INTRODUCTION TO ATTRIBUTE BASED ACCESS CONTROL

Harry Katzan, Jr., Webster University, USA

ABSTRACT

A major problem in the operational control of enterprise information systems is to promote information sharing while maintaining control over the integrity and privacy of information. Many organizations employ identity management and authentication for access, and then partition the application domain so that a separate access facility is required for each system. Simple access control lists are used for access control, so flexibility and information sharing is cumbersome and inefficient, often leading to a state where design objectives are easily diminished. With Attribute Based Access Control (ABAC), a highly effective means of information sharing, based on the use of attributes, can be achieved, while enhancing efficiency and efficacy among enterprise agencies. This paper provides an introduction to this important concept as it applies to federal and non-federal organizational structures.

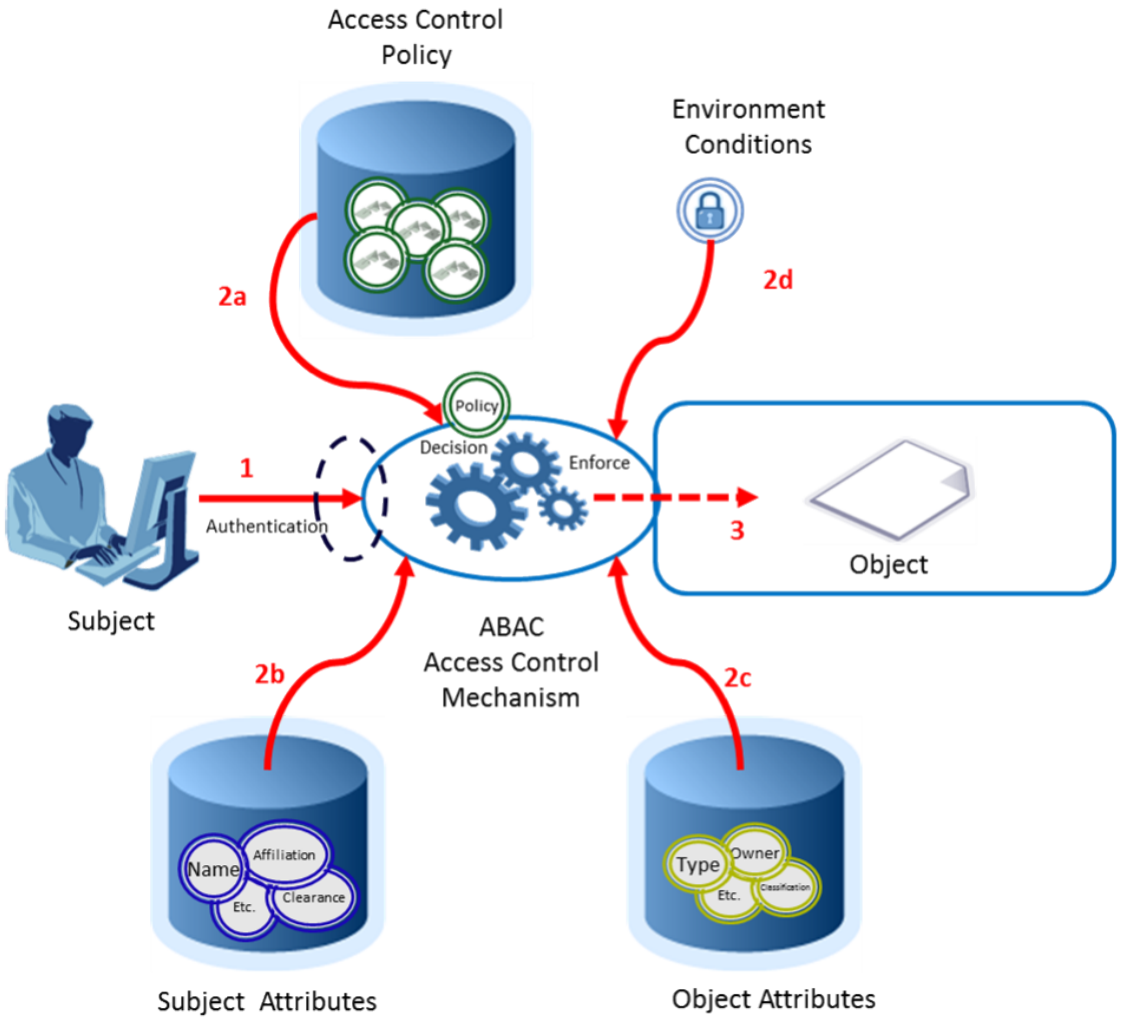
THE ACCESS CONTROL LANDSCAPE

This section gives a brief overview of access control in information systems and an executive summary of Attribute Based Access Control (ABAC). A government document (NIST 800-162) on that subject is out for review and the rationale underlying this paper is to promote that effort. Cybersecurity is a major subject in the modern world, and effective access control is an important aspect of security countermeasures.

In most information systems, access control is based on identity management. The user provides identity credentials to the system, and based on that identity, that person is permitted to perform certain well-defined operations. Control is maintained by access control lists, often implemented as a matrix that implicitly specifies the level of authorization between subjects and objects. Mandatory and discretionary controls are established on a system-wide basis and are typically the responsibility of the owners of the various objects. Access control management is the cumbersome process of adding and revoking privileges as organizational structures change.

With Attribute Based Access Control (ABAC), access control management relies on the use of subject attributes, object attributes, and control rules that define the allowable operations determined by the relationships between subject-object combinations. For example, an analyst in the supply-chain group would be assigned a set of subject attributes upon employment. Similarly, the database administrator would assign a set of supplier attributes when the supply-chain database is populated. Finally, the owner of the supplier database creates an appropriate set of access control rules that governs the permissible operations.

It follows that attributes of subjects and objects and the values of those attributes can be modified during the lifecycle of a project without having to change a subject/object relationship whenever a relevant event occurs. Access behavior can be adjusted dynamically adding to the flexibility and efficiency of the system. Thus, administrators can achieve policy decisions without requiring specific attention to changes of subjects, objects, and other environmental conditions. This scenario is depicted in Figure 1.



