Literature Review - ACSimulation

Aytar Akdemir

November 3, 2021

1 Review

In order to approach the subject more accurately, we need to delve into the history of the access control. First related model to protect the integrity of the data, Biba Integrity Model was proposed by Biba in [cite Biba]. In this paper, Biba does not focus on confidentiality of the data on their paper. They proposed the "read up, write down" model, which prevents subjects of lower clearance levels to modify high security objects.

Bell-LaPadula Model was proposed in [cite Bell-Lapadula], which focused on the confidentiality of the data using a similar method. It can be summarized by "write up, read down", subjects with low clearance levels cannot access to the high security objects. Subjects with high clearance levels cannot write down, thus maintaining the confidentiality of the data.

In the 1980s, U.S. Department of Defense (DoD), published Trusted Computer System Evaluation Criteria (TCSEC)[cite TCSEC]. The goal of the document was to set standards for the IT systems in the companies working for the U.S. government. These specifications lead to the Multilevel Security.

Multilevel security (MLS), is a security specification for systems to be secure. Objects are defined as files or a certain data in the system. Subjects are defined as the users that interact with the objects. In MLS, objects has classifications depending on how critical the data is. Subjects have security clearance levels, which let them access to the appropriate object.

Mandatory Access Control (MAC) and Discretionary Access Control (DAC) have been defined in the TCSEC. In MAC, the objects and the subjects cannot be altered and they interact with each other in a hierarchical manner. In DBAC, a subject with a clearance can give another subject a permission to access a specific security level.

The models that are going to be simulated in this paper, have their roots in the models we have introduced so far.

2 Related Work

The objective in this article is to develop a simulation enviroment for the various authorization schemes. This simulation will be used to perform vulnerability analysis on a system. This will help determining the best authorization scheme for a system, depending on its structure and needs.

In [cite blobel], Blobel defines various standards for modelling security services using formal models. In document model processes are documented and they show how processes interact with other data. Documents are protected by signatures. Another model defined is the policy model, which involves using a formal language to define a policy. Various examples are provided, such as Object Constraint Language (OCL) and XACML.

Ficco develops a simulation platform for testing cybersecurity systems in [cite Ficco]. The network the attacks are being carried out are modeled using various network modeling tools. Some of the network tools used are NS3, NetSim and OPNET. They create components that use channels to send data, simulate attackers behaviour. Data is collected afterwards for the analysis.