Post-Class Quiz: Security Architecture & Design Domain

1. “Preserving authorized restriction on information access and disclosure, including means for protecting personal privacy and proprietary information” is the definition for?

   A. Confidentiality

   B. Integrity

   C. Availability

   D. Non-repudiation

2. “Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authentication” is the definition for?

   A. Confidentiality

   B. Integrity

   C. Availability

   D. Non-repudiation

3. “Ensuring timely and reliable access and use of information” is the definition for?

   A. Confidentiality

   B. Integrity

   C. Availability

   D. Non-repudiation

4. A security policy that authorizes employees’ access to information that enable them to perform their assigned job functions is an implementation of what security principle?

   A. Need to know

   B. Least privilege

   C. Separation of duties

   D. Job rotation

5. What type of security requirement establishes level of confidence that the security function is meeting the security objectives?

   A. System specification

   B. Functional requirement

   C. Assurance requirement

   D. System requirement

6. A type of information security model that describes the system rules of behavior using abstract mathematics where the state variable represents the system state and its transition function defines the state changes?

   A. Graham-Denning

   B. Information flow

   C. Bell-LaPadula

   D. Non-Interference

7. Information flow model …

   A. allows for dynamically changing access controls.

   B. ensures one domain does not affect another domain.

   C. ensures that data moves in a way that does not violate security policy.

   D. ensures the system is secure through all state transitions.

8. What are the four operating states of a central processing unit (CPU)?

   A. Run, program, supervisory, suspend.

   B. Halt, supervisory, operating, application.

   C. Supervisory, wait, program, operating.

   D. Application, supervisory, operating, error.

9. What type of memory is non-volatile?

   A. Read Only Memory (ROM).

   B. Random Access Memory (RAM).

   C. Cache.

   D. Primary.

10. An address location that is specified in a program instruction contains the address of the final location is known as:

   A. Implied addressing.

   B. Indexed addressing.

   C. Indirect addressing.

D. Register addressing.

11. Which of the following hardware devices can be reprogrammed?

1 Read Only Memory (ROM).

2 Programmable Read Only Memory (PROM).

3 Erasable Programmable Read Only Memory (EPROM).

4 Electrically Erasable Programmable Read Only Memory (EEPROM).

A. 1 and 3.

B. 3 and 4.

C. 1 and 4.

D. 2 and 3.

12. A Processing methodology which executes two or more tasks on a single processor is known as:

A. Scalar.

B. Multiprocessing.

C. Multitasking.

D. Multiprogramming.

13. What is a type of high-level language?

A. BASIC.

B. Machine.

C. Assembly.

D. BIOS.

14. What is the purpose of Basic Input/Output System (BIOS)?

A. Memory management.

B. Basic operation of a computer.

C. File management.

D. ROM.

15. Which operating system is the best example of a closed system?

A. Windows 2000.

B. Solaris.

C. Linux.

D. Open BSD.

16. Which of the following are security concerns with distributed systems?

A. Downloaded data from the Internet via the web or through e-mail may infect other computers.

B. Desktop systems may not be properly secured.

C. Unauthorized access to a secured network could be made through remote control or terminal server programs running on a desktop.

D. A, B, and C.

17. Which of the following are controls that can be put in place to help mitigate vulnerabilities in distributed systems?

A. Security awareness training.

B. GUI interfaces for critical information.

C. Protection domains.

D. All of the above.

18. What combination of components is a Trusted Computing Base (TCB) comprised of?

1 Hardware.

2 Firmware.

3 Software.

A. 1 and 3.

B. 2 and 3.

C. 1 and 2.

D. All of the above.

19. Reference monitor ________.

A. controls access to subjects.

B. controls access to objects.

C. controls objects access by subjects.

D. controls objects access to subjects.

20. Which security mode best defines where users have both the required clearance and the need-to-know for all data on a system?

