UTM

UNIVERSITI TEKNOLOGI MALAYSIA

UNIVERSITI TEKNOLOGI MALAYSIA

SCHOOL OF COMPUTING

SEMESTER 1 2020/2021

SCSR3413-01 KESELAMATAN KOMPUTER (COMPUTER SECURITY)

Attribute Based Access Control

LECTURER

Prof. Shukorar

By

Abdulrahman Mohammed Aqel Assaggaf (A18CS4054)

Attribute Based Access Control (ABAC)

Attribute-based access control is a model that evolved from RBAC. This model is based on establishing a set of attributes for any element of your system. A central policy defines which combinations of user and object attributes are required to perform any action.
Let's consider the main components of the ABAC model:

- Attribute – a characteristic of any element in the network. An attribute can define:
- User characteristics – employee position, department, IP address, clearance level, etc.
- Object characteristics – type, creator, sensitivity, required clearance level, etc.
- Type of action – read, write, edit, copy, paste, etc.
- Environment characteristics – time, day of the week, location, etc.
- Subject – any user or resource that can perform actions in the network; a subject is assigned attributes in order to define its clearance level
- Object – any data stored in the network; objects are assigned attributes in order to describe and identify them

The ABAC model defines an access control paradigm whereby access rights are granted to users through the use of rules combining attributes. Thus, access policies can use any type of attribute (user attributes, resource attributes, object attributes, environment, etc.). To do this, this model applies Boolean logic, in which the rules contain "IF, THEN" statements about the identity of the requester, resource, and action. For example: IF the requestor has an Administrator profile, THEN give them read / write access to sensitive data.

Pros

1. Easy scalability.
2. Provides greater flexibility in a distributed, open, shareable and dynamic environment where the number of users is very high.
3. Fine granularity (model based on attributes).
4. Easy administration.
5. Provides central storage for user attributes, it increases interoperability and sharing among multiple service providers to decide user rights.

Cons

1. Strong need for provisioning and maintenance of attributes.
2. Complex analysis due to the heterogeneity of user information complexity. Therefore, all the attributes in the central database need to be in the same format.

In sum, attribute-based access control enables:
Flexibility — because the policies needed to meet ethical and legal privacy obligations are more complex now than ever before, and will continue to increase in complexity.
Simplicity — because it avoids role explosion and removes the burden on data teams to predetermine and create roles for each new data access request or data usage need.
Customized permissions — because it separates user attributes from where and when users have access to data, which in turn removes uncertainty about what data users implicitly have access to data when they are added to roles.

Applicability

This approach is suitable for a company of any size but is mostly used for large organizations. ABAC requires more time and effort than RBAC at the deployment and configuration stage, as security administrators need to define all attributes of the system. First, you need to assign attributes to each system component manually. But once you've created policies for most common job positions and resources in your company, you can simply copy them for every new user and resource. This is similar to how a role works in the RBAC model, but in the ABAC model, attributes can be modified for the needs of a particular user without creating a new role. Attributes make ABAC a more fine-grained access control model than RBAC.

Example of its application.

The ABAC can be used in Databases security because of the solutions that it offers for the Database administrator. ABAC allows you to design controls around the characteristics of data that warrant protection in the first place; this could be type of content, project, security clearance, and so on. Attribute Based Access Control also takes into account information about the user and the environment, including location, position, device, and network.

Controls can be written as simple versions of information sharing policies. Once written, a single policy can be deployed across multiple systems and hundreds of devices. Unlike traditional controls, which require permissions to be defined statically before an access attempt occurs, ABAC rules are evaluated dynamically with attributes presented at run-time. The attributes can come from multiple sources – even sources external to an organization.

Plus, enforcement adapts to risk level automatically. For example, if the classification of a document changes, or a user's team membership changes, access rights are automatically adjusted. No need to request new roles or update permissions.request new roles or update permissions. Implementing ABAC.

References :-

https://www.axiomatics.com/attribute-based-access-control/

https://www.okta.com/blog/2020/09/attribute-based-access-control-abac/

https://docs.aws.amazon.com/IAM/latest/UserGuide/introduction_attribute-based-access-control.html