Chapter 3
Security Architecture and Engineering (Domain 3)

1. Matthew is the security administrator for a consulting firm and must enforce access controls that restrict users' access based upon their previous activity. For example, once a consultant accesses data belonging to Acme Cola, a consulting client, they may no longer access data belonging to any of Acme's competitors. What security model best fits Matthew's needs?
    1. Clark-Wilson
    2. Biba
    3. Bell-LaPadula
    4. Brewer-Nash
2. Referring to the figure shown here, what is the earliest stage of a fire where it is possible to use detection technology to identify it?

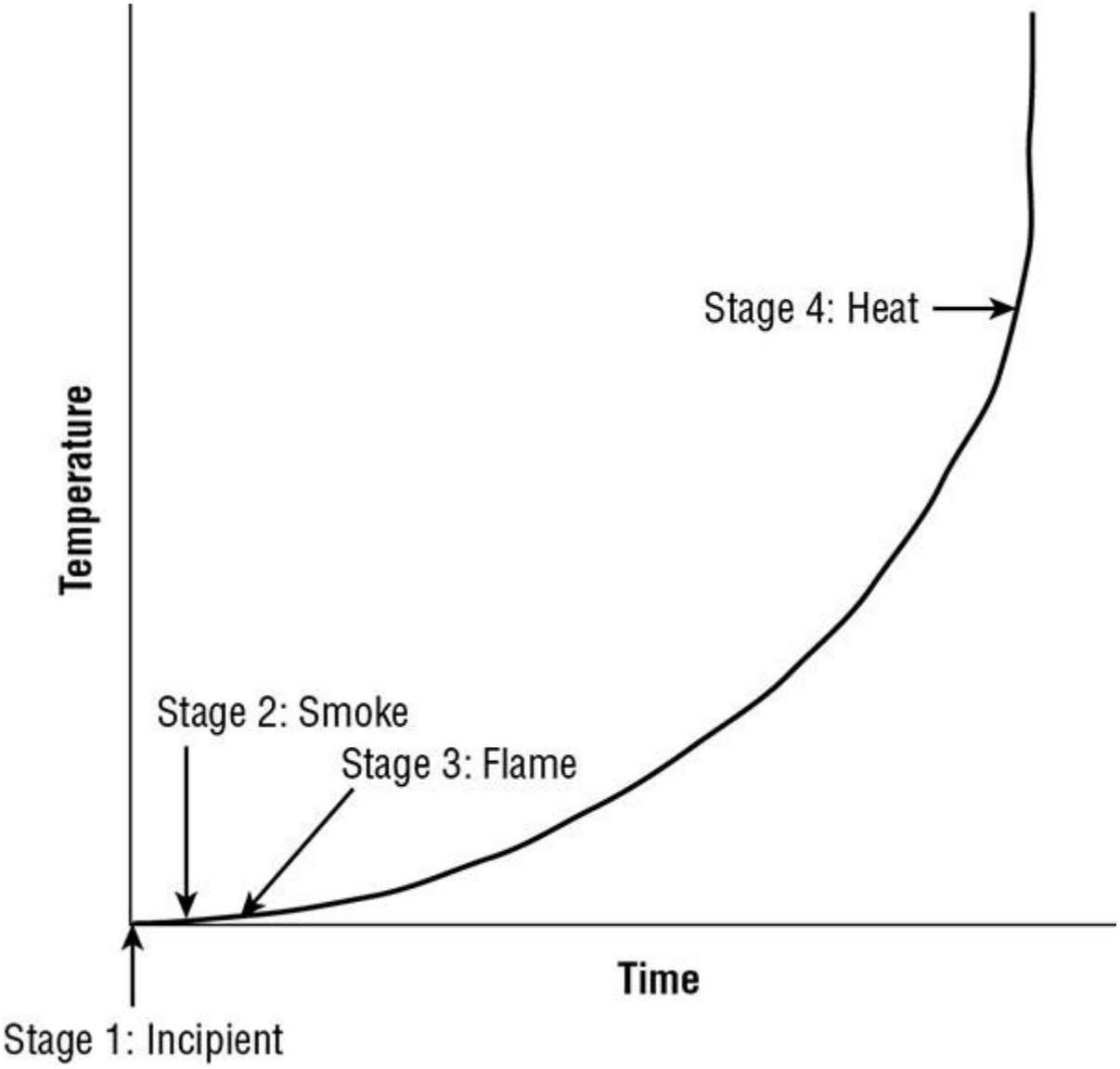


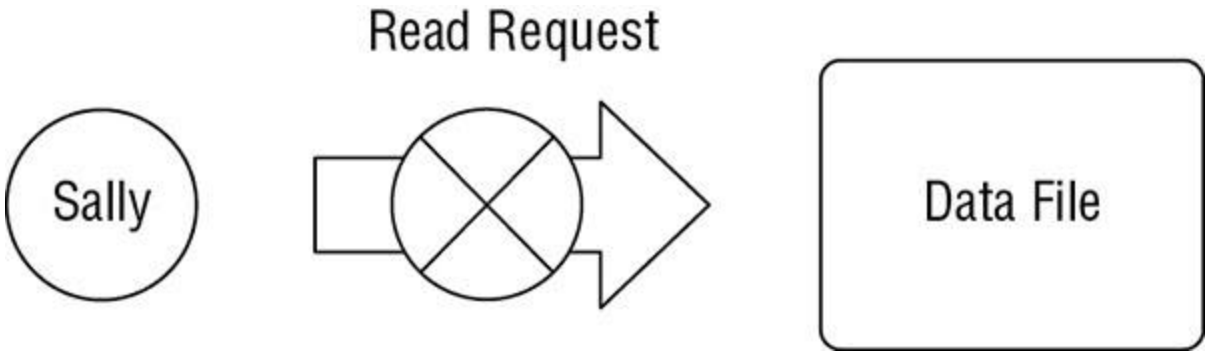
Image reprinted from *CISSP (ISC)^2 Certified Information Systems Security Professional Official Study Guide, 7th Edition* © John Wiley & Sons 2015, reprinted with permission.

1. Incipient
2. Smoke
3. Flame
4. Heat

3. Ralph is designing a physical security infrastructure for a new computing facility that will remain largely unstaffed. He plans to implement motion detectors in the facility but would also like to include a secondary verification control for physical presence. Which one of the following would best meet his needs?
    1. CCTV
    2. IPS
    3. Turnstiles

    4. Faraday cages
4. Harry would like to retrieve a lost encryption key from a database that uses m of n control, with m = 4 and n = 8. What is the minimum number of escrow agents required to retrieve the key?
    1. 2
    2. 4
    3. 8
    4. 12
5. Fran's company is considering purchasing a web-based email service from a vendor and eliminating its own email server environment as a cost-saving measure. What type of cloud computing environment is Fran's company considering?
    1. SaaS
    2. IaaS
    3. CaaS
    4. PaaS
6. Bob is a security administrator with the federal government and wishes to choose a digital signature approach that is an approved part of the federal Digital Signature Standard under FIPS 186-4. Which one of the following encryption algorithms is not an acceptable choice for use in digital signatures?
    1. DSA
    2. HAVAL
    3. RSA
    4. ECDSA
7. Harry would like to access a document owned by Sally and stored on a file server. Applying the subject/object model to this scenario, who or what is the subject of the resource request?
    1. Harry
    2. Sally
    3. Server
    4. Document
8. Michael is responsible for forensic investigations and is investigating a medium-severity security incident that involved the defacement of a corporate website. The web server in question ran on a virtualization platform, and the marketing team would like to get the website up and running as quickly as possible. What would be the most reasonable next step for Michael to take?
    1. Keep the website offline until the investigation is complete.
    2. Take the virtualization platform offline as evidence.
    3. Take a snapshot of the compromised system and use that for the investigation.
    4. Ignore the incident and focus on quickly restoring the website.
9. Helen is a software engineer and is developing code that she would like to restrict to running within an isolated sandbox for security purposes. What software development technique is Helen using?
    1. Bounds
    2. Input validation
    3. Confinement
    4. TCB

10. What concept describes the degree of confidence that an organization has that its controls satisfy security requirements?
    1. Trust
    2. Credentialing
    3. Verification
    4. Assurance
11. What type of security vulnerability are developers most likely to introduce into code when they seek to facilitate their own access, for testing purposes, to software they developed?
    1. Maintenance hook
    2. Cross-site scripting
    3. SQL injection
    4. Buffer overflow
12. In the figure shown here, Sally is blocked from reading the file due to the Biba integrity model. Sally has a Secret security clearance, and the file has a Confidential classification. What principle of the Biba model is being enforced?



    1. Simple Security Property
    2. Simple Integrity Property
    3. *-Security Property
    4. *-Integrity Property
13. Tom is responsible for maintaining the security of systems used to control industrial processes located within a power plant. What term is used to describe these systems?
    1. POWER
    2. SCADA
    3. HAVAL
    4. COBOL
14. Sonia recently removed an encrypted hard drive from a laptop and moved it to a new device because of a hardware failure. She is having difficulty accessing encrypted content on the drive despite the fact that she knows the user's password. What hardware security feature is likely causing this problem?
    1. TCB
    2. TPM
    3. NIACAP
    4. RSA

15. Chris wants to verify that a software package that he downloaded matches the original version. What hashing tool should he use if he believes that technically sophisticated attackers may have replaced the software package with a version containing a backdoor?
    1. MD5
    2. 3DES
    3. SHA1
    4. SHA 256

    For questions 16–19, please refer to the following scenario:

    Alice and Bob would like to use an asymmetric cryptosystem to communicate with each other. They are located in different parts of the country but have exchanged encryption keys by using digital certificates signed by a mutually trusted certificate authority.

