EINPRESSWIRE

Four Role-Based Access Control (RBAC) Limitations and How to Fix Them

Axiomatics identified four limitations to an RBAC-centric security approach and suggests enterprises evolve to an ABAC model.

CHICAGO, IL, USA, September 23, 2021 /EINPresswire.com/ -- In the advent of a “work anywhere, anytime” environment, enterprises face a rapid expansion of diverse users alongside an influx of applications, devices, APIs and microservices. Additionally, the amount of data created and consumed by these users, devices and services continues to explode, creating extraordinary security and compliance challenges.

> “By evolving RBAC with ABAC, administrators provide well-rounded access control that builds on RBAC while harnessing ABAC’s context to address today’s requirements and future needs.”
>
> *Dr. Srijith Nair, Chief Security Officer, Axiomatics*

Formalized by NIST in 1992, role-based access control (RBAC) has long been a standard approach to managing access to critical assets and data, particularly for enterprises managing more than 500 employees. However, to ensure secure access, enterprises can no longer afford to define authorization policies based solely on a user’s role.

Axiomatics, the originator and leading provider of runtime dynamic authorization solutions, has identified four limitations to an RBAC-centric security approach and suggests enterprises evolve their RBAC model to an attribute-based access control (ABAC) model. ABAC is recognized by NIST as a model that can “improve information sharing within organizations and between organizations while maintaining control of that information,” and is at the core of modern security approaches, including Zero Trust.

Four RBAC Limitations:
1)Role Explosion: RBAC is limited to defining access permissions by role, however, as each user often requires entirely unique access rights, one user may be assigned several roles, creating a ‘one size fits all’ solution that can result in too much (or too little) access. This also makes enterprises vulnerable to an exponential rise in roles versus users.

2)Toxic Combinations: Various roles assigned to a given user could contain conflicting data (i.e., someone is assigned a role allowing them to create a purchase order and another allowing them to approve the same order). This poses a significant business risk if not managed properly.

3) Management Nightmares: With an exponential growth of both users and roles, role engineering is a challenge. Administrators must constantly be aware of changes to both users and roles to ensure role assignment combinations are current, accurate and do not conflict with other roles a user is assigned.

4) No Context: RBAC was designed to be static, meaning it does not model policies that depend on contextual details including time of day, location, relationship between users, relationship between users and resources, etc. It was designed to address user access based on assigned role. Expanding user populations (including partners, consumers, regulators and auditors) and multi-role users requires authorization based on a finer level of information.

ABAC is the future of access control

- Roles are still – and always will be – an integral part of a successful access control strategy, but to address critical enterprise needs (complex regulatory requirements, scalability, remote workforces) these roles must be extended using attributes and policies derived through ABAC.

- ABAC adds context, ensuring authorization decisions can be made 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.

- The Axiomatics Application Authorization Platform is 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 the pressing need for policies be governed by fine-grain access controls available through attributes. Leveraging this platform, enterprises can roll access to applications under a single point of policy-based management, enabling scalability, visibility and control.

Supporting Quote:

- Dr. Srijith Nair, Chief Strategy Officer, Axiomatics

"Whether it's Zero Trust or another approach, more enterprises understand that a modern workforce requires a modern approach to security, which means evolving beyond RBAC. 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 while harnessing ABAC's context to address today's requirements and future needs."

Supporting Resources:

- White paper: Evolving RBAC to ABAC (https://www.axiomatics.com/resources/evolving-from-rbac-to-next-generation-abac)
- Solution info: Axiomatics Application Authorization Platform (https://www.axiomatics.com/platform/)

- Fact sheet: Five ways to get started with Dynamic Authorization (https://www.axiomatics.com/resources/5-ways-to-get-started-with-dynamic-authorization/)

Kelly O'Dwyer-Manuel
Axiomatics
+1 705-868-5114
kelly.odm@axiomatics.com
Visit us on social media:
Twitter
LinkedIn

This press release can be viewed online at: https://www.einpresswire.com/article/552093838

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.