1. Subject Requests Access to Object
2. Access Control Mechanism Assesses a) Rules, b) Subject Attributes, c) Object Attributes, and d) Environment Conditions to Determine Authorization
3. Subject is Given Access to Object if Authorized and Denied Access if Not authorized

Figure 1. ABAC Access Control Scenario. (Source: NIST Special Publication 800-162, *Guide to Attribute Based Access Control (ABAC) Definition and Consideration (Draft),* 54 pages, (April 2013), p. viii)

The implementation of ABAC is complex, because the underlying requirements are complicated. An enterprise deploying ABAC must develop attribute management facilities, policy rules, and access control methods, taking into consideration principles that are infrequently addressed in traditional systems design. Factors necessary for development are encompassed by the following design principles:[1]

1. Establish the business case for ABAC implementation;

[1] NIST Special Publication 800-162, *Guide to Attribute Based Access Control (ABAC) Definition and Consideration (Draft)*, p. ix-x)

2. Understand the operational requirement and overall enterprise architecture;
3. Establish or refine business processes to support ABAC;
4. Develop and acquire an interoperable set of capabilities; and
5. Operate with efficiency.

The principles apply to the Federal Government in particular and all business, educational, and governmental organizations in general. The National Institute for Science and Technology has prepared a draft of ABAC for Federal agencies; it is currently out for public review. The concepts apply equally well to non-federal organizations, such as business organizations and educational institutions. Accordingly, public awareness is required for effective review by concerned parties.

NECESSARY TERMINOLOGY

Several terms are implicitly understood in the security and control domains but are usually left undefined, some of which that are relevant to this paper are: object, subject, user, attribute, identity, credential, authentication, authorization, privileges, policy, policy decision point, and policy enforcement point. There are others, of course, but this list gives the main terms.

A resource that has value to the organization and is regarded by the object's owner as something that should be protected is referred to as an **object,** such as information, a computational facility, or a network. The person or non-person entity that requests access to the object is known as the **subject**. There are differing opinions of exactly what constitutes a subject, but it is safe to think of the subject as a **user**. Information about a subject – but not what a subject knows – is that subject's **attributes**, or more properly "subject attributes." A subject attribute could be a person's role in an organization. Subject attributes that uniquely distinguish one subject from another is known as an **identity**. Attributes applied to an object are known as **object attributes**. An object attribute may be inherent in the object or it may be a designation that someone has assigned to that object with the objective of restricting access.