16. If Alice wishes to send Bob an encrypted message, what key does she use to encrypt the message?
    1. Alice's public key
    2. Alice's private key
    3. Bob's public key
    4. Bob's private key
17. When Bob receives the encrypted message from Alice, what key does he use to decrypt the message?
    1. Alice's public key
    2. Alice's private key
    3. Bob's public key
    4. Bob's private key
18. Which one of the following keys would Bob not possess in this scenario?
    1. Alice's public key
    2. Alice's private key
    3. Bob's public key
    4. Bob's private key
19. Alice would also like to digitally sign the message that she sends to Bob. What key should she use to create the digital signature?
    1. Alice's public key
    2. Alice's private key
    3. Bob's public key
    4. Bob's private key
20. What name is given to the random value added to a password in an attempt to defeat rainbow table attacks?
    1. Hash
    2. Salt
    3. Extender
    4. Rebar
21. Which one of the following is not an attribute of a hashing algorithm?
    1. They require a cryptographic key.

2. They are irreversible.
3. It is very difficult to find two messages with the same hash value.
4. They take variable-length input.

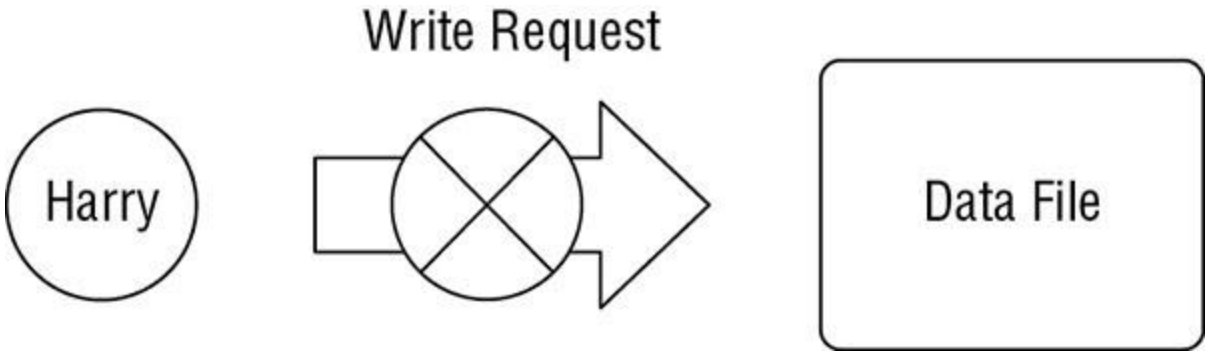
22. What type of fire suppression system fills with water when the initial stages of a fire are detected and then requires a sprinkler head heat activation before dispensing water?
    1. Wet pipe
    2. Dry pipe
    3. Deluge
    4. Preaction
23. Susan would like to configure IPsec in a manner that provides confidentiality for the content of packets. What component of IPsec provides this capability?
    1. AH
    2. ESP
    3. IKE
    4. ISAKMP
24. Which one of the following cryptographic goals protects against the risks posed when a device is lost or stolen?
    1. Nonrepudiation
    2. Authentication
    3. Integrity
    4. Confidentiality
25. What logical operation is described by the truth table shown here?

Input 1	Input 2	Output
0	0	0
0	1	1
1	0	1
1	1	0

    1. OR
    2. AND
    3. XOR
    4. NOR
26. How many bits of keying material does the Data Encryption Standard use for encrypting information?
    1. 56 bits

2. 64 bits
3. 128 bits
4. 256 bits

27. In the figure shown here, Harry's request to write to the data file is blocked. Harry has a Secret security clearance, and the data file has a Confidential classification. What principle of the Bell-LaPadula model blocked this request?



1. Simple Security Property
2. Simple Integrity Property
3. *-Security Property
4. Discretionary Security Property

28. Florian and Tobias would like to begin communicating using a symmetric cryptosystem, but they have no prearranged secret and are not able to meet in person to exchange keys. What algorithm can they use to securely exchange the secret key?
    1. IDEA
    2. Diffie-Hellman
    3. RSA
    4. MD5
29. Under the Common Criteria, what element describes the security requirements for a product?
    1. TCSEC
    2. ITSEC
    3. PP
    4. ST
30. Which one of the following is not one of the basic requirements for a cryptographic hash function?
    1. The function must work on fixed-length input.
    2. The function must be relatively easy to compute for any input.
    3. The function must be one way.
    4. The function must be collision free.
31. How many possible keys exist for a cipher that uses a key containing 5 bits?
    1. 10
    2. 16
    3. 32
    4. 64

32. What cryptographic principle stands behind the idea that cryptographic algorithms should be open to public inspection?
    1. Security through obscurity
    2. Kerckhoff's principle
    3. Defense in depth
    4. Heisenburg principle
33. Referring to the figure shown here, what is the name of the security control indicated by the arrow?

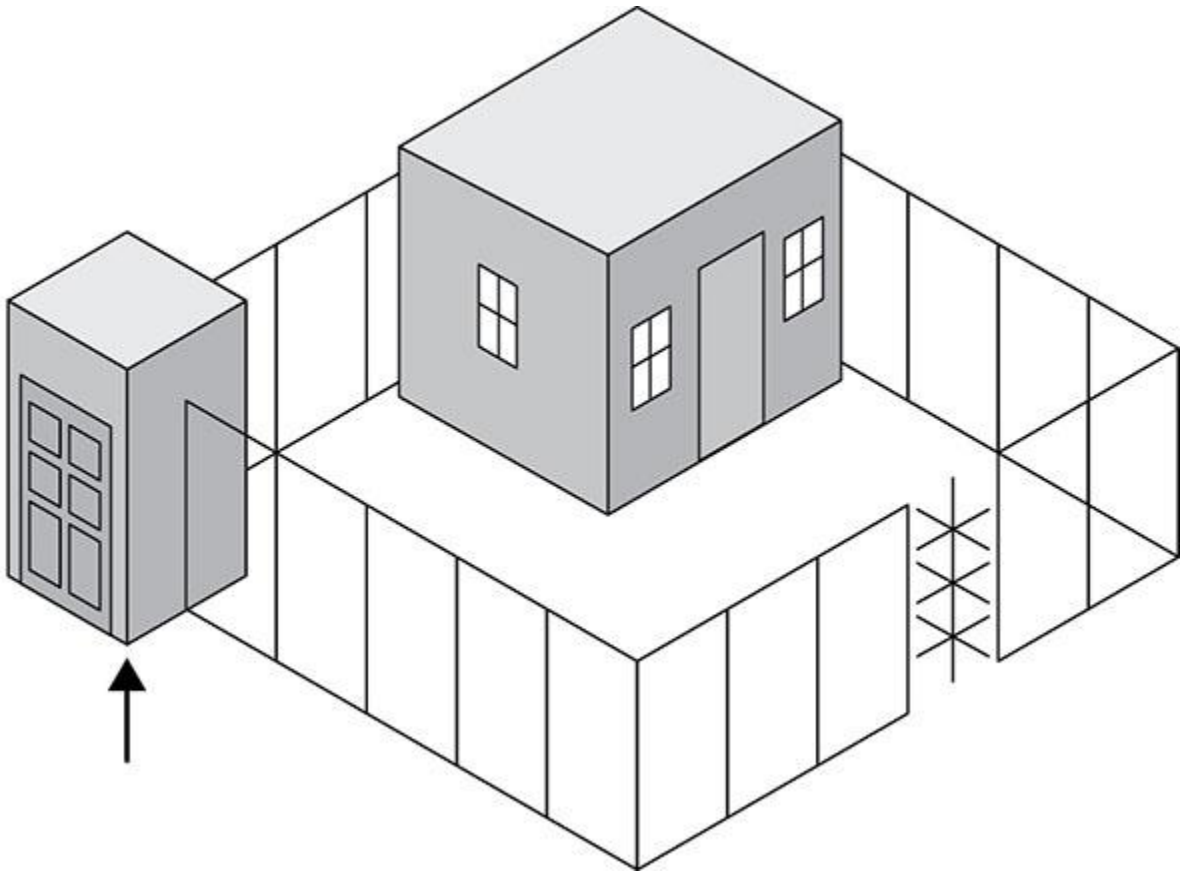
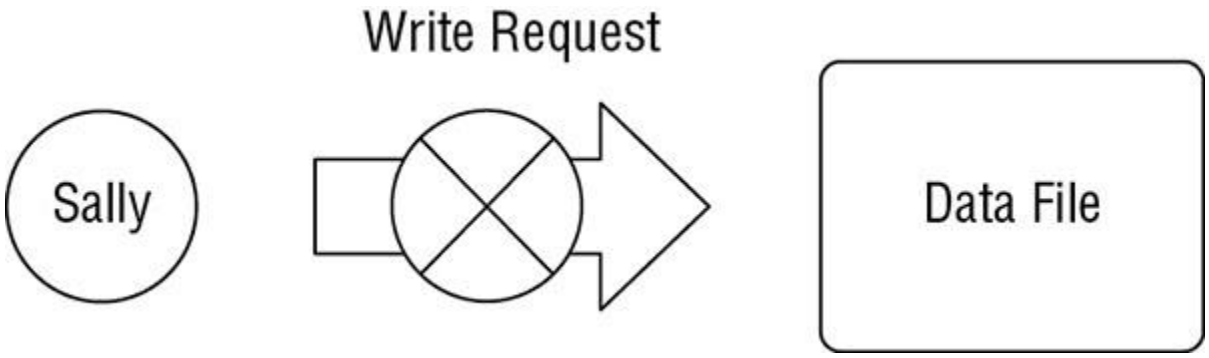


Image reprinted from *CISSP (ISC)* [2] *Certified Information Systems Security Professional Official Study Guide, 7th Edition* © John Wiley & Sons 2015, reprinted with permission.

