NISTIR 7657

A Report on the Privilege (Access) Management Workshop

NIST/NSA
Privilege Management Conference Collaboration Team

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

NIST IR 7657

A Report on the Privilege (Access) Management Workshop

NIST/NSA
Privilege (Access) Management Workshop Collaboration Team

March 2010

U. S. Department of Commerce
Gary Locke, Secretary

National Institute of Standards and Technology
Patrick D. Gallagher, Director

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

Preface

This document is based on the discussions and conclusions of the Privilege (Access) Management Workshop held on 1-3 September 2009 at the Gaithersburg, Maryland, facilities of the National Institute of Standards and Technology (NIST), sponsored by NIST and the National Security Agency (NSA). This document includes additional material resulting from in-scope comments made by workshop participants and the public during the review periods for this document. An overview of the workshop is available in the published proceedings of the workshop. [NISTIR 7665 - Proceedings of the Privilege Management Workshop, September 1-3, 2009]

Participants at the workshop generally agreed that access management is the umbrella under which to consider privilege management. At the same time, many workshop participants felt that the term "privilege management" was not needed at all, since all aspects of the discussions held in the various tracks could be described without use of the term. Yet, the term "privilege management" was being used in several contexts, with differing meanings, and there was a strong desire to clarify its meaning. Contributing to the reason to use the term was the definition of "privilege management" that appeared in the draft document[1] produced by the Identity, Credential, and Access Management (ICAM) Subcommittee just months earlier [FICAM-09 - Federal Identity, Credential, and Access Management.] That proposed definition seemed to be closely related to the area being examined at the workshop. Also, the view of privilege management expressed in this document generally aligns with the architectural and service framework for privilege management presented in the FICAM document. Both the FICAM document and this report treat privilege management as a subset of access management.

The results of the workshop, as described in this report, show that the central topic of the workshop turned out to be attribute and policy management. Whether attribute and policy management should be called "privilege management" is an open question at this point. Looking at the definitions of "privilege management" in the FICAM document and in this report, it appears that they address different levels of concern in the area of identity, credential, and access management. The FICAM definition appears to view privilege management as a governance and business process, while this report's definition focuses on computer-based management of attributes and policies. As the reader can easily discover, it is possible to substitute "attribute and policy management" for "privilege management" throughout this report without damage to the content. The question arises, then, as to whether a definition of "privilege management" as found in the FICAM extends to the area of access management covered in this report or should be limited to the governance and business process level. It remains for future deliberations, such as a follow-on workshop, to examine the issues involved and resolve such questions.

The discussion in this document is not comprehensive, dealing principally with those ideas, points, gaps, and concerns derived from presentations and discussions at the workshop. In particular, it does not address assurance issues associated with the topics covered because the workshop's scope specifically excluded assurance considerations, in order to achieve a useful first step in exploring privilege management. We believe, however, that this report provides a good basis for further exploration of the topics and issues and, in particular, for a follow-on workshop.

---

[1] *Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance*

Table of Contents

List of Figures and Tables

National Institute of Standards and Technology Interagency Report on the Privilege (Access) Management Workshop

Introduction

This National Institute of Standards and Technology (NIST) Interagency Report (NISTIR) on the Privilege (Access) Management Workshop is organized as follows:

- A Context for Thinking About Privilege Management: This section describes the full scope of enterprise-level access control and management, showing how privilege management fits under the umbrella of access management.
- Definitions and Standards: This section examines the need for definitions and standards, with a focus on eXtensible Access Control Markup Language (XACML).
- Access Control Methods: This section identifies current, distinguishable access control methods and focuses on the attribute-based access control method.
- Policies and Requirements: This section presents considerations about digital policy management.
- Research Agenda: This section identifies issues in several topical areas of privilege management, including policy and attribute management, standards, and several others.
- Conclusion: This section gives a brief summary of the document and provides a list of recommendations.
- Bibliography: This section provides references and other recommended reading.
- Annex A: Authorization and Attributes Glossary
- Annex B: A Survey of Access Control
- Annex C: Authoritative Attribute Source and Attribute Service Guidelines
- Annex D: Advanced Capabilities for Privilege Management
- Annex E: The Policy Machine
- Annex F: An Alternate View

A Context for Thinking About Privilege Management

This section describes enterprise-level access control and privilege management, both of which come under the umbrella of access management. At the enterprise level, access management encompasses all the practices, policies, procedures, data, metadata, and technical and administrative mechanisms used to manage access to the resources of an organization. Access management includes access control and privilege management as well as other related capabilities such as identity management. Considering things at the enterprise level ensures that all elements of privilege management are included so that the needs of all organizations, large and small, can be met.

