Chip Gardiner

Term Paper

CYBR 450 Advanced Cybersecurity Concepts

October 25, 2022

**Moving to attribute-based access control to create increased security and scalability for business growth**

**Abstract**

Access control is a major element for a business in their security policy. The logical access control model used is important in the protection of the data and information of a business and the work it does. Broken access control has been in the top ten of the OWASP reporting of vulnerabilities for web applications (OWASP, 2021).

Access control vulnerabilities had 275 incidents of attacks with 216 having confirmed data disclosure as reported in the Verizon Data Breach Investigation Report (Bassett, Hylender, Langlois, Pinto, & Widup, 2022). 80% of these incidents were from privilege misuse.

Access control is effective when used properly, but it has not been used properly in its current model of role-based access control and vulnerabilities have been discovered

Attribute-based access control is a more effective way at handling logical access for subjects in a more modern workforce. The introduction of remote work and access for users along with the interconnectivity of departments requires a more granular approach to what files are accessed by users. With a good defense-in-depth strategy and zero trust, attribute-based access control is more secure way to protect access to objects while allowing for scalability and flexibility in the business. Attribute-based access control is the most effective way for businesses that work on multiple projects with specific deadlines as well as those that have users who take on multiple roles at different times in the business.

**Business Problem**

Most access control models are effective but have smaller problems within the business unit for employees who are unable to access objects needed to perform duties in their position or asked of them by leaders in their organization. This is because access to the objects is denied based either on the role or security clearance assigned to the subject or the object. This methodology of access control does not allow for flexibility based on what the subject is working outside of their assigned role in the logical access. As this organization grows and becomes more dynamic many types of access controls models are not a good fit for the needs of the organization (Alohaly, Takabi, & Blanco, 2019).

**Executive Summary**

It is the recommendation of this group that the organization move to an attribute-based access control model. This model allows for access control to grow with the flexibility of the organization as users take on roles that stretch across what would be normally defined roles in the logical access control. The attribute-based access control model will more easily scale with the organization and increase security with defense in depth by layering work locations so if there is a breach at one location it will not as easily affect other locations. This model will also ensure team members are able to access all objects and information needed to effectively do their work and not have access to objects beyond the scope of their work and that data integrity will be more consistent across the organization.

**The Importance of Access Control**

Access control is one of the most important drivers for a business. The need to protect information is vital to avoid the risk that would happen if sensitive information was leaked from lack of protection on that information (Chapple, Access Control and Identity Management, 2021). Having the right resources for the right people at the right time is a cornerstone of our information security policy. Effective access control is the foundation of this entire policy because improper access means either people are not gaining access to the right information, or malicious actors are gaining access to our information. Attribute-based access control also allows for us to have the right resources for employees who are working on critical projects under specific timelines.

Access control is one part of the overall defense-in-depth strategy we employ. This move to attribute-based access control will also move us to a deny-by-default strategy that was not fully implemented under the access control lists. With deny-by-default if a subject does not have assigned access to an object, then that access is

denied. We can leverage inheritance is a more vital way with inheritance being granted to objects from access user groups and the attributes assigned to them.

The goal of access control is to protect the confidentiality, integrity, and availability of data by allowing access to the right people in the right place at the right time (Chapple, Ballad, Ballad, & Banks, 2014). This can be done with many types of access control, but an attribute-based model would be considered best to allow the organization to move forward with increased security from outside breaches, increased availability of the data for the team members who need it, and having assurance that the data is correct when accessed because it has been more properly secured from allowing access to other team members who did not need that level of access.

**What is Attribute-based Access Control**

Attribute-based access control is a model of access control where subjects are granted or denied access based on attributes assigned to the objects (the files and directories of a system), the subject (the user), or other conditions (Hu, Ferraiolo, Chandramouli, & Kuhn, 2018).

Attributes are typically broken down into two groups, subject attributes, and object attributes. There will also be some environmental attributes that will need to be considered to assign to certain objects to allow for more granular access for users who may work across multiple departments or for departments that are working together on a project with a specific timeline.

Each subject is assigned attributes based on criteria such as role, security clearance, or other characteristics that are in line with policy such as work done in another department.

Attributes assigned to the object based on the data it contains or what project it is associated with. Can also be assigned by other criteria such as clearance or application used for the object.

Environmental attributes will also be considered as we create our access control model. Environmental characteristics to be considered are if someone is covering tasks for another team member, working with another team that would have different attributes from the team they are assigned with.

With attribute-based access control, there are more inputs into a policy decision. Because of this, attributes can change at any point and this increased flexibility allows for access to an object to be based on attributes of the object (Hu, Ferraiolo, Chandramouli, & Kuhn, 2018). There is no need to consider what subjects may have access to an object when assigning attributes.

**What is Role-Based Access Control**

Role-based access control is the model currently in use in the organization. In this model, access is granted based on the role inside the company such as manager, programmer, buyer. This is an effective model to allow subject access and has been generally more cost-effective than using a model where everyone is granted access to specific objects. This broader approach allows for less time spent checking access to a person if they change roles because of a promotion and creates less errors in access control changes (Boyle & Panko, 2021).

Role-based access has some inheritance built into it allowing senior leaders to have access to specific objects but also keeping access to objects that members of their team would have as well.

This system has overall been effective for the organization but is lacking in the ability to allow access for individuals to specific objects without also creating excessive cost for the organization to move to a structure with individualized access.

**Differences between role-based and attribute-based access control**

The major difference between these two access control models is the reasoning behind the decision-making of each model. The decision making in attribute-based access allows for more granular assignments due to the assignments being based on attributes that are assigned to both to subject and the object.