    1. Mantrap
    2. Turnstile
    3. Intrusion prevention system
    4. Portal
34. Which one of the following does not describe a standard physical security requirement for wiring closets?
    1. Place only in areas monitored by security guards.
    2. Do not store flammable items in the closet.
    3. Use sensors on doors to log entries.
    4. Perform regular inspections of the closet.

35. In the figure shown here, Sally is blocked from writing to the data file by the Biba integrity model. Sally has a Secret security clearance, and the file is classified Top Secret. What principle is preventing her from writing to the file?



    1. Simple Security Property
    2. Simple Integrity Property
    3. *-Security Property
    4. *-Integrity Property

36. Match each of these following numbered architecture security concepts with the appropriate lettered description:

    Architectural security concepts

    1. Time of check
    2. Covert channel
    3. Time of use
    4. Maintenance hooks
    5. Parameter checking
    6. Race condition

    Descriptions

    7. A method used to pass information over a path not normally used for communication
    8. The exploitation of the difference between time of check and time of use
    9. The time at which the subject checks whether an object is available
    10. The time at which a subject can access an object
    11. An access method known only to the developer of the system
    12. A method that can help prevent buffer overflow attacks

37. What is the minimum number of independent parties necessary to implement the Fair Cryptosystems approach to key escrow?
    1. 1
    2. 2
    3. 3
    4. 4

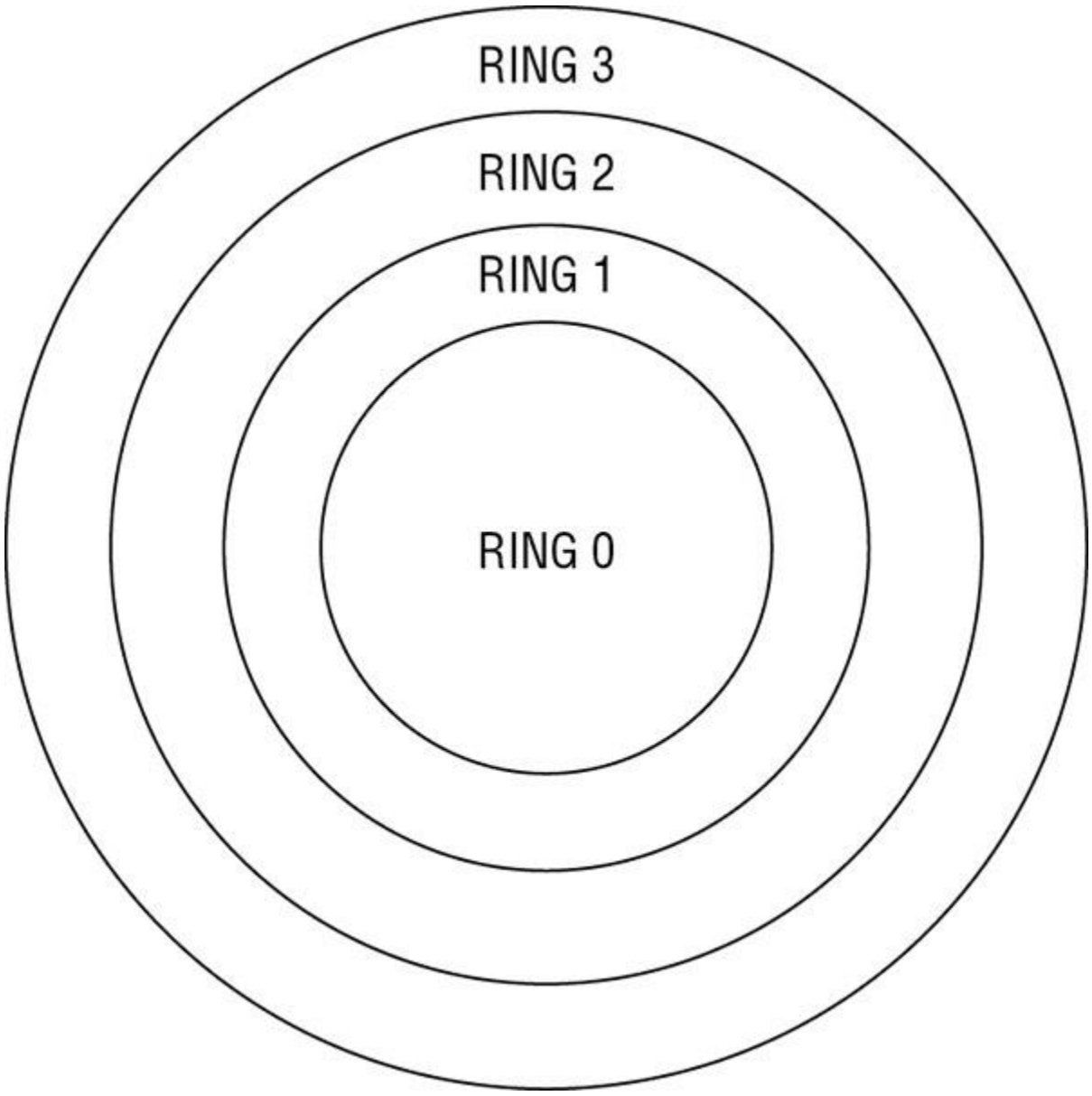
38. In what state does a processor's scheduler place a process when it is prepared to execute but the CPU is not currently available?
    1. Ready
    2. Running
    3. Waiting
    4. Stopped
39. Alan is reviewing a system that has been assigned the EAL1 evaluation assurance level under the Common Criteria. What is the degree of assurance that he may have about the system?
    1. It has been functionally tested.
    2. It has been structurally tested.
    3. It has been formally verified, designed, and tested.
    4. It has been methodically designed, tested, and reviewed.
40. Which one of the following components is used to assign classifications to objects in a mandatory access control system?
    1. Security label
    2. Security token
    3. Security descriptor
    4. Security capability
41. What type of software program exposes the code to anyone who wishes to inspect it?
    1. Closed source
    2. Open source
    3. Fixed source
    4. Unrestricted source
42. Adam recently configured permissions on an NTFS filesystem to describe the access that different users may have to a file by listing each user individually. What did Adam create?
    1. An access control list
    2. An access control entry
    3. Role-based access control
    4. Mandatory access control
43. Betty is concerned about the use of buffer overflow attacks against a custom application developed for use in her organization. What security control would provide the strongest defense against these attacks?
    1. Firewall
    2. Intrusion detection system
    3. Parameter checking
    4. Vulnerability scanning
44. Which one of the following terms is not used to describe a privileged mode of system operation?
    1. User mode
    2. Kernel mode
    3. Supervisory mode
    4. System mode

45. James is working with a Department of Defense system that is authorized to simultaneously handle information classified at the Secret and Top Secret levels. What type of system is he using?
    1. Single state
    2. Unclassified
    3. Compartmented
    4. Multistate
46. Kyle is being granted access to a military computer system that uses System High mode. What is not true about Kyle's security clearance requirements?
    1. Kyle must have a clearance for the highest level of classification processed by the system, regardless of his access.
    2. Kyle must have access approval for all information processed by the system.
    3. Kyle must have a valid need to know for all information processed by the system.
    4. Kyle must have a valid security clearance.
47. Gary intercepts a communication between two individuals and suspects that they are exchanging secret messages. The content of the communication appears to be the image shown here. What type of technique may the individuals use to hide messages inside this image?

    1. Visual cryptography
    2. Steganography
    3. Cryptographic hashing
    4. Transport layer security
48. Which one of the following terms accurately describes the Caesar cipher?
    1. Transposition cipher
    2. Block cipher
    3. Shift cipher

