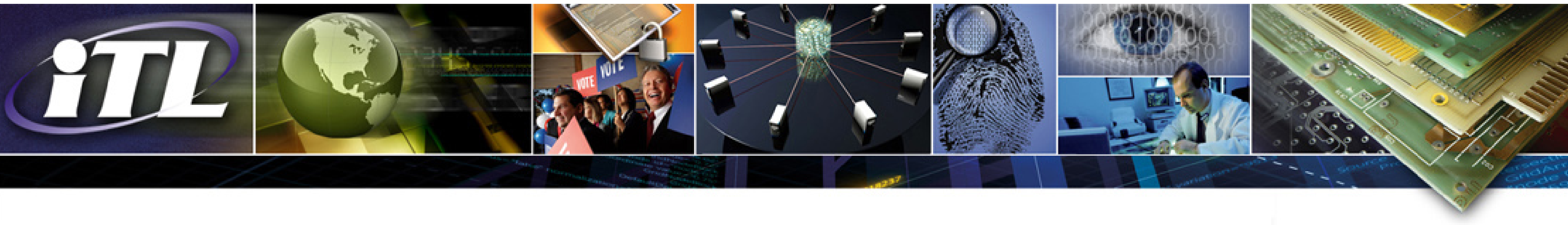


ITL BULLETIN FOR MARCH 2014

ATTRIBUTE BASED ACCESS CONTROL (ABAC) DEFINITION AND CONSIDERATIONS

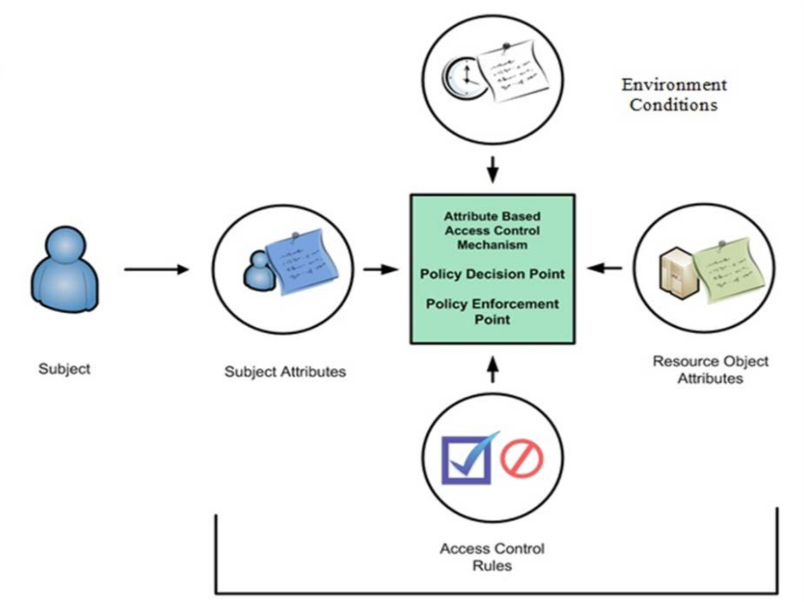
Vincent Hu, Editor
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
U.S. Department of Commerce

The concept of Attribute Based Access Control (ABAC) has existed for many years. It represents a point in the space of logical access control that includes access control lists, role-based access control, and the ABAC method for providing access based on the evaluation of attributes. Traditionally, access control has been based on the identity of a user requesting execution of a capability to perform an operation (e.g., read) on an object (e.g., a file), either directly, or through predefined attribute types such as roles or groups assigned to that user. Practitioners have noted that this approach to access control is often cumbersome to manage given the need to associate capabilities directly to users or their roles or groups. In addition, the requester qualifiers of identity, groups, and roles are often insufficient in the expression of real-world access control policies. An alternative is to grant or deny user requests based on arbitrary attributes of the user and arbitrary attributes of the object, and environment conditions that may be globally recognized and more relevant to the policies at hand. This approach is often referred to as ABAC.

In December 2011, the Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Plan v2.0 [FEDCIO2] called out ABAC as a recommended access control model for promoting information sharing between diverse and disparate organizations. In December 2012, the National Strategy for Information Sharing and Safeguarding included a Priority Objective that the federal government should extend and implement the FICAM Roadmap across federal networks in all security domains. The U.S. General Services Administration (GSA) and the Federal CIO Council are designated leads for this objective, and are preparing an implementation plan.

Over the past decade, vendors have begun implementing ABAC-like features in their security management and network operating system products, without general agreement as to what constitutes an appropriate set of ABAC features. Due to a lack of consensus on ABAC features, users cannot accurately assess the benefits and challenges associated with ABAC. Despite the clear guidance to implement the FICAM Roadmap and contextual (risk adaptive) role or attribute based access control, a comprehensive effort to formally define and guide the implementation of ABAC within the federal government is provided by NIST Special Publication (SP) 800-162, *Guide to Attribute Based Access Control (ABAC) Definition and Considerations*. This document serves a two-fold purpose. First, it provides federal agencies with a definition of ABAC and a description of the functional components of ABAC. Second, it provides planning, design, implementation, and operational considerations for employing ABAC within an enterprise with the goal of improving information sharing while maintaining control of that information. This document should not be interpreted as an analysis of alternatives between ABAC and other access-control capabilities, as it focuses on the challenges of implementing ABAC rather than on balancing the cost and effectiveness of other capabilities versus ABAC.

