Vision Statement for the Privilege Management Workshop

September 1-3, 2009
National Institute of Standards and Technology
Gaithersburg, MD

Privilege Management at the Enterprise level is a goal in many communities. However, the articulation of what constitutes “Privilege Management”, what other Enterprise-level services it requires and what are the “best practices” are all highly subjective topics.

The primary goal of this workshop is to craft a NIST InterAgency/Internal Report (NISTIR) that provides sufficient explanation of the Privilege Management landscape, challenges and opportunities. A secondary goal is to have sufficient information to begin drafting a series of Special Publications on the elements of a Privilege Management capability.

Through a series of Plenary and Track sessions, we will address four topics and capture the conversations, agreements and issues associated with Enterprise-wide Privilege Management.

In order to focus the Workshop, we must recognize that Privilege Management is a series of activities and technologies combined so that privileges limit the actions of users and their agents and narrow the access space from "all users can access all objects" to "specific users can perform specific operations on specific objects under specific circumstances". Ultimately, the community must move beyond Privilege Management to policy enforcement. To do so requires better definitions, the identification of strengths and weaknesses of existing technologies, and a research agenda.

Track 1 will focus on the supporting definitions to address the lack of consensus as to what actually constitutes Privilege Management and what part does it play in access control in general. The ability to control access to sensitive data in accordance with policy is perhaps the most fundamental security requirement. The output of this track will be shared with Federal and Industry/Standards glossary development activities to normalize Privilege Management terms.

Track 2 will focus on the variety of Models and Frameworks that have emerged in the Privilege Management realm. Well known examples include Mandatory Access Control (MAC) and Discretionary Access Control (DAC) from the early 1970s, Role-based Access Control (RBAC) from the early 90s, and more recently Attribute-based Access Control (ABAC) and XACML-conforming services and applications. The objective of this track is to describe these and other prominent Privilege Management models and frameworks and their specific advantages and disadvantages. The output of this track will provide valuable material for and serve as the basis of the NIST Special Publication on the topic of Privilege Management

Track 3 recognizes that each privilege management technology offering has unique features and functions, but they all share fundamental weaknesses. In general Privilege Management technologies are unable to create, consume and enforce many policies that are important to Government and industry, and are unable to dynamically adapt access policy to a changing risk environment. A current snapshot of technology along with a defined research agenda for the development of products and technologies will be the output of this track.

Track 4 will focus on capturing community requirements and desired operational capabilities for applications supporting both Federal Government and commercial systems. This track will

also identify opportunities for evolving Policy expression and compliance with the Federal Information Security Management Act (FISMA), the Health Insurance Portability and Accountability Act (HIPAA), and Sarbanes Oxley (SOX) standards. Gaps in existing policies will be identified and a recommended “way ahead” will be documented.

In two and a half days we will bring together a variety of policy, legal, technical and operational communities to structure “Privilege Management” in ways that will lead to meeting the needs of both Government and Industry.