4. Strong cipher

49. In the ring protection model shown here, what ring contains the operating system's kernel?



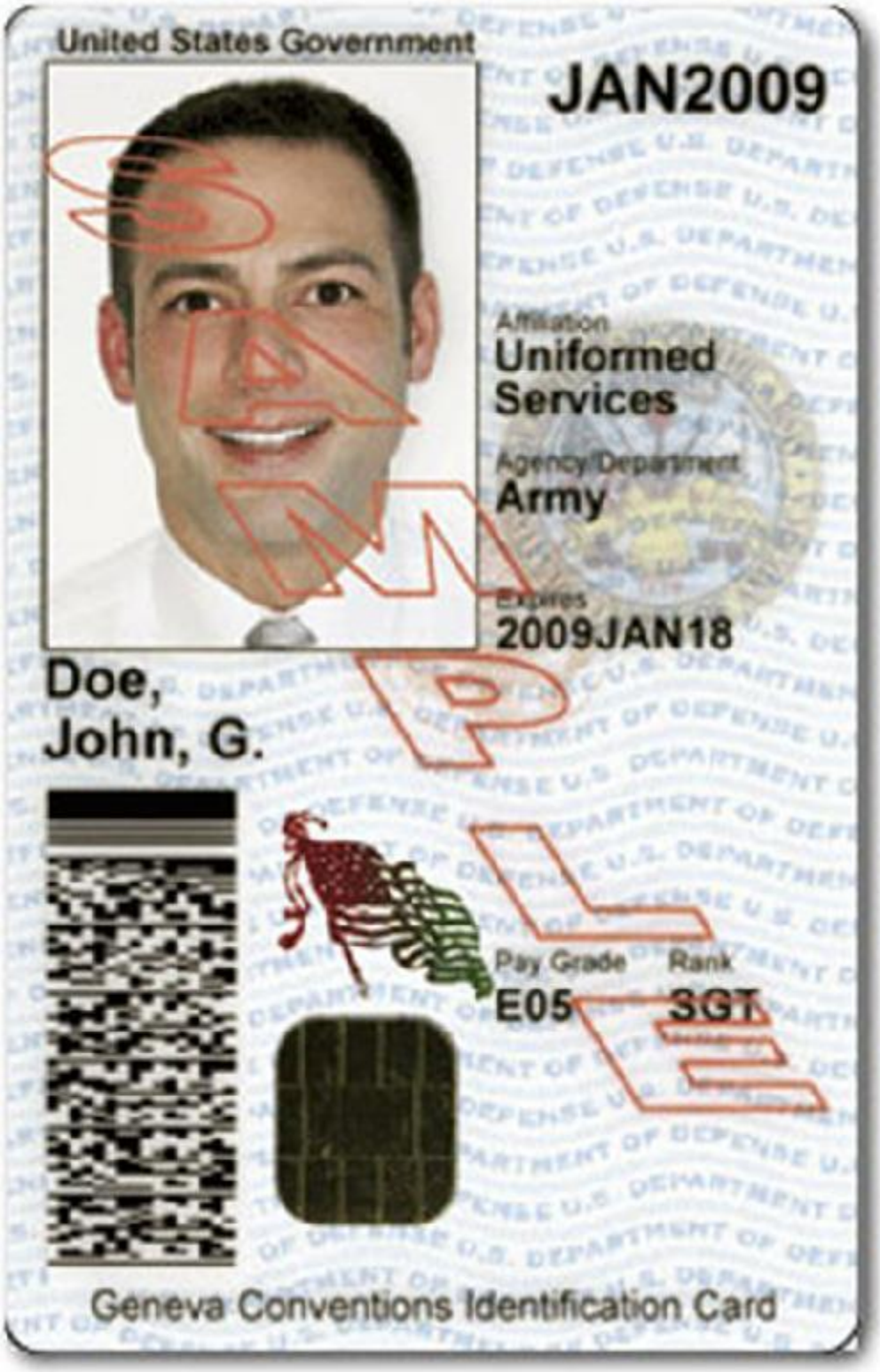
1. Ring 0
2. Ring 1
3. Ring 2
4. Ring 3

50. In an infrastructure as a service (IaaS) environment where a vendor supplies a customer with access to storage services, who is normally responsible for removing sensitive data from drives that are taken out of service?
    1. Customer's security team
    2. Customer's storage team

3. Customer's vendor management team
4. Vendor

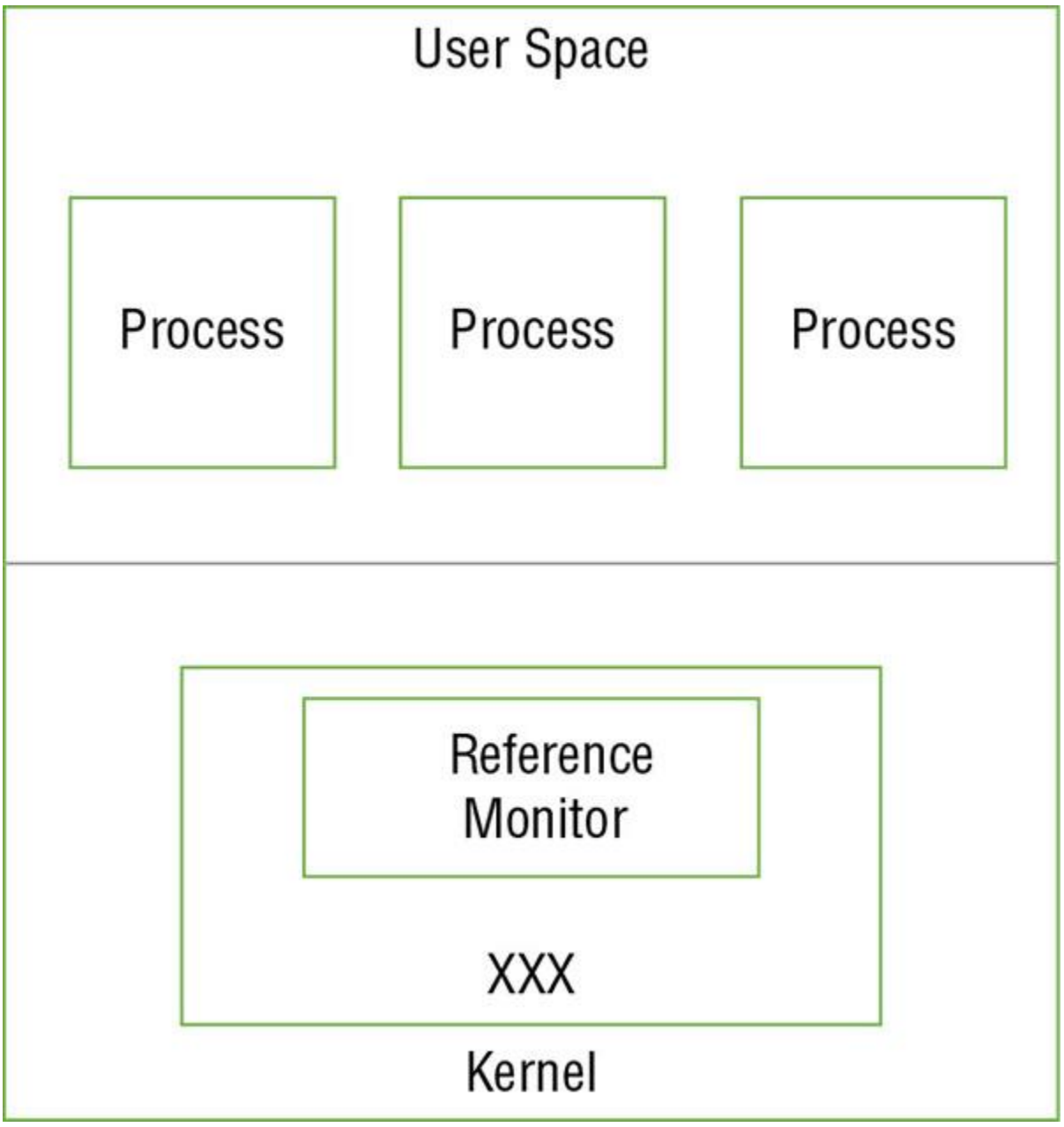
51. Which one of the following is an example of a code, not a cipher?
    1. Data Encryption Standard
    2. "One if by land; two if by sea"
    3. Shifting letters by three
    4. Word scramble
52. Which one of the following systems assurance processes provides an independent third-party evaluation of a system's controls that may be trusted by many different organizations?
    1. Certification
    2. Definition
    3. Verification
    4. Accreditation
53. Process _____ ensures that any behavior will affect only the memory and resources associated with a process.
    1. Restriction
    2. Isolation
    3. Limitation
    4. Parameters
54. Harold is assessing the susceptibility of his environment to hardware failures and would like to identify the expected lifetime of a piece of hardware. What measure should he use for this?
    1. MTTR
    2. MTTF
    3. RTO
    4. MTO
55. What type of fire extinguisher is useful only against common combustibles?
    1. Class A
    2. Class B
    3. Class C
    4. Class D
56. Gary is concerned about applying consistent security settings to the many mobile devices used throughout his organization. What technology would best assist with this challenge?
    1. MDM
    2. IPS
    3. IDS
    4. SIEM
57. Alice sent a message to Bob. Bob would like to demonstrate to Charlie that the message he received definitely came from Alice. What goal of cryptography is Bob attempting to achieve?
    1. Authentication
    2. Confidentiality
    3. Nonrepudiation
    4. Integrity

58. Rhonda is considering the use of new identification cards for physical access control in her organization. She comes across a military system that uses the card shown here. What type of card is this?



1. Smart card
2. Proximity card
3. Magnetic stripe card
4. Phase three card

59. Gordon is concerned about the possibility that hackers may be able to use the Van Eck radiation phenomenon to remotely read the contents of computer monitors in his facility. What technology would protect against this type of attack?
    1. TCSEC
    2. SCSI
    3. GHOST
    4. TEMPEST
60. In the diagram shown here of security boundaries within a computer system, what component's name has been replaced with XXX?



