Introduction to IT Security

Homework 5 – Authentication and Authorisation

Abraham Murciano

September 21, 2020

1 Access Control Lists and Capabilities

There are two prominent methods which are used to control access to objects (resources such as files and processes). One is called access control list (ACL) and the other is called capability list (C-list).

An ACL is a data structure that indicates which subjects have which permissions for each object. Conversely, a C-list is a data structure which indicates which permissions on which objects each subject has.

One advantage of using access control lists is that permissions for any given object are all stored together, so it is easy to view who has which permissions for an object. Another advantage is that if there are more resources than users (this is often the case) then it is a lot quicker to check if a specific user has access to a specific resource, than if we were using C-lists. This is because access control lists at least as shallow as the number of users, whereas the shallowness of C-lists are on the order of the number of resources. Additionally, with ACLs it is very easy to remove (or add) objects, since each list is only related to one single object, so it would only require deleting a single list.

However, C-lists also have their advantages. Firstly, it is very easy to remove (or add) users from a system which implements C-lists, since all of that user's permissions are stored together in one list, and there would be no need to traverse multiple lists in search of references to a specific user. Secondly, C-lists are not vulnerable to confused deputy attacks in the way which ACLs are. A confused deputy attack is when a program is acting on a resource on behalf of a user, and the user provides (as raw data) an identifier to a resource which they themselves do not have permission to use, but the program which is acting as an agent does. This is a problem in ACLs because when the access control check is performed, the list belonging to the resource whose identifier was passed is checked, and since the agent program is in that list, the access control check passes. However when using C-lists, in order for the access control check to be performed, the list of everything the user has permission to do must be passed along to the check. Therefore the correct list (that of the user, not the agent program) would be passed, and the access control check would correctly fail.