BUILDING BLOCK

ATTRIBUTE BASED ACCESS CONTROL

Draft
February 21, 2014
abac-nccoe@nist.gov

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

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

The National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology addresses businesses' most pressing cybersecurity problems with practical, standards-based solutions using commercially available technologies. The NCCoE collaborates with industry, academic and government experts to build modular, open, end-to-end reference designs that are broadly applicable and repeatable.

This document describes a problem that is relevant to many industry sectors. NCCoE cybersecurity experts will address this challenge through collaboration with a community of interest including vendors of cybersecurity solutions. The solution will become an NCCoE "building block": an approach that can be incorporated into multiple use cases. The solution proposed by this effort will not be the only one available in the fast-paced cybersecurity technology market. If you would like to propose an alternative architecture or know of products that might be applicable to this challenge, please contact us at abac-nccoe@nist.gov.

1. DESCRIPTION

Enterprises have long recognized the need to validate the identity (authentication) of subjects[1] interacting with their data, systems and networks. Once subjects are identified, strong access control (authorization) mechanisms are required to ensure that resources are only available to an authorized subject. To enable a wide array of automated security decisions within and between enterprises, the identity and access control field has moved from individual access control lists, to centralized identity stores (databases), to role based access control, and now attribute based access control (ABAC).

Goal

ABAC enables a rich set of access control policies that allow for fine-grain authentication and access control decisions based on information about a subject (such as title, division, certifications and training), rather than pre-provisioned enterprise roles. In conjunction with a service that enables a range of identity attributes to be accessed or verified, ABAC implementations enable a federated identity management environment, which makes it possible to share IT resources across multiple enterprises. When access control decisions can be this granular, enterprise risks—including insider threats, loss of personally identifiable information and fraud—are reduced.

This building block will use commercially available technologies to demonstrate an enterprise-class ABAC implementation that enables federated identity management between multiple

[1] Typically the *subject* we're referring to is a user or a device. For consistency with other literature on ABAC, we use the term *subject* throughout this document.

enterprises through the use of an attributed exchange service. These technologies enhance the granularity of access control policies by increasing the range of possible attributes available when making automated access control decisions in an enterprise. The ABAC technology solution stack demonstrated in this document is designed to be modular, allowing corporations flexibility in their implementations based on their current network infrastructures.

Background

The NIST Computer Security Division describes attribute based access control as an evolution from basic access control lists and more complex role based access. Attribute based access control "is a highly flexible method for providing access based on the evaluation of attributes."

They continue:

> "ABAC is a logical access control model that is distinguishable because it controls access to objects by evaluating rules against the attributes of the entities' (subject and object) actions and the environment relevant to a request. … In its most basic form, ABAC relies upon the evaluation of attributes of the subject, attributes of the object, environment conditions, and a formal relationship or access control rule defining the allowable operations for subject-object attribute and environment condition combinations. All ABAC solutions contain these basic core capabilities that evaluate attributes and environment conditions, and enforce rules or relationships between those attributes and environment conditions." …
>
> "The rules or policies that can be implemented in an ABAC model are limited only to the degree imposed by the computational language. This flexibility enables the greatest breadth of subjects to access the greatest breadth of objects without specifying individual relationships between each subject and each object." …
>
> "Provisioning ABAC describes attributes to subjects and objects governed by an access control rule set that specifies what operations can take place. This capability enables object owners or administrators to apply access control policy without prior knowledge of the specific subject and for an unlimited number of subjects that might require access. As new subjects join the organization, rules and objects do not need to be modified. As long as the subject is assigned the attributes necessary for access to the required objects, no modifications to existing rules or object attributes are required."[2]

[2] http://csrc.nist.gov/projects/abac/
NIST Special Publication 800-162, Draft: *Guide to Attribute Based Access Control (ABAC) Definition and Considerations*, http://csrc.nist.gov/publications/drafts/800-162/sp800_162_draft.pdf

2. SCENARIOS

While the security mechanisms employed in this building block could address a wide array of challenges across various enterprises, this building block will initially focus on a reference design that demonstrates an ABAC deployment for two first responder scenarios:

Example Scenario 1 – Dynamic Certificate Provisioning

A natural disaster causes a power outage for a major electric power distributor, Utility A. Line crews are dispatched from unaffected utilities in neighboring regions. Individual members of the line crews present credentials from their home utility, Utility B. Utilities A and B have both previously signed an agreement with a third party allowing for the validation of employee credentials and sharing of attributes.