1. Kernel
2. TCB
3. Security perimeter
4. User execution

61. Sherry conducted an inventory of the cryptographic technologies in use within her organization and found the following algorithms and protocols in use. Which one of these technologies should she replace because it is no longer considered secure?
    1. MD5
    2. 3DES
    3. PGP
    4. WPA2

62. What action can you take to prevent accidental data disclosure due to wear leveling on an SSD device before reusing the drive?
    1. Reformatting
    2. Disk encryption
    3. Degaussing
    4. Physical destruction
63. Tom is a cryptanalyst and is working on breaking a cryptographic algorithm's secret key. He has a copy of an intercepted message that is encrypted, and he also has a copy of the decrypted version of that message. He wants to use both the encrypted message and its decrypted plaintext to retrieve the secret key for use in decrypting other messages. What type of attack is Tom engaging in?
    1. Chosen ciphertext
    2. Chosen plaintext
    3. Known plaintext
    4. Brute force
64. A hacker recently violated the integrity of data in James's company by modifying a file using a precise timing attack. The attacker waited until James verified the integrity of a file's contents using a hash value and then modified the file between the time that James verified the integrity and read the contents of the file. What type of attack took place?
    1. Social engineering
    2. TOCTOU
    3. Data diddling
    4. Parameter checking
65. What standard governs the creation and validation of digital certificates for use in a public key infrastructure?
    1. X.509
    2. TLS
    3. SSL
    4. 802.1x
66. What is the minimum fence height that makes a fence difficult to climb easily, deterring most intruders?
    1. 3 feet
    2. 4 feet
    3. 5 feet
    4. 6 feet
67. Johnson Widgets strictly limits access to total sales volume information, classifying it as a competitive secret. However, shipping clerks have unrestricted access to order records to facilitate transaction completion. A shipping clerk recently pulled all of the individual sales records for a quarter and totaled them up to determine the total sales volume. What type of attack occurred?
    1. Social engineering
    2. Inference
    3. Aggregation
    4. Data diddling
68. What physical security control broadcasts false emanations constantly to mask the presence of true electromagnetic emanations from computing equipment?

1. Faraday cage
2. Copper-infused windows
3. Shielded cabling
4. White noise

69. In a software as a service cloud computing environment, who is normally responsible for ensuring that appropriate firewall controls are in place to protect the application?
    1. Customer's security team
    2. Vendor
    3. Customer's networking team
    4. Customer's infrastructure management team
70. Alice has read permissions on an object, and she would like Bob to have those same rights. Which one of the rules in the Take-Grant protection model would allow her to complete this operation?
    1. Create rule
    2. Remove rule
    3. Grant rule
    4. Take rule
71. As part of his incident response process, Charles securely wipes the drive of a compromised machine and reinstalls the operating system (OS) from original media. Once he is done, he patches the machine fully and applies his organization's security templates before reconnecting the system to the network. Almost immediately after the system is returned to service, he discovers that it has reconnected to the same botnet it was part of before. Where should Charles look for the malware that is causing this behavior?
    1. The operating system partition
    2. The system BIOS or firmware
    3. The system memory
    4. The installation media
72. Which one of the following computing models allows the execution of multiple concurrent tasks within a single process?
    1. Multitasking
    2. Multiprocessing
    3. Multiprogramming
    4. Multithreading
73. Alan intercepts an encrypted message and wants to determine what type of algorithm was used to create the message. He first performs a frequency analysis and notes that the frequency of letters in the message closely matches the distribution of letters in the English language. What type of cipher was most likely used to create this message?
    1. Substitution cipher
    2. AES
    3. Transposition cipher
    4. 3DES
74. The Double DES (2DES) encryption algorithm was never used as a viable alternative to the original DES algorithm. What attack is 2DES vulnerable to that does not exist for the DES or 3DES approach?
    1. Chosen ciphertext

2. Brute force
3. Man in the middle
4. Meet in the middle

75. Grace would like to implement application control technology in her organization. Users often need to install new applications for research and testing purposes, and she does not want to interfere with that process. At the same time, she would like to block the use of known malicious software. What type of application control would be appropriate in this situation?
    1. Blacklisting
    2. Graylisting
    3. Whitelisting
    4. Bluelisting
76. Warren is designing a physical intrusion detection system for his data center and wants to include technology that issues an alert if the communications lines for the alarm system are unexpectedly cut. What technology would meet this requirement?
    1. Heartbeat sensor
    2. Emanation security
    3. Motion detector
    4. Faraday cage
77. John and Gary are negotiating a business transaction, and John must demonstrate to Gary that he has access to a system. He engages in an electronic version of the "magic door" scenario shown here. What technique is John using?

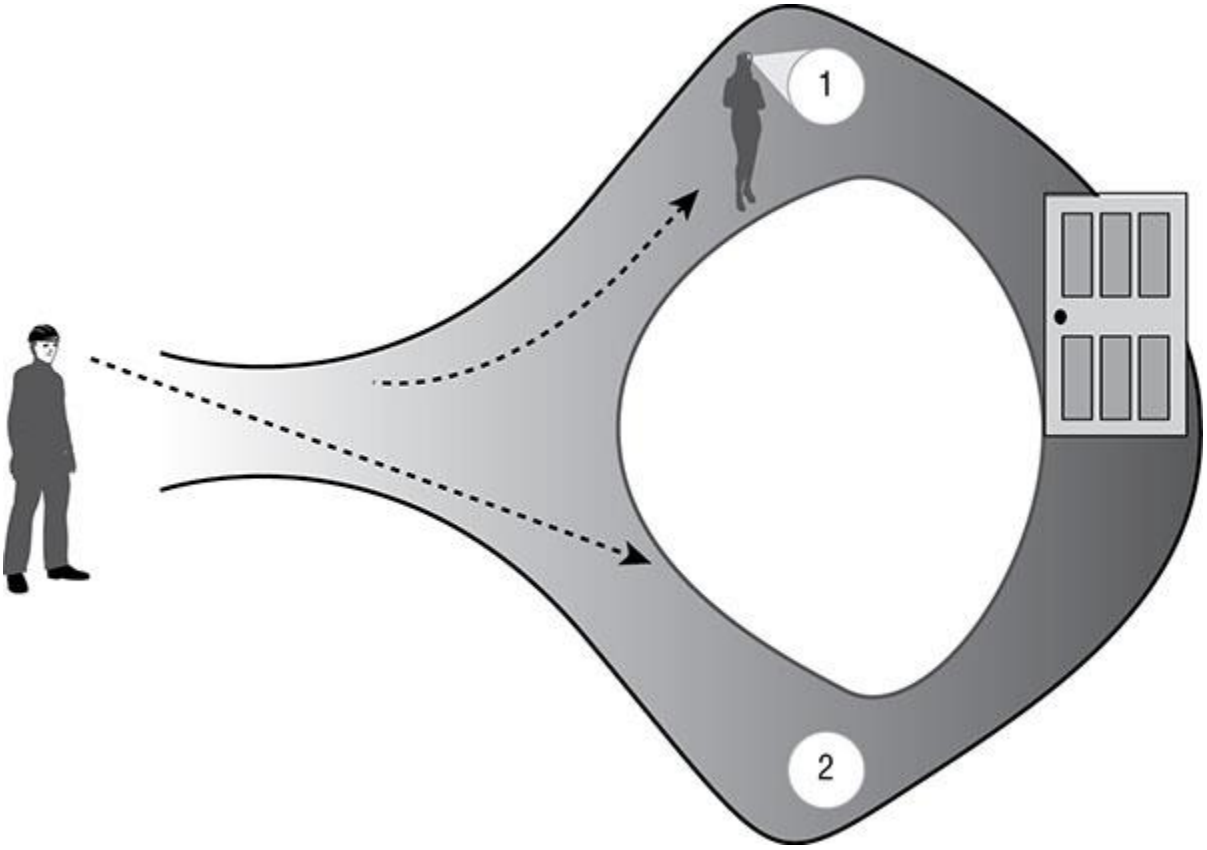


Image reprinted from *CISSP (ISC)^2 Certified Information Systems Security Professional Official Study Guide, 7th Edition* © John Wiley & Sons 2015, reprinted with permission.

1. Split-knowledge proof
2. Zero-knowledge proof
3. Logical proof
4. Mathematical proof

78. Raj is selecting an encryption algorithm for use in his organization and would like to be able to vary the strength of the encryption with the sensitivity of the information. Which one of the following algorithms allows the use of different key strengths?
    1. Blowfish
    2. DES
    3. Skipjack
    4. IDEA
79. Referring to the fire triangle shown here, which one of the following suppression materials attacks a fire by removing the fuel source?

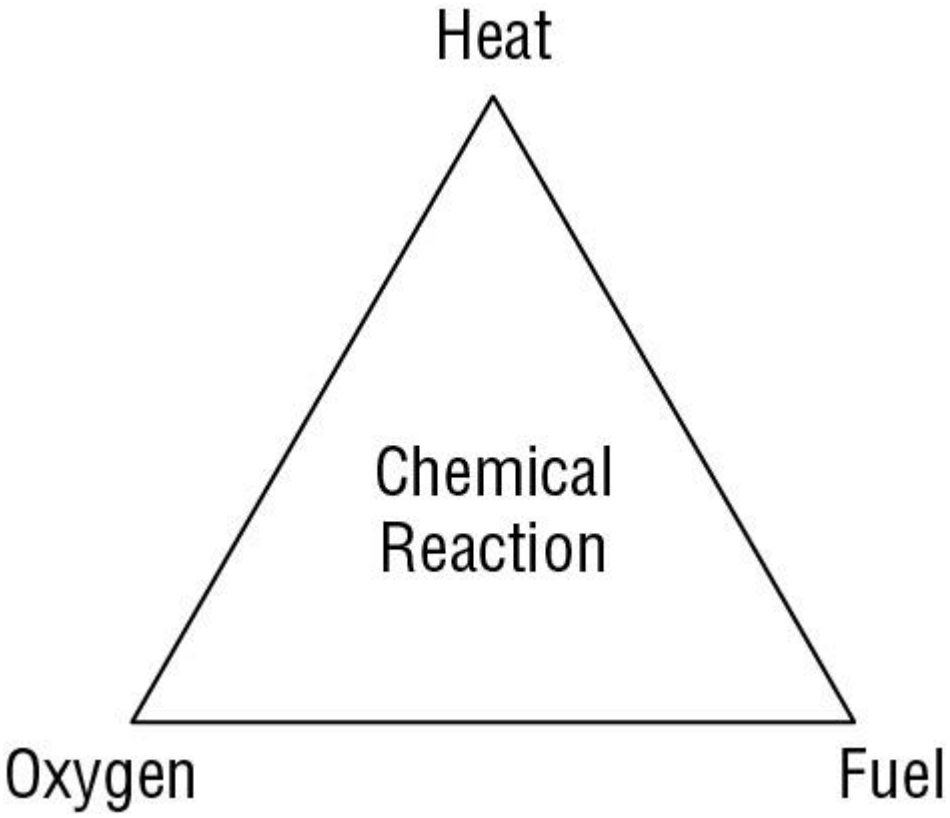


Image reprinted from *CISSP (ISC)^2 Certified Information Systems Security Professional Official Study Guide, 7th Edition* © John Wiley & Sons 2015, reprinted with permission.