A subset of a subject's attributes used to verify a subject is called a **credential**, and is used to permit access to a system or resource. **Authentication** is the process of verifying that a subject is who he or she says they are and does not necessarily give permission to do anything, except in elementary cases. **Authorization** gives the subject **privilege** to access a resource, based on a rule set, termed a **policy**. Policies are customarily digital, implying that their use is intended to be used by a computational resource as part of a total system configuration. A **policy decision point (PDP)** is the mechanism within access control where a decision is made to assign **privileges** to perform certain tasks in the application domain, and a **policy enforcement point (PEP)** serves as the point of enforcement for permission or denial to access services.

CONCEPTUAL MODEL OF ATTRIBUTE BASED ACCESS CONTROL

The basic purpose of access control is to protect objects, such as data, services, applications, and networks, from unauthorized use, taken to include discovery, reading, creating, modifying, deleting and otherwise performing operations involving those objects. The owner of an object in this domain is motivated to protect it for reasons that are not always explicitly known. A subject without the proper authority and need to access the object is customarily denied access. Access is therefore restricted to subjects with acceptable credentials and other necessary attributes – from the owner's perspective. Accordingly, the owner of an object has the need to establish a policy for the protection of objects based on the operations to be performed, by what entity, and for what reason – i.e., the operational context. Historically, methods of access control based on identity, higher authority (mandatory-access control – MAC), the owner's discretion (discretionary-access control – DAC), and the subject's function in the organization (role-based access – RBAC) have been used with reasonable success. The biggest problem

has been that privilege management has been inefficient and inflexible thereby limiting the inherent value of the objects protected. It is no exaggeration that most access-control facilities have been based primarily on identity management methods. In fact, when a subject from one organization requires access to an object from another organization, a supplementary account has to be created, as suggested by Figure 2. In the terms of the ABAC document, "… authenticated access to resource objects outside of the subject's originating organization would require the subject's identity to be pre-provisioned in the target organization and pre-populated on an access list." [***ibid***, p.6]

Clearly, what is needed is to enable access decisions to be made without knowledge of the object by the subject or knowledge of the subject by the object-owner. Explicit authorization is avoided through the use of object and subject attributes, as long as the attributes are consistently administered by the separate organizations.

DEFINITION OF ABAC AND CORE CAPABILITIES

The authors of NIST 800-162 provide the following high-level 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.*

A conceptual diagram of ABAC is given in Figure 1, displayed earlier.

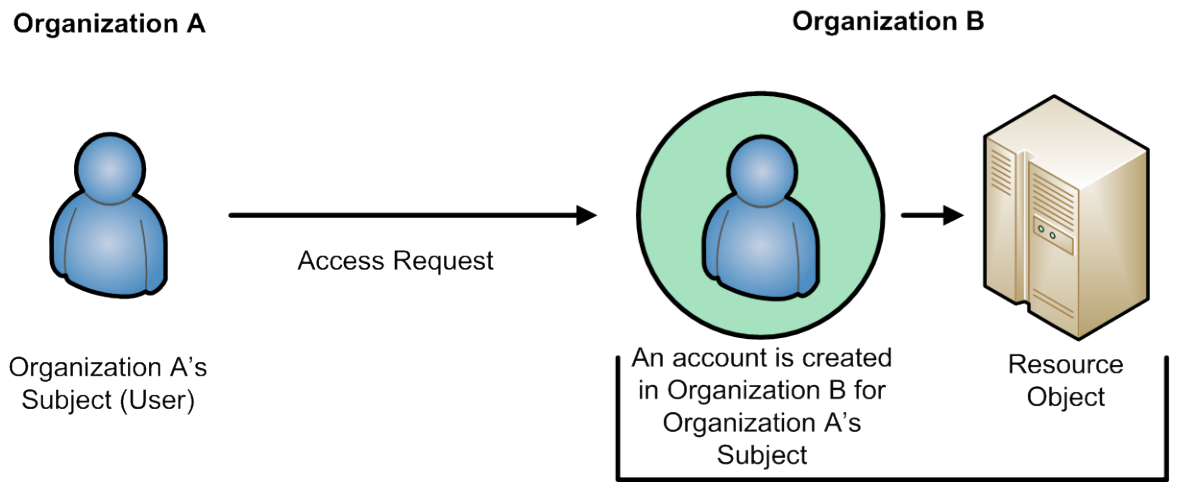


Figure 2. Multi-Organizational Access. (Source: NIST 800-162, op. cit., p. 7)

