Literature Review - ACSimulation

Aytar Akdemir

December 1, 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.

A model for determining the privileges of the subjects was proposed by Lampson in [cite Lampson]. In an access control matrix, columns are objects and each row is a subject. Permissions for each subjects is stored, namely, read (r), write(w), execute(x). Access control matrix is not used in practice mainly due to the space requirements.

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.

1.1 Formal Models

Clark-Wilson In [Cite ClarkWilson], Clark defines an integrity model that focuses on the consistency of the transactions. The data checked for integrity are called constrained data items (CDI). The data which is not controlled are called unconstrained data items (UDI). There are two mechanisms to ensure the integrity of the system.

- Integrity verification procedures (IVP): IVP ensures CDIs within the system comply with the integrity specifications.
- Transformation procedures (TP): TP ensures state transitions go smoothly, CDI should transition between a valid state to another valid state. No other entity then TP is permitted to change the CDIs.

Each TP and the every CDI it controls should be kept in a list in the form of relations. This list will be used for guaranteeing that the CDIs are not changed by something other than the TP.

The lists of relations may only be changed by a certain agent entitled to certify. This makes it clear that Clark-Wilson is not discretionary.

Take-Grant

Take-Grant model was introduced in [cite Take-Grant] by Lipton. The model uses directed graphs to prove the security of the system. In order to achieve the proof, several rules are defined;

- Take: Subject takes the rights of a subject if it has the t (take) right to it.
- Grant: Subject grants the pointed subject its rights if the subject has the g (grant) right pointing right to it.
- Create: Subject can create a new node with the tg rights to it.
- Remove: Subjects can remove the thier rights pointing to other object.

These rules are used to analyse the reach of an attack on the system.

State Machine

—

Petri Net (Place/Transition)

—

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 determine 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.

Penetration testing is another concept related to the simulation which is plannes for this study. In a penetration testing attempt, system security policy in place is exposed to controlled attacks. In [cite Weissman- Penetration testing], rules for developing a strong penetration testing plan is established by Weissman. The rules are satisfied when a predetermined amount of security vulnerabilities are found, testing has continued for a certain amount of time and the security measures are overcome in order to harm the system resources.

Linde showcases another penetration testing for operating systems [cite Linde]. Using the Flaw Hypothesis Methodology, system is analyzed for attack possibilities. The proposed methodology consists of four steps. A hypothesis for a flaw is developed, followed by the confirmation of the hypothesis by carrying out penetration testing such as large volume inputting. Next step is to generalize it by analyzing and categorizing the flaw. The final step is to fix the flaws which might lead to system damage.

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.