ACAMP Identity Services Summit 2009

Advanced CAMP: Identity Services Summit

Sponsored by EDUCAUSE, Internet2 and Jasig

Philadelphia, PA, June 18-19, 2009

- Summit wiki
- CAMP Access Management 2009
- MACE-paccman wiki
- Sakai 2 integration issues

The meeting was positioned as a way to explore common needs and issues around identity and access management. Many projects, institutions, and businesses are just starting to hit federated authorization requirements, and so it's a good time to work out new approaches. I attended as the representative of Sakai (and LMS in general, as it turned out). My notes are pretty rough, so just ask if you want anything clarified.

2009-06-18

Bob Morgan says the meeting's goal is to find ways to work together.

Tom Barton opens with a quote from "Opencast Matterhorn developer Josh Holtzman" about looking for an existing solution rather than inventing another project-specific one.
We should identify one or two needy areas of commonality and agree to an abstract service contract.

Q: How well does the pizza-with-everything diagram match our situation?
A: A couple of people say it's probably OK. (It conveys the complexity of the problem, but I'm not sure it really clarifies much.)

Kuali ID Management / KIM - Doesn't implement its own authn, just combines others. (No mention of existing authn bundlers like the CAS library or Spring Security.)
Provides reference implementations of entities, princials, groups, roles, resonsibility, with expectation that they'll often be overwritten.
Motives: Wanted to add roles and permission to the previous purely group-based authz. Wanted to extract a common approach for multiple Kuali projects. They believe it might be generic enough for non-Kuali uses.
Q: Did they search for existing products, libraries, standards?
A: They looked at Grouper, and took some terminology from other projects, but stayed driven by KIM requirements.
Kuali Service Bus : SOAP Client App, Java Client (with direct authn integration outside), Rice Standalone Server with admin GUI and service implementations (connects to Rice DB & institutional overrides).
Can now add permissions (to template start) without code changes.
Applies against documents in a type hierarchy with wildcard matching in the namespace.
"Workflow actions need to roll up to the same source as permissions." (Sounds like they hit the difference between implementation-level CRUD-like file-system-like access rights and UX-level roles.)
Moving metadata to the assignment & eliminating need for fake groups helped a lot.
They ended up adding another concept to authz: "Responsibilities" == more or less a bundle of lower-level application-defined permissions?

Afterward there were questions about the number of terms being introduced and whether there was any need to distinguish group from role. A good set-up for my presentation.
Everyone: We need a glossary. (Duffy Gilman and me: Isn't this how the CM API started?)

Q: Even if we build it, will anyone come? After all, why isn't everyone using EduCourse?
(In our case, it didn't meet the Sakai CM integration use cases that we met through enrollment sets and course sets.)

There was some mention of the Mellon-funded Bamboo project, which I haven't been following: "Nine months and three workshops into the planning process, Bamboo has involved over 440 individuals from more than 110 institutions in the discussion. Currently, participating institutions have come together to define the scope and direction of the project implementation phase... a possible 7-10 year vision..."

uPortal - I split my Sakai-oriented presentation with Andrew Petro's uPortal presentation so I don't have a lot of notes. Andrew's slides are excellent, though.
Topics for further research:

- JIT groups via rules about user attributes.
- Categories as a one-level hierarchy?
- Group scoped by portlet (allows equivalence to role).

Sakai / LMS - My presentation went well, I think, despite the bare-bones visuals. Luckily, people understood describing an LMS as a "Reese's peanut butter train wreck" of user expectations. (Style tip: dashing through slides faster than they can be read lends a air of urgency.) Anyway, the audience was very patient, and after all these years I finally seem able to describe our authorization needs in a way that security experts can follow.

OLE project (Mellon, Rutgers) - Library system.
Authz tends to be kept at the resource level. XMP license header in an electronic book. XACML embargo statement in METS dissertation package.
One hope is to tone down privacy issues relating to license/economic tracking (e.g., subpoenaed overdue records).

UPMC - Paris - IDM - national ID repository. Currently relies on interLdap to connect HR + Student systems, customized memberships all in LDAP.
Financial pressures to track enrolled students vs. others.
Future: Federated registries (HR, student). Master Data Management (MURAL, Sun) for mapping & sharing. openESB (transport, propagate, synch).

TeraGrid - Research grids. Largely non-HTTP – SOAP hasn't dislodged gram, gridftp, ssh. Strong user ID requirements with federated authn. Need to continue to work with X.509. https://go.teragrid.org/ can supply a TeraGrid certificate based on instituional authn.
More individual-based than OpenGrid: you get your ID and then you're granted group/project access through a human admin.

Bedework Calendar - ACLs are too hard for end users. Hitting CalDAV issues with Shibboleth authentication.

Digressing into file-system DAV, you can use Shib cookies against Win XP Dav if you set it up to do container-based authn. But still no solution for the Mac.

Moodle - No representatives showed up, sadly – I was hoping to find common integration ground at this meeting.

At this point, the meeting split up into four groups:

- KIM integration
- ID federation issues
- COmanage
- Roles & permissions ontology / glossary, which is where I ended up

A brief introduction to PerMIT's very interesting approach, which I blogged about earlier this month : Subject + Function (hierarchical) + Qualifier (hierarchical).

What do we want out of our "ontology"?

- Real-world definition
- Formal definition (e.g., through XML Schema)
- Reference implementation
- Reference use case clients

Everyone is hitting "Who + What + Where" in various ways. It should be abstractable.

Remember we can change "standard terms" over time, and we can experiment and learn from real-world use.
LevelOfAssurance was recently added to EduPerson more or less as a placeholder from which evidence could be gathered.