Utility A provides the line crew with a device (such as a laptop or tablet) that connects into its enterprise network and provides access to the ticketing system and other key information necessary to repair outages. To log into the device, and into the corporate network of Utility A, an individual from the line crew presents his Utility B credentials. This could be a subject name and password, physical token, or biometric. After the subject is authenticated, attributes such as employee status, certifications, specialties, training and safety record are authorized for exchange by the lineman and shared by an attribute provider (AP) with Utility A's identity and access management system (IDAM). Once received, the IDAM system makes decisions about assignments and access control. Utility A adds a corresponding temporary entry in its centralized identity management store and provisions a certificate for any device that the line crew may use in the field, sometimes without network connectivity.

Example Scenario 2 – Extended Federation

A hospital faces a crisis requiring the influx of temporary additional personnel (nurses, doctors, administrators, etc.). A doctor who works in a different region deploys to assist the hospital. In similar fashion to the first scenario, both the hospital and the doctor's home practice are subscribers of a third party service, which allows for the validation of member credentials and sharing of other attributes. Attributes such as employee status, medical specialization and certifications are authorized for release by the doctor and shared with the hospital through the third party service. Because the hospital is operating in an "always on" network-connected environment, an account is not created. When the doctor presents her home credentials to any hospital device or service, the service queries the third party network to authenticate her credentials and authorize access for that session.

3. SECURITY CHARACTERISTICS

To address these two scenarios, this project will use commercially available technology to demonstrate characteristics that are considered attributes of a secure solution. Each characteristic has one or more examples of security capabilities that can meet the intent of the

characteristic. The below list of characteristics and corresponding capabilities is not exhaustive. Furthermore, capabilities are defined to provide context for the characteristics and are not meant to be prescriptive. In implementing these characteristics, the build will focus on use of technologies that provide the greatest level of configurability and flexibility in achieving the below characteristics.

Security characteristics	**Example capabilities**
audit and monitoring	• logs all access requests, access decisions, attributes used and subject identities • provides canned reports, queries and analysis
data protection	• encrypts the transmission of attributes traveling between enterprises and across the attribute exchange service • encrypts data for all attribute and policy stores • protects attribute values used within policy decision logic
attribute integrity verification	• provides the relying party (RP) with assurance that the attributes received are from the intended source and have not been modified • supports strong authentication between the RP and attribute provider (AP)
policy enforcement	• ensures appropriate action is taken for failed authentication and authorization • reduces (or eliminates) false positive/false negative results
identity lifecycle management	• provisions and de-provisions accounts • manages: o subject attribute o object attribute o environment attribute o federated identity and attribute o policy, e.g., certificate expiration
attribute validation	• periodically revalidates each attribute in use
privacy protection	• identity providers should not know the relying party in any given transaction • prevents the attribute exchange service from tracking subject across multiple transactions • eavesdroppers cannot decode messages or determine that two authentication sessions involved the same subject
multi-factor authentication	• support requirements for multi-factor authentication to achieve degrees of authentication confidence using a combination of factors such as physical and logical tokens and biometric factors

4. APPROACH

This building block focuses on the demonstration of ABAC technologies and how they can be integrated to address challenges across a wide-array of business sectors. The initial focus is on the creation and demonstration of a service that supports identity and attribute verification and exchange between attribute providers, identity providers and relying parties.

It should be noted that this is an initial approach and that the building block process is intended to be iterative. As technologies and capabilities evolve, the initial technology stack of this building block may be augmented with additional functions.

Stage 0 – Creation and Demonstration of an Attribute Exchange Service

- set up RP, AP and identity provider (IdP)
- set up a server with a commercially available or open source operating system
- install a target identity management software for authentication and authorization that includes a database to serve as an identity store (RP)
- connect the identity management software to one or more target applications that require authentication and access control
- set up a server running a corporate identity store to serve as a repository for identity and attribute information and that has exposed application programming interfaces for federated connections (IdP, AP)
- connect the RP server to an attribute exchange (AE) service
- connect the IdP and AP server to the AE service

Stage 1 – Test RP Subject Authentication Based on Attribute Assertions

- set policy in the RP or AE for acceptable sources of identity information
- create a test account in the IdP
- ensure that the RP can validate a subject by connecting through the attribute exchange service to authenticate using subject name and password
- test dynamic certificate provisioning

Stage 2 – Test Authorization of RP Resources Based on Attribute Assertions from an AP

- validate policy decision and policy enforcement logic
- create and test multiple environmental contexts
- stand up audit server and log analysis engine

