Literature Review - ACSimulation

Aytar Akdemir

November 17, 2021

1 Review

It is necessary to delve into the history of the access control in order to approach the subject more accurately. First related model to protect the integrity of the data, Biba Integrity Model was proposed by Biba in [cite Biba]. Biba does not focus on confidentiality of the data on their paper. Biba proposes 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. The model 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.

United States Department of Defense (DoD) published Trusted Computer System Evaluation Criteria (TCSEC) [cite TCSEC] in the 1980s. The goal of the document was to set standards for the IT systems in the companies working for the United States government. These specifications led to the concept of 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. The objects have classifications depending on the importance of the data. The subjects have security clearance levels that allow them to 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. Subject-object interaction is performed 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 which are going to be simulated in this paper have their roots in the models which have been introduced up until now.

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 the document model, processes are documented and they show how processes interact with other data and 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 in which the attacks are being carried out are modeled using various network modeling tools. Some of the network tools used are NS3, NetSim and OPNET. The authors create components that use channels to send data, simulate attackers behaviour. Data is collected afterwards for the analysis.