INTROSEC HT2020

Problem 3

The ACL - Access Control List is popular as an access control method. However, it is not without problems. Imagine a scenario where you have 1000 users and 1 000 000 different objects (mostly files, but also some other resources). Furthermore, you have two different scenarios where in a) you have centralised control over all the subjects/users and objects, and in b) you have centralised control of whom the subjects are, but control of access rights is distributed over many different people and organisations. In all cases the access control method is the classic ACL without any wildcards.

What are the advantages and problems facing the organisation using this policy in the above case a) and b)? Does the policy work well in either case a) or in case b) (explain)?

Solution

The issues and positives in each separate case are the following:

a) When there is centralized control over the entire system that reminds us of MAC(mandatory access control). Subjects and Objects both have a set of security attributes attached with them. In this cases in every attemp by a subject to access an object the rules enforced by the operatings system will run and examine if that action is allowed or not. Here basically the acces the users can have are provided by the operating system. This in general is considered very secure access control. On the In this case though we have a huge number if users and subjects that it has to look over. To maintain all those rules and to enforce tehm every time or to enforce new oncewhen needed is an issue of maintanability. There will be needed manual configurations from the adminsitrators and that also takes time and maybe be incovinient fro such a big number of users and objects. Also this type os system is not known to be user friendly, meaning that the users have to request access for objects and in a system such as that with a centralized distribution of rights/privilages it's no the most efficient way.

b) This sounds similar to DAC (Distrecionary access control). In this case since control of access rights is distributed over many different people and organizations that leads to lower level of data protection. More people have control over more data, which doesn't make it the most secure in terms of keeping data protected. On the positive side here we have more flexibility, it is more granular since more users can configure data and access paarmeters. It is

also easier to maintain it since there are so many assigned people giving access over objects.

Which one suits better the situation

In my opinion and based in the above reasoning I could choose the first case.

The reason is because we have a big number of users and a very big number of data objects. We want to maintain security. The first case makes it easier to protect sensitive data and within an organization it is obvious that there are data such as that. Also since it is not made clear what type of organization the above is it is better to be more secure and put more effort into it other than less secure and face huge issues and impacts of that in the future. I understand that also time and ease of doing things is important for an organization which is provided more by the second option. But it is important to secure your data and put effort into it. Also big organizations do have the means to imlement such policies.