CSS Tutorial: Security Models

1. A principle of the BellLa Padula model was not mentioned in your class, called the tranquillity principle. It states that the classification of a subject or object does not change while it is being referenced. Explain the purpose of the tranquillity principle. What are the implications of a model in which the tranquillity principle is not true?

2. Briefly define the concepts of discretionary access control (DAC) and mandatory access control (MAC) explaining how they usually implemented. Compare between these two concepts.

3. Subjects can access objects, but they can also access other subjects. Describe how a reference monitor would control access in the case of a subject acting on another subject. Describe how a reference monitor would control access in the case of two subjects interacting.

4. According to the Bell La Padula model, what restrictions are placed on two active subjects (for example, two processes) that need to send and receive signals to and from each other? Justify your answer.

5. Compare the advantages of Public key Cryptography over Symmetric Key Cryptography and conversely.

6. In the context of Computer Security what does:
   a) MAC stand for?
   b) DAC stand for?

7. Can a user cleared for <secret;{dog, cat, pig}> have access to documents classified in each of the following ways under the military security model?
   a) <top secret;dog> (Yes / No)
   b) <secret;{dog}> (Yes / No)
   c) <secret;{dog,cow}> (Yes / No)
   d) <secret;{moose}> (Yes / No)
   e) <confidential;{dog,pig,cat}> (Yes / No)
   f) <confidential;{moose}> (Yes / No)

8. The BLP model is based on, (TRUE or FALSE)
   a) an Information flow model (TRUE / FALSE)
   b) an integrity model (TRUE / FALSE)
   c) a privacy model (TRUE / FALSE)
   d) some other model (TRUE / FALSE)

9. In BLP there must be no information flow from _____ (HIGH / LOW) security level objects to _____ (HIGH / LOW) security level objects.

10. In the Chinese Wall model there must be no information flow _____ objects which have datasets with a _____.

11. A security policy provides a way to _____
    a) establish a cost model for security activities.
    b) allow management to define system recovery requirements.
    c) identify and clarify security goals and objectives.
    d) enable management to define system access rules.

12. Which security model focuses on confidentiality only?
    a) Bell-LaPadula.
    b) Biba.
    c) Clark-Wilson.
    d) Biba and Clark-Wilson

13. Information flow models:
    a) Allow for dynamically changing access controls.
    b) Ensure one domain does not affect another domain.
    c) Ensure that data moves in a way that does not violate security policy.
    d) Ensure the system is secure through all state transitions.

14. Which security model addresses integrity?
    a) Bell-LaPadula.
    b) Clark-Wilson.
    c) Biba.
    d) Chinese Wall

15. What determines the assignment of data classifications in a mandatory access control (MAC) philosophy?
    a) The analysis of the users in conjunction with the audit department
    b) The assessment by the information security department
    c) The user's evaluation of a particular information element
    d) The organization's published security policy for data classification

16. A security policy provides a way to…?
    a) establish a cost model for security activities.
    b) allow management to define system recovery requirements.
    c) identify and clarify security goals and objectives.
    d) enable management to define system access rules.

17. What is a set of step-by-step instructions used to satisfy control requirements called?
    a) Policy
    b) Standard
    c) Guideline
    d) Procedure

18. Which of the following is not true regarding security policy?
    a) It is a general statement
    b) It is promulgated by senior IT security staff
    c) It describes the role of security in the organization
    d) It is broad

19. Robert has been given the responsibility of installing doors that provide different types of protection. He has been told to install doors that provide fail-safe, fail-secure, and fail-soft protection. Which of the following statements is true about secure door types?
    a) Fail-soft defaults to the sensitivity of the area.
    b) Fail-safe defaults to locked.
    c) Fail-secure defaults to unlocked.
    d) Fail-secure defaults to double locked.