



Authorization Infrastructure Landscape

RL "Bob" Morgan, University of Washington

Common Solutions Group, University of Virginia, May 2004



The Authorization Space

As everyone knows by now:

- “Authentication says who you are, authorization says what you can do.” OK as far as it goes, but ...

A higher-level definition:

- “configuration and operation of systems so actions in support of organization goals are permitted and other actions are prohibited”
- representation and enforcement of organizational policy in software
- all scales from macro-level policy (“comply with HIPAA”) to micro-level (“set permission on this file”)

A little philosophy (from Dennett)

Origins of Ethics

- the origin of civilization / morality / cooperation requires:
 - mutual recognition, and
 - promises (making and keeping and verifying)
 - i.e., authentication and authorization ...

Exaptation: reuse in a new context

- everything useful today originated as something else
 - so: mechanisms/data will get applied in ways we don't expect ...

Decision-making via “satisficing”

- time-pressured, heuristic, can't know all consequences
 - i.e., it's all risk management ...



Risk management

it's all about accountability

- that's why they're called “accounts”

the basic principle

- don't spend more to control access to the resource than it would cost if it were stolen
- what do we spend to administer access?

everyone wants fine-grained policies

- but no one wants to actually manage them
- and even fewer want to look at the audit logs
- so: plan for the policies you can actually enforce



The basic access-control scenario

The vanilla scenario (client-server, session-based)

- client (or peer) connects to server, authenticates as a “subject”
- result of authentication is “security context”
 - and a session associated with that context
 - further operations in session take place in that context
- security attributes of subject are obtained, added to context
 - typically group memberships
 - “userid” (or subject name) is one attribute among many
- client requests operation on a resource
- server must answer the access-control question:
 - is this operation on this resource by this subject permitted?

The access-control decision

Inputs are

- the session security context
- the policy applicable to the resource
- any other relevant security attributes of the subject
- environment (time of day, load, etc)

Output is: yes or no

- there are more complicated policy scenarios too
- e.g., output is “how much” or “yes, and also do X”

Where do all these policies and attributes come from?

- this is “policy management”



Policy expressions

Policy expressions exist at many levels of abstraction

- organizational goals, guidelines, compliance rules
- per-system operational policies and business rules
- group membership and management
- atomic per-resource controls
- expressions at different levels of abstraction often contribute to single access control decision

An authorization infrastructure success metric:

- how much human effort and elapsed time does it take to implement a high-level policy change



Authorization challenges

Requirements advancing in all directions

- more systems, more functions, more users
- more fundamental high-risk processes becoming automated
- more complex interconnection of systems, processes
- more diversity of system architectures

Our response: infrastructure for authorization

- i.e., manage policies, manage attributes, re-use institutional source data, make access-control decisions, etc.
- this has worked well for authentication ...
- but authorization infra successes have been rare
- ... and diversity in authz will likely remain the rule



the I2MI approach

Scope the problem

- based on issues architects confront today
- find/develop models of problem and solution domains

Seek out nascent solutions

- best (or at least good) practices at campuses
- sharable code
- vendor products
- emerging technology/research

Develop/evangelize working technologies

- document, generalize, package, support



Some infrastructure components

aka, things campuses might be working on ...

- authorization service
- authorization API in applications
- policy expression languages
- policy/attribute distribution objects
- directories and attribute definitions
- group management
- provisioning service
- privilege management service
- per-business-area policy practices



Authorization service

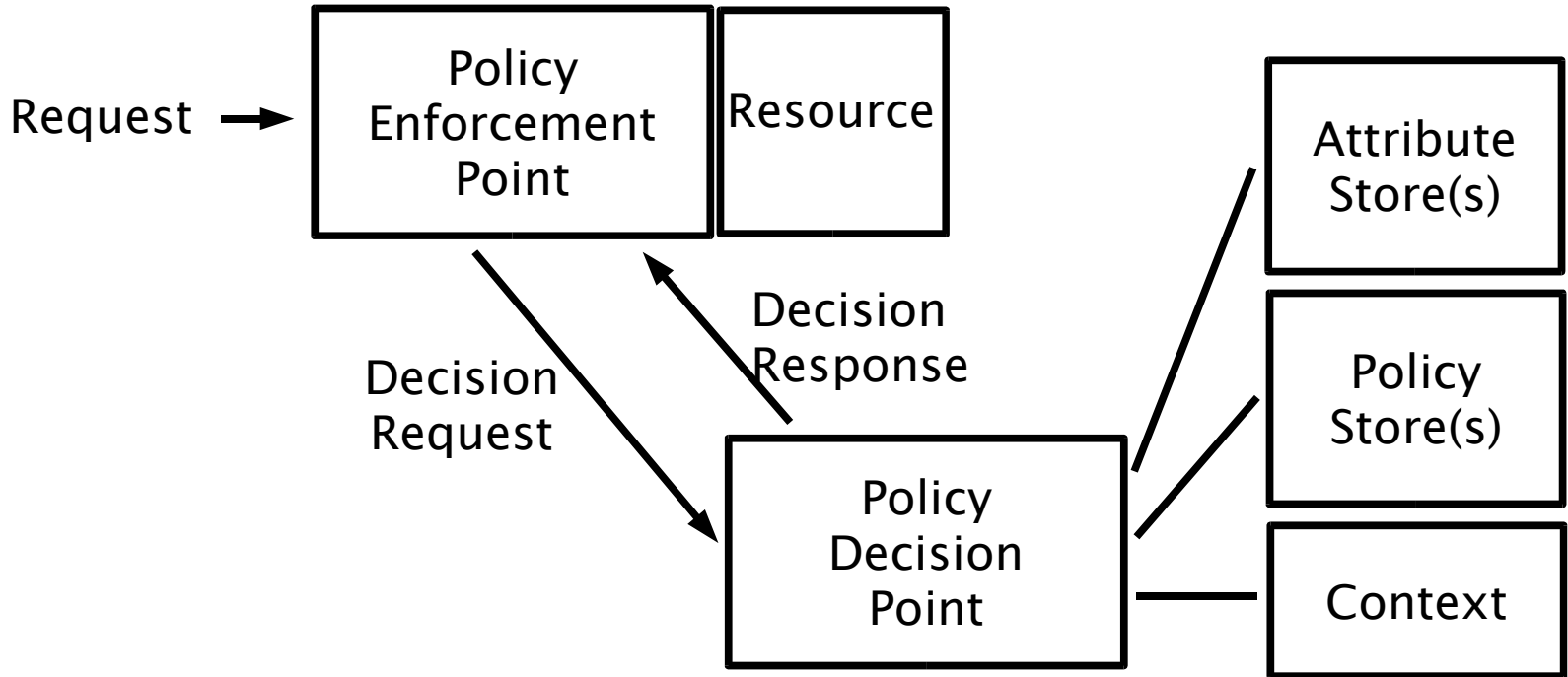
aka “policy decision point”