ABAC relies on the assignment and management of attributes and the evaluation of those attributes by an access-control mechanism. The relationships are reflected in the set of access-control rules, representing the access policy, and used by the policy decision and enforcement points. Contextual attributes are added to the control set and referred to as environmental conditions. Moreover, the attributes can be grouped in various ways, such as descriptive, operational, and so forth. Combinations of attributes, for example, subject-object, form the basis for access rules.

Subjects must be assigned subject attributes, such as name, role, organizational affiliation, and functional capability. Other attributes could include country status, nationality, and security clearance. Thus, a subject authority is required to assign and manage subject attributes. Similarly, object attributes must be identified and controlled. Operations that can be performed with or on an object are also of concern and must be supported by at least one subject-object rule. Subjects and objects can be grouped into categories, such that attributes are assigned individually or according to an enclosing category.

Subject attributes are assigned individually or by an organizational affiliation. In general, an administrator is needed for this function, and that person necessarily requires a software facility specifically designed for this purpose. The management of subject attribute is a major part of an Access Control Mechanism (ACM), and an access control language that will satisfy the demands of interoperability is required. An analogous facility for object and environmental attributes is also required, so the ACM has the capability to enforce the rule sets for the Policy Decision and Policy Enforcement Points. The ACM process is summarized in Figure 3.

OPERATION AND MANAGEMENT OF ABAC

In one form or another, most aspects of ABAC have been implemented in specific systems for particular purposes. The objectives of the ABAC document are to propagate the concept across organizational systems for diverse objects and subjects under varying conditions. Clearly, each object under consideration must be assigned attributes, and each user must be assigned the requisite attributes. These are up-front tasks, as well as policy determination. During operation, the ACM must be established to provide the required functionality.

SUMMARY

Access control is an important component of a total cybersecurity program. A single insecure system can undermine the security of an otherwise secure operating environment. If a common conceptual methodology is adopted between organizations, together with packaged support facilities, then the overall level of risk can be improved.

ACKNOWLEDGEMENT

The major reference for this paper is the following document, available as a download from the National Institute of Standards and Technology:

NIST Special Publication 800-162
Guide to Attribute Based Access Control (ABAC) Definition and Considerations (Draft)
National Institute of Standards and Technology
U.S. Department of Commerce
Authors: Vincent C. Hu, David Ferraiolo, Rick Kuhn, Arthur R. Friedman, Alan J. Lang, Margaret M. Cogdell, Adam Schnitzer, Kenneth Sandlin, Robert Miller, Karen Scarfone

The report is extensive and supplies the technical and theoretical basis of Access Based Access Control.

