Policy Machine
Enabling an Enterprise-wide, Data Centric Operating Environment

David Ferraiolo & Serban Gavrila

National Institute of Standards and Technology

A New Foundation for Computing

- If properly designed Access Control (AC) and in particular, the Policy Machine can be more fundamental to computing than one might expect.

  In theory: At a basic level AC and Data Services (DSs) can be built from the same elements.

- Some consequences
  - Computing goes from multiple operating environments each delivering different DSs TO a single operating environment delivering all DSs
    - Single sign-on
    - Data interoperability among DSs
    - Comprehensive policy enforcement across DSs

Policy Machine (PM)

A logical “machine” comprising:

- a standard set of data and relations used to express access control policies and deliver capabilities of data services to perform operations on objects
- a standard set of administrative operations for configuring the data and relations
- a standard set of functions for trapping and enforcing policy on requests to execute operations on objects, and for computing access decisions to accommodate or reject those requests

Data Services (DSs)

- A basic objective of enterprise computing (via a data center, a cloud, etc.) is the controlled delivery of DS capabilities to its users.
- DSs enable execution of operations on data (capabilities) to read, manipulate, perform computations on, manage, and/or share data.
  - E.g., email, workflow management, enterprise calendar, time and attendance, and records management.
  - Not all DSs are applications. E.g., file management is a DS that is typically implemented in system software.

Today’s Operating Environments (OEs)

- Capabilities of DSs are supported by a wide variety of OEs
  - E.g., operating system instances, operating system applications, web services, middleware, and database and database applications
- As OEs differ, so do the DS operation and object types that they implement.
  - E.g., Email enables capabilities to send, receive, and read messages and attachments; while workflow management enables users to specify and impose workflow instances and approve or reject work items.
- OEs do not necessarily recognize each other’s data or operation types.
  - E.g., an OS that controls access to files, may view a database as just one giant file and not be aware of the DBMS object types, and email applications may distribute files to users regardless of an operating system’s protection settings on those files.

Management and Usability Challenges

- Administrators must contend with a multitude of OE domains
  - Create and manage numerous user accounts for each user
  - Coordinate AC policies and manage privileges across different OEs with different operation and object types, through different administrative interfaces.
- Ordinary users and administrators alike must authenticate to and establish sessions within different OEs in order to exercise legitimate capabilities.

Enforcement Challenges

- Even if properly coordinated AC policies are not always globally enforced over DSs.
- A large variety of access control policies have been specified, but only a relatively small subset of these policies can be enforced through off-the-shelf technology, and even a smaller subset can be enforced by any one mechanism.

What Can the PM Do?

- Enables an enterprise-wide Operating Environment that can implement and execute capabilities of arbitrary DSs, and can specify and enforce mission tailored AC policies over those executions.
- The OE is object type agnostic and the data of DSs naturally interoperate
- Creates a data centric view. Users can see and consume all their authorized data (regardless of its kind) under a single authenticated session.

How? (1)

- Ops of different DSs (e.g., read, write, send, transfer, submit, approve, reject) can be implemented as simple read or write ops on data or as admin ops on the AC data of the PM.
- Our ops either allow users to read or write data, or they alter the access state under which users can read or write data.
- All other kinds of ops (e.g., font manipulation, spell checking, ordering by date or sender) are implemented in DS logic alone, but are viewed as read and write ops by the OE.

How? (2)

- Users obtain DS capabilities in terms of associations between operation sets (of r, w, and admin), and user and object attributes (modeled as containers).
- AC policies are based on configurations of these same associations (plus others).
- This not only accommodates different DSs, and different ACs, but also enables data interoperability of DSs and global policy enforcement of select ACs over DSs.

PM Data & Relations

- Basic elements
  - Users, processes, operations (r, w, admin. ops), and objects
- Containers
  - User attributes, object attributes, and policy classes
- Relations
  - Assignments (define membership in containers)
  - Associations (define privileges)
  - Prohibitions (denies for users and processes capabilities)
  - Event pattern/Response (can dynamically alter the current access state)

