# Domain 3 Questions

1. The components of this security model include subjects, objects, clearances and who can have access to what. These components are related to which of the following security models?

- ☐ a. The Bell-LaPadula Model
- ☐ b. The Clark-Wilson Model
- ☐ c. The Lipner Model
- ☐ d. The Biba Model

2. Which of the following statements is true of the Common Criteria's Evaluation Assurance Levels (EALs)?

- ☐ a. Common Criteria has 7 EALs against which a security product may be able to be certified.
- ☐ b. Common Criteria has 7 EALs against which a security product may be able to be accredited.
- ☐ c. Common Criteria EALs can be used to cross-certify with the Information Technology Security Evaluation Criteria (ITSEC) ratings, but not the Trusted Computer System Evaluation Criteria (TCSEC) ratings.
- ☐ d. Common Criteria EALS can be used to cross-certify with the Trusted Computer System Evaluation Criteria (TCSEC) ratings, but not the Information Technology Security Evaluation Criteria (ITSEC) ratings.

3. A stream cipher works by using which of the following?

- ☐ a. The Rail/Fence cipher
- ☐ b. The Running Key cipher
- ☐ c. The Vigenere cipher
- ☐ d. The Vernam cipher

5. Which statement below BEST describes the difference between the Electronic Code Book (ECB) and the Counter (CTR) method of encryption?

- ☐ a. ECB is a block cipher, whereas CTR does not stop errors from propagating.
- ☐ b. ECB is a stream cipher, whereas CTR is a block cipher.
- ☐ c. Encryption errors can propagate when ECB is used, but do not propagate when Counter is used.
- ☐ d. ECB can only secure short messages, whereas CTR can secure long ones as well.

6. Which of the following allows two cooperating processes to transfer information in such a way that it violates the system's security policy?

- ☐ a. Partial disclosure
- ☐ b. Full disclosure
- ☐ c. Covert channel
- ☐ d. Open source

7. Protection and security of information is the responsibility of everyone within the company. Which of the following describes an individual or function that protects the information on behalf of the owner?

- ☐ a. The data custodian
- ☐ b. The information systems auditor
- ☐ c. The help desk administrator
- ☐ d. The business continuity planner

8. A Certificate Authority (CA) will occasionally have to revoke a certificate it has published. How does the CA make this fact known to users who are trusting it to deliver reliable certificates?

- ☐ a. The CA informs the RA and the RA sends the information to the CA's membership.
- ☐ b. The CA destroys its Digital Certificate Signing Key and creates a new one.
- ☐ c. The CA informs the major browser vendors and they change their browsers so that they do not accept any certificates signed by that version of the CA's key.
- ☐ d. The CA publishes a special list which includes details about revoked certificates.

9. Which of the following describes the correct way to create and use a digital signature?

- ☐ a. Add the sender's name to the document, then encrypt it with the recipient's public key, send the encrypted document to the recipient.
- ☐ b. Encrypt the document with the sender's Private key, and then send the encrypted document to the recipient.
- ☐ c. Hash the document, then encrypt both the hash and the document with the sender's private key, then send the encrypted information to the recipient.
- ☐ d. Hash the document, then encrypt only the hash with the sender's private key, send both the plain text document and the encrypted hash to the recipient.

10. What is the difference between a Registration Authority (RA) and a Certificate Authority (CA)?

- ☐ a. The RA verifies the user credentials, and the CA issues the digital certificate.
- ☐ b. An RA generates the user's public/private key pair and saves them in the PKI database.
- ☐ c. The CA generates the user's public/private key pair and the RA generates the certificate.
- ☐ d. The RA verifies the user credentials, and the CA generates the user's public/private key pair.

11. Given the plaintext "rambo", which of the following statements is correct?

- ☐ a. A Caesar cipher for "rambo" would yield "abrmo".
- ☐ b. A collision occurs when two different cryptographic keys encrypt "rambo" and produce the same result.
- ☐ c. A transposition cipher, with reorder sequence 53421 would yield "ombar".
- ☐ d. The SHA1 hash value "rambo" would be exactly 16 bytes long

12. Which of the following is correct?

- ☐ a. An initialization vector (IV) is used to make sure that the encryptions of important texts do not change each time they are encrypted.
- ☐ b. Confusion refers to making the relationship between the ciphertext and the key as complex as possible, diffusion refers to dissipating the statistical structure of the plaintext over the bulk of the ciphertext.
- ☐ c. Only one substitution and one permutation can occur in an SP-network.
- ☐ d. The avalanche effect in an encryption algorithm means that the algorithm is resistant to small changes in the plaintext.

