CAMP Notes

CAMP: Practical Building Blocks for Access Management

June 15-17, Philadelphia

Day 1 (15-June-2009)

Welcome and Introductions

* *Thomas J. Barton, Senior Director for Integration, University of Chicago* and **Ann West, Sr. Program Manager, Internet2/EDUCAUSE, Michigan Technological University*

- The perspective of CAMP is that there are small things that can be done in access management that are a good start and are easier to do than the large things. There are modest problems that need an access management solution.
- Rob Carter of Duke has developed categorized **use cases** to make things clear.
- We will attempt to identify a small set of **solution patterns** to address use cases.
- We look forward to hearing wisdom and experience from folks in the room.

Access Management Building Blocks

* *Tom Dopirak,Senior Consulting IT Architect, Carnegie Mellon University* (slides)

Q: What are the different terminologies in this access management space?

A: There are different vocabularies for policy and for software. XACML has a terminology, Kerberos has a terminology, Active Directory has a terminology. The MACE-paccman working group wiki has a comparison between XACML and Signet and are hoping to build more terminology mappings in the glossary.

Q: How should we handle scalability issues that arise when role-based access management is embedded in the application?

A: That's a problem. If you build a wonderful access management program and it can't interact with the applications, that's also a problem. Ways of doing application integration will change as new technologies come into view.

Categorizing Access Management Challenges

* *Rob Carter, Consultant, IT, Duke University* , * *Scott Fullerton, Sr IT Architect, University of Wisconsin-Madison* (slides)

Q: Thinking in terms of an application a campus might buy, how do you hook it up? Who has what role? What questions should we ask vendors?
A: When we are looking at implementations, think in terms of what IdM info we have available and what will the applications want to consume? Also, ask to what extent the potential application meshes with business processes you have in place, and If it does not mesh, how does the data support the new business process it's forcing on you.

Q: How to handle a very complicated workflow, with many roles, ranks, schools, etc.?

A: Try to figure out if there are groupings that can be more broadly provisioned.

Discussion and Lightning Rounds: What are Your Use Cases?

* *Moderator: Tom Barton, Senior Director for Integration, University of Chicago*

---

* *Caleb Racey, Newcastle University*

Access Controlling Online Resources -- Wikis, Lecture capture, Room Booking (notes)

---

* *Michael McDermott Brown University*

Security Faculty Information Systems(slides)

---

* *David Langenberg, University of Chicago*

Quarterly Instructor Access, Student testing(slides)

---

* *Jimmy Vuccolo, Pennsylvania State University*

Financial Workflows (notes)

---

* *Liz Salley, University of Michigan*

Organizations as Subjects (notes)

---

* *Jim Beard, University of Oregon*

Thorns in Password Reset (notes)

Day 2 (16-June-2009)

Describing the Solution Patterns and Real World Examples

* *Elizabeth A. Salley, Product Manager, Michigan Administrative Information Services, University of Michigan-Ann Arbor (Moderator and Presenter),*

* *Tom Barton, Senior Director for Integration, University of Chicago*

* *Caleb Racey*, Middleware ISS, Newcastle University

(slides - Elizabeth, Tom and Caleb)

* *Steven Carmody, IT Architect, Brown University* (slides)

Discussion and Lightning Rounds: Testing the Solution Patterns

* *Moderator: Tom Barton, Senior Director for Integration, University of Chicago*

* *Jean Marie Thia, University Pierre et Marie Curie*

Shibboleth attributes for SharePoint (slides)

---

* *Paul Hill, MIT*

perMIT (notes)

---

* *Caleb Racey, Newcastle University*

Access control with Shibboleth and Grouper. How to populate identity stores. (notes)

---

* *David Bantz, University of Alaska*

Organizational hierarchy & the phone book   (slides)

---

* *Luca Fillipozzi, University of British Columbia*

A physical access management solution (notes)

---

* *Astrid Fingerhut, University of Chicago*

Trusted Agent program (notes)

Environmental Scan - What Technology Tools Work (and Don't Work)?

