EXECUTIVE SUMMARY

Evolving from RBAC to Next-Generation ABAC

AXIOMATICS
a LEONARDO company

Overview

Enterprises face a rapid expansion of diverse users alongside an influx of applications, devices, APIs, and microservices.

The amount of data created and consumed by these users, devices and services continues to explode, creating extraordinary security and compliance challenges.

Enterprises must find a way to ensure business users are able to access the data and assets they require while ensuring critical information remains secure and adheres to a growing number of compliance regulations.

To ensure secure access, enterprises can no longer afford to define authorization policies based solely on a user's role. The context surrounding that user, their data and the interaction between the two is essential as it enables the enterprise to provide the right access at the right time, in the right location, and by meeting regulatory compliance.

That means evolving an existing role-based access control (RBAC) model to an attribute-based access control (ABAC) model.

ABAC or contextualized authorization builds on existing roles and expands the range of attributes used in the authorization process while using a context-rich policy language that easily caters to both simple and complex use cases.

Equally important, ABAC enables access policies to be defined and enforced within one manageable central service instead of being hard-coded into the hundreds of thousands of applications in a typical enterprise's portfolio.

As a result, enterprises can provide well-rounded access control that builds on RBAC's strengths while harnessing ABAC's ability to capture contextual information.

What is RBAC?

Role-based access control (RBAC) was designed for a simpler world. Formalized by NIST in 1992, RBAC quickly became the standard for enterprises managing more than 500 employees.

Outpacing previous models, RBAC was largely implemented within provisioning systems, attempting to streamline the joiner/mover/leaver process which gave enterprises the ability to manage access control by role, rather than by an employee's individual user ID.

This new strategy provided an extra level of abstraction, acting as a collection of permissions or entitlements. It enabled user access to be based on functional business roles (manager, director, etc.) or functional IT roles (IT manager, system administrator, etc.). Because each role could be assigned to one or hundreds of users, management was a far simpler task.

At its most basic, RBAC works by allowing administrators to assign access permissions or entitlements to roles. Once defined, these roles can be assigned to individual users who may have one or several roles, each with different access rights. As a business moves forward, new roles can be created and allocated to employees if/when they are required.

Additionally, as employees join the company, change positions within the company, or leave the company, administrators simply update their roles via a hierarchical abstraction layer, assigning or removing them from the appropriate role(s).

RBAC Limitations

Role Explosion

As RBAC is limited to defining access permissions by role, an ever-increasing number of users requires an exponentially increasing number of roles to accommodate various permissions combinations. Additionally, because each user often requires entirely unique access rights, one user may be assigned several roles, creating a "one size fits all" solution that often results in too much (or too little) access, making the enterprise vulnerable to an exponential rise in roles versus users.

Conflicting Data Causes Confusion

In short, various roles assigned to a given user could contain conflicting data. For example, one user could be assigned a role allowing them to create a purchase order and another allowing them to approve it. This obviously poses a significant business risk if not managed properly, as the user could create a purchase order payable to themselves and then approve the payment. In a dynamic authorization system that enforces corporate policies, this scenario would not be possible.

Management Nightmares

With the exponential growth of both users and roles, role engineering is an increasingly difficult task. Administrators must constantly be aware of changes to users and to roles and ensure role assignment combinations are current, accurate and do not conflict with other roles a user is assigned. Any attempts to audit or certify such an environment are also challenging. Conversely, ABAC not only supports dynamic authorization, but also the effective auditing of user permissions.

No Context

RBAC is static in nature, meaning it is unable to model policies that depend on contextual details including time of day, location, relationship between users, etc. In short, RBAC has no way to delineate relationships between users or to use that information to make policy decisions. This is by design, as RBAC was originally designed to answer one question: "What access does a user have based on their assigned role(s)?"

Expanding user populations (partners, consumers, regulators, auditors, etc.) and multi-role users, not to mention rapidly escalating application and database complexity requires authorization based on a finer level of information. Authorization must go beyond answering, "What is a user's role(s)?" to also answer:

- "Who or what is that user related to?"
- "What resources should this user have access to?"
- "What can this user do with this data?"
- "Where is data being accessed from?"
- "At what time?"

These relationships are key to defining safe and secure access control in an ever-changing environment. By defining the context between users and attributes, robust policies can be defined specifying that though a user may create purchase orders and may approve purchase orders, this user is only able to approve purchase orders unique from the ones they created.

Knowing a user's role is no longer enough to ensure safe and secure access control. Organizations need context and the relationship information between the various entities involved in the system. Organizations need ABAC.

The future of access control: Evolving RBAC to ABAC

Despite limitations, there's no need to reboot and start over. Users are most often the central point around which access control is based.