13. Which statement BEST describes how the term "key space" affects "cryptanalysis"?

- ☐ a. The larger the key space, the easier the cryptanalysis.
- ☐ b. The key space doubles each time you add a bit to the key length, which makes cryptanalysis more difficult.
- ☐ c. Cryptanalysis is designing algorithms, and key space means testing the keys to ensure they work properly.
- ☐ d. Cryptanalysis is most often accomplished by systematically reducing the size of the key space.

14. What are the key and block sizes for the AES algorithm?

- ☐ a. Keys are 128 bits, blocks are 128 and 256 bits.
- ☐ b. Keys are 128 bits, as are blocks.
- ☐ c. Both keys and blocks can be 128, 192 and 256 bits.
- ☐ d. Keys are 128, 192 and 256 bits and blocks are 128 bits.

15. Which of the following contains BOTH a hashing and an asymmetric key algorithm?

- ☐ a. DES and SHA2
- ☐ b. SHA2 and MD5
- ☐ c. MD5 and ECC
- ☐ d. AES and ECC

16. Which of the following is an attack against hashes?

- ☐ a. Known or Chosen Plaintext Attack
- ☐ b. Dictionary Attack
- ☐ c. Frequency Analysis
- ☐ d. Cipher text attack

17. Which of the following includes a pair of the OWASP Top Ten Web attacks, ordered from most to least dangerous?

- ☐ 17. Which of the following includes a pair of the OWASP Top Ten Web attacks, ordered from most to least dangerous?
- ☐ b. Cross-Site Request Forgery (CSWF), and Injection Flaws.
- ☐ c. Broken Authentication and Session Management, and Injection Flaws.
- ☐ d. Cross-Site Request Forgery (CSWF), and Cross-Site Scripting (XSS).

18. Which of the following BEST describes a Common Criteria “Protection Profile”?

- ☐ a. A set of security requirements to be used to evaluate a Security Target.
- ☐ b. A set of security requirements for a category of products that meet specific consumer security needs.
- ☐ c. An implementation-independent set of functional security requirements for a category of products that meet specific consumer security needs.
- ☐ d. An implementation-specific set of assurance requirements for products that meet specific consumer security needs.

19. Which of the following is no longer a common and effective attack on wireless networks?

- ☐ a. A Plaintext attack
- ☐ b. A Rainbow Table attack
- ☐ c. A Stream Cipher attack
- ☐ d. A Ciphertext attack

20. The Simple Integrity Property provides for the following permissions: Being able to _____.

- ☐ a. Read at the same level or at a higher level.
- ☐ b. Write at the same level or at a lower level.
- ☐ c. Read at the same level or at a lower level.
- ☐ d. Write at the same level or at a higher level.

21. Which security model is designed to help ensure that high level activities (inputs) do not determine what low-level users can see (outputs)?

- ☐ a. The Lattice model
- ☐ b. The Information Flow model
- ☐ c. The Clark-Wilson model
- ☐ d. The Non-interference model

22. Which of the following demonstrates the authenticity and origin of a communication, thereby providing for non-repudiation?

- ☐ a. Using Elliptic Curve Cryptography techniques
- ☐ b. Assigning Denial of Service certificates to senders
- ☐ c. Digital signatures
- ☐ d. E-commerce Digital certificates

23. Which security model focuses on preventing conflicts of interest when a given subject would otherwise have access to objects with sensitive information associated with two competing parties?

- ☐ a. Information Flow
- ☐ b. Non-Interference
- ☐ c. Clark-Wilson
- ☐ d. Brewer and Nash

24. Which of the following is MOST accurate with respect to individual computing devices (ICDs) on a cluster versus on a grid system?

