NIST Special Publication 800-162
Attribute Based Access Control Definition and Considerations

Vincent Hu
Adam Schnitzer
Ken Sandlin

NIST Special Publication 800-162
Attribute Based Access Control Definition and Considerations

Background

Motivated by increasing importance of ABAC, recognizing there was no available guidance for entire USG.

Work started in 2012 by group members from NIST, NSA, and contractors: MITRE, and Booz Allen Hamilton.

Has gone through 27 internal and public reviewers.

Now in the stage of updating by public review, plan to have final version available in September 2013.

It's a start of a serial of future works related to ABAC, next coming is the ABAC formal models.

NIST Special Publication 800-162
Attribute Based Access Control Definition and Considerations

Purpose

Provides Federal agencies with a definition of Attribute Based Access Control (ABAC) and considerations for using ABAC to improve information sharing while maintaining control of that information.

Scope

The functional components of ABAC, as well as a set of considerations for employing ABAC within a large enterprise.

NIST Special Publication 800-162
Attribute Based Access Control Definition and Considerations

Contents

Terminology and basic understanding of ABAC; Provide readers with an overview of the current state of logical access control, a working definition of ABAC, and an explanation of core and enterprise ABAC concepts.

ABAC enterprise employment considerations during the initiation, acquisition/development, implementation/assessment, and operations and maintenance phases.

ABAC examples.

Notes

The terminology used in the SP is not meant to be authoritative, merely consistent within the confines of the document itself. Where possible, terminology that is used elsewhere within NIST publications and across the Federal Government was adopted to maintain consistency.

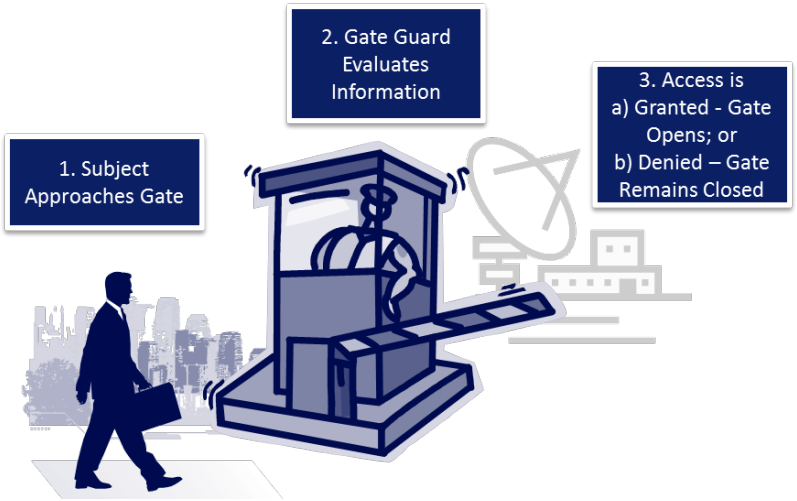
Extends the fundamental concepts of policy, models, and properties of Access Control (AC) systems in

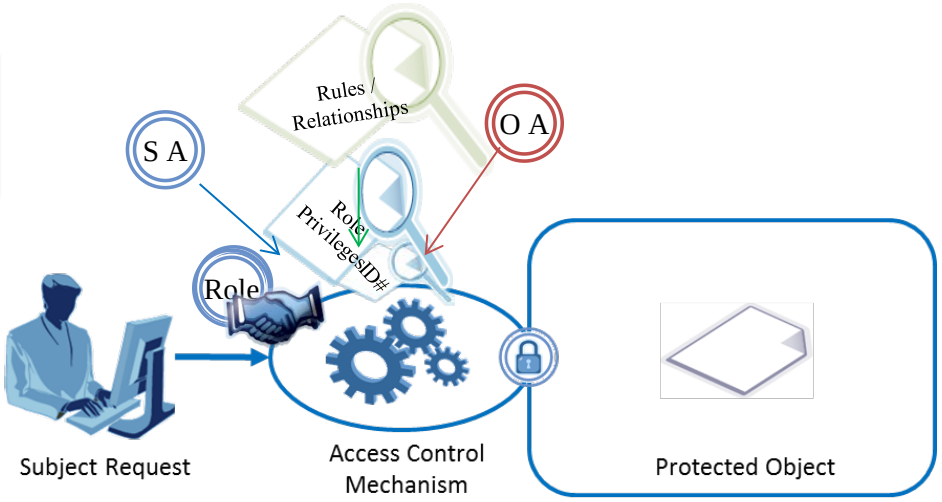
- NIST IR 7316, Assessment of Access Control Systems
- NIST IR 7874, Guidelines for Access Control System Evaluation Metrics
- NIST IR 7665, Proceedings of the Privilege Management Workshop
- NIST IR 7657, A Report on the Privilege (Access) Management Workshop

Authentication is not the same as access control or authorization. Authentication is the act of verifying that the subject performing an operation is actually who they say they are. Authentication method is not pertinent to ABAC.

