a quiz assignment for CS7349, Data and Network Security. This quiz is due at the end of the synchronous class period in which the unit is discussed or whenever the instructor tells you to hand it in; whichever comes first. Enter your answer to each question in the CS 7349 Quiz Answer Sheet PDF document. Be sure to place your name and due date in the Quiz Answer Sheet and place your last name and the unit number at the beginning of the file name. For example, the filename for the quiz answer sheet for Quiz #1 for John Doe should be *Doe01CS7349QuizAnswerSheet.pdf*.

For each multiple-choice question, in the Quiz Answer Sheet state the letter of your chosen answer and write out the explanation why the answer is correct. Note that the explanation involves also explaining why the other answers are not correct. Failure to address ALL options will result in a 0 for this assignment.

For each short answer question, in the Quiz Answer Sheet state your answer to the question and then write out at least a one paragraph explanation why the answer is correct.

Your answer pdf document should be submitted on the appropriate Canvas location.

1) What is the one word that defines the foundations of cyber security?

Solution: Confidentiality

Explanation: Confidentiality represents the principle of ensuring that information is only accessible to those who are authorized to view it. This is a core aspect of cybersecurity. Other terms like Integrity, Availability, or Authentication, while important, are part of the broader framework of cybersecurity but do not singularly define its foundation as confidentiality does.

2) What defines 'security' for a particular location?

Solution: Measures to protect people, property, and information.

Explanation: Security for a location is defined by the measures taken to protect the physical premises, the people within it, and the assets including data from theft, damage, or unauthorized access. This includes physical security measures like locks, surveillance systems, and access control, as well as cyber security measures for protecting data.

3) Name the five key objectives for computer security.

Solution: Confidentiality, Integrity, Availability, Authenticity, Non-repudiation.

Explanation:

(a) Confidentiality: Ensuring that information is not disclosed to unauthorized individuals, entities, or processes.

(b) Integrity: Maintaining and assuring the accuracy and completeness of data over its entire lifecycle.

(c) Availability: Ensuring that authorized users have access to information and associated assets when required.

(d) Authenticity: Ensuring that the identities of individuals or entities involved are validated.

(e) Non-repudiation: Ensuring that the origin of a message or transaction is verifiable and cannot be denied later.

These five objectives cover the broad scope of what computer security aims to achieve. Confidentiality ensures data privacy, Integrity ensures data accuracy, Availability ensures data is accessible when needed, Authenticity ensures the validation of data origin, and Non-repudiation ensures actions cannot be denied after the fact. Any other objectives would be subcategories or extensions of these core five.

4) Name at least five security mechanisms.

Solution:
Encryption, Firewalls, Antivirus software, Access control, Intrusion detection systems

Explanation:

(a) Encryption: Protecting data by transforming it into an unreadable format.

(b) Firewalls: Monitoring and controlling incoming and outgoing network traffic based on predetermined security rules.

(c) Antivirus software: Protecting against malware through detection, prevention, and removal.

(d) Access control: Limiting access to resources only to those who are authorized.

(e) Intrusion detection systems (IDS): Monitoring network traffic for suspicious activity and issuing alerts.

5) Identify two passive attacks.

Solution: Eavesdropping, Traffic analysis

Explanation:

(a) Eavesdropping: Unauthorized real-time interception of private communications.

(b) Traffic analysis: Monitoring patterns of communication and movement of data to extract information.

6) Identify at least three active attacks.

Solution: Denial of Service (DoS), Man-in-the-middle (MitM), SQL Injection

Explanation:

(a) Denial of Service (DoS) attacks: Overwhelming a system's resources so that it cannot respond to service requests.

(b) Man-in-the-middle (MitM) attacks: Intercepting and altering communication between two parties.

(c) SQL Injection: Injecting malicious code into a database query to manipulate or destroy data.

7) In the design of a computer network, what is the fundamental design approach used to manage the system complexity?

Solution: Modularity

Explanation: Modularity involves breaking the network into manageable, independent components, making it easier to manage complexity. Other approaches like simplicity or redundancy are important but do not directly address the management of complexity in network design like modularity does.

8) What types of attacks are likely to occur over a computer network? Where within the network will these attacks occur?

Solution:
Cyber attacks like phishing, malware; Insider attacks; Eavesdropping. These occur at end-user devices, servers, communication channels, and network entry or exit points.

Explanation:

(a) Cyber attacks like phishing, malware distribution, and DDoS attacks.

(b) Insider attacks, including intentional data breaches or unintentional information leaks.

(c) Eavesdropping or interception attacks.

These attacks can occur at various points in a network, such as at end-user devices, servers, communication channels, and network entry or exit points.

9) What security mechanisms are appropriate for use in a computer network? Where are they most likely to be used?

Solution:
Encryption, Firewalls, IDPS, SSL/TLS, VPNs. Used at network boundaries, servers, databases, end-user devices.

Explanation: The following Security mechanisms are appropriate for use in a computer network:

(a) Encryption, especially in data transmission and storage.

(b) Network firewalls to control traffic.

(c) Intrusion detection and prevention systems (IDPS) for monitoring.

(d) Secure socket layer (SSL)/transport layer security (TLS) protocols for secure communication.

(e) Virtual Private Networks (VPNs) for secure remote access.

These mechanisms are often used at critical points like network boundaries, servers, databases, and on end-user devices.

10) Give at least three reasons why security is a problem in the cyber world today.

Solution: Rapid Technological Advancements, Sophistication of Cyber Attacks, Human Factor.

Explanation:

(a) Rapid Technological Advancements: New technologies often introduce new vulnerabilities faster than they can be secured.

(b) Sophistication of Cyber Attacks: Attackers are constantly developing more advanced methods to breach security measures.

(c) Human Factor: Human error or insider threats remain a significant risk, often due to lack of awareness or intentional malicious actions.

These three reasons cover the major challenges in cybersecurity. Technological advancements and sophisticated attacks constantly evolve the threat landscape, while the human factor remains a constant vulnerability due to potential for error or malicious actions. Other factors might contribute to security issues but are not as universally impactful as these three.