



Free Questions for 212-82 by dumpshq

Shared by Newton on 09-08-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Andre, a security professional, was tasked with segregating the employees' names, phone numbers, and credit card numbers before sharing the database with clients. For this purpose, he implemented a deidentification technique that can replace the critical information in database fields with special characters such as asterisks (*) and hashes (#).

Which of the following techniques was employed by Andre in the above scenario?

Options:

- A- Tokenization
- B- Masking
- C- Hashing
- D- Bucketing

Answer:

B

Explanation:

Masking is the technique that Andre employed in the above scenario. Masking is a deidentification technique that can replace the critical information in database fields with special characters such as asterisks (*) and hashes (#). Masking can help protect sensitive data from unauthorized access or disclosure, while preserving the format and structure of the original data . Tokenization is a deidentification technique that can replace the critical information in database fields with random tokens that have no meaning or relation to the original data. Hashing is a deidentification technique that can transform the critical information in database fields into fixed-length strings using a mathematical function. Bucketing is a deidentification technique that can group the critical information in database fields into ranges or categories based on certain criteria.

Question 2

Question Type: MultipleChoice

Grace, an online shopping freak, has purchased a smart TV using her debit card. During online payment, Grace's browser redirected her from ecommerce website to a third-party payment gateway, where she provided her debit card details and OTP received on her registered mobile phone. After completing the transaction, Grace navigated to her online bank account and verified the current balance in her savings account.

Identify the state of data when it is being processed between the ecommerce website and the payment gateway in the above scenario.

Options:

- A- Data at rest
- B- Data in inactive
- C- Data in transit
- D- Data in use

Answer:

C

Explanation:

Data in transit is the state of data when it is being processed between the ecommerce website and the payment gateway in the above scenario. Data in transit is data that is moving from one location to another over a network, such as the internet, a LAN, or a WAN. Data in transit can be vulnerable to interception, modification, or theft by unauthorized parties, so it needs to be protected by encryption, authentication, and other security measures . Data at rest is data that is stored on a device or a media, such as a hard drive, a flash drive, or a cloud storage. Data in active is data that is currently being accessed or modified by an application or a user. Data in use is data that is loaded into the memory of a device or a system for processing or computation.

Question 3

Question Type: MultipleChoice

Riley sent a secret message to Louis. Before sending the message, Riley digitally signed the message using his private key. Louis received the message, verified the digital signature using the corresponding key to ensure that the message was not tampered during transit.

Which of the following keys did Louis use to verify the digital signature in the above scenario?

Options:

- A- Riley's public key
- B- Louis's public key
- C- Riley's private key
- D- Louis's private key

Answer:

A

Explanation:

Riley's public key is the key that Louis used to verify the digital signature in the above scenario. A digital signature is a cryptographic technique that verifies the authenticity and integrity of a message or document. A digital signature is created by applying a hash function to the message or document and then encrypting the hash value with the sender's private key. A digital signature can be verified by decrypting the hash value with the sender's public key and comparing it with the hash value of the original message or document .

Riley's public key is the key that corresponds to Riley's private key, which he used to sign the message. Louis's public key is the key that corresponds to Louis's private key, which he may use to encrypt or decrypt messages with Riley. Louis's private key is the key that only Louis knows and can use to sign or decrypt messages. Riley's private key is the key that only Riley knows and can use to sign or encrypt messages.

Question 4

Question Type: MultipleChoice

Paul, a computer user, has shared information with his colleague using an online application. The online application used by Paul has been incorporated with the latest encryption mechanism. This mechanism encrypts data by using a sequence of photons that have a spinning trait while traveling from one end to another, and these photons keep changing their shapes during their course through filters: vertical, horizontal, forward slash, and backslash.

Identify the encryption mechanism demonstrated in the above scenario.

Options:

- A- Quantum cryptography
- B- Homomorphic encryption

C- Rivest Shamir Adleman encryption

D- Elliptic curve cryptography

Answer:

A

Explanation:

Quantum cryptography is the encryption mechanism demonstrated in the above scenario. Quantum cryptography is a branch of cryptography that uses quantum physics to secure data transmission and communication. Quantum cryptography encrypts data by using a sequence of photons that have a spinning trait, called polarization, while traveling from one end to another. These photons keep changing their shapes, called states, during their course through filters: vertical, horizontal, forward slash, and backslash. Quantum cryptography ensures that any attempt to intercept or tamper with the data will alter the quantum states of the photons and be detected by the sender and receiver. Homomorphic encryption is a type of encryption that allows computations to be performed on encrypted data without decrypting it first. Rivest Shamir Adleman (RSA) encryption is a type of asymmetric encryption that uses two keys, public and private, to encrypt and decrypt data. Elliptic curve cryptography (ECC) is a type of asymmetric encryption that uses mathematical curves to generate keys and perform encryption and decryption.