1. Water
2. Soda acid
3. Carbon dioxide

4. Halon

80. Howard is choosing a cryptographic algorithm for his organization, and he would like to choose an algorithm that supports the creation of digital signatures. Which one of the following algorithms would meet his requirement?
    1. RSA
    2. DES
    3. AES
    4. Blowfish
81. Laura is responsible for securing her company's web-based applications and wishes to conduct an educational program for developers on common web application security vulnerabilities. Where can she turn for a concise listing of the most common web application issues?
    1. CVE
    2. NSA
    3. OWASP
    4. CSA
82. The Bell-LaPadula and Biba models implement state machines in a fashion that uses what specific state machine model?
    1. Information flow
    2. Noninterference
    3. Cascading
    4. Feedback
83. The _____ of a process consist(s) of the limits set on the memory addresses and resources that the process may access.
    1. Perimeter
    2. Confinement limits
    3. Metes
    4. Bounds
84. What type of motion detector senses changes in the electromagnetic fields in monitored areas?
    1. Infrared
    2. Wave pattern
    3. Capacitance
    4. Photoelectric
85. Which one of the following fire suppression systems uses a suppressant that is no longer manufactured due to environmental concerns?
    1. FM-200
    2. Argon
    3. Inergen
    4. Halon
86. Which one of the following statements is correct about the Biba model of access control?
    1. It addresses confidentiality and integrity.
    2. It addresses integrity and availability.
    3. It prevents covert channel attacks.
    4. It focuses on protecting objects from integrity threats.

87. In Transport Layer Security, what type of key is used to encrypt the actual content of communications between a web server and a client?
    1. Ephemeral session key
    2. Client's public key
    3. Server's public key
    4. Server's private key
88. Beth would like to include technology in a secure area of her data center to protect against unwanted electromagnetic emanations. What technology would assist her with this goal?
    1. Heartbeat sensor
    2. Faraday cage
    3. Piggybacking
    4. WPA2
89. In a virtualized computing environment, what component is responsible for enforcing separation between guest machines?
    1. Guest operating system
    2. Hypervisor
    3. Kernel
    4. Protection manager
90. Rick is an application developer who works primarily in Python. He recently decided to evaluate a new service where he provides his Python code to a vendor who then executes it on their server environment. What type of cloud computing environment is this service?
    1. SaaS
    2. PaaS
    3. IaaS
    4. CaaS
91. A software company developed two systems that share information. System A provides information to the input of System B, which then reciprocates by providing information back to System A as input. What type of composition theory best describes this practice?
    1. Cascading
    2. Feedback
    3. Hookup
    4. Elementary
92. Tommy is planning to implement a power conditioning UPS for a rack of servers in his data center. Which one of the following conditions will the UPS be unable to protect against if it persists for an extended period of time?
    1. Fault
    2. Blackout
    3. Sag
    4. Noise
93. Which one of the following humidity values is within the acceptable range for a data center operation?
    1. 0%
    2. 10%
    3. 25%

4. 40%

94. Chris is designing a cryptographic system for use within his company. The company has 1,000 employees, and they plan to use an asymmetric encryption system. How many total keys will they need?
    1. 500
    2. 1,000
    3. 2,000
    4. 4,950
95. What term is used to describe the formal declaration by a designated approving authority (DAA) that an information technology (IT) system is approved to operate in a specific environment?
    1. Certification
    2. Accreditation
    3. Evaluation
    4. Approval
96. Object-oriented programming languages use a black box approach to development, where users of an object do not necessarily need to know the object's implementation details. What term is used to describe this concept?
    1. Layering
    2. Abstraction
    3. Data hiding
    4. Process isolation
97. Todd wants to add a certificate to a certificate revocation list. What element of the certificate goes on the list?
    1. Serial number
    2. Public key
    3. Digital signature
    4. Private key
98. Alison is examining a digital certificate presented to her by her bank's website. Which one of the following requirements is not necessary for her to trust the digital certificate?
    1. She knows that the server belongs to the bank.
    2. She trusts the certificate authority.
    3. She verifies that the certificate is not listed on a CRL.
    4. She verifies the digital signature on the certificate.
99. Which one of the following is an example of a covert timing channel when used to exfiltrate information from an organization?
    1. Sending an electronic mail message
    2. Posting a file on a peer-to-peer file sharing service
    3. Typing with the rhythm of Morse code
    4. Writing data to a shared memory space
100. Which one of the following would be a reasonable application for the use of self-signed digital certificates?
    1. E-commerce website
    2. Banking application
    3. Internal scheduling application
    4. Customer portal

101. Mike has been tasked with preventing an outbreak of malware like Mirai. What type of systems should be protected in his organization?
    1. Servers
    2. SCADA
    3. Mobile devices
    4. Internet of Things (IoT) devices
102. A component failure in the primary HVAC system leads to a high temperature alarm in the data center that Kim manages. After resolving the issue, what should Kim consider to prevent future issues like this?
    1. A closed loop chiller
    2. Redundant cooling systems
    3. Swamp coolers
    4. Relocating the data center to a colder climate
103. As part of his team's forensic investigation process, Matt signs drives and other evidence out of storage before working with them. What type of documentation is he creating?
    1. Criminal
    2. Chain of custody
    3. Civil
    4. CYA
104. Lauren implements ASLR to help prevent system compromises. What technique has she used to protect her system?
    1. Encryption
    2. Mandatory access control
    3. Memory address randomization
    4. Discretionary access control
105. During a system audit, Casey notices that the private key for her organization's web server has been stored in a public Amazon S3 storage bucket for more than a year. What should she do?
    1. Remove the key from the bucket
    2. Notify all customers that their data may have been exposed
    3. Request a new certificate using a new key
    4. Nothing, because the private key should be accessible for validation
106. Joanna wants to review the status of the industrial control systems her organization uses for building control. What type of systems should she inquire about access to?
    1. SCADA
    2. DSS
    3. BAS
    4. ICS-CSS
107. After scanning all of the systems on his wireless network, Mike notices that one system is identified as an iOS device running a massively out-of-date version of Apple's mobile operating system. When he investigates further, he discovers that the device is an original iPad and that it cannot be updated to a current secure version of the operating system. What should Mike recommend?
    1. Retire or replace the device

2. Isolate the device on a dedicated wireless network
3. Install a firewall on the tablet
4. Reinstall the OS

108. During a third-party vulnerability scan and security test, Danielle's employer recently discovered that the embedded systems that were installed to manage her company's new buildings have a severe remote access vulnerability. The manufacturer has gone out of business, and there is no patch or update for the devices. What should Danielle recommend that her employer do about the hundreds of devices that are vulnerable?
    1. Identify a replacement device model and replace every device
    2. Turn off all of the devices
    3. Move the devices to a secured network segment
    4. Reverse engineer the devices and build an in-house patch

109. Alex's employer creates most of their work output as PDF files. Alex is concerned about limiting the audience for the PDF files to those individuals who have paid for them. What technology can he use to most effectively control the access to and distribution of these files?
    1. EDM
    2. Encryption
    3. Digital signatures
    4. DRM

110. Match the following numbered security models with the appropriate lettered security descriptions:

Security models

1. Clark-Wilson
2. Graham-Denning
3. Bell-LaPadula
4. Sutherland
5. Biba

Descriptions

6. This model blocks lower-classified objects from accessing higher-classified objects, thus ensuring confidentiality.
7. The * property of this model can be summarized as "no write-up."
8. This model uses security labels to grant access to objects via transformation procedures and a restricted interface model.
9. This model focuses on the secure creation and deletion of subjects and objects using eight primary protection rules or actions.
10. This integrity model focuses on preventing interference in support of integrity.

