**Chapter 5 - Security Architecture Answers**

1. Which of the following choices describe a condition when RAM and Secondary storage are used together?
   1. Primary storage
   2. Secondary storage
   3. Virtual storage
   4. Real storage

Pg 308

1. The Trusted Computer System Evaluation Criteria were not intended to provide which of the following?
   1. A standard by which integrity of information systems could be evaluated.
   2. A standard as to what security features the vendors should build into commercial products.
   3. A metric that DoD units can use to evaluate systems' trustworthiness for secure processing of sensitive information.
   4. A basis for specifying security requirements in acquisition specifications.

Pg 366

TCSEC built off Bell-Lapadula (confidentiality only)

1. What is it called when a computer uses more than one CPU in parallel to execute instructions?
   1. Multiprocessing
   2. Multitasking
   3. Multithreading
   4. Parallel running

Pg 295

1. Which of the following models does NOT include data integrity?
   1. Biba
   2. Clark-Wilson
   3. Bell-LaPadula
   4. Brewer-Nash

Pg 366

1. Which of the following is the lowest TCSEC class wherein the systems must support separate operator and system administrator roles?
   1. B2
   2. B1
   3. A1
   4. A2

Pg 361

1. Which Orange Book evaluation level is described as "Verified Design"?
   1. A1
   2. B3
   3. B2
   4. B1

Pg 362

1. Which of the following statements pertaining to the Trusted Computer System Evaluation Criteria (TCSEC) is incorrect?
   1. With TCSEC, functionality and assurance are evaluated separately.
   2. TCSEC provides a means to evaluate the trustworthiness of an information system.
   3. The Orange book does not cover networks and communications.
   4. Database management systems are not covered by the TCSEC.

Pg 366

1. Which of the following is not a common integrity goal?
   1. Prevent unauthorized users from making modifications.
   2. Maintain internal and external consistency.
   3. Prevent authorized users from making improper modifications.
   4. Prevent paths that could lead to inappropriate disclosure.

Pg 344

1. Which security model uses division of operations into different parts and requires different users to perform each part?
   1. Bell-LaPadula model
   2. Biba model
   3. Clark-Wilson model
   4. Non-interference model

Pg 344

1. Which of the following are necessary components of a Multi-Level Security Policy (common to Bell-lapadula)?
   1. Sensitivity Labels and a "system high" evaluation.
   2. Sensitivity Labels and Discretionary Access Control
   3. Sensitivity Labels and Mandatory Access Control
   4. Object Labels and a "system high" evaluation.

Pg 361

1. Which of the following security mode of operation does not require all users to have the clearance for all information processed on the system?
   1. Compartmented security mode
   2. Multilevel security mode
   3. System-high security mode
   4. Dedicated security mode

Pg 336

1. 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?
   1. The reference monitor
   2. The security kernel
   3. The trusted computing base
   4. The security domain

Pg 330

1. A mechanism that enforces the authorized access relationships between subjects and objects is known as:
   1. The reference monitor.
   2. discretionary access control.
   3. trusted kernel.
   4. mandatory access control.

Pg 330

1. What does the simple integrity axiom mean in the Biba model?
   1. No write down
   2. No read down
   3. No read up
   4. No write up

Pg 339

1. What is necessary for a subject to have write access to an object in a Multi-Level Security Policy?
   1. The subject's sensitivity label must dominate the object's sensitivity label
   2. The subject's sensitivity label subordinates the object's sensitivity label
   3. The subject's sensitivity label is subordinated by the object's sensitivity label
   4. The subject's sensitivity label is dominated by the object's sensitivity label

Pg 337

1. Which security model ensures that actions that take place at a higher security level do not affect actions that take place at a lower level?
   1. The Bell-LaPadula model
   2. The information flow model
   3. The noninterference model
   4. The Clark-Wilson model

Pg 347

1. What is the name of the first mathematical model of a multi-level security policy used to define the concept of a secure state, the modes of access, and rules for granting access?
   1. Clark and Wilson Model
   2. Harrison-Ruzzo-Ullman Model
   3. Rivest and Shamir Model
   4. Bell-LaPadula Model

Pg

1. Which of the following statements pertaining to the ITSEC is false?
   1. The functionality is rated from F1 to F10.
   2. It is only used in Europe, not internationally.
   3. The assurance is rated from E1 to E10.
   4. Most ITSEC ratings can be mapped to the Orange Book ratings, but ITSEC took a step farther and added more levels to address specific needs not covered by the TCSEC.