Privilege management at the enterprise level is usefully viewed in relation to enterprise-level access control. *Access control* ensures that resources are made available only to authorized users, programs, processes, or systems by reference to rules of access that are defined by attributes and policies. *Privilege management* is the definition and management of attributes and policies that are used to decide whether a user's request for access to some resource should be granted. In this context, resources can be both computer-based entities (files, Web pages, and so on) and physical entities (buildings, safes, and so on), and users requesting access to resources can be people, processes running on a computer, or devices. Please note that this description of privilege management is a working definition for the purposes of this report. Any definition, to be an approved, agreed-upon term, must go through a formal review process by bodies such as the Authorization and Attribute Services Committee (AASC) and NIST. As noted in the Preface of this report, work needs to be done to formalize any terminology beyond that being proposed by organized committees such as the Identity, Credential, and Access Management (ICAM) Subcommittee and the AASC.

To have a clear notion of the meaning and scope of privilege management, we start by considering how access control works at a high level, as shown in Figure 1.

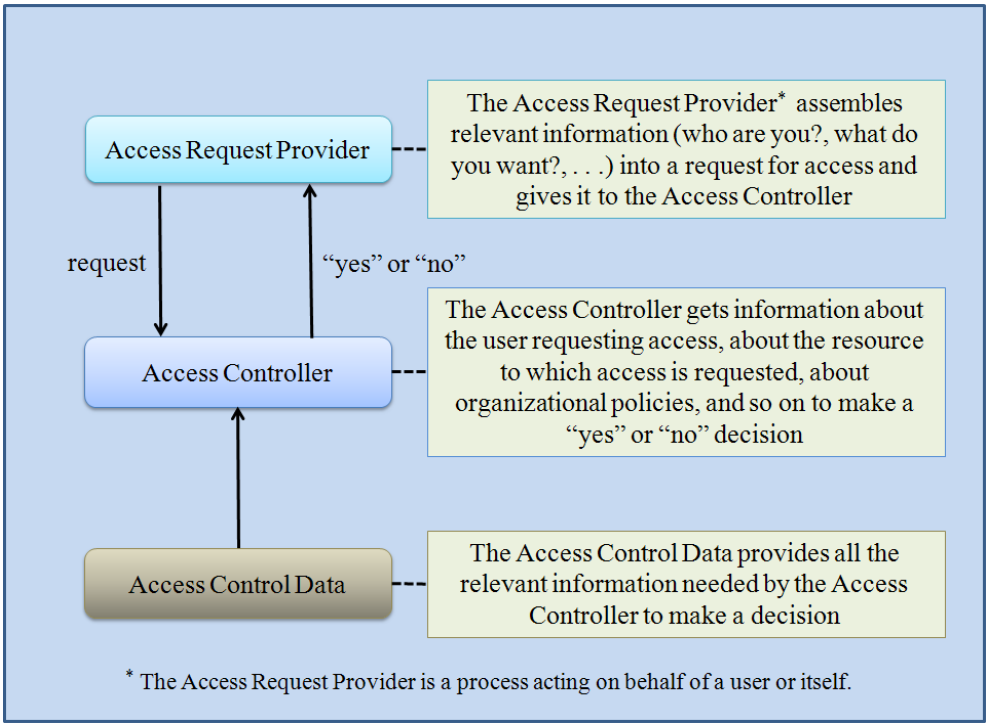

Figure 1. High-Level View of Access Control

Figure 2 depicts the real-time framework for access control in more detail, introducing terminology that is used in this report.

