NIST SPECIAL PUBLICATION 1800-3A

Attribute Based Access Control

Volume A:
Executive Summary

Bill Fisher
National Cybersecurity Center of Excellence
Information Technology Laboratory

Norm Brickman
Prescott Burden
Santos Jha
Brian Johnson
Andrew Keller
Ted Kolovos
Sudhi Umarji
Sarah Weeks
The MITRE Corporation
McLean, VA

September 2017

SECOND DRAFT

This publication is available free of charge from:
https://nccoe.nist.gov/projects/building-blocks/attribute-based-access-control

National Institute of Standards and Technology
U.S. Department of Commerce

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Executive Summary

Traditionally, granting or revoking access to information technology (IT) systems or other networked assets requires an administrator to manually enter information into a database—perhaps within several systems. This method is inefficient and does not scale as organizations grow, merge, or reorganize. Further, this approach may not be best for preserving privacy and security: all users of a database have access to all its information, or administrators must limit access by constructing groups with specific permissions.

Attribute based access control (ABAC) is an advanced method for managing access rights for people and systems connecting to networks and assets. Its dynamic capabilities offer greater efficiency, flexibility, scalability, and security than traditional access control methods, without burdening administrators or users.

Despite ABAC's advantages and federal guidance that comprehensively defines ABAC and the considerations for enterprise deployment (NIST Special Publication 800-162), adoption has been slow. In response, the National Cybersecurity Center of Excellence (NCCoE), part of the National Institute of Standards and Technology (NIST), developed an example of an advanced access control system. Our ABAC solution can manage access to networked resources more securely and efficiently, and with greater granularity that traditional access management. It enables the appropriate permissions and limitations for the same information system for each user based on individual attributes, and allows for permissions to multiple systems to be managed by a single platform, without a heavy administrative burden.

Our approach uses commercially available products that can be included alongside your current products in your existing infrastructure.

This example solution is packaged as a "How To" guide that demonstrates implementation of standards-based cybersecurity technologies in the real world. It can save organizations research and proof-of-concept costs for mitigating risk through the use of context for access decisions.

CHALLENGE

Enterprises face the continual challenge of providing access control mechanisms for subjects requesting access to corporate resources (e.g., applications, networks, systems, and data). The growth and distributed nature of enterprise resources, increasing diversity in users, credentials, and access needs, as well as the need to share information among stakeholders that are not managed directly by the enterprise, has given rise to the demand for an access control system that enables fine-grained access decisions based on a range of users, resources, and environmental conditions.

Consider a patient submitting a health insurance claim. A claims examiner needs to know just billing and diagnostic codes and a few pieces of demographic data in order to permit reimbursement. Interacting with the same system, the patient's doctor needs to verify that the diagnosis and referral information is for the correct patient, but does not need to see payment or address information. The patient needs access to the claim's status, while the patient's employer only needs to see the number of claims submitted by the employee. The insurance company provides a single service, claims processing, but each user of the service has different access needs.

An advanced method of access management would increase security and efficiency by seamlessly limiting some users' views to more granular data. It would enable the appropriate permissions and limitations for the same information system for each user based on individual attributes, and allow for permissions to multiple systems to be managed by a single platform, without a heavy administrative burden.

SOLUTION

This document details our approach in developing a standards-based ABAC solution. Through discussions with identity and access management (IdAM) experts and collaborating technology partners, the NCCoE developed a set of security characteristics required to meet the IdAM risks facing today's enterprises. The NCCoE mapped security characteristics to standards and best practices from NIST and other standards organizations, then used products from our technology partners as modules in an end-to-end example solution that mitigates IdAM risks.

While the NCCoE used a suite of commercial products to address this challenge, this guide does not endorse these particular products, nor does it guarantee compliance with any regulatory initiatives. Your organization's information security experts should identify the products that will best integrate with your existing tools and IT system infrastructure. Your organization can adopt this solution or one that adheres to these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing parts of a solution.

RISKS

Access control systems implement a process for defining security policy and regulating access to resources such that only authorized entities are granted access according to that policy. They are fundamental to mitigating the risk of unauthorized access from malicious external users and insider threats, as well as acts of misfeasance. In the absence of a robust access control system, enterprises struggle to control and audit access to their most sensitive data and risk the loss or exposure of critical assets, loss of trust in employees and from customers, and harm to brand reputation.

As technology pervades all business processes, access control systems must support increasing diversity in users, credentials, and access needs, including digital identities from external security domains. This increases the overhead associated with managing access control systems and introduces increased risk of unauthorized access as organizational policies escalate in complexity.

BENEFITS

Our example implementation:

- allows products and capabilities to be adopted on a component-by-component basis, or as a whole
- supports organizations with a diverse set of users and access needs, reducing the risks of "privilege creep" (a user obtains access levels beyond those needed), and creating efficiencies in the provisioning of accesses

- reduces the number of identities managed by the enterprise, thereby reducing costs associated with those management activities
- enables a wider range of risk-mitigation decisions by allowing organizations to define attribute-based policy on subjects and objects, and by using a variety of environmental decisions
- supports business collaboration by allowing the enterprise to accept federated identities and eliminating the need to pre-provision access for identities being federated
- supports the centralization of auditing and access policy management, creating efficiencies of policy management and reducing the complexity of regulatory compliance

SHARE YOUR FEEDBACK

You can view or download the guide at https://nccoe.nist.gov/projects/building-blocks/attribute-based-access-control. Help the NCCoE make this guide better by sharing your thoughts with us as you read the guide. If you adopt this solution for your own organization, please share your experience and advice with us. We recognize that technical solutions alone will not fully enable the benefits of our solution, so we encourage organizations to share lessons learned and best practices for transforming the processes associated with implementing this guide. To provide comments or to learn more by arranging a demonstration of this example implementation, contact the NCCoE at abac-nccoe@nist.gov.

TECHNOLOGY PARTNERS/COLLABORATORS

Organizations participating in this project submitted their capabilities in response to an open call in the Federal Register for all sources of relevant security capabilities from academia and industry (vendors and integrators). The following respondents with relevant capabilities or product components (identified as "Technology Partners/Collaborators" herein) signed a Cooperative Research and Development Agreement to collaborate with NIST in a consortium to build this example solution.

CISCO Microsoft NEXTLABS Ping Identity RSA Symantec

Certain commercial entities, equipment, products, or materials may be identified by name or company logo or other insignia in order to acknowledge their participation in this collaboration or to describe an experimental procedure or concept adequately. Such identification is not intended to imply special status or relationship with NIST or recommendation or endorsement by NIST or NCCoE; neither is it intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.

The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity challenges. Through this collaboration, the NCCoE applies standards and best practices to develop modular, easily adaptable example cybersecurity solutions using commercially available technology.

LEARN MORE
Visit https://nccoe.nist.gov
nccoe@nist.gov
301-975-0200