Introductoryin control focus on physical protection of information

ASSIGN BUSTER

IntroductoryIn the context of Information Security, access control is a security technique that can be used to regulate who or what can view or use resources in a computing environment. It is also a collection of mechanism that work together to protect the information assets of the enterprise from unauthorized access. The access control is enforced by security policy and different security policy provides different protection. There are two types of access control, physical and logical.

Physical access control focus on physical protection of information and assets. Logical control focus on limit the connection to computer networks, system files and data. An access control system perform authorization, identification, authentication, access approval, and accountability of entities though login credentials including passwords, PINs, biometric scans, and physical or electronic keys. Access control is very important because it used to enhance the security of the users, buildings and assets, it protect them from being destroy. For Operating Systems (OS), access control focuses on the logical access control. The OS validates the user before allowing it to access the resources. Access control is one of the key security feature which is available on both Windows 10 and Ubuntu.

In general, there are two aspects in which the access control manages which is file-level security and process-level security. File-level security is the permission to access resources and how the resources can be accessed while process-level security is the user’s capability in accessing the system. Comparison between the Windows 10 Version 1803 and Ubuntu 16. 04.

3 LTSFeaturesWindows 10 Version 1803Windows 10 utilizes the Access Control List (ACL) in file-level security. In Windows 10, The ACL contains a list of entries which is called access control entries (ACE). An unique security identifiers (SID) is used to represent users and groups in the access control model. Each ACE in an ACL identifies the trustee through SID and specifies their access rights and permission. When a security principle wishes to access any resources, their rights and permission are being examined to determine if they are allowed to access the resources and how they can access it.

Window 10's ACL has two types of ACLs which is discretionary access control list (DACL) and system access control list (SACL). A DACL identifies the security principle who are allowed or denied access to a resource. The system checks the ACEs in the resource's DACL when it is being access to determine whether to allow access to it.

If the resource does not have a DACL, the system will allow full access to everyone. If the event that the resource has DACL but no ACEs, the system will deny all attempts to access to the recourse because the DACL does not allow any access rights. The system checks the ACEs in sequence until it finds one or more ACEs that allow all the requested access rights, or until any of the requested access rights are denied. On the other hand, a SACL is being used to log the attempts to access the resources. The ACEs in SACL specifies the type of access attempts in which will cause the system to generate a record in the security event log.

Meaning that, if any attempts of accessing the record matches the ACE in SACL, the attempt will be recorded down in a security event log. An ACE in a SACL can generate audit records when an access attempt fails, when it succeeds, or both. Meanwhile for the process level security, Windows has developed a technology named User Account Control (UAC). Before the introduction of UAC, Windows generally give their user full administrative access and/or privileged access which allows the user to access everything on the system, even the most crucial parts. Thus, Windows invented the UAC to prevent this from happening. The UAC prevents modification to the Windows setting by requiring an administrator permission. A normal account user will be denied to make changes to Windows settings unless they are explicitly permitted by administrator or by signing in as an administrator. Ubuntu 16.

04. 3 LTSUbuntu uses two technology in file-level security, the UNIX owner-group-world permission model and ACL. The usage of the UNIX permission model is more preferable in Ubuntu although ACL services are provided too. The UNIX permission model explicitly define what can the owner, group and world rights to access, modify and execute a certain resources. A basic command ‘ chmod mode filename’ is being use to change the rights of the specific resources. An octal format mode is based upon an octal number representing the different mode permissions, where each of the permission groups (user, group, others) has an octal value representing the read, write and execute bits. The octal format mode is used to decide which entity is allow to perform what action on the resource.

To further enhance the file-level security, sticky bit (a. k. a restricted deletion flag) is used to make sure that a file or a directory only lets the owner of the file/directory or the root user to delete or rename the file. No other user is given privileges to delete the file created by some other user. The user may also chooses to use the ACL service which is also provided by Ubuntu. There are two (2) basic classes of ACLs for Ubuntu, minimum ACL and extended ACL.

A minimum ACL merely comprises the entries for the types owner, owning group, and other, which correspond to the conventional permission bits for files and directories. Minimum ACL have three ACL entries, ACLs with more than the three entries are called extended ACLs. Extended ACLs also contain a mask entry and may contain any number of named user and named group entries. ACL can be configured with a basic command called setfacl. There is a prerequisite in order to run the command, the partition for the file or directory which wishes to implement ACL must be mounted with ACL support. Meanwhile, Ubuntu utilized the least-privilege approach in process-level security.

