QUESTIONS & ANSWERS

Kill your exam at first Attempt

KILL EXAMS

ISACA

CISA

ISACA CISA (Certified Information Systems Auditor)

QUESTION: 390
Applying a digital signature to data traveling in a network provides:

A. confidentiality and integrity.
B. security and nonrepudiation.
C. integrity and nonrepudiation.
D. confidentiality and nonrepudiation.

Answer: C

Explanation:
The process of applying a mathematical algorithm to the data that travel in the network and placing the results of this operation with the hash data is used for controlling data integrity, since any unauthorized modification to this data would result in a different hash. The application of a digital signature would accomplish the non repudiation of the delivery of the message. The term security is a broad concept and not a specific one. In addition to a hash and a digital signature, confidentiality is applied when an encryption process exists.

QUESTION: 391
Which of the following would an IS auditor consider a weakness when performing an audit of an organization that uses a public key infrastructure with digital certificates for its business-to- consumer transactions via the internet?

A. Customers are widely dispersed geographically, but the certificate authorities are not.
B. Customers can make their transactions from any computer or mobile device.
C. The certificate authority has several data processing subcenters to administer certificates.
D. The organization is the owner of the certificate authority.

Answer: D

Explanation:
If the certificate authority belongs to the same organization, this would generate a conflict of interest. That is, if a customer wanted to repudiate a transaction, they could allege that because of the shared interests, an unlawful agreement exists between the parties generating the certificates, if a customer wanted to repudiate a transaction, they could argue that there exists a bribery between the parties to generate the certificates, as shared interests exist. The other options are not weaknesses.

QUESTION: 392
Which of the following implementation modes would provide the GREATEST amount of security for outbound data connecting to the internet?

A. Transport mode with authentication header (AH) plus encapsulating security payload (ESP)
B. Secure Sockets Layer (SSL) mode
C. Tunnel mode with AH plus ESP
D. Triple-DES encryption mode

Answer: C

Explanation:
Tunnel mode provides protection to the entire IP package. To accomplish this, AH and ESP services can be nested. The transport mode provides primary protection for the higher layers of the protocols by extending protection to the data fields (payload) of an IP package. The SSL mode provides security to the higher communication layers (transport layer). The triple-DES encryption mode is an algorithm that provides confidentiality

QUESTION: 393
Which of the following is the MOST reliable sender authentication method?

A. Digital signatures
B. Asymmetric cryptography
C. Digital certificates
D. Message authentication code

Answer: C

Explanation:
Digital certificates are issued by a trusted third party. The message sender attaches the certificate and the recipient can verify authenticity with the certificate repository. Asymmetric cryptography, such as public key infrastructure (PKl), appears to authenticate the sender but is vulnerable to a man-in-the-middle attack. Digital signatures are used for both authentication and confidentiality, but the identity of the sender would still be confirmed by the digital certificate. Message authentication code is used for message integrity verification.

QUESTION: 394
Which of the following provides the GREATEST assurance of message authenticity?

A. Theprehash code is derived mathematically from the message being sent.
B. Theprehash code is encrypted using the sender's private key.
C. Theprehash code and the message are encrypted using the secret key.
D. The sender attains the recipient's public key and verifies the authenticity of its digital certificate with a certificate authority.

Answer: B

Explanation:
Encrypting the prehash code using the sender's private key provides assurance of the authenticity of the message. Mathematically deriving the prehash code provides integrity to the message. Encrypting the prehash code and the message using the secretkey provides confidentiality.

QUESTION: 395
Which of the following internet security threats could compromise integrity?

A. Theft of data from the client
B. Exposure of network configuration information
C. A Trojan horse browser
D. Eavesdropping on the net

Answer: C

Explanation:

Internet security threats/vulnerabilities to integrity include a Trojan horse, which could modify user data, memory and messages found in client-browser software. The other options compromise confidentiality.

QUESTION: 396
Which of the following is a concern when data are transmitted through Secure Sockets Layer (SSL) encryption, implemented on a trading partner's server?

A. The organization does not have control over encryption.
B. Messages are subjected to wire tapping.
C. Data might not reach the intended recipient.
D. The communication may not be secure.

Answer: A

Explanation:
The SSL security protocol provides data encryption, server authentication, message integrity and optional client authentication. Because SSL is built into all major browsers and web servers, simply installing a digital certificate turns on the SSL capabilities. SSL encrypts the datum while it is being transmitted over the internet. The encryption is done in the background, without any interaction from the user; consequently, there is no password to remember. The other choices are incorrect. Since the communication between client and server is encrypted, the confidentiality of information is not affected by wire tapping. Since SSL does the client authentication, only the intended recipient will receive the decrypted data.All data sent over an encrypted SSL connection are protected with a mechanism to detect tampering, i.e., automatically determining whether data has been altered in transit.

QUESTION: 397
If inadequate, which of the following would be the MOST likely contributor to a denial-of-service attack?

A. Router configuration and rules
B. Design of the internal network
C. Updates to the router system software
D. Audit testing and review techniques

Answer: A

Explanation:
Inadequate router configuration and rules would lead to an exposure to denial-of-service attacks. Choices B and C would be lesser contributors. Choice D is incorrect because audit testing and review techniques are applied after the fact.

QUESTION: 398
The Secure Sockets Layer (SSL) protocol addresses the confidentiality of a message through:

A. symmetric encryption.
B. message authentication code.
C. hash function.
D. digital signature certificates.

Answer: A

Explanation:
SSL uses a symmetric key for message encryption. A message authentication code is used for ensuring data integrity. Hash function is used for generating a message digest; it does not use public key encryption for message encryption. Digital signature certificates are used by SSL for server authentication.

QUESTION: 399
The PRIMARY goal of a web site certificate is:

A. authentication of the web site that will be surfed.
B. authentication of the user who surfs through that site.
C. preventing surfing of the web site by hackers.
D. the same purpose as that of a digital certificate.

Answer: A

Explanation:
Authenticating the site to be surfed is the primary goal of a web certificate. Authentication of a user is achieved through passwords and not by a web site certificate. The site certificate does not prevent hacking nor does it authenticate a person.

QUESTION: 400
An IS auditor performing detailed network assessments and access control reviews should FIRST:

A. determine the points of entry.
B. evaluate users' access authorization.
C. assess users' identification and authorization.
D. evaluate the domain-controlling server configuration.

Answer: A

Explanation:
In performing detailed network assessments and access control reviews, an IS auditor should first determine the points of entry to the system and review the points of entry accordingly for appropriate controls. Evaluation of user access authorization, assessment of user identification and authorization, and evaluation of the domain-controlling server configuration are all implementation issues for appropriate controls for the points of entry.