Pg 368

1. Which of the following can be used as a covert channel?
   1. Storage and timing
   2. Storage and low bits
   3. Storage and permissions
   4. Storage and classification
2. Which of the following uses a directed graph to specify the rights that a subject can transfer to an object, or that a subject can take from another subject?
   1. Take-Grant model
   2. Access Matrix model
   3. Biba model
   4. Bell-LaPadula model
3. What is the main concern of the Bell-LaPadula security model?
   1. Accountability
   2. Integrity
   3. Confidentiality
   4. Availability
4. Which of the following places the Orange Book classifications in order from most secure to least secure?
   1. A, B, C, D
   2. D, C, B, A
   3. D, B, A, C
   4. C, D, B, A
5. The Orange Book states that "Hardware and software features shall be provided that can be used to periodically validate the correct operation of the on-site hardware and firmware elements of the TCB [Trusted Computing Base]." This statement is the formal requirement for:
   1. Security Testing
   2. Design verification
   3. System Integrity
   4. System Architecture Specification
6. The acronym CC stands for:
   1. enCrypted Communication
   2. Common Criteria for Information Security Evaluation
   3. Certificate Creation
   4. Circular Certificate rollover
7. What would best define a covert channel?
   1. An undocumented backdoor that has been left by a programmer in an operating system
   2. An open system port that should be closed.
   3. A communication channel that allows transfer of information in a manner that violates the system's security policy.
   4. A trojan horse.
8. Which of the following statements pertaining to protection rings is false?
   1. They provide strict boundaries and definitions on what the processes that work within each ring can access.
   2. Programs operating in inner rings are usually referred to as existing in a privileged mode.
   3. They support the CIA triad requirements of multitasking operating systems.
   4. They provide users with a direct access to peripherals
9. Which of the following describes a logical form of separation used by secure computing systems?
   1. Processes use different levels of security for input and output devices.
   2. Processes are constrained so that each cannot access objects outside its permitted domain.
   3. Processes conceal data and computations to inhibit access by outside processes.
   4. Processes are granted access based on granularity of controlled objects.
10. Which of the following statements relating to the Biba security model is FALSE?
    1. It is a state machine model.
    2. A subject is not allowed to write up.
    3. Integrity levels are assigned to subjects and objects.
    4. Programs serve as an intermediate layer between subjects and objects.
11. Memory management in TCSEC levels B3 and A1 operating systems may utilize "data hiding". What does this mean?
    1. System functions are layered, and none of the functions in a given layer can access data outside that layer.
    2. Auditing processes and their memory addresses cannot be accessed by user processes.
    3. Only security processes are allowed to write to ring zero memory.
    4. It is a form of strong encryption cipher.
12. Which of the following classes is defined in the TCSEC (Orange Book) as minimal protection?
    1. D
    2. C
    3. B
    4. A
13. What are the components of an object's sensitivity label?
    1. A Classification Set and a single Compartment
    2. A single classification and a single compartment
    3. A Classification Set and user credentials
    4. A single classification and a Compartment Set
14. What can best be defined as the sum of protection mechanisms inside the computer, including hardware, firmware and software?
    1. Trusted system
    2. Security kernel
    3. Trusted computing base
    4. Security perimeter
15. What is defined as the hardware, firmware and software elements of a trusted computing base that implement the reference monitor concept?
    1. The reference monitor
    2. Protection rings
    3. A security kernel
    4. A protection domain
16. In the Bell-LaPadula model, the Star-property is also called:
    1. The simple security property
    2. The confidentiality property
    3. The confinement property
    4. The tranquility property
17. What is the Biba security model concerned with?
    1. Confidentiality
    2. Reliability
    3. Availability
    4. Integrity
18. Which of the following is best defined as an administrative declaration by a designated authority that an information system is approved to operate in a particular security configuration with a prescribed set of safeguards?
    1. Certification
    2. Declaration
    3. Audit
    4. Accreditation
19. Which security model introduces access to objects only through programs?
    1. The Biba model
    2. The Bell-LaPadula model
    3. The Clark-Wilson model
    4. The information flow model
20. Which of the following classes is defined in the TCSEC (Orange Book) as mandatory protection?
