Federated Collaboration Approaches

COmanage
SURFNet eduSocial
Google Apps for Education
Presenters

- COmanage
  - Heather Flanagan, Stanford University
  - Michael Gettes, Massachusetts Institute of Technology

- SURFNet and eduSocial
  - Niels van Dijk, SURFnet

- Google Apps for Education
  - Steven Carmody, Brown University
  - Susan Gautsch, Pepperdine University
Reminder: What problems are we trying to solve?

- IdM is a critical dimension of collaboration, crossing many applications and user communities.

- Virtual organizations represent critical communities of researchers sharing domain resources and applications as well as general collaboration tools. Providing a unified identity management platform for collaboration is essential in a multi-domain, multi-tool world.

- Lots of activities in domesticating applications to work in a federated world, moving from tool-based identity to collaboration-centric identity.
How are we trying to solve them?

- By pulling together an integrated set of collaboration apps (wikis, listprocs, CVS, file share, calendaring, etc)
- Planning for the integration of at least identity and access control via group memberships
- All this repackages successful approaches for a collaborative/project/VO setting
  - Federated identity, group management, directories, and security token services (aka credential convertors)
What we’ll look at today

- COmanage
  - [http://middleware.internet2.edu/co/](http://middleware.internet2.edu/co/)

- SURFNet

- Google Apps for Education

- *(which isn’t to say other things aren’t out there: Commercial offerings – Sharepoint, Adobe Connect, Google Sites, Google Wave, Google Apps; Repurposed LMS – Sakai, Croquet)*
COmanage

- 2007: Internet2/NSF grant approved
  - "Applying federated identity management to a set of collaboration tools (protected wikis, shared file stores, shared calendaring, video conferencing, audio conferencing, list processing, etc.) and adding VO support as an inlay within the overall federated identity management infrastructure."

- 2008: First round of design and test instances created

- 2009: Second round of design and exploration by early adopters
COmanage

- 2010: Focusing on the meaning of life, or
  - Create a body of documentation for others to use
  - Fully defining domestication, to give applications a goal to develop towards
  - Determining the right place for attribute management in a CO infrastructure
  - Develop a service model
Domestication

- “to bring to the level of ordinary people” – Merriam-Webster Dictionary
- The work of re-factoring applications to use the emergent identity services infrastructure
- Begins with federated identity and authentication, use of directories; gains a lot from group management for access control, etc
- Needs a fine grain set of authorization tools down the road
- Domesticated apps can receive IdM attributes via LDAP, SAML, X.509, SQL, Kerberos PAC, and maybe all of the above
Starting to look at responsibilities

- Typical activities in collaboration management:
  - Add or remove people from groups
  - Create new subgroups, identify overlapping memberships, etc.
  - Permit or deny access control to wiki pages, calendars, computing resources, version control systems, etc.
  - Add people to mailing lists, wikis, etc.
  - Create and delete/archive users, accounts, keys
  - Identify group membership on a given date

- Who now “owns” this information? Who is responsible for its upkeep?
Roles, schema and attributes

- Research communities have their own cultures, vocabularies, needs
- Building community-wide consistency on roles, privileges, groups provides tremendous leverage for collaborations
- Keeping it simple is critical and difficult
- Examples: groups/permissions might include PI's, lab assistants, ability to write to wiki, ability to control who can write to wiki, who can reset instruments, who can read instruments, who can expense on travel, etc...
- Now is a good time to explore web services as a way to handle attributes
COmanage Elements

- Dashboard
- Shib SP
- Shib IdP
- Grouper
- STS
- LdapPC Including provisioning

Applications

Data Store
What’s in a COmanage data store

<table>
<thead>
<tr>
<th>Enterprise Attributes</th>
<th>Project/VO attributes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Federated Id</td>
<td>PI groups</td>
</tr>
<tr>
<td>Enrolled classes</td>
<td>Wiki editing permissions</td>
</tr>
<tr>
<td>Display name</td>
<td>Instrument permissions</td>
</tr>
<tr>
<td>Citizenship</td>
<td>VO certificates</td>
</tr>
<tr>
<td>Enterprise affiliation</td>
<td>…</td>
</tr>
</tbody>
</table>
What forms does COmanage take?

• Usually as an assembled set of services
  • A dashboard, directory product, Shibboleth IdP and SP, Grouper, and a set of applications provisioned on other servers
  • On an enterprise level to serve its collaborations and VO’s, within a large VO, or at a federation level to serve a national community
  
• Can also be a VM, a VM in the cloud, or a service with the applications in the cloud.

• Can be embedded in a science portal or gateway
Some key issues

- Extent of application domestication
- Waiting for other technologies to happen – interfederation, discovery, metadata tagging, etc.
- GUI approach
- Domain application/science portal integration
Next steps

- Documentation
- Create a better set of service models
- Bring in new CO/VO collaborators
- Build an international community of developers and deployers, sharing expertise on domesticating apps.
- Develop approaches for provisioning and deprovisioning
- Bring in domain apps appropriate to types of CO/VO collaborators we’re seeing engage