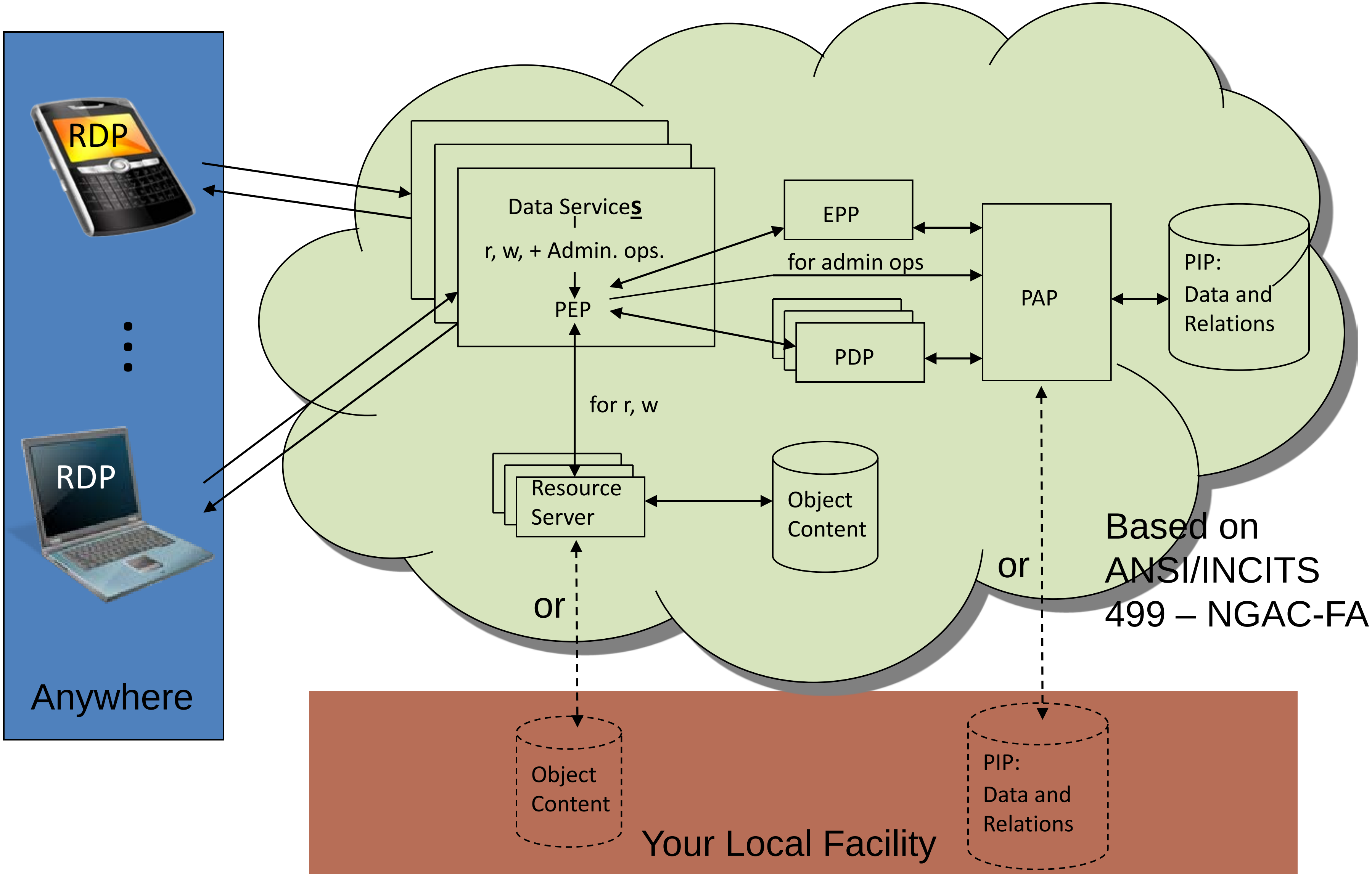
Reference Implementation

- **Data Services**: Office applications, file management, e-mail, workflow, records management, cut/copy-paste
- **Policies:** Combinations of discretionary, mandatory, and history based access controls:
  - DAC
  - RBAC
  - History and object-based Separation of Duty
  - Workflow
  - Forms of confinement (read with restrictive write)
    - E.g., Only doctors can read medical records, MLS, only users in group *abc* can read message *xyz*
    - Trojan resistant leakage
    - Sensitive data can’t be leaked by email or cut/copy - paste
  - Tracking access - I know who can currently access to my data
  - Chinese wall (conflict of interest)

Cloud-Like Deployment

- IaaS is an OE that implements the Policy Machine and composed of its functional components (i.e., PEPs, PDPs, …) that run in VMs
- Users and objects are provisioned, and DSs are selected by the subscriber.
- DSs may be provided as SaaS or PaaS so long as they conform to the Policy Enforcement Point (PEP) API.
- Policies are imported from a library of predefined PM data and relation configurations or configured from scratch, by the subscriber - POLICYaaS

PM Deployment/Architecture



Based on ANSI/INCITS 499 – NGAC-FA

Other Benefits of Deployment

- Can be configured so that data can’t be stored or leaked into local environment
  - If lap/desk top, tablet, smart phone is lost, stolen, or damaged, data is not compromised/lost
  - No need to encrypt data locally
  - Enforcement is difficult to bypass
- Device can be used for business (through RDP) and personal purposes
- All operations exist in PM Cloud so nothing needs to be installed or updated on local device
- Work from virtually anywhere
- Desktop computing aaS - Teleworking