NIST Special Publication 800-162
Attribute Based Access Control Definition and Considerations

Introduction to Logical Access Control





MAC/DAC*

IBAC/ACL's

RBAC

ABAC

1960's **1970's** **1980's** **1990's** **2000's** **Now**

Definition of ABAC

Attribute Based Access Control (ABAC): A logical access control methodology where authorization to perform a set of operations is determined by evaluating attributes associated with the subject, object, requested operations, and, in some cases, environment conditions against policy, rules, or relationships that describe the allowable operations for a given set of attributes.

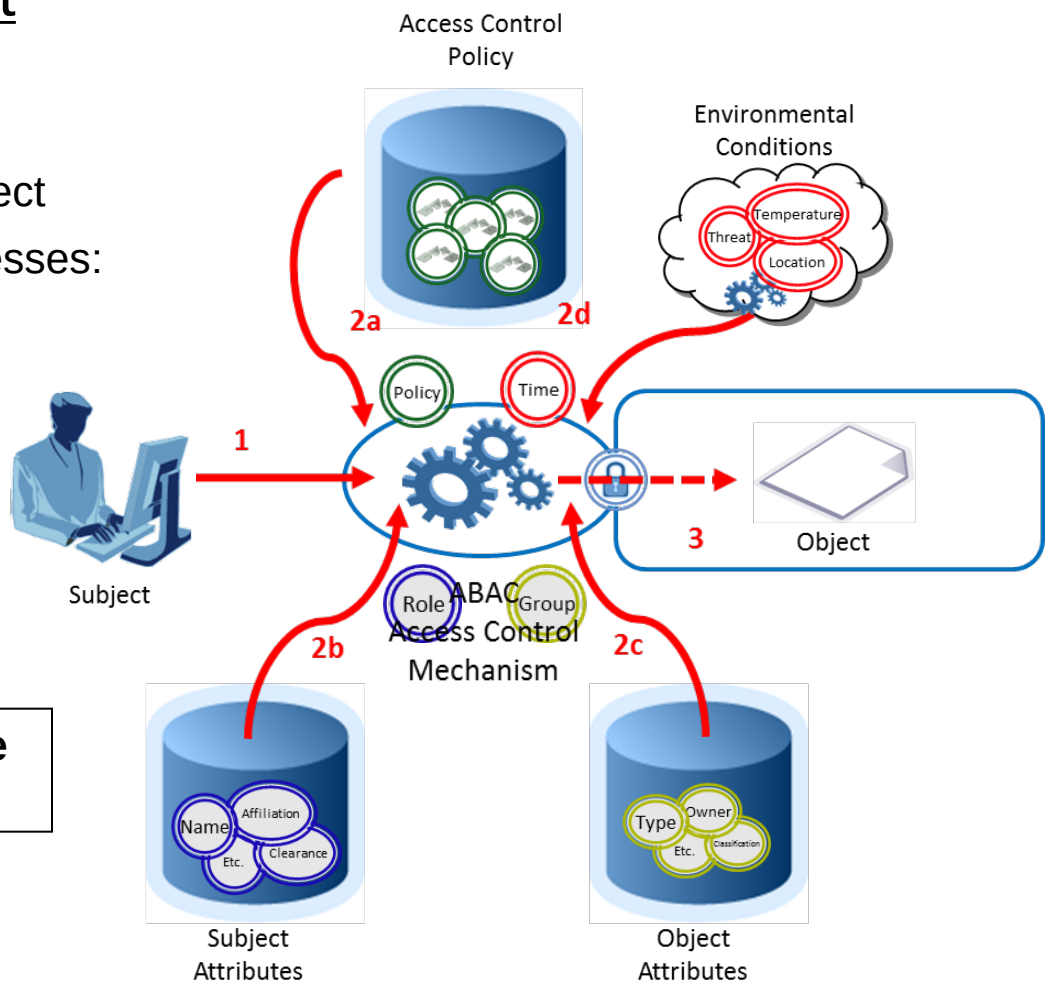
- **Attributes** are characteristics that define specific aspects of the subject, object, environment conditions, and/or requested actions that are predefined and pre-assigned by an authority.
- A **subject** is an active entity (generally an individual, process, or device) that causes information to flow among objects or changes the system state. It can be the user, requestor, or mechanism acting on behalf of the user or requestor.
- An **object** is a passive information system-related entity containing or receiving information. It can be the resource or requested entity, as well as anything upon which an operation may be performed by a subject including data, applications, services, devices, and networks.
- **Environmental conditions** are dynamic factors, independent of subject and object, that may be used as attributes at decision time to influence an access decision. Examples of environment attributes include time, location, threat level, temperature, etc.
- An **operation** is the execution of a function at the request of a subject upon an object. Operations include read, write, edit, delete, author, copy, execute, and modify.
- **Policy** is the formal representation of rules or relationships that define the set of allowable operations a subject may perform upon an object in permitted environment conditions.