    1. B
    2. A
    3. C
    4. D
21. Common Criteria has assurance level from EAL 1 to EAL 7 regarding the depth of design and testing. Which of following assure the TOE is methodically designed, tested and reviewed?
    1. EAL 3
    2. EAL 4
    3. EAL 5
    4. EAL 6
22. Which access control model was proposed for enforcing access control in government and military applications?
    1. Bell-LaPadula model
    2. Biba model
    3. Sutherland model
    4. Brewer-Nash model
23. Which criteria effort was the first to introduce the notions of integrity and availability?
    1. The Information Technology Security Evaluation Criteria
    2. The Canadian Trusted Computer Product Evaluation Criteria
    3. The Trusted Computer System Evaluation Criteria
    4. The Common Criteria
24. Which of the following organizations produces and publishes the Federal Information Processing Standards (FIPS)?
    1. The National Computer Security Center (NCSC)
    2. The National Institute of Standards and Technology (NIST)
    3. The National Security Agency (NSA)
    4. The American National Standards Institute (ANSI)
25. Which evaluation class of the Trusted Network Interpretation (TNI) offers controlled access protection?
    1. C
    2. C1
    3. C2
    4. B
26. Which of the following statements pertaining to the Bell-LaPadula is false?
    1. It does not allow "read up."
    2. It does not address covert channels.
    3. It does not address management of access controls.
    4. It does not allow to "write up."
27. What is a "system high" policy?
    1. A system with data that contains data of the highest security classification
    2. A system where all users are cleared to view the most highly classified data on the system
    3. A system that contains only data of one security classification.
    4. A system that uses a Multi-Level Security Policy to separate the highly classified data from the other data residing on the system
28. Trusted Distribution is required at what Orange Book evaluation level?
    1. A1
    2. B3
    3. B2
    4. B1
29. Which of the following security models does not concern itself with the flow of data?
    1. The information flow model
    2. The Biba model
    3. The Bell-LaPadula model
    4. The noninterference model
30. Which TCSEC level is labeled Controlled Access Protection?
    1. C1
    2. C2
    3. C3
    4. B1
31. Which of the following is a characteristic of a trusted process, where operations are performed without allowing the user direct access to sensitive data?
    1. confined domain
    2. restricted resource
    3. limited privilege
    4. validated execution
32. What is another name for the Orange Book?
    1. The Trusted Computer System Evaluation Criteria (TCSEC)
    2. The Trusted Computing Base (TCB)
    3. The Information Technology Security Evaluation Criteria (ITSEC)
    4. The Common Criteria (CC)
33. How do the Information Labels of Compartmented Mode Workstations differ from the Sensitivity Levels of B3 evaluated systems?
    1. Information Labels in CMW are homologous to Sensitivity Labels, but a different term was chosen to emphasize that CMW's are not described in the Orange Book.
    2. Information Labels contain more information than Sensitivity Labels, thus allowing more granular access decisions to be made.
    3. Sensitivity Labels contain more information than Information Labels because B3+ systems should store more sensitive date than workstations.
    4. Information Labels contain more information than Sensitivity Labels, but are not used by the Reference Monitor to determine access permissions
34. Which division of the Orange Book deals with discretionary protection (need-to-know)?
    1. D
    2. C
    3. B
    4. A
35. Which of the following is not an Orange Book-defined life cycle assurance requirement?
    1. Security testing
    2. Design specification and testing
    3. Trusted distribution
    4. System integrity
36. In what security mode can a system be operating if all users have the clearance or authorization and need-to-know to all data processed within the system?
    1. Dedicated security mode
    2. System-high security mode
    3. Compartmented security mode
    4. Multilevel security mode
37. Which of the following statements pertaining to the Trusted Computer Systems Evaluation Criteria (TCSEC) is true?
    1. It is oriented at evaluating systems for the private sector rather than government and military organizations.
    2. It focuses on integrity, availability and authenticity.
    3. It addresses security evaluation topics for networks and network components.
    4. It looks specifically at the operating system and not other issues.
38. Which Orange Book evaluation level is described as "Controlled Access Protection"?
    1. A1
    2. B3
    3. C2
    4. B1
39. Which of the following classes is defined in the TCSEC (Orange Book) as discretionary protection?
    1. C
    2. B
    3. A
    4. D
40. Trusted recovery is required at which TCSEC level?
    1. C2
