Privilege Management Framework

An introductory presentation at the Privilege Management Workshop sponsored by the National Institute of Standards and Technology and the National Security Agency
September 1-3, 2009

Presented by Len LaPadula
Overview

- Context
- A Focus
- Interfaces
- Access Control Models
- The Four Tracks and The Interfaces
Context

A playing field on which to think about privilege management
Descriptions of the Management Systems

Identity Management: uniquely identifying an entity

Credential Management: creating, issuing, renewing, and revoking credentials for an entity

Attribute Management: managing the properties that describe an entity

Real Time Risk Management: generating a current state of the environment or situation as a real time input

Digital Policy Management: creating, validating, translating, distributing, synchronizing, and de-conflicting authorization policies

Metadata Management: collecting, storing, and disseminating structural metadata for information resources and services
A Focus

A subset of the enterprise-level access control context for considering some aspects of privilege management
Policy Enforcement Point (PEP)

Policy Decision Point (PDP)

Identity

Environment/Situation

Digital Policy

Resource

Identity Store

Credential Store

Attribute Store

Policy Store

Metadata Store

Identity Management

Credential Management

Attribute Management

Real Time Risk Management

Digital Policy Management

Metadata Management
Interfaces

An operational representation of the enterprise-level access control context
But... there’s another way to look at this.
But...

there are disadvantages to each of the architectures.
Yes . . .

and exploring the advantages and disadvantages of each architecture, and perhaps others you can think of, provides another discussion theme for the four tracks.
Access Control Models

A brief look at five access control models in relation to each other
Increasingly Finer Granularity of Access Control

Access Control Models

Increasing Policy Basis for Access Control Decision

Increasingly Finer Granularity of Access Control

ACL → RBAC → PBAC → ABAC → RAdAC → ?

17
The Four Tracks and the Interfaces

Some questions for discussion
Interfaces and the Four Tracks

Standards and Definitions

- Which existing standards can effectively be used for implementing interfaces?
- Are new standards needed?
- Are standardized definitions needed for describing and implementing interfaces?
Interfaces and the Four Tracks

Models and Frameworks

- Which existing models apply to which interfaces or sets of interfaces?
- Are new models needed?
- Do appropriate frameworks exist for describing and implementing interfaces?
- Are new frameworks needed?
Interfaces and the Four Tracks

State of the Practice and Research Agenda

- What products, technologies, models, and/or frameworks are commonly used for describing, designing, and implementing interfaces?
- Where are the gaps?
- What are the priorities for a research agenda to fill the gaps?
Interfaces and the Four Tracks

Policies and Requirements

• What policies and requirements impose constraints on interfaces, such as security constraints?
• How do policies and requirements in various sectors affect prioritization of work on the interfaces?
• Where are the needs for which policies and requirements have not been stated in a usable form?
Summary

A brief review
Summary

- Context
- A Focus
- Interfaces
- Access Control Models
- The Four Tracks and The Interfaces
The End

Thank you for your attention