A. Dedicated.

B. Limited access.

C. Controlled.

D. Compartmented.

21. Otherwise known as a trap door, this vulnerability is often built into a system.

A. Covert channel.

B. Maintenance hook.

C. TOC/TOU.

D. No parameter checking.

22. If a computer component fails but the computer continues to function, this system is called a ___ system.

A. fail safe

B. fail soft

C. failover

D. fault-tolerant

23. Which Evaluation Criteria is also known as the Orange Book?

A. Common Criteria

B. Information Technology Security Evaluation Criteria (ITSEC)

C. Trusted Computer System Evaluation Criteria (TCSEC)

D. National Information Assurance Certification and Accreditation Process (NIACAP)

24. Which area does the Rainbow Series Red Book cover?

A. Hardware platform.

B. Networking components.

C. Operating systems.

D. Cryptographic support.

25. Which criteria went into the Common Criteria?

A. Trusted Computer System Evaluation Criteria (TCSEC)

B. Information Technology Security Evaluation Criteria (ITSEC)

C. Canadian Trusted Computer Evaluation Criteria.

D. All of the above.

26. Which of the following is the European evaluation criteria standard?

A. TCSEC.

B. ITSEC.

C. IPSec.

D. CTCEC.

27. Evaluation Assurance Level (EAL) is used in which Evaluation Criteria?

A. Common Criteria.

B. Rainbow Series.

C. ITSEC.

D. CTCPEC.

28. In the following top-down Common Criteria evaluation process, what is the missing component:

Protection Profile → Target of Evaluation → <???> → Security Functionality/Assurance Requirements → Evaluation → Evaluation Assurance Level

A. Certification Domain.

B. Integrity Assessment.

C. Security Domain.

D. Security Target.

29. Per Common Criteria Evaluation and Validation Scheme (CCEVS), what is a "protection profile"?

A. An implementation-independent specification.

B. An implementation-dependent specification.

C. A vendor response that contains implementation-dependent specification.

D. A government provided security target.

30. Per ISO/IEC 15408, *Evaluation Criteria for IT Security*, what Evaluation Assurance Level (EAL) is "Semi formally designed and tested"?

A. EAL 2

B. EAL 3

C. EAL 4

D. EAL 5

31. The difference between certification and accreditation is:

A. Accreditation is the technical evaluation of a system.

B. Management provides a certification for a system.

C. Accreditation is the formal acceptance of a certified system.

D. Certification happens to a stand-alone system, accreditation happens when a system is connected to other systems.

32. In Common Criteria, requirements for future products are defined by:

A. Protection Profile.

B. Target of Evaluation.

C. Evaluation Assurance Level 3.

D. Evaluation Assurance Level 7.

33. In Common Criteria, security target is defined by:

A. The product consumer or end user.

B. The vendor or developer.

C. The evaluation authority.

D. NIST.

34. In Trusted Computer System Evaluation Criteria (TCSEC), A1: Verified Design is equivalent of what for Information Technology Security Evaluation Criteria (ITSEC)?

A. F3+E3

B. F4+E4

C. F5+F5

D. F6+F6

35. Which of the following security model focuses on confidentiality only?

1 Bell-LaPadula.

2 Biba.

3 Clark-Wilson.

A. 1 Only.

B. 2 Only.

C. 3 Only.

D. 2 and 3.

36. A characteristic of security model that enforces information flow in only one direction is:

A. Access triple.

B. Lattice.

C. Star property.

D. Chinese wall.

37. The star property deals with:

A. Reading.

B. Writing.

C. Confidentiality.

D. Integrity.

38. Which of the following security models address integrity?

1 Bell-LaPadula.

2 Clark-Wilson.

3 Biba.

4 Chinese Wall.

A. 1 Only.
B. 1 and 2.
C. 2 and 3.
D. 3 and 4.

39. Which rights are granted or restricted in an access control matrix?

1 Read.
2 Write.
3 Modify.
4 Delete.

A. 1 Only.
B. 1 and 2.
C. 1, 2 and 3.
D. All of the above.

40. In Trusted Computing Base (TCB), what are the security objectives?

A. Confidentiality and integrity.
B. Confidentiality, integrity, and availability.
C. Need-to-know, least privilege, and separation of duties.
D. Need-to-know, least privilege, separation of duties, job rotation, and mandatory vacation.

41. In security kernel, which ring has access to kernel functions of an operating system?

A. Ring 0
B. Ring 1
C. Ring 2
D. Ring 3