Free essay about access control models

Law, Security

Access control is a mechanism that is used to control the access of users to a certain resource. There are various levels of controlling access to a resource in information systems. One of the methods is to control access at the operating systems level. The other access control levels are client/server access control, and web-based service oriented architecture access control.

In the operating system access control, one example is the use of JVM Sandbox mechanism. This is the access control that enables users to be able to download the Java Applets without having to be worried about the execution code that might take place at the machine of the user. With the use of the JVM Sandbox, it is possible to restrict the applet from accessing the local disk drives of the users. This applet will only enable the user to communicate with the originator of the code. This was achieved with the construction of the JVM Sandbox to have limited access to the machine of the user. The JVM has been designed to run in a secure Sandbox environment where it will allow for the applets to get security. One advantage with this access control for the JVM Sandbox is that it enables the security of Java binary to be achieved with the use of the machines. It is possible to have safe vulnerability assessment for machines to be protected from the bugs that come with operating systems (Ni et al., 2010).

In the operating system based access control model, there is the use of access-matrix model. The access-matrix model is a subset of the security model of the computer where the security of the computer is achieved through the control of the access to the computer resources. This model provides the restrictions for users who want to access the computer resources which are not allowed. One limitation of access-matrix model is

that it has an error called Discretionary Access Control where is possible to be attacked by Trojan Horses (Subashini, & Kavitha, 2011).

Another model is that of proof-carrying code mechanism. This is a model which has a code that will prove that the program code will not be harmful to the computer. One advantage is that users can safely download the code that is required in their machines without any harm to the computers. One limitation is that any modification by any malicious program code will prove the proof-carrying mechanism as useless.

The client/server access control mechanisms enable the control of users from accessing vital network resources and security mechanisms. One of the access control model for client/server is mandatory access model which is used to enforce security policies without regard to the actions that are done by the user. One advantage of the MAC is that that it is straightforward and fit to work in the military systems. They are good for hostile environments. One disadvantage of MAC is that it is hard to enhance the security mechanism in hostile situations because of the lack of dynamism.

Another client/server access control mechanism is Discretionary Access Control (DAC). With this access control the subjects (users) have the liberty to define the access rights to the objects that they own. It is beneficial in controlling systems with least privileges for access. One problem with this access model is that it is vulnerable to Trojan Horses.

Another access model mechanism is that of role based access control where the access is given basing on the roles of the subjects on the network. One advantage is that it enhances system integrity because it controls how systems are accessed. One problem is that it is difficult to implement in large

organizations where there is a need to have memberships.

The last level is that of web-based service oriented architecture access control. This is achieved with the use of the security stack of the web-based architecture. Access control in the SOA architecture is part of the security stack. The components of the access control include eXtensible Access Control Markup Language (XACML) and Security Assertion Markup Language (SAML). These two make the security stack of SOA (Yu, Wang, Ren, & Lou, 2010).

References

Ni, Q, Bertino, E, Lobo, J, Brodie, C, Karat, CM., Karat, J, & Trombeta, A 2010, Privacy-aware role-based access control, ACM Transactions on Information and System Security (TISSEC), Vol 13, Issue 3, pp 24.

Subashini, S, & Kavitha, V 2011, A survey on security issues in service delivery models of cloud computing, Journal of Network and Computer Applications, Vol 34, Issue 1, pp 1-11.

Yu, S, Wang, C, Ren, K, & Lou, W 2010, Achieving secure, scalable, and fine-grained data access control in cloud computing, InINFOCOM, 2010 Proceedings IEEE (pp. 1-9). IEEE.