Chapter 3: Security Architecture and Engineering (Domain 3)

1. D. The Brewer-Nash model allows access controls to change dynamically based upon a user's actions. It is often used in environments like Matthew's to implement a "Chinese wall" between data belonging to different clients.
2. A. Fires may be detected as early as the incipient stage. During this stage, air ionization takes place, and specialized incipient fire detection systems can identify these changes to provide early warning of a fire.
3. A. Closed-circuit television (CCTV) systems act as a secondary verification mechanism for physical presence because they allow security officials to view the interior of the facility when a motion alarm sounds to determine the current occupants and their activities.
4. B. In an *m of n* control system, at least *m of n* possible escrow agents must collaborate to retrieve an encryption key from the escrow database.
5. A. This is an example of a vendor offering a fully functional application as a web-based service. Therefore, it fits under the definition of software as a service (SaaS). In infrastructure as a service (IaaS), compute as a service (CaaS), and platform as a service (PaaS) approaches, the customer provides their own software. In this example, the vendor is providing the email software, so none of those choices is appropriate.
6. B. The Digital Signature Standard approves three encryption algorithms for use in digital signatures: the Digital Signature Algorithm (DSA); the Rivest, Shamir, Adleman (RSA) algorithm; and the Elliptic Curve DSA (ECDSA) algorithm. HAVAL is a hash function, not an encryption algorithm. While hash functions are used as part of the digital signature process, they do not provide encryption.
7. A. In the subject/object model of access control, the user or process making the request for a resource is the subject of that request. In this example, Harry is requesting resource access and is, therefore, the subject.
8. C. Michael should conduct his investigation, but there is a pressing business need to bring the website back online. The most reasonable course of action would be to take a snapshot of the compromised system and use the snapshot for the investigation, restoring the website to operation as quickly as possible while using the results of the investigation to improve the security of the site.
9. C. The use of a sandbox is an example of confinement, where the system restricts the access of a particular process to limit its ability to affect other processes running on the same system.
10. D. Assurance is the degree of confidence that an organization has that its security controls are correctly implemented. It must be continually monitored and reverified.
11. A. Maintenance hooks, otherwise known as backdoors, provide developers with easy access to a system, bypassing normal security controls. If not removed prior to finalizing code, they pose a significant security vulnerability if an attacker discovers the maintenance hook.
12. B. The Simple Integrity Property states that an individual may not read a file classified at a lower security level than the individual's security clearance.
13. B. Supervisory control and data acquisition (SCADA) systems are used to control and gather data from industrial processes. They are commonly found in power plants and other industrial environments.
14. B. The Trusted Platform Module (TPM) is a hardware security technique that stores an encryption key on a chip on the motherboard and prevents someone from accessing an encrypted drive by installing it in another computer.

15. D. Intentional collisions have been created with MD5, and a real-world collision attack against SHA 1 was announced in early 2017. 3DES is not a hashing tool, leaving SHA 256 (sometimes called SHA 2) as the only real choice that Chris has in this list.
16. C. In an asymmetric cryptosystem, the sender of a message always encrypts the message using the recipient's public key.
17. D. When Bob receives the message, he uses his own private key to decrypt it. Since he is the only one with his private key, he is the only one who should be able to decrypt it, thus preserving confidentiality.
18. B. Each user retains their private key as secret information. In this scenario, Bob would only have access to his own private key and would not have access to the private key of Alice or any other user.
19. B. Alice creates the digital signature using her own private key. Then Bob, or any other user, can verify the digital signature using Alice's public key.
20. B. The salt is a random value added to a password before it is hashed by the operating system. The salt is then stored in a password file with the hashed password. This increases the complexity of cryptanalytic attacks by negating the usefulness of attacks that use precomputed hash values, such as rainbow tables.
21. A. Hash functions do not include any element of secrecy and, therefore, do not require a cryptographic key.
22. D. A preaction fire suppression system activates in two steps. The pipes fill with water once the early signs of a fire are detected. The system does not dispense water until heat sensors on the sprinkler heads trigger the second phase.
23. B. The Encapsulating Security Payload (ESP) protocol provides confidentiality and integrity for packet contents. It encrypts packet payloads and provides limited authentication and protection against replay attacks.
24. D. The greatest risk when a device is lost or stolen is that sensitive data contained on the device will fall into the wrong hands. Confidentiality protects against this risk.
25. C. The exclusive or (XOR) operation is true when one and only one of the input values is true.
26. A. DES uses a 64-bit encryption key, but only 56 of those bits are actually used as keying material in the encryption operation. The remaining 8 bits are used to detect tampering or corruption of the key.
27. C. The *-Security Property states that an individual may not write to a file at a lower classification level than that of the individual. This is also known as the confinement property.
28. B. The Diffie-Hellman algorithm allows for the secure exchange of symmetric encryption keys over a public network.
29. C. Protection Profiles (PPs) specify the security requirements and protections that must be in place for a product to be accepted under the Common Criteria.
30. A. Hash functions must be able to work on any variable-length input and produce a fixed-length output from that input, regardless of the length of the input.
31. C. Binary keyspaces contain a number of keys equal to two raised to the power of the number of bits. Two to the fifth power is 32, so a 5-bit keyspace contains 32 possible keys.
32. B. Kerckhoff's principle says that a cryptographic system should be secure even if everything about the system, except the key, is public knowledge.
33. A. Mantraps use a double set of doors to prevent piggybacking by allowing only a single individual to enter a facility at a time.
34. A. While it would be ideal to have wiring closets in a location where they are monitored by security staff, this is not feasible in most environments. Wiring closets must be distributed geographically in multiple locations across each building used by an organization.

35. D. The *-Integrity Property states that a subject cannot modify an object at a higher integrity level than that possessed by the subject.
36. The architecture security concepts match with the descriptions as follows:
    1. Time of check: C. The time at which the subject checks whether an object is available.
    2. Covert channel: A. A method used to pass information over a path not normally used for communication.
    3. Time of use: D. The time at which a subject can access an object.
    4. Maintenance hooks: E. An access method known only to the developer of the system.
    5. Parameter checking: F. A method that can help prevent buffer overflow attacks.
    6. Race condition: B. The exploitation of difference between time of check and time of use.
37. B. In the Fair Cryptosystem approach to key escrow, the secret keys used in communications are divided into two or more pieces, each of which is given to an independent third party.
38. A. The Ready state is used when a process is prepared to execute but the CPU is not available. The Running state is used when a process is executing on the CPU. The Waiting state is used when a process is blocked waiting for an external event. The Stopped state is used when a process terminates.
39. A. EAL1 assurance applies when the system in question has been functionally tested. It is the lowest level of assurance under the Common Criteria.
40. A. Administrators and processes may attach security labels to objects that provide information on an object's attributes. Labels are commonly used to apply classifications in a mandatory access control system.
41. B. Open-source software exposes the source code to public inspection and modification. The open-source community includes major software packages such as the Linux operating system.
42. A. Adam created a list of individual users that may access the file. This is an access control list, which consists of multiple access control entries. It includes the names of users, so it is not role-based, and Adam was able to modify the list, so it is not mandatory access control.
43. C. Parameter checking, or input validation, is used to ensure that input provided by users to an application matches the expected parameters for the application. Developers may use parameter checking to ensure that input does not exceed the expected length, preventing a buffer overflow attack.
44. A. *Kernel mode*, *supervisory mode*, and *system mode* are all terms used to describe privileged modes of system operation. User mode is an unprivileged mode.
45. D. Multistate systems are certified to handle data from different security classifications simultaneously by implementing protection mechanisms that segregate data appropriately.
46. C. For systems running in System High mode, the user must have a valid security clearance for all information processed by the system, access approval for all information processed by the system, and a valid need to know for some, but not necessarily all, information processed by the system.
47. B. Steganography is the art of using cryptographic techniques to embed secret messages within other content. Some steganographic algorithms work by making alterations to the least significant bits of the many bits that make up image files.
48. C. The Caesar cipher is a shift cipher that works on a stream of text and is also a substitution cipher. It is not a block cipher or a transposition cipher. It is extremely weak as a cryptographic algorithm.
49. A. The kernel lies within the central ring, Ring 0. Conceptually, Ring 1 contains other operating system components. Ring 2 is used for drivers and protocols. User-level programs and applications run at Ring 3. Rings 0 through 2 run in privileged mode while Ring 3 runs in user

mode. It is important to note that many modern operating systems do not fully implement this model.

50. D. In an infrastructure as a service environment, security duties follow a shared responsibility model. Since the vendor is responsible for managing the storage hardware, the vendor would retain responsibility for destroying or wiping drives as they are taken out of service. However, it is still the customer's responsibility to validate that the vendor's sanitization procedures meet their requirements prior to utilizing the vendor's storage services.
51. B. The major difference between a code and a cipher is that ciphers alter messages at the character or bit level, not at the word level. DES, shift ciphers, and word scrambles all work at the character or bit level and are ciphers. "One if by land; two if by sea" is a message with hidden meaning in the words and is an example of a code.
52. C. The verification process is similar to the certification process in that it validates security controls. Verification may go a step further by involving a third-party testing service and compiling results that may be trusted by many different organizations. Accreditation is the act of management formally accepting an evaluating system, not evaluating the system itself.
53. B. When a process is confined within certain access bounds, that process runs in isolation. Isolation protects the operating environment, the operating system kernel, and other processes running on the system.
54. B. The mean time to failure (MTTF) provides the average amount of time before a device of that particular specification fails.
55. A. Class A fire extinguishers are useful only against common combustible materials. They use water or soda acid as their suppressant. Class B extinguishers are for liquid fires. Class C extinguishers are for electrical fires, and Class D fire extinguishers are for combustible metals.
56. A. Mobile Device Management (MDM) products provide a consistent, centralized interface for applying security configuration settings to mobile devices.
57. C. Nonrepudiation occurs when the recipient of a message is able to demonstrate to a third party that the message came from the purported sender.
58. A. The card shown in the image has a smart chip underneath the American flag. Therefore, it is an example of a smart card. This is the most secure type of identification card technology.
59. D. The TEMPEST program creates technology that is not susceptible to Van Eck phreaking attacks because it reduces or suppresses natural electromagnetic emanations.
60. B. The Trusted Computing Base (TCB) is a small subset of the system contained within the kernel that carries out critical system activities.
61. A. The MD5 hash algorithm has known collisions and, as of 2005, is no longer considered secure for use in modern environments.
62. B. Encrypting data on SSD drives does protect against wear leveling. Disk formatting does not effectively remove data from any device. Degaussing is only effective for magnetic media. Physically destroying the drive would not permit reuse.
63. C. In a known plaintext attack, the attacker has a copy of the encrypted message along with the plaintext message used to generate that ciphertext.
64. B. In a time of check to time of use (TOCTOU) attack, the attacker exploits the difference in time between when a security control is verified and the data protected by the control is actually used.
65. A. The X.509 standard, developed by the International Telecommunications Union, contains the specification for digital certificates.
66. D. Fences designed to deter more than the casual intruder should be at least 6 feet high. If a physical security system is designed to deter even determined intruders, it should be at least 8 feet high and topped with three strands of barbed wire.