Possible formula for cross-project translation: "Externalized groups and entitlements."

Another attempt at working out the KIM terms: "Dean" is the Role; "ThorntonCollege" is the Group; "Approver" is the Responsibility; "OkLargeExpenditure" is the Permission?

Duffy wants a descriptive model with precise language that he can use.

What is PerMIT using to describe its dynamic rule-based criteria? Nothing. It's done by import into the database. Truly dynamic decisions can't be handled at this point.

Andrew: Upcoming uPortal release has improved groups navigation.

Grace Agnew: Authz integration use case: The library's subject matter liaison should get content-adding access to all Chem course workspaces.

Another dynamic-query-based use case: IP-address-based access.

A recommendation for the book Role-Based Access Control. (The RBAC summaries I've seen don't match our context-sensitive roles and resource-specific permission overrides. Maybe the book ventures into that territory, though?)

Federation issues: Provisioning / deprovisioning. Harmonization across levels of assurance and qualifiers. Discovery services.

Kantara - Identity management coalition, just started: "Roger Sullivan, vice president Oracle Identity Management, has been elected president." "... solutions could be built based on one or a combination of several IAF, ID-WSF, IGF, Information Card, OAuth, OpenID SAML 2.0, WS-*, XACML and XDI standards."

Various: We want a Fluid component for selecting and managing groups. (I mentioned that the Sakai 3 group managmenet

project team includes Fluid contributors.)

I had problems experimenting with Grouper a year or two ago. But it's improved recently, and so uPortal's considering it again.

2009-06-19

Lightning talks from current service libraries:

OpenRegistry - Ben Oshrin - Rutgers

Rutgers ID card services are currently a spaghetti pile of processes from Libraries, Recreation, Payroll, Student Registrar....
The new design centralizes a registry which then fans out to LDAP, Parking, Dining/Housing, ...
The registry reconciles, deals with conflicts, then sends out to message queues, reports, etc.
First release scheduled for this fall.

Grouper - Tom Barton

Folder == namespace (with subfolders)
Composite groups == union
LDAP provisioning connector. Also a Subject API.
SOAP and REST interfaces.
Hooks (plug-ins) to veto and notify.
Clients: Brown U. uses for course groups. French national portal for HE (ESUP Portail), although the portlet UI needs improvement. SURFnet group management for Dutch HE & public. COmanage. NIH Cancer BioInformatics Grid.
Might share some namespace issues with other projects?

COmanage - Digant C. Kasundra

Framework + guidance + small appliance for collaboration apps that use identity services.
Gives you a central spot to support multiple application clients.
Go through COmanage front page, link to Confluence, COmanage tells Confluence what it needs to know.
For alpha, putting a preconfigured VM appliance out to Drupal & Confluence.

Shibboleth - Steve Carmody

Plug-in allows users to control transmission of attributes for given resource targets.
OpenID being added now.
Support trusted transport of assertions through multiple tiers.
Beginning to support linked identities, aggregating from multiple ID providers.
Has helped encourage use of shared attributes/values: eduPerson, UK librarian roles, Library vendor entitlement value.
Looking into non-web approaches. WinXP DAV, ssh for grid... "It's hard."

CAS - Scott Battaglia

V. 3 can store authn in memcache.
Will support multiple existing protocols to ease integration with other vendors.

PerMIT - Paul Hill

First step was moving from Oracle to MySQL.
Q: Why not a cross-DB approach? A: Tightly coupled at this point with stored procedures. Partly for efficient handling of hierarchies.
Currently has 4 million rows in DB, since all subject-level triples are stored.
Q: What's the subject population? (MIT has 10,000 students. UCB has 30,000.) A: 24,000 active users.

Miscellaneous notes

In the break, I got to meet Kevin Foote, who gave me the good news that the Sakai 2.* CM integration has been working well for IUP's needs.

uPortal is going straight to the CAS library for one-stop authentication. But there seemed to be general agreement that Sakai would probably be better off using Spring Security as a central configurable spot. (I was planning to experiment with both.)

In the "small world" department, Kenneth Klingenstein suggested that I take a look at UC Berkeley's own report on collaboration technologies, as passed on to him by campus CIO Shel Waggener.

I also met Leif Johansson, who along with Klas Lindforss Shibbolized Sakai 2. I pitched the idea of reducing upgrade costs in Sakai 3 by supporting Shibboleth integration out-of-the-box. Leif is moving off Sakai to full-time ID management, but Klas might be able to help contribute to the project. I'll send him email about the integration BOF at Boston (and try to provide access through Skype).

Q: Should someone talk to Spring Security?
A (me): The Spring team's great, but they have a different focus. (Spring's always been up-front about wanting to improve access to proven techniques and libraries instead of experimenting with less well determined requirements.) A more natural outside-higher-ed group to contact might be Google Apps Education Edition. There are already a lot of schools trying to

integrate authz better with Google Apps, and Google obviously stands to benefit by meeting our needs in a less one-off fashion. Bob Morgan has had talks with Google about group support. Steve Carmody is also interested.

Assigned Tasks

- Through MACE-paccman, I'll map terms between some roles/groups/permissions systems: IMS LIS, PerMIT, Sakai 2, Sakai K2... Others at the conference will take other pieces of the ontology task, and we'll see how far we can take it.
- KIM will look into using Grouper for groups management.
- I'll report on the conjunction of the Sakai community, Google Apps, and authz integration with SIS-type groups and roles. (Of course, one of the existing integrators might want to take over this task, or might already be spearheading an integration effort. I just happened to be the Sakai developer available at the summit.)