NIST Special Publication 800-162
Attribute Based Access Control Definition and Considerations

Basic ABAC Concept

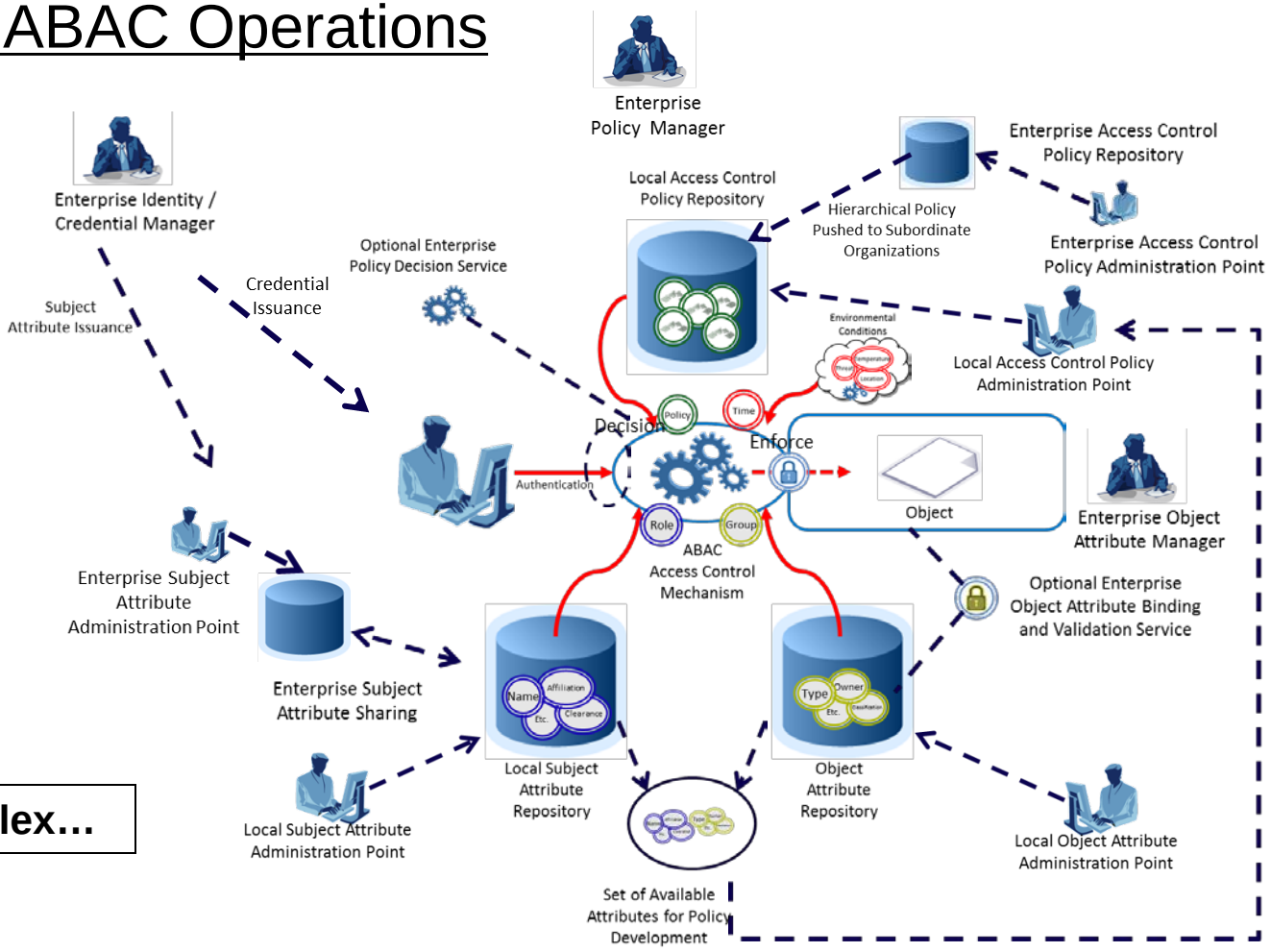
1. Subject Requests Access to Object
2. Access Control Mechanism Assesses:
   a) Rules
   b) Subject Attributes
   c) Object Attributes
   d) Environmental Conditions
3. Subject is Given Access to Object if Authorized and Denied Access if Not Authorized