67. C. In an aggregation attack, individual(s) use their access to specific pieces of information to piece together a larger picture that they are not authorized to access.
68. D. While all of the controls mentioned protect against unwanted electromagnetic emanations, only white noise is an active control. White noise generates false emanations that effectively "jam" the true emanations from electronic equipment.
69. B. In a software as a service environment, the customer has no access to any underlying infrastructure, so firewall management is a vendor responsibility under the cloud computing shared responsibility model.
70. C. The grant rule allows a subject to grant rights that it possesses on an object to another subject.
71. B. The system Charles is remediating may have a firmware or BIOS infection, with malware resident on the system board. While uncommon, this type of malware can be difficult to find and remove. Since he used original media, it is unlikely that the malware came from the software vendor. Charles wiped the system partition, and the system would have been rebooted before being rebuilt, thus clearing system memory.
72. D. Multithreading permits multiple tasks to execute concurrently within a single process. These tasks are known as threads and may be alternated between without switching processes.
73. C. This message was most likely encrypted with a transposition cipher. The use of a substitution cipher, a category that includes AES and 3DES, would change the frequency distribution so that it did not mirror that of the English language.
74. D. The meet-in-the-middle attack uses a known plaintext message and uses both encryption of the plaintext and decryption of the ciphertext simultaneously in a brute-force manner to identify the encryption key in approximately double the time of a brute-force attack against the basic DES algorithm.
75. A. The blacklisting approach to application control allows users to install any software they wish except for packages specifically identified by the administrator as prohibited. This would be an appropriate approach in a scenario where users should be able to install any nonmalicious software they wish to use.
76. A. Heartbeat sensors send periodic status messages from the alarm system to the monitoring center. The monitoring center triggers an alarm if it does not receive a status message for a prolonged period of time, indicating that communications were disrupted.
77. B. In a zero-knowledge proof, one individual demonstrates to another that they can achieve a result that requires sensitive information without actually disclosing the sensitive information.
78. A. Blowfish allows the user to select any key length between 32 and 448 bits.
79. B. Soda acid and other dry powder extinguishers work to remove the fuel supply. Water suppresses temperature, while halon and carbon dioxide remove the oxygen supply from a fire.
80. A. Digital signatures are possible only when using an asymmetric encryption algorithm. Of the algorithms listed, only RSA is asymmetric and supports digital signature capabilities.
81. C. The Open Web Application Security Project (OWASP) produces an annual list of the top ten web application security issues that developers and security professionals around the world rely upon for education and training purposes. The OWASP vulnerabilities form the basis for many web application security testing products.
82. A. The information flow model applies state machines to the flow of information. The Bell-LaPadula model applies the information flow model to confidentiality while the Biba model applies it to integrity.
83. D. Each process that runs on a system is assigned certain physical or logical bounds for resource access, such as memory.

84. C. Capacitance motion detectors monitor the electromagnetic field in a monitored area, sensing disturbances that correspond to motion.
85. D. Halon fire suppression systems use a chlorofluorocarbon (CFC) suppressant material that was banned in the Montreal Protocol because it depletes the ozone layer.
86. D. The Biba model focuses only on protecting integrity and does not provide protection against confidentiality or availability threats. It also does not provide protection against covert channel attacks. The Biba model focuses on external threats and assumes that internal threats are addressed programmatically.
87. A. In TLS, both the server and the client first communicate using an ephemeral symmetric session key. They exchange this key using asymmetric cryptography, but all encrypted content is protected using symmetric cryptography.
88. B. A Faraday cage is a metal skin that prevents electromagnetic emanations from exiting. It is a rarely used technology because it is unwieldy and expensive, but it is quite effective at blocking unwanted radiation.
89. B. The hypervisor is responsible for coordinating access to physical hardware and enforcing isolation between different virtual machines running on the same physical platform.
90. B. Cloud computing systems where the customer only provides application code for execution on a vendor-supplied computing platform are examples of platform as a service (PaaS) computing.
91. B. The feedback model of composition theory occurs when one system provides input for a second system and then the second system provides input for the first system. This is a specialized case of the cascading model, so the feedback model is the most appropriate answer.
92. B. UPSs are designed to protect against short-term power losses, such as power faults. When they conduct power conditioning, they are also able to protect against sags and noise. UPSs have limited-life batteries and are not able to maintain continuous operating during a sustained blackout.
93. D. Data center humidity should be maintained between 40% and 60%. Values below this range increase the risk of static electricity, while values above this range may generate moisture that damages equipment.
94. C. Asymmetric cryptosystems use a pair of keys for each user. In this case, with 1,000 users, the system will require 2,000 keys.
95. B. Accreditation is the formal approval by a DAA that an IT system may operate in a described risk environment.
96. B. Abstraction uses a black box approach to hide the implementation details of an object from the users of that object.
97. A. The certificate revocation list contains the serial numbers of digital certificates issued by a certificate authority that have later been revoked.
98. A. The point of the digital certificate is to prove to Alison that the server belongs to the bank, so she does not need to have this trust in advance. To trust the certificate, she must verify the CA's digital signature on the certificate, trust the CA, verify that the certificate is not listed on a CRL, and verify that the certificate contains the name of the bank.
99. C. Covert channels use surreptitious communications' paths. Covert timing channels alter the use of a resource in a measurable fashion to exfiltrate information. If a user types using a specific rhythm of Morse code, this is an example of a covert timing channel. Someone watching or listening to the keystrokes could receive a secret message with no trace of the message left in logs.
100. C. Self-signed digital certificates should be used only for internal-facing applications, where the user base trusts the internally generated digital certificate.

101. D. Mirai targeted “Internet of Things” devices, including routers, cameras, and DVRs. As organizations bring an increasing number of devices like these into their corporate networks, protecting both internal and external targets from insecure, infrequently updated, and often vulnerable IoT devices is increasing important.
102. B. A well-designed data center should have redundant systems and capabilities for each critical part of its infrastructure. That means that power, cooling, and network connectivity should all be redundant. Kim should determine how to ensure that a single system failure cannot take her data center offline.
103. B. Matt is helping to maintain the chain of custody documentation for his electronic evidence. This can be important if his organization needs to prove that the digital evidence they handled has not been tampered with. A better process would involve more than one person to ensure that no tampering was possible.
104. C. Lauren has implemented address space layout randomization, a memory protection methodology that randomizes memory locations, which prevents attackers from using known address spaces and contiguous memory regions to execute code via overflow or stack smashing attacks.
105. C. The first thing Casey should do is notify her management, but after that, replacing the certificate and using proper key management practices with the new certificate’s key should be at the top of her list.
106. A. Supervisory Control and Data Acquisition systems, or SCADA systems, provide a graphical interface to monitor industrial control systems (ICS). Joanna should ask about access to her organization’s SCADA systems.
107. A. When operating system patches are no longer available for mobile devices, the best option is typically to retire or replace the device. Building isolated networks will not stop the device from being used for browsing or other purposes, which means it is likely to continue to be exposed to threats. Installing a firewall will not remediate the security flaws in the OS, although it may help somewhat. Finally, reinstalling the OS will not allow new updates or fix the root issue.
108. C. The most reasonable choice presented is to move the devices to a secure and isolated network segment. This will allow the devices to continue to serve their intended function while preventing them from being compromised. All of the other scenarios either create major new costs or deprive her organization of the functionality that the devices were purchased to provide.
109. D. Alex can use digital rights management technology to limit use of the PDFs to paying customers. While DRM is rarely a perfect solution, in this case, it may fit his organization’s needs. EDM is electronic dance music, which his customers may appreciate but which won’t solve the problem. Encryption and digital signatures can help to keep the files secure and to prove who they came from but won’t solve the rights management issue Alex is tackling.
110. The security models match with the descriptions as follows:
    1. Clark-Wilson: C. This model uses security labels to grant access to objects via transformation procedures and a restricted interface model.
    2. Graham-Denning: D. This model focuses on the secure creation and deletion of subjects and objects using eight primary protection rules or actions.
    3. Bell-LaPadula: A. This model blocks lower-classified objects from accessing higher-classified objects, thus ensuring confidentiality.
    4. Sutherland: E. This integrity model focuses on preventing interference in support of integrity.
    5. Biba: B. The * property of this model can be summarized as “no write-up.”