Thesis Journal 2

Aytar Akdemir
150170115

September 12, 2021

1 Progress Since the Last Entry

Instead of the term "Access control model", we are going to focus on "Authorization model". Access control models are superset of Authorization models and they have many functions such as authentication, authorization, and audit.

In light of these developments, some of the AC models proposed in the last journal entry have been discarded.

This week, I researched and summarized the Authorization models and Multilevel Security. While researching I familiarized myself with some other concepts and summarized them at the end of the document.

2 Multilevel Security

It is the system that processes information with different security levels, permits access to users with different security clerances. MLS restricts access to the users without authorization.

2.1 Trusted Operating Systems

MLS operating environment needs a TRUSTED operating system that supports MLS. Because all information in an MLS is accessible by the OS. Historically, few OSs have MLS range from unclassified to top secret.

2.2 Problem Areas

Sanitization: How can a high clearance user share a high security object with lower clearance users? MLS systems circumvent this problem via privileged functions that lets high clearance user to bypass the MLS and change a file's security classification (not reliable).

Covert Channels: A top secret process should not be able to send signal to lower security processes. However, the unaccounted channels may pose a risk, such as changes in memory or disk space, changes in process timing. These are called covert channels.

Bypass: Wikipedia definition: "A common example is to extract data from a secret system high object to be sent to an unclassified destination, citing some property of the data as trusted evidence that it is 'really' unclassified (e.g. 'strict' format). A system high system cannot be trusted to preserve any trusted evidence, and the result is that an overt data path is opened with no logical way to securely mediate it."

3 Authorization Models

Mandatory Access Control: Subjects have clearance labels and objects have security labels (secret, top secret etc.). Only the authorized clearance labels can access to objects. MAC cannot be bypassed or controlled.

Discretionary Access Control: Restricts based on the identity of the subject. DAC is implemented by using Access Control Lists. ACL identifies who can access the object and what they can do with it (read, write etc.). SUBJECTS CAN MANIPULATE IT. Owner of a resource and the security administrator can identify who can access the object.

Role-based Access Control: Roles are used instead of identities. Roles are assigned either statically or dynamically according to their responsibilities. In environments where change is frequent, dynamic roles are used.

Attribute-based Access Control: Access rights are granted to users through the use of policies that combine attributes together. Attributes of the subject, object, environment conditions can be used.

4 Other Related Concepts

Bell LaPadula Model: Focuses on data confidentiality. WURD (Write up, Read down). Three rules, one from DAC, two from MAC:

- Simple Security: Subjects can't read higher security level than their clearance.
- Star Property: Subjects can't write to lower security level than their clearance.
- Discretionary Security Property: Discretionary access is defined using the ACCESS MATRIX.

Biba Integrity Model: Focuses on data integrity. Three properties; first two are inverse of the Bell LaPadula Model (No WU, No RD).

- Simple Integrity: Subjects can't read lower security than their clearance.
- Star Integrity: Subjects can't write to higher security level than themselves.
- Invocation Property: A process cannot request higher access. Only lower or same.

Protection vs Security: Protection is a mechanism while security is a policy. Mechanisms should not dictate the policies. Protection separates assets from threats. Security is achieved when there is a resistance to the threats by the protection mechanisms.