- ☐ a. If a grid ICD fails, the grid must be restarted.
- ☐ b. If a cluster ICD fails, the cluster must be restarted.
- ☐ c. Grid systems are homogenous, while cluster systems are heterogeneous.
- ☐ d. Cluster ICDs all share the same operating system (OS) and application software, but Grid ICDs can have many different OSs while still working on solving the same problem.

25. Originally there were three Cloud Service models (CSMs) and four Cloud Deployment models (CDMs). Which group below has two original CSMs and 2 CDMs?

- ☐ a. SaaS, IDaaS, Public and Private
- ☐ b. SaaS, PaaS, Community, and Hybrid
- ☐ c. IaaS, PaaS, On-site, and Off-site
- ☐ d. NaaS, CaaS, Hybrid, and Commercial

26. Which fire prevention system does not hold water above the area it protects, contains heat-sensing elements, and only begins to fill with water when the valve is triggered by excessive heat?

- ☐ a. A dry-pipe system
- ☐ b. A deluge system
- ☐ c. A wet-pipe system
- ☐ d. A pre-action system

27. Alex received a message sent to him over the Internet by James. Alex changed the content of the message and then claimed that the altered message was the one he'd received from James. Which technique would prevent Alex from being able to make this claim?

- ☐ a. James used Public Key Cryptography to deliver the message.
- ☐ b. James digitally signed the message.
- ☐ c. James used the 512 bit version of SHA2 to hash the message and then sent this hash along with the message to Alex.
- ☐ d. James used hybrid encryption with the strong AES256 algorithm and the ECC public key algorithm to send the message to Alex.

28. What is the name of the imaginary boundary that separates the components from maintaining security from the non-security relevant components?

- ☐ a. Security kernel
- ☐ b. Security model
- ☐ c. Security perimeter
- ☐ d. Security session

29. The Trusted Computer Security Evaluation states that labeling for mandatory access control is first introduced at what level?

- ☐ a. C1
- ☐ b. B2
- ☐ c. B1
- ☐ d. A1

30. Covert channel analysis is often aided through the use of:

- ☐ a. An access control matrix
- ☐ b. Graham-Denning model
- ☐ c. Information Flow model
- ☐ d. Chinese Wall model

31. What can be defined as an abstract machine that mediates all access to objects by subjects to ensure that subjects have the necessary access rights and to protect objects from unauthorized access?

- ☐ a. The reference monitor
- ☐ b. The security kernel
- ☐ c. The trusted computing base
- ☐ d. The security domain

32. Which of the following describes a logical form of separation used by secure computing systems?

- ☐ a. Processes use different levels of security for input and output devices.
- ☐ b. Processes are constrained so that each cannot access objects outside its permitted domain
- ☐ c. Processes conceal data and computations to inhibit access by outside processes.
- ☐ d. Processes are granted access based on granularity of controlled objects.

33. Typically, an operating system performs all of the following functions, EXCEPT

- ☐ a. input or output tasks
- ☐ b. accounting and resource allocation
- ☐ c. storage assignment tasks
- ☐ d. user access to database views

34. What security problem is most likely to exist if an operating system permits objects to be used sequentially by multiple users without forcing a refresh of the objects?

- ☐ a. Disclosure of residual data
- ☐ b. Unauthorized obtaining of a privileged execution state
- ☐ c. Denial of service through a deadly embrace
- ☐ d. Buffer overflow

35. A key management philosophy is to identify the business problem and then find a solution. Which architecture formalized this but also focuses on the security architecture?

- ☐ a. SABSA
- ☐ b. ISO7498
- ☐ c. Zachman
- ☐ d. TOGAF

36. Which statement of the Clark-Wilson model is incorrect?

- ☐ a. Prevents unauthorized users from making modifications
- ☐ b. Prevents authorized users from making improper modifications
- ☐ c. Maintains internal and external consistency
- ☐ d. Prevents authorized users from making modifications

37. Which statement is incorrect for the Bell-LaPadula model?

- ☐ a. With the Simple Security Property you are able to read at your level or read at a lower level.
- ☐ b. With the Star Property you are able to write at your level or at a lower level
- ☐ c. With the Strong Star Property you are able to read and write at your level
- ☐ d. Is a Mandatory Access Control model