Users are given least-privilege in Ubuntu. Su and sudo is the administrative account which has privilege access to the system. The su and sudo is separated from the user accounts. Thus, when a user is compromised, the system will not be affected as the affected user does not have privilege access and unable to escalate their privilege. StrengthsBy using ACLs, it is easier for the admin to check which users are able to access a given file. It is also able to scale up well, work efficiently with distributed systems. Furthermore, ACLs does not have to get involved in creating a new group. It can make the two users involved members of the group and then only change the file or directory access permission for the group.

The user can decide who can gain access to his files. WeaknessesRegarding on the weaknesses, there are a few aspect to be discussed. First of all, Windows is giving their users full access control, which mean that every users have full access the system. Without a doubt, this brings benefits to the attackers. If one of the user being infected with a virus, it is easy for the attackers to gain access to the system as the user itself have privilege access. Therefore, giving users full access control is not a good idea. Furthermore, ACLs itself contains some weaknesses.

The complexity of ACLs is one of the few weakness. In an ACL environment, it is easy to answer the question " who are the users that have access to this object", but it is difficult to determine all privileges for a user, not just for that object. Meaning that is difficult to assign, remove and modify the rights to a user on all files in ACLs.

One would require to search for all the ACLs, but it is especially difficult to do so in large system with many groups and users or system which is constantly changing. In addition, there is no centralized way to implement ACL. Different system has different format of ACLs, which means that the ACL is platform-dependent. When changing one policy model to another policy model, it may cause trouble because different system have different format of ACLs. Moreover, the other drawback of ACL is that the lack of expressiveness in the number of operations one can specify since it just extends the traditional read/write/execute permissions such that one can specify more users than just the owner and more groups than just the file's primary group.

Justification on different platformsFor Windows, the permission can be grant by owner and anyone who is authorized to grant permissions, which is the administrators. Normally, all the users are allow to access to all the file, the permission is implicitly granted unless manually change to deny. This action is insecure because everyone can access to the all the files. There are some sensitive and confidential files that should not be access, read or modify by certain users, however, with the implicitly allow permission, they are able to access the files.

Therefore, the admin should always remember to set the ACLs to explicitly denied the unauthorized users to access confidential files. However, the file access permission in Ubuntu is implicitly denied by default, unless manually change to explicitly allow. Except superuser, a. k. a root user able to access all the files, other users can only access to certain files. In order to access all the files, the users have to sudo or su to login as root user. Compare to Windows, Ubuntu is more secure because normal users are not allow to access the sensitive or confidential files at first. They are not authorized to access, read, and write to certain files unless set the ACLs to granted permission.

Selection between these two platformsIn file-level security, both Windows 10 and Ubuntu both uses the ACL technology but Ubuntu users generally uses the UNIX system-group-world permission model. The UNIX model does specific the rights and permission of a security principle, however, these permission sets have limitations. For example, different permissions cannot be configured for different users. The ACL on the other hand provides better file security by enabling one to define file permissions on “ per-user/per group” basis. Although the ACL increases the complexity due to the system admin are unable to fully understand the model, the ACL provides the system admin capabilities to define file permissions on “ per-user/per group” basis.

ACL also provides the ability for a file to be owned by several groups, instead of single group like the classic Unix permission scheme. They also have higher priority than standard Unix permission and overwrite them in case of conflict. Since Ubuntu does provide ACL services, we cannot define which of the OS has a better solution as it depends on which technology the user chooses to use. In process-level security, Ubuntu has a better solution compared to Windows.

Ubuntu relied heavily on the su and sudo tools to delegate authority and normal users are given the least privilege while the users in Windows were given full access to the system instead of being controlled. Although Windows 10 have the UAC in place to protect the users from modifying the system settings but it is simply not enough. ConclusionBoth OS provides great solutions in access controls. The technology provided has to be utilized in order to have a secure environment. The choice of user is critical thus the user need to self educate and constantly update themselves on the latest technology and how the technology works. Only with knowledge can one know what is the best to protect themselves.