What happens when we scale this up to an Enterprise?



NIST Special Publication 800-162
Attribute Based Access Control Definition and Considerations

Enterprise ABAC Operations



This gets complex…

NIST Special Publication 800-162
Attribute Based Access Control Definition and Considerations

Why ABAC?

- **Requires no advance knowledge of requestors.**
- **An individual's attributes can be correlated from multiple sources to create a unified identity.**
- **Highly adaptable to changing needs; efficient for agencies where individuals come and go frequently.**
- **Policy, attributes, and access decisions can be managed centrally for a large enterprise.**
- **Allows for fine-grained access decisions and accountability to address unique challenges like the insider threat.**

However…

- **Lengthy implementation time due to the need to correlate information and attributes from multiple sources for all potential users.**
- **Reliant on authoritative identity/entitlement data – difficulty managing attribute conflicts between source systems.**
- **Not natively supported by common operating systems.**
- **Not appropriate for all environments (i.e., those with significant changes in risk level).**

List derived from: FICAM Roadmap and Implementation Guidance; V2.0; December 2, 2011

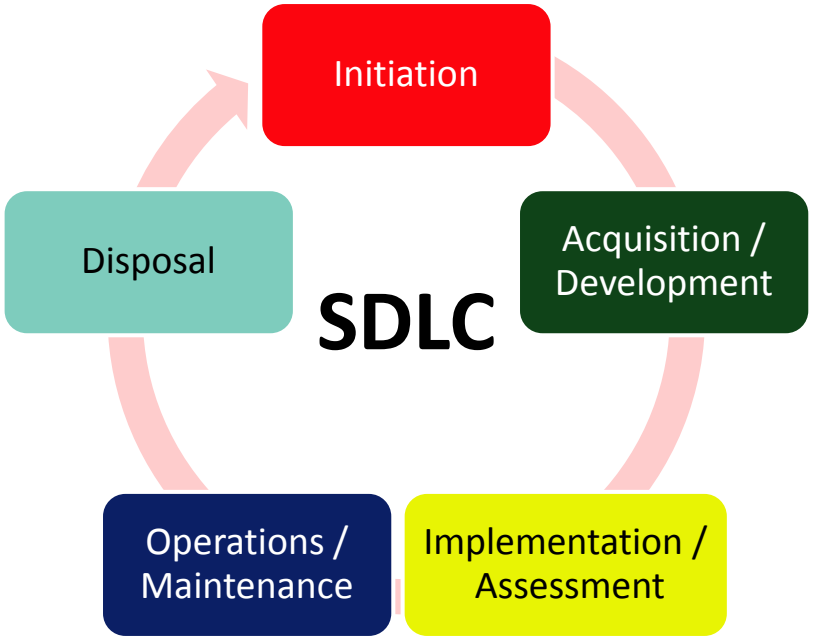
NIST Special Publication 800-162
Attribute Based Access Control Definition and Considerations

ABAC Enterprise Employment Considerations

This section attempts to consolidate available guidelines based on the state of the technology to date and lessons learned through multiple attempts within the Federal Government to deploy ABAC capabilities throughout a large enterprise.

