Leveraging Group Management Middleware at Cornell

Andrea Beesing
Internet2 Fall Meeting
December 6, 2006
Topics

- General problem to be solved and user context
- Current and future application requirements for groups at Cornell
- Cornell Grouper implementation
The problem

• Many applications can perform actions based on group membership of people or things
• Each application has its own group management function
• Groups have to be maintained in multiple places
User context: expanding community

Students 20,000
Faculty 2,600
Staff 11,000
Alumni 204,000*

Medical graduate and professional units in NYC and Doha, Qatar

* with NetID’s after 12/06
Summing it up

The problem + Expanding user community (total numbers and number of groups) + Demand for new online services = Scalability challenge

Middleware needed here!
Coarse-grained access management

Can I access cit.cornell.edu/internal/?
Yes

amb3

Is amb3 a member of cit. staff group?
Yes

Central repository of group information
Common desktop

Provide staff in the College of Agriculture and Life Sciences (CALS) with the tools and information needed to do their jobs, in one place.

Six groups defined
Common desktop: role-based content delivery

Jane Doe is a faculty member in the College of Agriculture and Life Sciences. Provide her with easy access to reports and information of interest to research faculty in CALS.

Jane is member of CALS academic research group.
My College Channel

- Presents each student with uPortal channel content based on his/her college
- Further development of tailored content in progress for PeopleSoft self-service
Emerging application needs

- Support privilege management service (Signet): Assign privileges to groups
- Workflow support for Kuali: Routing of information is workgroup-based
- Subscription service: Information routed to individuals who have opted in to specific groups
- Supporting the Cornell federation: Group information for use in Shibboleth assertions
And other potential applications…

- Routing of information based on organizational tree
- Extend common group management infrastructure for use with a campus Active Directory Service
- What are yours?
Group management at Cornell

- “Permit Server” in use since early 90’s
  - Admin UI designed for the 1990s
    - Limited delegation features
    - Limited visibility (what groups does user X belong to?)
  - Proprietary technology limits integration with other IT components and applications
  - No group math
  - No self-enrollment options
- Project under way to replace the Permit Server with Grouper, an open source solution developed by Internet2 working group
The Grouper advantage

- Common API for program access
  - Better integration with applications and other middleware components
  - Better support for automated provisioning and adjusting of institutional groups/roles based on source data
- Support for distributed, delegated model for group management
  - Common interface for users, customizable using tiles and struts
  - Delegation of admin and ownership of groups through naming stems
- Advantages of RDBMS-based “Groups Registry”
  - Sophisticated group management capabilities--group math, group nesting, negative authorizations
  - Traceback of indirect membership
  - Future version to include aging of groups and memberships
The big picture for access management

Identity Management
- Institutional roles, other attributes
- Groups
- Privileges

HR
- faculty, staff, temp

Student
- undergraduate, graduate, postdoc

Finance
- PI, approver, budget officer

Courses
- instructor, teaching assistant, student

Grouper

Signet

ERPs
- Network Services
- Library
- Schools & Depts.

External Partner

PROVOST

REGISTRAR

BURSAR

SCHOOLS, DEPTS.

LIBRARY
Opportunities for business process improvement

• Better support for automated provisioning of institutional groups/roles based on source data: staff, faculty, student

• Support for distributed, delegated model for group management
  • From IT-centric model to business-centric
  • Providing tools to allow business-unit staff to manage groups vs. tools used largely by central IT staff
Distributed, delegated model: access management example

Data access policy & standards

Dean
College of Ag & Life Sciences

Grouper stem: College of Agriculture & Life Sciences
Admin 1: Dan
Admin 2: Tim

Grouper stem: Plant Science
Admin: Marion

Grouper stem: Int. Agriculture
Admin: Judy

Grouper stem: Animal Science
Admin: Joe

Plant Science Faculty group

MPS/Peace Corps Students group

Dairy Mgmt Series group
For more information

• Grouper:
  http://middleware.internet2.edu/dir/groups/grouper/

• Signet
  http://middleware.internet2.edu/signet/

• Cornell project
  amb3@cornell.edu
Questions?