Attribute Based Access Control

Executive Summary

- 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. In fact, Gartner recently predicted that "by 2020, 70% of enterprises will use attribute-based access control … as the dominant mechanism to protect critical assets, up from less than 5% today."[1]
- Despite federal guidance that comprehensively defines ABAC and the considerations for enterprise deployment[2], adoption of ABAC has been slow.
- The National Cybersecurity Center of Excellence (NCCoE) addressed this challenge by developing an example ABAC reference model using commercial products that can be included alongside those in your existing infrastructure.
- The ABAC solution provided by this "How to" guide incorporates relevant security characteristics, standards, and best practices from the National Institute of Standards and Technology (NIST) and other organizations.
- The guide demonstrates the 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.

THE CHALLENGE

Traditionally, granting or revoking access to 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 doesn't 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.

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 doesn't need to see payment or address information. The patient needs access to the clam'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.

1.Market Trends: Cloud-Based Security Services Market, Worldwide, 2014, https://www.gartner.com/doc/2607617 [accessed August 21, 2015].
2.National Institute of Standards and Technology Special Publication (SP) 800-162, *Guide to Attribute Based Access Control (ABAC) Definition and Considerations*

THE SOLUTION

The NCCoE, part of NIST, demonstrated an advanced method, attribute based access control (ABAC), that uses granular attributes such as title, division, certifications and training—rather than a person's role—to authorize an individual's access. Access to an organization's network or assets can be made based on information that is available to systems across an organization, or among organizations, about a person, the action she wants to execute, and the resource she wants to access. An orthopedist responding to a mass casualty event in a neighboring state can quickly gain access to a hospital's patient records and radiology and pharmacy ordering systems, and only to those systems, based on authentication of her credentials and attributes such as employee status, medical specialization, and certifications. Additional visiting orthopedists are immediately granted the same permissions based on the same rules.

ABAC offers efficiencies and enhanced security in non-emergency scenarios, too. ABAC can provide separation of duties to help guard against fraud: a car insurance claims adjuster, for example, can be permitted to enter data about damage and generate a check, but only his supervisor can electronically sign the check. In addition to authorizing people, ABAC can be used to efficiently manage access among networked tools, devices, and systems that request access to corporate resources like applications, networks, systems, and data.

The NIST Cybersecurity Practice Guide *Attribute Based Access Control* shows how commercially available technologies can meet your organization's needs to make access decisions for a diverse set of people and things, including those seeking access from external organizations. The complete guide is available at http://nccoe.nist.gov.

Approach

In our lab at the NCCoE, we simulated a typical electronic file library with a diverse set of resources from different divisions in an organization. Different files have different security levels.

We demonstrated how detailed attributes can be assigned to users and networked resources, and how fine-grained environmental considerations like time of day or IP address can provide context for access decisions, allowing for more informed, finely-tuned access decisions that increase security.

The guide:

- maps security characteristics to guidance and best practices from NIST and other standards organizations
- provides
  - a detailed example solution with capabilities that address security controls
  - instructions for implementers and security engineers, including examples of all the necessary components and their installation, configuration, and integration
- uses products that are readily available and interoperable with existing information technology (IT) infrastructure and investments
- is suitable for organizations of all sizes

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

BENEFITS

Our example solution:

- 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, offering efficiencies in provisioning access
- reduces the number of identities managed by the enterprise, thereby reducing costs
- enables a wider range of risk-mitigation decisions by allowing organizations to define attribute-based policies for users and networked devices that include factors such as environment and time of day
- supports collaboration among organizations by allowing an enterprise to accept identities authorized by other enterprises, eliminating the need to pre-provision access for those identities
- 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 get the guide at http://nccoe.nist.gov and help improve it by contributing feedback. As you review and adopt this solution for your own organization, we ask you and your colleagues to share your experience and advice with us. We recognize that technical solutions alone will not fully enable the benefits of ABAC, so we encourage organizations to share lessons learned and best practices for transforming the business processes associated with implementing ABAC.

- email abac-nccoe@nist.gov
- participate in our forums at https://nccoe.nist.gov/forums/attribute-based-access-control

Or learn more by arranging a demonstration of this reference solution by contacting us at abac-nccoe@nist.gov

TECHNOLOGY PARTNERS

The NCCoE designed and implemented this project with its National Cybersecurity Excellence Partnership (NCEP) partners.

The National Cybersecurity Center of Excellence at the National Institute of Standards and Technology addresses businesses' most pressing cybersecurity problems with practical, standards-based example solutions using commercially available technologies. As the U.S. national lab for cybersecurity, the NCCoE seeks problems that are applicable to whole sectors, or across sectors. The center's work results in publicly available NIST Cybersecurity Practice Guides that provide modular, open, end-to-end reference designs.

LEARN MORE
Visit http://nccoe.nist.gov

ARRANGE A DEMONSTRATION
nccoe@nist.gov
240-314-6800