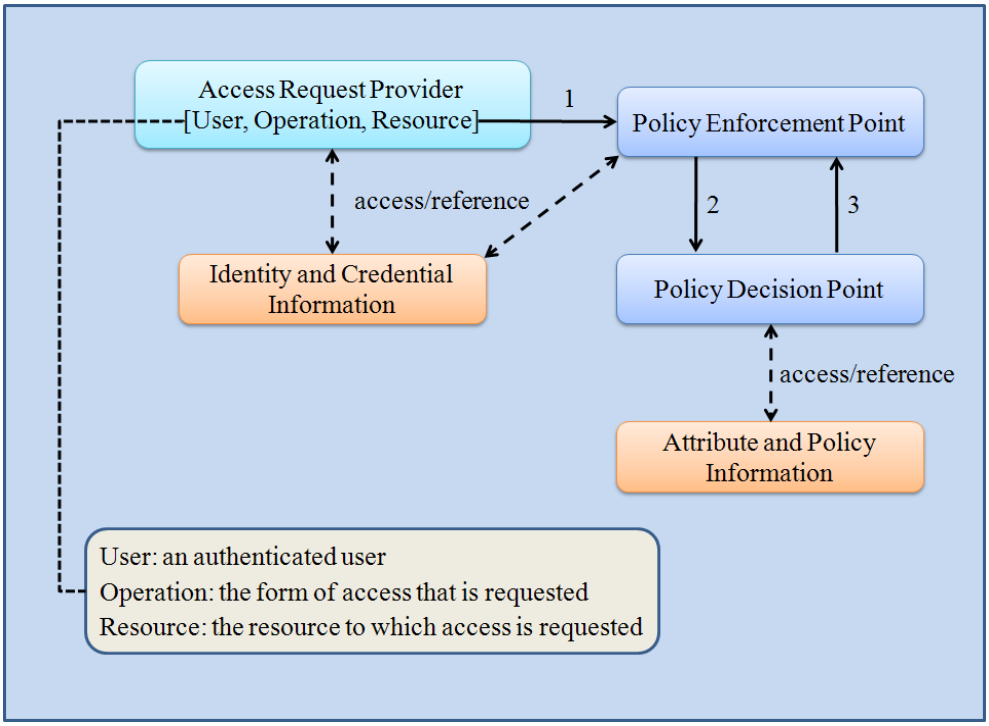

Figure 2. High-Level View of Real-Time Access Control

In Figure 2, the Access Controller of Figure 1 is split into two parts—Policy Enforcement Point and Policy Decision Point—and Attribute and Policy Information replaces Access Control Data. The meanings of the Policy Enforcement Point and Policy Decision Point (as described in Annex A: Authorization and Attributes Glossary) are as follows:

- **Policy Decision Point (PDP):** A *system entity* that makes *authorization decisions* for itself or for other system entities that request such decisions.
- **Policy Enforcement Point (PEP):** A *system entity* that requests and subsequently enforces *authorization decisions*.

"Attribute and policy information" is being used in a very general sense and is intended to have the same scope as access control data. Thus, it includes any form of information that can be used for access control. For example, it includes traditional access control lists (ACLs.) For an ACL, the attribute might be a group or user name while the policy[2] is implicit. In this context, "policy" denotes digital policy—policy that can be processed by computer. The rationale for this scope of the terminology is to enable discussion without having to deal with the details of the many forms of access control data, while at the same time distinguishing the main categories of access control data—attributes and policies.

A *user* is a person, process, or device. The term "user" is defined for the context of this report, as suggested by RFC 4949, and shares connotations of meaning with the terms "subject," "system entity," and "system user" as defined in RFC 4949 and with the terms "subject" and "user" as defined in CNSSI-4009. *Attributes* are distinguishable characteristics of users or resources, conditions defined by an authority, or aspects of the environment. Attributes might provide, describe, or be contact information, membership in communities of interest, roles within a community of interest, sensitivity of data, permission bits, location of the user or the resource, properties of the user session, conditions in the enterprise network or in the environment, priorities associated with individuals, status of resources, current bank account balance, and so on. *Policies* are rules that specify how to use attributes to render an access decision. A policy might specify that a user's signature authority must equal or exceed signature-level-two in order for the user to authorize a monetary account withdrawal.

The view of real-time access shown in Figure 2 does not reflect assurance mechanisms and other entities that might enter into the activity, except for the high-level reference to credentials. So, for example, in a real system, the policy enforcement point might use a credential validation service to convert authorization credentials[3] into attributes that it then provides to the policy decision point. As noted in the Preface, however, assurance is not being addressed in this document.

As suggested in Figure 2, the Access Request Provider uses identity and credential information that is relevant to the context in which the request is being made. The level of trust associated with the identity's credentials can vary widely as can the form of the credentials, and the same holds true for attribute and policy information. In addition, the policy enforcement point may

---

[2] Policy: The process requesting access to the resource is allowed read access if the "read" permission bit is enabled.

[3] Authorization credential is an attribute assertion digitally signed by the issuer so that it can be cryptographically validated. An attribute assertion is a statement made by an attribute authority that an entity possesses a particular set of attributes.