38. The Simple Integrity Property of the Biba Model has the following permissions:

- ☐ a. Being able to write at the same level or at a lower level
- ☐ b. Being able to read at the same level or at a lower level
- ☐ c. Being able to read at the same level or at a higher level
- ☐ d. Being able to write at the same level or at a higher level

39. Which one of the following statements of these security models is true?

- ☐ a. Bell LaPadula was only a form of Discretionary Access Control
- ☐ b. Biba used an access triple
- ☐ c. Clark and Wilson allowed controls to be put into place to only prevent unauthorized users from making changes to data and to maintain internal and external consistency
- ☐ d. Brewer and Nash tried to ensure that users would not be put into a potential conflict of interest

40. In what way does Rivest-Shamir-Adleman (RSA) algorithm differ from the Data Encryption Standard (DES)?

- ☐ a. It is based on a symmetric algorithm.
- ☐ b. It uses a public key for encryption.
- ☐ c. It eliminates the need for a key distribution center.
- ☐ d. It cannot produce a digital signature.

41. Which one of the following is NOT a valid X.509 V.3 certificate field?

- ☐ a. Subject’s public key information
- ☐ b. Subject’s X.500 name
- ☐ c. Issuer’s unique identifier
- ☐ d. Subject’s digital signature

42. Key clustering is defined as

- ☐ a. Two different plaintext files that are hashed with the same algorithm yield the same message digest.
- ☐ b. Two exact plaintext files, that are hashed using the same algorithm, yield the same message digest.
- ☐ c. The same plaintext file, when encrypted by two separate keys, produces the same ciphertext.
- ☐ d. The same plaintext files, when encrypted by two separate keys, produces different ciphertext.

43. The best way to defeat frequency analysis as a method to determine the key is to use:

- ☐ a. Substitution ciphers
- ☐ b. Transposition ciphers
- ☐ c. Polyalphabetic ciphers
- ☐ d. Inversion ciphers

44. Which of the following represents an addition to a message digest algorithm to increase its cryptographic strength?

- ☐ a. Internet Security Association and Key Management Protocol (ISAKMP)/Oakley
- ☐ b. Keyed-Hash Message Authentication Code (HMAC)
- ☐ c. Triple Data Encryption Standard (3DES)
- ☐ d. Message Digest 5 (MD5)

45. When is a cryptographic security product considered at the end of its cryptographic life cycle?

- ☐ a. The cryptographic decryption algorithm is posted online
- ☐ b. The cryptographic algorithm key has reached the end of its cryptoperiod.
- ☐ c. The cryptographic algorithm is susceptible to cryptanalytic attacks.
- ☐ d. The cryptographic algorithm uses a key length of less than 128 bits.

46. Which of the following statements is true about digital signature?

- ☐ a. It is a method used to encrypt confidential data.
- ☐ b. It is the art of transferring handwritten signature to electronic media.
- ☐ c. It allows the recipient of data to prove the source and integrity of the data.
- ☐ d. It can be used as a signature system and a cryptosystem.

47. What characteristic of Electronic Code (ECB) mode makes it unsuitable for long messages?

- ☐ a. Block fragmentation causes message cipher instability.
- ☐ b. Weak keys will produce symmetric message holes.
- ☐ c. Repeated message blocks produce repeated cipher text blocks.
- ☐ d. Message errors cannot be contained.

48. In cryptography, collisions are defined as

- ☐ a. Two different plaintext files that are hashed with the same algorithm yield the same message digest.
- ☐ b. Two exact plaintext files, that are hashed using the same algorithm, yield the same message digest.
- ☐ c. The same plaintext file, when encrypted by two separate keys, produces the same ciphertext.
- ☐ d. The same plaintext files, when encrypted by two separate keys, produces different ciphertext.

49. In what type of attack does an attacker try having access to the plaintext block and the corresponding cipher text block, to figure out the key used in the encryption process?

- ☐ a. Known Plaintext Attack
- ☐ b. Ciphertext Only Attack
- ☐ c. Chosen Ciphertext Attack
- ☐ d. Side Channel Attack

50. In what type of attack does an attacker try having access to only several encrypted messages, to figure out the key used in the encryption process?

- ☐ a. Known Plaintext Attack
- ☐ b. Ciphertext Only Attack
- ☐ c. Chosen Ciphertext Attack
- ☐ d. Side Channel Attack

51. Where parties do not have a shared secret and large quantities of sensitive information must be transmitted, the most efficient means of transferring information is to use a hybrid encryption technique. What does this mean?