- app sends request-for-decision, including context, etc
- service “decision engine” accesses policy, attributes, etc, produces and returns yes/no decision
- would also provide means of setting/managing policy and fetching attributes from other places

but ... a radical shift for most apps

- ... also a different kind of infra service than we usually run
- so in real life campuses don't see urgency in this service

PEP-PDP Model





Authorization API

authorization API in applications

- first step to use of authz-decision service by app
- helps app to clarify “policy knobs” in application space
- can permit pluggable providers
- most applicable to new in-house applications
- a few standard ones available
 - OpenGroup aznAPI, Windows authz, JAAS
 - OKI Authorization OSID is a little different
- ... also little-used so far, but may be ready for prime time as apps are designed better for infra-readiness
- standard API for attribute-acquisition may be useful ...

Policy expression languages

Syntax/structure/conventions for policy statements

- e.g., access control lists, access rules
- e.g., XACML, XrML, SPOCP, PERMIS
- typically associated with engine(s) for rendering decisions based on policies in that language
- permit policies to be compared, manipulated, transported
- main requirement for use is good tools to create/modify/process policies
- some useful shared work learning how to use these
 - but no I2MI projects at this time
 - European projects integrating SPOCP (new 2.0 just out)

Transportable privilege objects

Policy/attribute objects for distributed systems

- e.g. X.509 attribute certificates
 - signed objects, so verifiable even when passed around
 - express permissions, etc to applications
- SAML, XACML, XrML, SPKI, Kerberos have similar objects
- complex to specify and to use
 - dealing with signatures is inherently tricky
 - embedding in applications also tricky
- may have near-term application in inter-campus, multi-tier models
 - Shib poised to look at multi-tier with SAML
 - some campuses doing multi-tier with WebISOs



Directories, etc

Directories, metadirectories, person registries

- mainstream tools for managing, publishing person data
- we continue to promote LDAP directory deployment
- widening scope to include XML access methods (SAML and others) and schema methods
- work to be done in defining/publishing application data/policies

Standardized attribute definitions

- e.g. eduPerson and CourseId
- not just names but values, including templates for values



Groups

- manage/express simple “member of” relationships
- groups are most basic form of “improved” authz data
- provide both level of indirection and aggregation
- prior group work focused on directory-based methods
- new group management work based on “groups registry” and methods for auto-management, import, export
- useful in itself and as component of other authz infra
- Grouper design work proceeding via mace-dir
- standard groups API may be related work



Provisioning service

- industry term for automated account management in applications, and user setup in other kinds of systems
- supports authorization by moving policy and user data to places where it can be used by apps at decision-time
- campuses typically do this in home-grown fashion
 - and big-time products are high-priced ...
- new OASIS standard SPML protocol may bear investigation
 - will it be used in products we care about? e.g. LMSes?
- can be looked at as application of more general EAI/MOM service
 - a whole nother potential area of work



Privilege management

- yet another registry, for privilege info
- represent per-app/system permissions, conditions, qualifiers
- support organizational authority and hierarchy
- UI for management, viewing, and interfaces for integration
- export to provision apps, or publish for runtime consumption
- Signet project starting, based on Stanford Authority Manager
- MIT Roles DB similar, more examples at other campuses

Role-based access control

- more a design principle than a tool
- definition and use of organizational roles needs investigation

Business-area policy practices

Authorization infra requires policy analysis

- in light of risk management, process clarification, rule visibility, audit requirements, etc
- at best, can achieve “radical simplification” and real savings
- can this analysis be shared between institutions?
- common technical framework, vocabulary may provide basis
- who would do the sharing?



Authorization stuff coming soon

Papers

- “authorization landscape” describing concepts, tools
- “privilege management recipe” using Stanford and other cases

Toolkits

- Signet privilege management toolkit
- Grouper groups management toolkit

Events

- Advanced CAMP June 30-July 2, all about authorization



Conclusion

Authorization presents many challenges

Understanding diversity of problems is part of developing solutions

There are promising models and technologies

I2MI is working on new infra projects to meet the needs

Come help!