The guidelines are presented according to the phases of the NIST System Development Life Cycle (SDLC). (Disposal Phase not covered in the SP).

Enterprise section contains considerations for ABAC project teams.



NIST Special Publication 800-162
Attribute Based Access Control Definition and Considerations

Considerations During the Initiation Phase

Focused on high-level business and operational requirements as well as the enterprise architecture.

Building the Business Case for Deploying ABAC Capabilities

As with any major system deployment, the deployment of enterprise ABAC capabilities should be preceded by significant requirements evaluation, trade studies, and planning activities to include the determination of whether ABAC is the right type of access control capability needed and feasible given the application portfolio.

Scalability, Feasibility, and Performance Requirements

Enterprise ABAC requires a complex level of interaction between ABAC components. Often these components are distributed throughout the enterprise.

Developing Operational Requirements and Architecture

Identify objects, rules or policies, processes, subject and object attributes .

NIST Special Publication 800-162
Attribute Based Access Control Definition and Considerations

Considerations during Acquisition/Development Phase

Focused on how the system is designed, purchased, programmed, developed, or otherwise constructed.

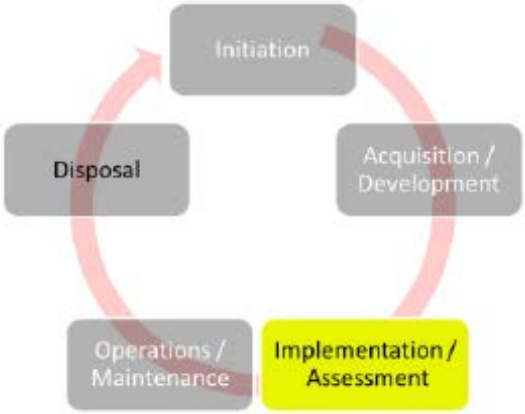
Business Process Generation and Deployment Preparation
Includes documentation of rules of who can interact with protected resources, and how. Policy customization considerations.

System Development and Solution Acquisition Considerations
Standardization and interoperability considerations, identity management integration, attribute considerations.

Considerations for Advanced Enterprise ABAC Capabilities
Environmental (or Contextual) attribute considerations.

Considerations during Implementation/Assessment Phase

Focused on optimizing performance and ensuring security features work as expected.



Attribute caching
Considerations for network bandwidth challenged environments, including caching security tradeoffs

Attribute Minimization
Considerations to improve performance and simplify security by minimizing the number of attributes used in authorization decisions

Interface Specification Availability
Considerations for interface, interaction, and precondition requirements

Considerations during Operations/Maintenance Phase

Focused on operating, enhancing, and/or modifying the system.

Availability of Quality Data
Considerations for maintaining high availability for quality attribute values.

Distribution of Timely and Accurate Subject Attributes
Additional considerations for special situation attribute caching (in disconnected or austere environments).

SP Public Comments and Replies

The SP is focused on core ABAC functional components as well as a set of considerations for employing ABAC within a large enterprise, details and extended topics we haven't focused on will be considered in the future documents including:

- **Attribute engineering and management**
- **Integration with identity management**
- **Federation and situation awareness applications**
- **Policy management**
- **NPL translation to DP**

Other AC models were used to explain the evolution of AC models, each has its own advantages and limitations, therefore, no in-depth comparison with ABAC.

The SP assumes subjects are bound to trusted identities or identity providers.

SP Public Comments and Replies (continue)

The SP assumes "user" and "subject" are synonymous. We realized that it is necessary to distinguish them for formal ABAC models, which are used for example to simulate other none ABAC models.

The SP is based on published government documents, terms and concepts from none government "standards" (e.g. XACML) or implementations of ABAC are used for references.

Some figures in the SP might contain elements, which were not discussed in the text. The reason is that instead of illustrating process between functions, they are used for presenting scenarios or examples.

SP Public Comments and Replies (continue)

Updates will be made

- Define and explain “environment conditions”, which is also an important attribute in ABAC.
- Executive Summary will be downsized to contain main points only.
- Clarify relations between AC models.
- Fix Consistency of figures.
- Reorganize section 2.2 and section 2.3, to improve the flow of the document.
- Add more references for related discussion if available.
- Fix/remove terms for their redundancy.
- Add in-depth information provided from reviewers.

Questions?

vhu@nist.gov