* *Moderator: Tom Barton,Senior Director for Integration, University of Chicago*

**Bill Kasenchar, Project Leader, University of Pennsylvania* (slides)

* *Laura Hunter, Identity Architect, Oxford Computer Group* (slides)

* *Bob Bailey*, Sr. Developer, Lafayette College (slides)

Q for Bob Bailey: How are you dealing with latency issues for synchronous writes into the OpenLDAP directory?
A: we only have 5000 entries in our LDAP dir. So we don't have a problem.

Q: If someone in the business school, for example, wants to know groups in other part of campus. How do you handle appropriate boundaries for sharing?

A: from Bill Kasenchar: You can allow or deny that level of sharing.
A: from Bob Baily: with OpenLDAP, you just add somebody to a group. The simple solution is that access is granted based on group affiliation.
A: from Laura Hunter: AD natively makes that challenging, everyone has access to everything. There are ways to tweek around it.

Environmental Scan - What Policy and Process Approaches Work (and Don't Work)?

** Elizabeth A. Salley, Product Manager, Michigan Administrative Information Services, University of Michigan-Ann Arbor (moderator and panelist)* (slides)

**Andrea Beesing Assistant Director, IT Security, Cornell University* (slides)

** Renee Shuey, Senior Systems Engineer, The Pennsylvania State University* (slides)

Q: Why did the University of Michigan project need to go back several times to get funded? What was that process like?
A: Our project was one of the first, and there was the question of "how do we fund projects like this." We thought we could get funded without knowing what technology to put in place. Then we did the RFP, and we chose Novell IdM. Key stakeholders wanted to know the technology before approving funding.

Q: What are the key awareness and education issues involved?
A: We need to work hard to find ways to create the understanding that this is not just an IT effort, it's about the community.

Bringing the Workshop Home: Applying Your Knowledge to Your Access Mangement Challenges

BREAKOUT SESSIONS:

- **Hierarchy** notes
- **Implementation** notes
- **Use Cases** notes
- **Providing Input to perMIT and Grouper projects** notes

photo of breakout session

Day 3 (17-June-2009)

Lightning Rounds of Use Cases, Solutions Integration, and Related Topics

** Moderator: Jens Hauesser, Director, Strategy, The University of British Columbia*

** Chris Hyzer, University of Pennsylvania*

Grouper Future Features, (slides)

** Kent Fong, University of British Columbia*

UBC's IdM program

(notes)

** Jim Beard, University of Oregon*

IdM Implementation from the Rear View Mirror (notes)

Looking Forward

Moderator: Elizabeth A. Salley, Product Manager, Michigan Administrative Information Services, University of Michigan-Ann Arbor

*Panel: * Ken Klingenstein, Director, Internet2 Middleware and Security, Internet2*

** Tom Dopirak, Senior Consulting Architect, Carnegie Mellon University*

** Michael McDermott, Senior Programmer/Analyst, Brown University*

** Bob Bailey, Sr. Developer, Lafayette College*

Q: We spent time in lightning rounds talking about use cases and solution patterns and trying to build that into a design pattern library. What would you like to see as next steps for making some of that happen?

A: Clear writing and scribing those use cases anad patterns and recipes for how they might be implemented is really helpful to a lot of people to understand how to approach the space in different ways.

Q: Why shouldn't we look at open source as being as viable as a sole proprietor solution?

A: Issues detering people from open source solutions include desire for a support contract, desire for "someone to yell at" if things go wrong, need to have folks on your team who can modify it, worries about scalability.

Comment: it can be possible to get a support contract for open source, such as with Debian or Open LDAP

Next Steps and Continuing the Conversation

Buddy Groups were formed for ongoing consultation and support with access management issues.

See Buddy Groups page

Feedback and Suggestions for Future CAMPs

- Looking at use cases and solution patterns was helpful. It's important to continue the approach.

- Would be nice to have more breakout session opportunities.

- At future CAMPs, it would be good to facilitiate a dinner out, where people can go to a certain restaurant and chat about a designated topic of common interest.