104062203 陳涵宇

1. Problem Set

1. What are the main differences between capability lists and access lists?

Access list are lists for each object consisting of the domains with a nonempty set of access rights for that object.

Capability lists are lists of objects and the operations allowed on those objects for each domain.

2. 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.

Use a counter to keep tracking times of accessing.

3. 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?

Capability lists are considered to be "protected objects", so the users can only access the capability lists indirectly, thus prevent the lists modified by users.

4. Consider a computer system in which computer games can be played by students only between 10 P.M. and 6 A.M., by faculty members between 5 P.M. and 8 A.M., and by the computer center staff at all times. Suggest a scheme for implementing this policy efficiently.

Use a dynamic protection structure that changes the set of resources available with respect to the time. When the time is in the right interval, the user is available to play computer games. When the time is over, the a revocation process occurs. It can be immediate, selective, total and temporary.

5. Discuss the need for rights amplification in Hydra. How does this practice compare with the cross-ring calls in a ring-protection scheme?

Rights amplification is required to deal with cross-domain calls where code in the calling domain does not have the access privileges to perform certain operations on an object but the called procedure has an expanded set of access privileges on the same object. When a cross-ring call occurs, a set of checks are made to ensure that the calling code has sufficient rights to invoke the target code. Assuming that the checks are satisfied, the target code is invoked and the ring number associated with the process is modified to be ring number associated with the target code, thereby expanding the access rights associated with the process.