In a role-based access model a manager over a team that handles a team of customer support representatives would have access to objects assigned to them that have the assignment of the manager role and the customer support role. With the role assignments as they are the manager would not have access to human resource objects without having a different access role created that would allow access to both manager and human resource roles.

In attribute-based access control objects and subjects are assigned attributes to allow the subject access to an object with the same attributes. In the example above the manager over customer support would have attributes of manager and customer support. These two attributes would grant access to objects that have those same attributes. Environmental attributes can be applied as well to grant the manager access to human resource files pertaining to customer support. If the manager was also given tasks to oversee the financial health of their team, they could be given attributes that allow them to see objects pertaining to that as well.

Attribute-based access requires more workload than role-based with the need to assign attributes overall if there are changes to what an individual is doing currently, but

some of these will be able to be handled by senior leaders. This increased workflow will be worth the extra security granted with an ABAC model combined a zero-trust architecture. In zero trust, if a subject is asking for access but there are not attributes that match from the policies or policy sets then access is denied.

Overall, an ABAC model allows for more granular assignments while keeping more broad assignments that are found in the RBAC model. This increased flexibility will require more workload, but not to the degree that individualized access would require.

The workload required will not be as much of a burden on the system administrators who are having to modify access to all subjects, but instead can also be handled by managers and other leaders who will be able to assign attributes to their team based on the work they are doing.

**Deployment of new access control model**

The deployment for this model will be use the Extensible Access Control Markup Language (XACML). This language is the most widely used standard for implementation of attribute-based access control and covers all elements needed for this. XACML is an XML based language that is platform neutral and will provide a single standardized language for assigning attributes (Hu, Ferraiolo, Chandramouli, & Kuhn, 2018).

XACML policy language uses three main components:

* + - Rule
    - Policy
    - Policy set

These are hierarchical in organization, a policy contains multiple rules, and multiple policies are contained in a policy set. Policy sets can also be nested with policy sets

inside of another policy set. Only two of the three components can be used in the structure of an authorization database, typically a policy or policy set because a rule only is not in-depth enough to be built upon. A policy or policy set will always be used as the root XML tag in the policy language.

XACML uses a data flow model to make access decisions with five key functional models:

* Policy Enforcement Point (PEP)
* Context Handler
* Policy Decision Point (PDP)
* Policy Administration Point (PAP)
* Policy Information Point (PIP)

The five elements listed each play a role the decision-making process and help break down the Boolean decision of deny or authorize based on the wider range of attributes that are applied to both subjects and objects in the model.

These elements work in the following way on the data flow model:

1. The PAP writes the policy sets and policies that are available to the PDP.
2. The request for access is sent to the PEP.
3. The PEP sends the access request to the context handler.
4. The context handler constructs a request in XACML context and sends it to the PDP.
5. The PDP requests any additional attribute values from the context handler.
6. The context handler requests the attributes from the PIP.
7. The PIP obtains the requested attributes.
8. The context handler forwards the attributes to the PDP.
9. The PDP requests the PAP for policies matching the target from the request.
10. The PAP returns the requested policy.
11. The PDP evaluates the policies and returns the decision for authorization to the context handler.
12. The context handler translates the response from XACML to the native format of the PEP and returns the response to the PEP.
13. The PEP enforces the decision of allow or deny. (Hu, Ferraiolo, Chandramouli, & Kuhn, 2018)

The context handler acts as the central hub sending all information across the data flow translating requests from XACML to the original language of the requests from the other policy points.

**Timeline for implementation of attribute-based access control model**

To completely change models will require this to be done in stages with some testing along the way to ensure that all criteria are being met in the security policy and that team members can access all the required information for their job.

Attributes will be assigned based on current roles, job site, departmental interactions, and current projects. Attributes for users who handle information across departments will be considered and implemented.

Attributes will be assigned to objects, files and directories, based on the data the objects have, the department that the object originated from.

Environmental attributes will also be assigned based on criteria such as a project with a specific deadline that would contain work from multiple departments working together, team members who are taking on extra assignments to cover for others that are out for an extended period.

A single department that works across multiple sites will be the first to be tested on the new role to determine how well access has worked for the users as they test access for information related to their department, their position, and for their specific location.

Testing will be done on a specified regular timeline to determine effectiveness and for vulnerabilities. Team members of the test department will take an assessment to determine the effectiveness of the current iteration of the ABAC model.

The model will be modified to any changes that are appropriate and the deployment to live environment will begin.

# References

Alohaly, M., Takabi, H., & Blanco, E. (2019). Automated extraction of attributes from natural language attribute-based access control (ABAC) Policies. *Cybersecurity vol. 2*, 1-25. Retrieved from https://doi.org/10.1186/s42400-018-0019-2

Bassett, G., Hylender, C. D., Langlois, P., Pinto, A., & Widup, S. (2022). *Verizon Data Breach Investigations Report.* Verizon.

Boyle, R. J., & Panko, R. R. (2021). *Corporate Computer Security.* Boston: Pearson.

Chapple, M. (2021). *Access Control and Identity Management.* Burlington: Jones & Bartlett Learning.

Chapple, M., Ballad, B., Ballad, T., & Banks, E. K. (2014). *Access Control, Authentication, and Public Key Infrastructure, Second Edition.* Burlington: Jones and Bartlett Learning.

Hu, V. C., Ferraiolo, D. F., Chandramouli, R., & Kuhn, D. R. (2018). *Attribute-Based Access Control.* Boston: Artech House.

OWASP. (2021). *A01:2021 Broken Access Control*. Retrieved from OWASP.org: https://owasp.org/Top10/A01\_2021-Broken\_Access\_Control/