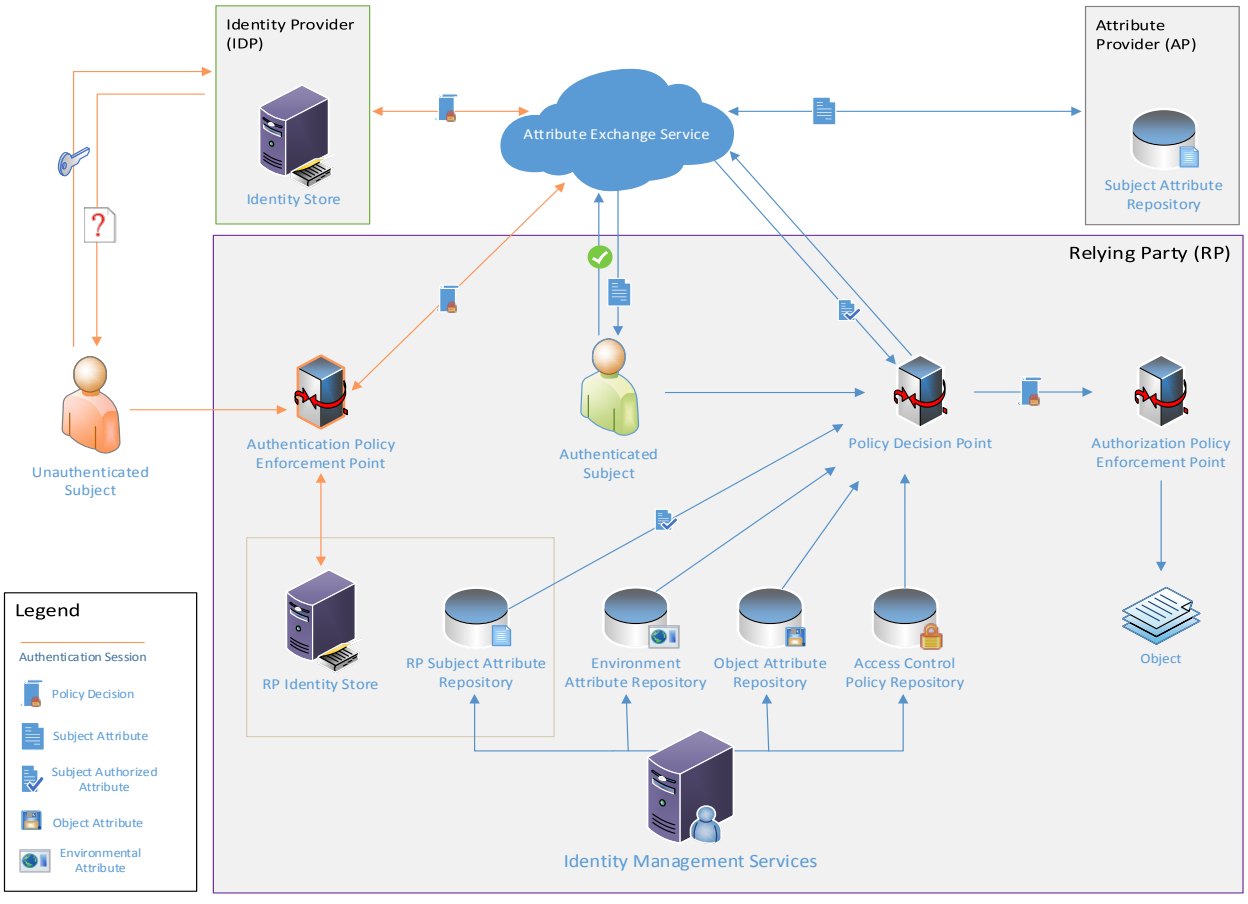
Stage 3 – Add Multifactor Authentication Components to RP Authentication of Subjects

- implement tiered multifactor authentication based on risk analysis (including data sensitivity, environmental attributes, user attributes, etc.)

5. REFERENCES

- NIST Special Publication 800-162: Guide to Attribute Based Access Control (ABAC) Definition and Considerations
- NIST Special Publication 800-63 rev. 2: Electronic Authentication Guideline
- NIST Policy Machine: Features, Architectures, and Specifications
- OIX: Attribute Exchange Trust Framework Specification
- ICAM Backend Attribute Exchange ver. 2
- Organization for the Advancement of Structured Information Standards (OASIS) Security Assertion Markup Language (SAML) v2.0 Standard
- Organization for the Advancement of Structured Information Standards (OASIS) eXtensible Access Control Markup Language (XACML) v2.0
- RFC 6749 - The OAuth 2.0 Authorization Framework
- OpenID Authentication 2.0 Final Specification

6. HIGH-LEVEL ARCHITECTURE



7. COMPONENT LIST

- commercially available operating system
- identity management software that includes functions like: account provisioning, de-provisioning, multi-factor authentication, group assignment, role assignment, user self service and federation
- attribute exchange service
- commercially available database (policy database, identity store, subject attribute repository, object attribute repository)
- access control mechanism (policy decision point, policy enforcement point, context handler)
- cryptographic means to protect subject privacy during interactions between RPs, IDPs, APs, and the attribute exchange service. Privacy mechanisms must protect subject behavior from being tracked (i.e. which RPs the subject interacts with) and protect the confidentiality of subject attributes
- standard method for the exchange of authentication and authorization data between parties