- ☐ a. Use of public key encryption to secure a secret key, and message encryption using the secret key
- ☐ b. Use of the recipient's public key for encryption and decryption based on the recipient's private key
- ☐ c. Use of software encryption assisted by a hardware encryption accelerator
- ☐ d. Use of elliptical curve encryption

52. If a cryptographic algorithm is found to be susceptible to Chosen Ciphertext Attacks, it may allow an attacker to

- ☐ a. Determine how many rounds are being used during the encryption process
- ☐ b. Reveal the secret key
- ☐ c. Encrypt any desired plaintext to achieve a desired ciphertext
- ☐ d. Simply exhaustive search through all possible keys supported by the algorithm

53. Why is projection lighting mounted at the same height as the barbed wire topping of a fence?

- ☐ a. It makes it easier to observe an intruder climbing over the fence.
- ☐ b. It increases the field of view for those observing the scene.
- ☐ c. It lowers the height and cost of observation the scene.
- ☐ d. It blinds the approaching intruder's view of the scene.

54. Security Guards are appropriate whenever the functions required by the security program involve

- ☐ a. the use of discriminating judgment
- ☐ b. the operation of access control devices
- ☐ c. the operation of intrusion detection devices
- ☐ d. the need to detect changes in the physical environment

55. Under what conditions would use of a "Class C" hand-held fire extinguisher to be preferred to use of a "Class A"?

- ☐ a. When the fire is in its incipient stage
- ☐ b. When the fire involves electrical equipment
- ☐ c. When the fire is located in an enclosed area
- ☐ d. When the fire is caused by flammable products

56. How does closed-circuit television (CCTV) help management and security forces minimize loss during a disaster or emergency?

- ☐ a. Facilitates direction of resources to hardest hit area
- ☐ b. Records instances of looting and other criminal activities
- ☐ c. Documents shortcomings of plans and procedures
- ☐ d. Captures the exposure of assets to physical risk

57. When considering the Heating, Ventilation, and Air Conditioning (HVAC) requirements for a data processing center, why should an information security architect be concerned with the effect of humidity on data availability?

- ☐ a. Low humidity may cause condensation to occur, which would lead to data loss through a short circuit
- ☐ b. High humidity may lead to high electrostatic buildup, which could lead to data loss through static discharge
- ☐ c. High humidity may cause condensation to occur, which would lead to data loss through a short circuit
- ☐ d. Low humidity may lead to high electrostatic buildup, which could lead to data loss through static discharge

58. Which of these is NOT a common method of achieving memory protection?

- ☐ a. Segmentation
- ☐ b. Paging
- ☐ c. Reference monitor
- ☐ d. Keying

59. Which of these is NOT an advantage of an Enterprise Security Architecture (ESA)?

- ☐ a. Provides a monolithic solution
- ☐ b. It presents a long-term, strategic view of the system
- ☐ c. It unifies security controls
- ☐ d. It leverages existing technology investments

60. Which of these is a confidentiality model?

- ☐ a. Biba
- ☐ b. Graham-Denning
- ☐ c. Brewer-Nash
- ☐ d. Clark-Wilson

61. In lattice models, the STAR property refers to _____

- ☐ a. reading only
- ☐ b. writing only
- ☐ c. reading and writing
- ☐ d. invocation

62. Which of these security models is the combination of two other models?

- ☐ a. Lipner
- ☐ b. Clark-Wilson
- ☐ c. Brewer-Nash
- ☐ d. Biba

63. The main evaluation model in use today is

- ☐ a. The Rainbow Series
- ☐ b. TCSEC (Trusted Computer System Evaluation Criteria)
- ☐ c. ITSEC (Information Technology System Evaluation Criteria)
- ☐ d. Common Criteria

64. PCI-DSS is mandated via _____

- ☐ a. law
- ☐ b. regulation
- ☐ c. contract
- ☐ d. ISO standard

65. A CPU must be able to support two states, which are _____

- ☐ a. privilege and problem
- ☐ b. supervisor and problem
- ☐ c. Ring 2 and Ring 1
- ☐ d. supervisor and error

66. Which of the following BEST describes the differences in a thin client solution versus a diskless workstation solution?

