AXIOMATICS

Case Study

Efficient Enterprise-Wide Risk Management and Secure Collaboration using ABAC

Executive Summary

A major US automotive manufacturer was faced with a consolidation challenge. As with many large enterprises, security authorization had historically been handled by individual business units or product owners. Over time, this car company wanted the benefits of moving to a standardized approach to access control, and built their own authorization engine.

The team was moving in the right direction from a security perspective, but challenges began to emerge. The management of both system maintenance as well as in the ability to grow and scale were the main areas, as they had begun to see bottlenecks in authorization, and that the system was not fully meeting the authorization challenges.

As a first step the company took their propriety access control policies, role-based access control and access control lists, and implemented a home-grown XACML solution in-house. The natural evolution from this in-house solution, was to enlist a third-party vendor to help further grow and scale.

They chose Axiomatics and the Axiomatics Policy Server, to take the pressure off of maintaining and growing their system, and to get the development teams refocused on writing other valuable code. Axiomatics Policy Server replaced the homegrown Solution, controlling access to critical applications by using externalized dynamic authorization, delivered through Attribute Based Access Control (ABAC)

Customer Background

Our Client
A US-based Fortune 100 automotive manufacturer

Number of Employees
199,000

Car Production Output
6 Million

Applications
1000s of global applications

Applications
Replace in-house authorization engine with Axiomatics Policy Server

Users
Millions of constituents across third parties, dealers, business units and global customer base

Background

The policy-based access control approach used by this car company has evolved over several years. 160 applications use the company's centralized authorization solution, and they created a very simple UI for application owners to write policies. The policies are mainly role-based and identity-based (access control lists).

As requirements became more complex, it was harder to maintain the home-grown solution. In particular, the functionality to do reverse queries was missing.

Growing Challenges

- The authorization changes were causing slow time to market for their applications. As the organization matured, they were concerned about the impact of the shifting to new technology, and how the performance of the access control system would be affected if they moved it off obsolete systems.
- Using XACML certainly helped their policies be portable, but they were doing more and more custom-coding in the process, and the application developers were overwhelmed.
- The team was hearing more frequent complaints from business lines in not being able to grant access to various systems quickly. In some cases, collaboration was hindered when the system would default to a fail/close.
- Policy needs grew, and soon bloated policies hard-coded within applications became too complex to manage.
- There was a need to reduce overlap in the policies while maintaining isolation between business units for IP protection and privacy; so on the other hand they need to continue supporting duplication in commonality among policies.

This set the stage to look at external vendors.

Use Cases Solved with ABAC

By implementing common policies that can be dynamically enforced and managed by prominent business units, the company enabled collaboration while protecting critical assets. There were various use cases across the enterprise that took advantage of the policy-based approach. Two of these use cases are the evolution of their role-based system, and achieving data-level security.

Use Case #1

Achieving Value on Specific Enterprise Needs

Historically a lot of the role-granting logic was written in code for their home-grown solution. This approach is an indirect use of ABAC for user role provisioning, in which users can request a role for themselves or for other users, and the Axiomatics Policy Server is used to determine whether a user can request a given role. In essence, the use case uses ABAC for entitlements orchestration via an enterprise access provisioning catalog, with the Axiomatics Reverse Query being a key component for success.

The applications at the company consume these roles to determine whether a user can access the requested application functionality. In this use case, the Axiomatics Policy Server is used to determine whether a user can request a given role. The policies consider the role as the resource. The policies also refer to the requestor and the recipient of the role.

Outcomes:

- More control over authorization provisioning
- Standardized, policy-based approach
- More control over user populations, ability to filter roles
- Prevents toxic combinations
- Eases the evolution away from a pure RBAC approach

> We've been able to leverage our existing access control setup in our use of ABAC, which sets the stage for our process to grow and scale over time.
> *Access Management Architect*

Use Case #2

Data-Level Entry

The company wanted to use global policies that get applied automatically to all access control at the company. Global policies can include things like enterprise-wide checks, such as no access outside of work hours, or outside of the company network. In this case granular provisioning rules were needed. Implementation of common policies are managed by the business unit owners.