    2. B2
    3. B3
    4. B1
41. Why do buffer overflows happen?
    1. Because buffers can only hold so much data
    2. Because input data is not checked for appropriate length at time of input
    3. Because they are an easy weakness to exploit
    4. Because of insufficient system memory
42. Which Orange Book evaluation level is described as "Structured Protection"?
    1. A1
    2. B3
    3. B2
    4. B1
43. If an operating system permits executable objects to be used simultaneously by multiple users without a refresh of the objects, what security problem is most likely to exist?
    1. disclosure of residual data
    2. unauthorized obtaining of a privileged execution state
    3. data leakage through covert channels
    4. denial of service through a deadly embrace
44. Mandatory Access requires that sensitivity labels be attached to all objects. Which of the following would be designated as objects on a MAC system?
    1. files, directories, processes, and sockets
    2. devices, processes and sockets
    3. users, windows, and programs
    4. files, directories and devices
45. Which TCSEC level first addresses object reuse?
    1. B1
    2. B2
    3. B3
    4. C2
46. What is used to protect programs from all unauthorized modification or executional interference?
    1. A protection domain
    2. A security perimeter
    3. Security labels
    4. Abstraction
47. A channel within a computer system or network that is designed for the authorized transfer of information is identified as a(n)?
    1. Covert channel
    2. Overt channel
    3. Opened channel
    4. Closed channel
48. Device labels are required for which of the following Orange Book ratings?
    1. C2
    2. B1
    3. B2
    4. D6
49. The Orange Book describes four hierarchical levels to categorize security systems. Which of the following levels require mandatory protection?
    1. A and B
    2. B and C
    3. A, B, and C
    4. B and D
50. What Orange Book security rating is reserved for systems that have been evaluated but fail to meet the criteria and requirements of the higher divisions?
    1. A
    2. D
    3. E
    4. F
51. Which of the following is a straightforward approach that provides access rights to subjects for objects?
    1. Access Matrix model
    2. Take-Grant model
    3. Bell-LaPadula model
    4. Biba model
52. What does it mean if a system uses "Trusted Recovery"?
    1. A single account on the system has the administrative rights to recover or reboot the system after a crash.
    2. A failure or crash of the system cannot be used to breach security.
    3. The recovery process is done from media that have been locked in a safe.
    4. There is no such principle as "Trusted Recovery" in security.
53. Which of the following was developed by the National Computer Security Center (NCSC)?
    1. TCSEC
    2. ITSEC
    3. DITSCAP
    4. NIACAP
54. What mechanism does a system use to compare the security labels of a subject and an object?
    1. Validation Module
    2. Reference Monitor
    3. Clearance Check
    4. Security Module
55. Which of the following statements pertaining to the trusted computing base (TCB) is false?
    1. It addresses the level of security a system provides.
    2. It originates from the Orange Book.
    3. It includes hardware, firmware and software.
    4. A higher TCB rating will require that details of their testing procedures and documentation be reviewed with more granularity.
56. Which of the following Orange Book ratings represents the highest security level?
    1. B1
    2. B2
    3. F6
    4. C2
57. Which Orange book security rating is the first to be concerned with covert channels?
    1. A1
    2. B3
    3. B2
    4. B1
58. Which Orange book security rating introduces the object reuse protection?
    1. C1
    2. C2
    3. B1
    4. B2
59. Configuration Management controls what?
    1. Auditing of changes to the Trusted Computing Base
    2. Control of changes to the Trusted Computing Base
    3. Changes in the configuration access to the Trusted Computing Base
    4. Auditing and controlling any changes to the Trusted Computing Base
60. The Information Technology Security Evaluation Criteria (ITSEC) was written to address which of the following that the Orange Book did not address?
    1. integrity and confidentiality
    2. confidentiality and availability
    3. integrity and availability
    4. none of the above
61. Compartmented Mode Workstations (CMW) are most similar to what Orange Book evaluation level?
    1. A1
    2. B3
    3. B2
    4. B1
62. Which TCSEC class specifies discretionary protection?
    1. B2
    2. B1
    3. C2
    4. C1
63. There are more than 20 books in the Rainbow Series. Which of the following covers password management guidelines?
    1. Orange Book
    2. Green Book
    3. Red Book
    4. Lavender Book
64. The Orange Book requires auditing mechanisms for any systems evaluated at which of the following levels?
    1. C1 and above
    2. C2 and above
    3. B1 and above
    4. B2 and above