Those users' roles play an integral part in managing safe and secure access control across an enterprise. RBAC provides a solid foundation upon which the future can be built.

That said, it is integral for organizations to know the context surrounding those users and be able to express complex relational policies at a fine-grained level.

Modern data sharing and collaboration scenarios must provide access to the right user, at the right time, in the right location, and by meeting regulatory compliance.

By evolving RBAC with ABAC, administrators provide well-rounded access control that builds on RBAC's strengths with roles while harnessing ABAC's context for today's requirements as well as for future needs.

RBAC already has some of the functionality necessary to provide safe and secure access control in an evolving environment, stemming from a user's role.

Roles are roles

Roles are still – and will always be – an integral part of a successful access control strategy, however, to scale for the future, those roles must be extended using attributes and policies derived through ABAC. ABAC enables an enterprise to extend existing roles using attributes and policies. By adding context, authorization decisions can be made based not only on a user's role, but also by considering who or what that user is related to, what that user needs access to, where that user needs access from, when that user needs access, and how that user is accessing the requested information.

But policies are the game changer

ABAC does this by using policies built on individual attributes using natural language. For example, a policy may be written as follows: "Doctors can view medical records of any patient in their department and update any patient record directly assigned to them during working hours and from an approved device." By creating a policy that is easy to understand and that includes context around a user and what they should have access to, access control becomes far more robust.

This functionality expands the scope of RBAC significantly. Hundreds of overloaded roles are no longer required and administrators can add, remove, or reorganize departments and other attributes without rewriting policy. In addition, ABAC enables business initiatives not previously available using RBAC alone. Specifically, ABAC can be used for:

- Delegation
- Contextual awareness
- Collaboration; and
- End-to-end user experience enhancement

Axiomatics helps you transition from RBAC to ABAC

Axiomatics Authorization Platform is designed to help organizations evolve RBAC using ABAC for fine-grained, contextually-aware access control that can scale with an organization across applications, databases and APIs.

We offer the most complete platform available for enterprise-wide roll out of ABAC and to begin the transition from a role-based system to one that addresses access context through attributes and policies.

With our dynamic authorization platform, enterprises can roll access to applications under a single point of policy-based management, enabling scalability, visibility and control.

Once authorization has transitioned from RBAC to ABAC, organizations can also improve information asset protection at the data layer. The Axiomatics Data Access Filter uses the same attribute-based approach to protect content. It dynamically masks or filters data directly in the database, only allowing user or application access to the data they've been approved to touch, in accordance with business policies.

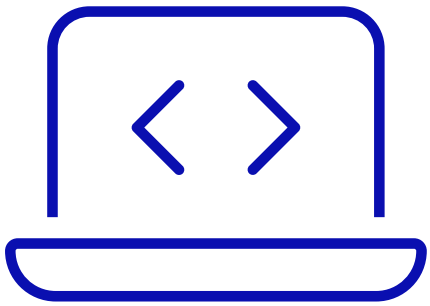
The Axiomatics platform easily integrates with new or existing applications and API projects to employ fine-grained authorization that ensures data is protected when needed and shared only when the right circumstances are met.

No matter your existing infrastructure, the Axiomatics platform is compatible with a variety of tools supporting RBAC, including IAM solutions, API gateways, federated identity solutions and more.

Take the next steps

Learn how how a security vendor can help secure your access control while allowing you to focus on your core business initiatives.

Meet with our solution experts for a demo of our Axiomatics Authorization Management Platform and discuss how our approach can save your organization time and money.



Stay connected and informed

Get the latest insights, announcements, and assets from our thought leaders and customer success team:

- Blog articles
- Press releases and announcements
- Resources, solution briefs, and tools
- Join us on LinkedIn
- Subscribe to our Linkedin Newsletter
- Subscribe to our YouTube channel

Axiomatics - a Leonardo Company is the originator and leading provider of runtime, fine-grained authorization delivered with attribute-based access control (ABAC) for applications, data, APIs, and microservices.

The company enables enterprises to effectively and efficiently connect Axiomatics' award-winning authorization platform to critical security implementations, such as Zero Trust or identity-first security. The world's largest enterprises and government agencies continually depend on Axiomatics' award-winning authorization platform to share sensitive, valuable, and regulated digital assets – but only to authorized users and in the right context.

Follow us on LinkedIn: https://linkedin.com/company/axiomatics

Join us on YouTube: https://youtube.com/@axiomatics

Learn more or request a demo of our solution:

axiomatics.com

info@axiomatics.com

US Office: +1 (312) 374-3443 | Europe Office: +46 8 51 510 240