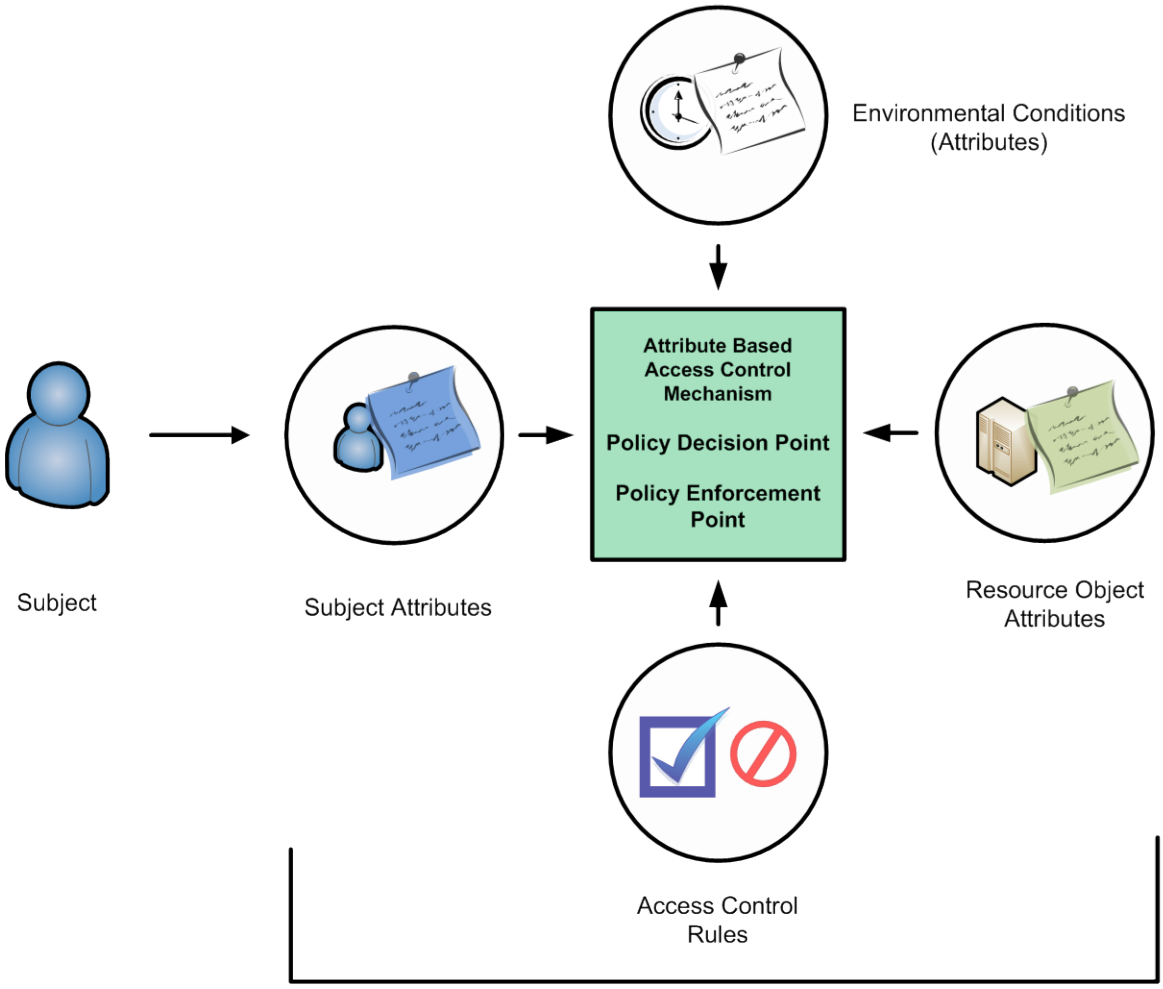


Figure 3. ABAC Operation. (Source: NIST 800-162, op. cit., p. 10)

REFERENCES

[1] NIST Special Publication 800-12: *An Introduction of Computer Security, The NIST Handbook.*

[2] NIST Special Publication 800-53r4: *Security and Privacy Controls for Federal Information Systems and Organizations,* April 2012, Joint Task Force Transformation Initiative.

[3] NIST Special Publication 800-63-2: *Electronic Authentication Guideline,* February 2013, Authors: W. Burr, D. Dodson, E. Newton, R. Perlner, W. Polk, S. Gupta, E. Nabbus.

[4] NIST Special Publication 800-100: *Information Security Handbook: A Guide for Managers,* October 2006, Authors: P. Bowen, J. Hash, M. Wilson.

[5] NIST Special Publication 800-162: *Guide to Attribute Based Access Control (ABAC): Definition and Considerations (Draft*), April 2012, Authors: V. Hu, D. Ferraiolo, R. Kuhn, A. Friedman, A. Lang, M. Cogdell, A. Schnitzer, K. Sandlin, R. Miller, K. Scarfone.

[6] Katzan, H., Essentials of Cybersecurity, *2012 Southeastern INFORMS Conference Proceedings,* October 2012, p.523-527.

[7] Katzan, H., *Privacy, Identity, and Cloud Computing,* New York: iUniverse, Inc., 2010.

[8] Shoemaker, D. and W. Conklin, *Cybersecurity: The Essential Body of Knowledge,* Boston: Course Technology, 2012.

[9] Whitman, M. and H. Mattord, *Principles of Information Security (4e),* Boston: Course Technology, 2012.