65. What is the lowest Orange Book evaluation level requiring Security Domains?
    1. A1
    2. B3
    3. B2
    4. B1
66. At what Orange Book evaluation levels are configuration management required?
    1. C1 and above
    2. C2 and above
    3. B1 and above
    4. B2 and above
67. Which evaluation class of the Trusted Network Interpretation (TNI) offers labeled security protection?
    1. C2
    2. B
    3. B1
    4. B2
68. Which integrity model defines a constrained data item, an integrity verification procedure and a transformation procedure?
    1. The Take-Grant model
    2. The Biba integrity model
    3. The Clark Wilson integrity model
    4. The Bell-LaPadula integrity model
69. Which of the following statements pertaining to the security kernel is incorrect?
    1. The security kernel is made up of mechanisms that fall under the TCB and implements and enforces the reference monitor concept.
    2. The security kernel must provide isolation for the processes carrying out the reference monitor concept and they must be tamperproof.
    3. The security kernel must be small enough to be able to be tested and verified in a complete and comprehensive manner.
    4. The security kernel is an access control concept, not an actual physical component.
70. What can best be defined as the process of independently assessing a system against a standard of comparison, such as evaluation criteria?
    1. Acceptance testing
    2. Evaluation
    3. Certification
    4. Accreditation
71. What prevents a process from accessing another process' data?
    1. Memory segmentation
    2. Process isolation
    3. The reference monitor
    4. Data hiding
72. What does the simple security (ss) property mean in the Bell-LaPadula model?
    1. No read up
    2. No write down
    3. No read down
    4. No write up
73. In Mandatory Access Control, sensitivity labels contain what information?
    1. the item's classification
    2. the item's classification and category set
    3. the item's classification, category and compartment
    4. the item's classification and its compartment
74. According to the Orange Book, trusted facility management is not required for which of the following security levels?
    1. B1
    2. B2
    3. B3
    4. A1
75. Which of the following is not an Orange Book-defined operational assurance requirement?
    1. System architecture
    2. Trusted facility management
    3. Configuration management
    4. Covert channel analysis
76. In what security mode can a system be operating if all users have the clearance to all data processed by the system, but might not have the need-to-know and formal access approval?
    1. Multilevel security mode
    2. Compartmented security mode
    3. System-high security mode
    4. Dedicated security mode
77. What can be described as an imaginary line that separates the trusted components of the TCB from those elements that are not trusted?
    1. The security kernel
    2. The reference monitor
    3. The security perimeter
    4. The reference perimeter
78. Which of the following is least likely to be found in the Orange Book?
    1. Security policy
    2. Documentation
    3. Accountability
    4. Networks and network components
79. Which of the following can best be described as simultaneous execution of 2 or more programs by a computer?
    1. Multitasking
    2. Multiprogramming
    3. Pipelining
    4. Multiprocessing
80. The Orange Book is founded upon which security policy model?
    1. The Biba Model
    2. The Bell LaPadula Model
    3. Clark-Wilson Model
    4. TEMPEST
81. What does the \* (star) property mean in the Bell-LaPadula model?
    1. No write up
    2. No read up
    3. No write down
    4. No read down
82. What can best be described as a domain of trust that shares a single security policy and single management?
    1. The reference monitor
    2. A security domain
    3. The security kernel
    4. The security perimeter
83. Which access control model achieves data integrity through well-formed transactions and separation of duties?
    1. Clark-Wilson model
    2. Biba model
    3. Non-interference model
    4. Sutherland model
84. The concept of the Trusted Computing Base (from the Orange Book) includes which of the following?
    1. trusted hardware only
    2. trusted software only
    3. trusted hardware and software
    4. trusted computer operators and system managers
85. Who first described the DoD multilevel military security policy in abstract, formal terms?
    1. David Bell and Leonard LaPadula
    2. Rivest, Shamir and Adleman
    3. Whitfield Diffie and Martin Hellman
    4. David Clark and David Wilson
86. What are the three conditions that must be met by the reference monitor?
    1. Confidentiality, availability and integrity
    2. Policy, mechanism and assurance
    3. Isolation, layering and abstraction
    4. Isolation, completeness and verifiability
87. What does the \* (star) integrity axiom mean in the Biba model?
    1. No read up
    2. No write down
    3. No read down
    4. No write up