Chapter: Chapter 14

Multiple Choice

1. In the UNIX operating system, a domain is associated with the ____.
A) user
B) process
C) procedure
D) task

Ans: A
Section: 14.3.2
Difficulty: Easy

2. In MULTICS, the protection domains are organized in a _____.
A) star structure
B) linear structure
C) ring structure
D) directory structure

Ans: C
Section: 14.3.3
Difficulty: Easy

3. In an access matrix, the ____ right allows a process to change the entries in a row.
A) owner
B) copy
C) control.
D) switch

Ans: C
Section: 14.4

Difficulty: Medium

4. The ____ implementation of an access table consists of sets of ordered triples.
A) global table
B) access list for objects
C) lock-key mechanism
D) capability list

Ans: A
Section: 14.5.1
Difficulty: Easy

5. In capability lists, each object has a ____ to denote its type.
A) gate
B) tag
C) key
D) lock

Ans: B
Section: 14.5.3
Difficulty: Medium

6. Which of the following implementations of the access matrix is a compromise between two other implementations listed below?
A) access list
B) capability list
C) global table
D) lock-key

Ans: D
Section: 14.5
Difficulty:Medium

7. In the reacquisition scheme for implementing the revocation of capabilities, ____.
A) a key is defined when the capability is created
B) the capabilities point indirectly, not directly, to the objects
C) a list of pointers is maintained with each object that point to all capabilities associated with that object
D) capabilities are periodically deleted from each domain

Ans: D
Section: 14.7
Difficulty: Medium

8. Which of the following is an advantage of compiler-based enforcement of access control?
A) Protection schemes are programmed as opposed to simply declared.
B) Protection requirements are dependant of the facilities provided by a particular operating system.
C) The means for enforcement needs to be provided by the designer of the subsystem.
D) Access privileges are closely related to the linguistic concept of a data type.

Ans: D
Section:14.9.1
Difficulty: Difficult

9. Which of the following is a true statement regarding the relative merits between access rights enforcement based solely on a kernel as opposed to enforcement provided largely by a compiler?
A) Enforcement by the compiler provides a greater degree of security.
B) Enforcement by the kernel is less flexible than enforcement by the programming language for user-defined policy.
C) Kernel-based enforcement has the advantage that static access enforcement can be verified off-line at compile time.
D) The fixed overhead of kernel calls cannot often be avoided in a compiler-based enforcement.

Ans: B
Section: 14.9
Difficulty: Difficult

10. Which of the following is true of the Java programming language in relation to protection?
A) When a class is loaded, the JVM assigns the class to a protection domain that gives the

permissions of that class.
B) It does not support the dynamic loading of untrusted classes over a network.
C) It does not support the execution of mutually distrusting classes within the same JVM.
D) Methods in the calling sequence are not responsible for requests to access a protected resource.

Ans: A
Section: 14.14.9.2
Difficulty: Medium

Essay

11. Explain the meaning of the term object as it relates to protection in a computer system. What are the two general types of objects in a system?

Ans: A computer system is a collection of processes and objects. Each object has a unique name that differentiates it from all other objects in the system, and each can be accessed only through well-defined and meaningful operations. Objects are essentially abstract data types and include hardware objects (such as the CPU, memory segments, printer, and disks) and software objects (such as files, programs, and semaphores).
Section: 14.3
Difficulty: Medium

12. A process is said to operate within a protection domain which specifies the resources that the process may access. List the ways that a domain can be realized.

Ans: A domain may be realized where each user, process, or procedure may be a domain. In the first case, the set of objects that can be accessed depends on the identity of the user. In the second case, the set of objects that can be accessed depends upon the identity of the process. Finally, the third case specifies that the set of objects that can be accessed depends on the local variables defined with the procedure.
Section: 14.3.1
Difficulty: Medium

13. What is an access matrix and how can it be implemented?

Ans: An access matrix is an abstract model of protection where the rows represent domains and the columns represent objects. Each entry in the matrix consists of a set of access rights. Access matrices are typically implemented using a global table, an access list for objects, a capability list for domains, or a lock-key mechanism.
Section: 14.4
Difficulty: Difficult

14. What was the main disadvantage to the structure used to organize protection domains in the MULTICS system?

Ans: The ring structure had the disadvantage in that it did not allow the enforcement of a need-to-know principle. For example, if an object needed to be accessible in one domain, but not in another, then the domain that required the privileged information needed to be located such that it was in a ring closer to the center than the other domain. This also forced every object in the outer domain to be accessible by the inner domain which is not necessarily desired.
Section: 14.3.3
Difficulty: Medium

15. Why is a global table implementation of an access matrix not typically implemented?

Ans: The global table implementation suffers from a couple of drawbacks that keep it from being a popular implementation type. The first drawback is that the table is usually large and cannot be stored in main memory. If the table cannot be stored in main memory, extra I/O must be used to access this table. In addition, a global table makes it difficult to take advantage of special groupings of objects or domains.
Section: 14.5.1
Difficulty: Medium

16. How does the lock-key mechanism for implementation of an access matrix work?

Ans: In a lock-key mechanism, each object is given a list of unique bit patterns, called locks. Similarly, each domain has a list of unique bit patterns, called keys. A process in a domain can only access an object if that domain has the matching key for the lock. Users are not allowed to examine or modify the list of keys (or locks) directly.
Section: 14.5.4

Difficulty: Medium

17. What is a confinement problem?

Ans: A confinement problem is the problem of guaranteeing that no information initially held in an object can migrate outside of its execution environment. Although copy and owner rights provide a mechanism to limit the propagation of access rights, they do not provide appropriate tools for preventing the propagation (or disclosure) of information. The confinement problem is in general unsolvable.
Section: 14.4
Difficulty: Medium

18. What is rights amplification with respect to the Hydra protection system?

Ans: Rights amplification allows certification of a procedure as trustworthy to act on a formal parameter of a specified type on behalf of any process that holds a right to execute the procedure. The rights held by the trustworthy procedure are independent of, and may exceed, the rights held by the calling process.
Section: 14.8.1
Difficulty: Medium

19. Describe the two kinds of capabilities in CAP.

Ans: Data capabilities only provide the standard read, write, and execute operations of the individual storage segments associated with the object. Data capabilities are interpreted by the microcode in the CAP machine. Software capabilities are protected, but not interpreted by the CAP microcode. These capabilities are interpreted by a protected procedure which may be written by an application programmer as part of a subsystem.
Section:
Difficulty:

20. Explain how Java provides protection through type safety.

Ans: Java's load-time and run-time checks enforce type safety of Java classes. Type safety

ensures that classes cannot treat integers as pointers, write past the end of an array, or otherwise access memory in arbitrary ways. Rather, a program can access an object only via the methods defined on that object by its class. This enables a class to effectively encapsulate its data and methods from other classes loaded in the same JVM.
Section: 14.9.2
Difficulty: Medium

True/False

21. Domains may share access rights.

Ans: True
Section: 14.3.1
Difficulty: Medium

22. An access matrix is generally dense.

Ans: False
Section: 14.4
Difficulty: Medium

23. A capability list associated with a domain is directly accessible to a process executing in that domain.

Ans: False
Section: 14.5.3
Difficulty: Medium

24. Most systems use a combination of access lists and capabilities.

Ans: True

Section: 14.5.5
Difficulty: Medium

25. The "key" scheme for implementing revocation allows selective revocation.

Ans: False
Section: 14.7
Difficulty: Medium