They needed to eliminate potential toxic combinations that would inadvertently permit access, reduce potential data leakage between brands and new release, reduce or eliminate duplication of efforts and reduce the time for the authorization response.

Using an ABAC approach and the Axiomatics Policy Server, they were able to implement global policies that would apply enterprise –wide, while also giving individual business units the ability to write policies specific to their security needs.

Outcomes:

- Ability to control the order policies are checked, to ensure the central corporate policies are checked first
- Using global policies makes it easier to quickly apply enterprise checks consistently and transparently, yet app owners have freedom to apply unique policies.
- The overall policy structure was simplified
- Ensure security and regulatory compliance, and provide audit capabilities

Overall Business Benefits

The automotive manufacturer continues to add new applications to the new Axiomatics Policy Server authorization engine, under various ABAC-based use cases. They are seeing improvements in performance, speed to market and reductions in staff time spent on hard-coding and authorization tasks.

The outcome of the project includes these gains:

- Application developers do not need to write their own authorization solution.
- Facilitates faster time-to-market, by reducing effort and application costs of implementing local solutions.
- Authorization rules are externalized so changes to those rules do not affect application code.
- Business owners can define authorization policies with out the involvement of IT.
- Provides centralized and consistent management of authorization policies across the enterprise.
- Facilitates common, repeatable, auditable security practices
- Easily integrated into Java COE frameworks and tools

Results

The scope of the project has included several accomplishments:

- 300+ global applications and services
- Benchmarked new Policy Decision Point from Axiomatics, has achieved 10x faster responses with consistent results
- Achieved 100-fold ROI in development cost
- Standards-based approach has maintained core interoperability
- Can handle more complex rules and build robust policies without slowing response time.

Conclusions: New Use Cases and Beyond

This automotive leader continues to add new use cases to the program to creatively solve their access control challenges. The Axiomatics solution will allow them to scale: To migrate other types of systems to the ABAC approach, scale throughout the enterprise, and continue to streamline the number of policies being managed. By enlisting the Axiomatics Policy Server to take over their home-grown XACML-based ABAC system, they have saved time, reduced cost and achieved a 10x improvement in authorization performance.

> “We’re adding more applications every day, and couldn’t be more pleased with the improvement of performance and reduction in staff burden.”

Solution

As the best-in-class vendor for policy-based dynamic authorization, Axiomatics was chosen to help address various specific use cases, and provide a solution that would ultimately provide authorization for every application.

Enabling infrastructures with Attribute Based Access Control (ABAC) capabilities is a priority at global manufacturers like this automotive manufacturing leader. The Axiomatics Policy Server provides dynamic authorization for applications, and is an independent solution which easily integrates with existing Identity and Access Management (IAM) tools. In addition, this suite provides friendly policy authoring and life-cycle management, service administration and monitoring.

The Axiomatics Policy Server boasts the industry’s most robust Policy Decision Point, meaning that the improvements in performance and authorization, as well as the capability to do reverse queries, auditing and reporting.

AXIOMATICS

Axiomatics is the premier vendor of dynamic authorization delivered through Attribute Based Access Control (ABAC) solutions. With a global customer base within healthcare, finance, manufacturing, insurance, media and the public sector, Axiomatics offers proven authorization solutions that can be tailored to meet the demands of virtually any organization.

WWW.AXIOMATICS.COM | WEBINFO@AXIOMATICS.COM

525 W Monroe St., Suite 2310
Chicago, IL 60661, USA
+1 (312) 374-3443

42395 Ryan Road
Suite 112- PB Box 805
Brambleton, VA 20148, USA
+1 (801) 556-9994
sales@axiomaticsfederal.com

Västmannagatan 4
S-111 24 Stockholm, Sweden
+46 (0)8 51 510 240