ABAC is a logical access control model that is distinguishable because it controls access to objects by evaluating rules against the attributes of entities (subject and object), operations, and the environment relevant to a request (see figure below). ABAC systems are capable of enforcing both Discretionary Access Control (DAC) and Mandatory Access Control (MAC) concepts. ABAC enables precise access control, which allows for a higher number of discrete inputs into an access control decision, providing a larger set of possible combinations of those variables to reflect a larger and more definitive set of possible rules to express policies.



When an access request is made, Attributes and Access Control Rules are evaluated by the Attribute Based Access Control Mechanism to provide an access control decision. In ABAC's basic form, the Access Control Mechanism contains both a Policy Decision Point, and a Policy Enforcement Point.

The access control policies that can be implemented in ABAC are limited only by the computational language and the richness of the available attributes. 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. For example, a subject is assigned a set of subject attributes upon employment (e.g., Nancy Smith is a Nurse Practitioner in the Cardiology Department). An object is assigned its object attributes upon creation (e.g., a folder with Medical Records of Heart Patients).

Objects may receive their attributes either directly from the creator or as a result of automated scanning tools. The administrator or owner of an object creates an access control rule using attributes of subjects and objects to govern the set of allowable capabilities (e.g., all Nurse Practitioners in the Cardiology Department can View the Medical Records of Heart Patients). Under ABAC, access decisions can change between requests by simply changing attribute values, without the need to change the subject/object relationships defining underlying rule sets. This provides a more dynamic access control management capability and limits long-term maintenance requirements of object protections.

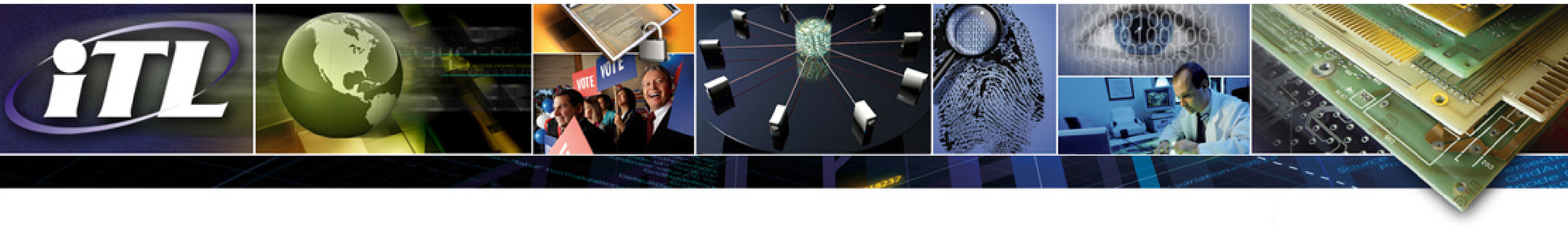
Further, ABAC enables object owners or administrators to apply access control policy without prior knowledge of the specific subject and for an unlimited number of subjects that might require access. As new subjects join the organization, rules and objects do not need to be modified. As long as the subject is assigned the attributes necessary for access to the required objects (e.g., all Nurse Practitioners in the Cardiology Department are assigned those attributes), no modifications to existing rules or object attributes are required. This benefit is often referred to as accommodating the external (unanticipated) user and is one of the primary benefits of employing ABAC.

When deployed across an enterprise for the purposes of increasing information sharing among diverse organizations, ABAC implementations can become complex—supported by the existence of an attribute management infrastructure, machine-enforceable policies, and an array of functions that support access decisions and policy enforcement.

In addition to the basic policy, attribute, and access control mechanism requirements, the enterprise must support management functions for enterprise policy development and distribution, enterprise identity and subject attributes, subject attribute sharing, enterprise object attributes, authentication, and access control mechanism deployment and distribution. The development and deployment of these capabilities requires the careful consideration of a number of factors that will influence the design, security, and interoperability of an enterprise ABAC solution. These factors can be summarized around a set of activities:

- Establish the Business Case for ABAC Implementation;
- Understand the Operational Requirements and Overall Enterprise Architecture;
- Establish or Refine Business Processes to Support ABAC;
- Develop and Acquire an Interoperable Set of Capabilities; and
- Operate with Efficiency.

NIST SP 800-162 serves as a first step to help planners, architects, managers, and implementers fulfill the information sharing and protection requirements of the U.S. federal government, through the employment of ABAC.



ITL Bulletin Publisher: Elizabeth B. Lennon
Information Technology Laboratory
National Institute of Standards and Technology
elizabeth.lennon@nist.gov

Disclaimer: Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by NIST nor does it imply that the products mentioned are necessarily the best available for the purpose.