- ☐ a. Storage in on external media such a thumb drive when using a diskless workstation, but in the cloud when using a thin client.
- ☐ b. Storage is on a central computer when using a diskless workstation, but in the cloud when using a thin client.
- ☐ c. Thin clients do processing on the station itself, but diskless workstations do it on a central computer.
- ☐ d. Diskless workstations do processing on the station itself but thin clients do it on a central computer.

67. Which statement about grid computing is FALSE?

- ☐ a. Grid computers can have different operating systems.
- ☐ b. Idle resources on a desktop computer can be made part of a grid
- ☐ c. Grid nodes can be geographically dispersed
- ☐ d. Grid computers are also known as computing clusters

68. In cloud computing, the responsibility for effective controls and countermeasures _____

- ☐ a. remains with the original data owner, but also becomes the responsibility of the cloud provider.
- ☐ b. Shifts to the cloud provider.
- ☐ c. Transfers entirely to the cloud provider.
- ☐ d. Are the same as they were before moving to the cloud.

69. A digital signature does NOT _____

- ☐ a. provide non-repudiation of origin.
- ☐ b. Provide proof of integrity
- ☐ c. Provide proof of delivery
- ☐ d. Use asymmetric keys

70. In a hybrid protocol such as SSL/TLS, the session key is encrypted with the _____

- ☐ a. sender’s private key
- ☐ b. sender’s public key
- ☐ c. receiver’s private key
- ☐ d. receiver’s public key

71. In SSL/TLS, the session key is _____

- ☐ a. based on the previous session key.
- ☐ b. A random number generated by the server.
- ☐ c. A random number generated by the client.
- ☐ d. Exchanged via out-of-band communication.

72. Which of the entries on this list happens before the others when establishing a SSL/TLS session?

- ☐ a. Validate that the certificate has not expired.
- ☐ b. Validate that the name on the certificate matches the domain name on the website.
- ☐ c. Check the CRL (Certificate Revocation List).
- ☐ d. Exchange certificates.

73. Given that a cryptanalyst has several samples of plaintext and ciphertext to work with, which of these techniques is most likely to reveal the key in the shortest amount of time?

- ☐ a. known plaintext
- ☐ b. chosen plaintext
- ☐ c. chosen ciphertext
- ☐ d. brute force

74. Which of these is a step in creating a digital signature?

- ☐ a. Encrypt the message with receiver's public key
- ☐ b. Encrypt the message with the sender's public key
- ☐ c. Encrypt the hash with the receiver's public key
- ☐ d. Encrypt the hash with the sender's private key

75. Which of the following is a transposition cipher?

- ☐ a. Caesar cipher
- ☐ b. Vigenere cipher
- ☐ c. Spartan scytale
- ☐ d. Enigma machine

76. Which of the following is NOT a component of CPTED (Crime Prevention Through Environmental Design)?

- ☐ a. Access Control
- ☐ b. Guards
- ☐ c. Surveillance
- ☐ d. Territoriality

77. Which of these types of glass is LEAST able to withstand wide temperature variations?

- ☐ a. Plate glass
- ☐ b. Tempered glass
- ☐ c. Acrylic glass
- ☐ d. Polycarbonate glass

78. Which of these is most dangerous when a wiring closet catches fire?

- ☐ a. Power outage
- ☐ b. Internet data outage
- ☐ c. Telephone outage
- ☐ d. Noxious fumes

79. Attacking Supervisory Control and Data Acquisition (SCADA) systems via a virus or worm _____

- ☐ a. is easy because there's no built in security
- ☐ b. is difficult, they use DNP3 which is not compatible with IPv4.
- ☐ c. Is of moderate difficulty, it requires human assistance – but social engineering is easy
- ☐ d. Is impossible, SCADA systems are stand-alone devices not connected to the Internet.

80. There are five essential characteristics of cloud computing. Which grouping contains three of these?

- ☐ a. broad network access, rapid elasticity, IaaS
- ☐ b. resource pooling, measured service, on-demand self-service
- ☐ c. rapid elasticity, hybrid cloud, broad network access
- ☐ d. PaaS, measured service, resource pooling