Question 5

Question Type: MultipleChoice

Hayes, a security professional, was tasked with the implementation of security controls for an industrial network at the Purdue level 3.5 (IDMZ). Hayes verified all the possible attack vectors on the IDMZ level and deployed a security control that fortifies the IDMZ against cyber-attacks.

Identify the security control implemented by Hayes in the above scenario.

Options:

- A- Point-to-point communication
- B- MAC authentication
- C- Anti-DoS solution
- D- Use of authorized RTU and PLC commands

Answer:

D

Explanation:

The use of authorized RTU and PLC commands is the security control implemented by Hayes in the above scenario. RTU (Remote Terminal Unit) and PLC (Programmable Logic Controller) are devices that control and monitor industrial processes, such as power generation, water treatment, oil and gas production, etc. RTU and PLC commands are instructions that are sent from a master station to a slave station to perform certain actions or request certain data. The use of authorized RTU and PLC commands is a security control

that fortifies the IDMZ (Industrial Demilitarized Zone) against cyber-attacks by ensuring that only valid and authenticated commands are executed by the RTU and PLC devices. Point-to-point communication is a communication method that establishes a direct connection between two endpoints. MAC authentication is an authentication method that verifies the MAC (Media Access Control) address of a device before granting access to a network. Anti-DoS solution is a security solution that protects a network from DoS (Denial-of-Service) attacks by filtering or blocking malicious traffic.

Question 6

Question Type: MultipleChoice

Leo has walked to the nearest supermarket to purchase grocery. At the billing section, the billing executive scanned each product's machine-readable tag against a readable machine that automatically reads the product details, displays the prices of the individual product on the computer, and calculates the sum of those scanned items. Upon completion of scanning all the products, Leo has to pay the bill.

Identify the type of short-range wireless communication technology that the billing executive has used in the above scenario.

Options:

A- Radio-frequency identification (RFID)

B- Near-field communication (NFC)

C- QUIC

D- QR codes and barcodes

Answer:

A

Explanation:

Radio-frequency identification (RFID) is the type of short-range wireless communication technology that the billing executive has used in the above scenario. RFID uses radio-frequency electromagnetic waves to transfer data for automatic identification and for tracking tags attached to objects . RFID tags are machine-readable tags that store information about the products, such as name, price, expiry date, etc. RFID readers are readable machines that scan the RFID tags and display the product details on the computer . RFID technology is widely used in supermarkets, warehouses, libraries, and other places where inventory management and tracking are required .

Question 7

Question Type: MultipleChoice

Stephen, a security professional at an organization, was instructed to implement security measures that prevent corporate data leakage on employees' mobile devices. For this purpose, he employed a technique using which all personal and corporate data are isolated on an employee's mobile device. Using this technique, corporate applications do not have any control of or communication with the private applications or data of the employees.

Which of the following techniques has Stephen implemented in the above scenario?

Options:

- A- Full device encryption
- B- Geofencing
- C- Containerization
- D- OTA updates

Answer:

C

Explanation:

Containerization is the technique that Stephen has implemented in the above scenario. Containerization is a technique that isolates personal and corporate data on an employee's mobile device. Containerization creates separate encrypted containers or partitions on the device, where corporate applications and data are stored and managed. Containerization prevents corporate data leakage on

employees' mobile devices by restricting access, sharing, copying, or transferring of data between containers. Containerization also allows remote wiping of corporate data in case of device loss or theft . Full device encryption is a technique that encrypts all the data on a mobile device using a password or a key. Geofencing is a technique that uses GPS or RFID to define geographical boundaries and trigger actions based on the location of a mobile device. OTA (Over-the-Air) updates are updates that are delivered wirelessly to mobile devices without requiring physical connection to a computer.

To Get Premium Files for 212-82 Visit

<https://www.p2pexams.com/products/212-82>

For More Free Questions Visit

<https://www.p2pexams.com/eccouncil/pdf/212-82>

