Principles of Computer Security

Alvin Lin

January 2018 - May 2018

Access Control Principles

Subjects make requests to active entities such as users or processes. Subjects can be active users or processes, and objects are usually passive entities manipulated by a subject such as records, relations, or files. Access control helps protect objects from unauthorized disclosure and unauthorized modification. It is an approach to regulate access requests by subjects to objects to perform certain operations through a set of access policies.

Access Control Policies

- Discretionary Access Control (DAC): based on requestor identity and access rules stating what requestors are allowed or not allowed to do.
- Mandatory Access Control (MAC): based on comparing security labels with security clearances.
- Role-based Access Control (RBAC): based on user roles within the system and on rules stating what accesses are allowed to users in given roles.
- Attribute-based Access Control (ABAC): based on user attributes, the resource to be accessed, and current environmental conditions.
- Content-based, Context-based, History-based, etc.

Access Control Matrix

	Object 1	Object 2	Object 3	Object 4	Object 5
S1	r	r	rw		
S2	rw		r	wx	
S3	r	rw	rwx	rwx	w
S4					

Each column in this matrix is an access control list that determines each object's list of access rights to subjects. Each row in the matrix is a capabilities list that determines each subject's list of capabilities for each object.

DAC Overview

With discretionary access control, entities are able to access resources based on some access control matrix. Each entry in the access matrix controls a subject's permission to access some object. The UNIX file access control uses discretionary access control by allowing file users, various groups, or the public to read, write, or execute the file based on the permission bits set for the file.

MAC Overview

The mandatory acccess control model is sometimes known as the non-discretionary model. It works with multi-level security and is suited for handling data with multiple sensitivity levels. It permits simultaneous data access by users with different clearance levels and need-to-know, while prevent users from obtaining access to information for which they lack authorization.

Clearance Groups	Read Access	Write Access
Top Secret	✓	✓
Secret	✓	✓
Confidential	✓	
Public	✓	

A lattice is often used to categorize different objects into categories under a clearance level. If a subject's access label does not encompass the object's label and category, then the subject is denied access.

Multi-level Security Models

Bell-LaPadula:

- Designed to protect confidentiality
- Top secret, Secret, Confidential, Public
- No Read Up, No Write Down
- Trusted subjects are allowed to violate insert, update, and delete MACs

Biba:

- Designed to protect integrity
- Top secret, Secret, Confidential, Public
- No Read Down, No Write Up
- Trusted subjects are allowed to violate insert, update, and delete MACs

RBAC Overview

- A subject has access to an object based on an assigned role.
- Roles are typically defined based on job functions.
- Permissions are defined based on job authority and responsibilities within a job function.
- Operations on an object invoked based on permissions.
- Object access depends on a subject's role, not the subject.

This system is much more pragmatic, but has a lack of granularity and flexibility. Improper actions are not always the same as unauthorized actions. Certain users may be able to perform actions that are not proper for their role because it would be logistically difficult to enforce that level of granularity with RBAC systems. There is no connection between who the person is and who gets permission.

ABAC Overview

- Can define authorizations that express conditions on properties of both the resource and the subject.
- Strength is its flexibility and expressive power.
- The main obstacle to its adoption in real systems is its performance impact when evaluating predicates on both resource and user properties for each access.
- Web services have been pioneering technologies through the introduction of the eXtensible Access Control Markup Language (XAMCL).
- There is a considerable interest in applying this model to cloud services.
- Subject attributes in this model define the identity and characterestics of the subject.
- Objects have attributes that can be leveraged to make access control decisions.
- Environment attributes describe operational, technical, and situational environment or context in which information access occurs. It is largely ignored in most other access control policies.

ABAC systems are capable of enforcing DAC, RBAC, and MAC concepts. They allow an unlimited number of attributes to be combined to satisfy any access control rule.

RBAC vs ABAC

RBAC	**ABAC**
Static	Dynamic
Coarse-grained	Fine-grained
Access decisions made in advance	Access decisions made at run-time
Simply policy	Complex policy
Complex setup	Simple setup

You can find all my notes at `http://omgimanerd.tech/notes`. If you have any questions, comments, or concerns, please contact me at alvin@omgimanerd.tech