Tecnológico de Costa Rica

Escuela de Ingeniería en Computación
Principios de Sistemas Operativos

26 de octubre de 2017

Samantha Arburola León
2013101697

Operating System Concepts

Chapter 14

14.1 What are the main differences between capability lists and access lists?

Una lista de acceso es una lista para cada objeto que consta de los dominios con un conjunto no vacío de derechos de acceso para ese objeto. Una lista de capacidades es una lista de objetos y las operaciones permitidas en esos objetos para cada dominio

14.2 A Burroughs B7000/B6000 MCP file can be tagged as sensitive data. When such a file is deleted, its storage area is overwritten by some random bits. For what purpose would such a scheme be useful?

Esto sería útil como una medida de seguridad adicional para que el viejo contenido de la memoria no pueda ser accedido, ya sea intencionalmente o por accidente, por otro programa. Esto es especialmente útil para cualquier información altamente clasificada.

14.3 In a ring-protection system, level 0 has the greatest access to objects, and level n (where n > 0) has fewer access rights. The access rights of a program at a particular level in the ring structure are considered a set of capabilities. What is the relationship between the capabilities of a domain at level j and a domain at level i to an object (for j > i)?

Dj es un subconjunto de Di .

14.4 The RC 4000 system, among others, has defined a tree of processes (called a process tree) such that all the descendants of a process can be given resources (objects) and access rights by their ancestors only. Thus, a descendant can never have the ability to do anything that its ancestors cannot do. The root of the tree is the operating system, which has the ability to do anything. Assume the set of access rights is represented by an access matrix, A. A(x,y) defines the access rights of process x to object y. If x is a descendant of z, what is the relationship between A(x,y) and A(z,y) for an arbitrary object y?

A(x,y) es un subconjunto de A(z,y).

14.5 What protection problems may arise if a shared stack is used for parameter passing?

El contenido de la pila podría verse comprometido por otro proceso (s) compartiendo la pila

14.6 Consider a computing environment where a unique number is associated with each process and each object in the system. Suppose that we allow a process with number n to access an object with number m only if n > m. What type of protection structure do we have?

Estructura jerarquica

14.7 Consider a computing environment where a process is given the privilege of accessing an object only n times. Suggest a scheme for implementing this policy.

Agregue un contador de enteros con la capacidad

14.8 If all the access rights to an object are deleted, the object can no longer be accessed. At this point, the object should also be deleted, and the space it occupies should be returned to the system. Suggest an efficient implementation of this scheme.

Recuentos de referencia

14.9 Why is it difficult to protect a system in which users are allowed to do their own I/O?

En los capítulos anteriores, identificamos una distinción entre el kernel y el modo de usuario, donde el modo kernel se usa para llevar a cabo operaciones privilegiadas como E / S. Una razón por la cual las E / S deben realizarse en modo núcleo es que las E / S requieren acceder al hardware y es necesario el acceso adecuado al hardware para la integridad del sistema. Si permitimos que los usuarios realicen sus propias E / S, no podemos garantizar la integridad del sistema.

14.10 Capability lists are usually kept within the address space of the user. How does the system ensure that the user cannot modify the contents of the list?

Una lista de capacidades se considera un "objeto protegido" y el usuario solo accede indirectamente. El sistema operativo garantiza que el usuario no pueda acceder directamente a la lista de capacidades.