perMIT Lightning Talk

Lightning Talk at CAMP in Philadelphia, June 16, 2009

perMIT in 5 minutes:

MIT has had a centralized privilege management systems for about a dozen years.

We're in the process of rebranding this with the name perMIT and we are making this a open source product. perMIT is the next generation of MIT Roles. http://mit.edu/permit

Technologies:

MySQL database

SOAP based Web Service for reading and writing

perMIT's basic building blocks:

1. Categories, which typically are used to lump all of the relations that encompass a particular application. However, categories in some cases lump the relations that span more than one application. For example, privilege management in the financial domain may span the ERP and the Data Warehouse, and a forecasting system.
2. ASPECs are within a Category. ASPECs == Subject + Function + Qualifier or "Who" + "What" + "Where or when"
3. ASPECS can have starting and ending dates.
4. ASPECS can have a GRANTOR flag which determines if the SUBJECT of an ASPEC can also grant this ASPEC to others.

Qualifiers are defined in a hierarchy. This has two benefits:

1. It gives us an inheritance model which reduces data entry when defining authorizations.
2. We are not restricted to a single organizational view of the organizations.

Examples:

- HR org structure
- Financial org structure
- Course or school hierachy
- Physical location
- ...

Structured Rules evaluation engine provides the ability to take data from any system of record and create ASPECS populated with individual SUBJECTS. We call this implied authorizations.

Example:

- Implied Authorizations: Housing data used to create ASPECS for dorm door access control.
- Explicit Authorizations: House masters able to grant additional exceptions.

Example:

- Implied Authorizations: Organizational data used to populate ASPECS that are queried by Library's EzProxy for fined grained access control to some 3rd party databases.
- Explicit Authorizations: Librarians and some DLC AO's able to grant exceptions. E.g. for visiting faculty member

perMIT does not yet manage all applications at MIT but it is used by many systems including:

- SAP
- Departmental Telephone Contacts
- Environmental Health and Safety
- Graduate Admissions
- Undergraduate Admissions
- Payroll
- HR
- Labor Distribution
- Portal
- VoIP
- Touchstone Account Administration
- Warehouse
- Student Information Services
- Libraries
- MIT ID DB
- Master Departmental Hierarchy