Meeting Notes - 2008-06-10 at UCD

Meeting Notes - 2008-06-10 at UCD

Day 1 - UCTrust Work Group Meeting

Attendees

Arlene Allen, UCSB Curtis Bray, UCD Chet Burgess, UCOP Dedra Chamberlin, UCB Matt Elder, UCSD Greg Fellin, UCM Patrick Flannery, UCDHS Jannelle Fong, UCSF	Eric Goodman, UCSC Karl Grose, UCB Mike Helm, LBNL Bruce James, UCOP Brian Koehmstedt, UCM Chris Lambertus, UCDHS Debbie Lauriano, UCD	Warren Leung, UCLA Simon Litvak, UCB Jeff Mc Cullough, UCB Kiltesh Patel, UCDHS Chris Peters, UCI Tom Poage, UCD Lucas Rockwell, UCB	Brian Roode, UCI Heidi Schmidt, UCSF Robert Schwartz, UCDHS Hampton Sublett, UCD David Walker, UCOP Troy Wright, UCSC Albert Wu, UCLA

Introductions and Significant Campus Events

- UCD and UCDHS are currently planning their identity management strategy. They currently use CAS for internal applications and Shibboleth for external.
  - UCSD uses Shibboleth for all applications; they currently have approximately 130 SPs.
- UCLA is looking into group management.
- UCB is looking into using Sun Identity Manager. They're also educating service providers to the UCTrust rules.
- UCOP certified for UCTrust Basic at the end of May. The first application was Project Tracker, an ASP.net application that President Yudof brought from the University of Texas.
- UCSF recently hired Jann Fong from UCB to head their identity management project.
- UCSC has Shibboleth installed.
- ESnet (LBNL) is looking to federate with various Shibboleth infrastructures globally.
- After some study, UCI is continuing with their use of home-grown identity management software.

Updates

- The UC Grid community has implemented their UCTrust integration and is currently putting it into production.
- Technical management for Human Resources's "learning" management system is moving to Human Resources and Benefits's technology group at UCOP. Sean Baglin, who had been the project manager within Human Resources has left the University.
- The integration of Connexxus into UCTrust is complete, and UCSD and UCR have started to use it. There is still significant work to do, however, on the provisioning feed that must be sent from the campuses.
- UC Ready is a system-wide incarnation of Restarting Berkeley that is being implemented at UCB. Simon Litvak (of that project) attended the meeting to discuss UCTrust integration.
- The new Enterprise Risk Management (ERM) system is being implemented by IBM under contract to Risk Management at UCOP. It will be integrated with UCTrust.
- InCommon's work on their Bronze and Silver assurance profiles continues. Karl Heins and David Walker are involved with the effort.
- A "Federation Soup" meeting was held in Seattle at the beginning of the month to discuss global interfederation issues. Karl Heins, Mike Helm, and David Walker attended.
- Campuses are starting to plan for IPv6. We'll want to track that to ensure Shibboleth interoperability.
- UC's library community is starting to be interested in UCTrust. It's a good time to reach out the campus library staff who may be interested.
- Warren Leung, Albert Wu, and David Walker will be giving a session at UCCSC on integrating applications with UCTrust.

Identity Management Collaboration at UCD and UCDHS

Hampton Sublett, Curtis Bray, and Gary Jellis talked about joint planning that is underway for the UCD campus and Health System

- The Burton Group did a study of identity management for UCD in 2006; they are going forward with selected recommendations and increasing the emphasis on Health System issues.
- The campus is looking at various implementation issues as they migrate from their legacy system.
- The Health System didn't get much attention in the Burton Group study.
  - Most application do their own identity management.
  - They have mainframe and lost of Windows and Citrix. There aren't very many web applications, so Shibboleth isn't a major driver.
- The campus and Health System are merging their Active Directory forests.
- Next steps are to identify resource needs and to educate departments.

Shibboleth 2.0

Tom Poage and Matt Elder gave an overview of the 2.0 release of Shibboleth, using slides selected from the Shib InstallFest materials.

- Shibboleth 2.0 uses SAML 2.0, so it should be much more compatible with commercial SAML implementations.   Liberty Alliance, Google Apps for Education, Cardspace, and ADFS have been tested.
- Installation has been simplified, particularly for IIS. There is no upgrader from Shibboleth 1.3, however; the differences are too fundamental.
- New IdP features

    - The installation process now automatically generates keys, certificate requests, metadata, *etc*.
    - The attribute resolver and filtering are now more flexible.
    - The IdP can now be integrated in JAAS, the Java Authentication and Authorization Service, rather than using the REMOTE_USER web server environment variable.
- New SP features
    - The installation process now automatically generates keys, certificate requests, metadata, *etc*.
        - Also, there is a standard URL that can be used to harvest an SP's metadata.
    - Metadata can be filtered.
    - There is support for protocols other than SAML 2.0
    - There is better support for clustering.
- Discovery services (*i.e.*, WAYF) can now be chained, and SPs can provide their own discovery services, based on metadata.
- Manageability
    - Much of the metadata can be updated without a restart.
    - The protocol has been simplified. It no longer requires a "call-back" for attributes. This should help with firewall interactions.
- Single Logout has been implemented, but there still a lot of issues.
- Benefits for UC
    - Broader commercial support for SAML 2.0
    - Possibility of a UCTrust discovery service?
    - Easier installation and better manageability.
- Rollout strategies
    - Shibboleth 2.0 is backward compatible with previous versions.
    - UCSD is starting with SPs. (They have ~130 of them.) Campuses with only a few SPs might want to upgrade the IdP quickly before they get more SPs.
    - We need to track what InCommon is doing.
    - We may want to form a group to look at single logout issues.

Token-Level / Two-Factor Assurance

- Demonstration of UCB's two-factor authentication - Dedra Chamberlin and Simon Litvak
    - Users register for a CalNetKey by answering AYSO's security questions.
    - When an application requires two-factor authentication, the user is presented with a virtual hexadecimal key pad in their web browser to enter their CalNetKey.
- Overview of NIST levels 3 and 4 - David Walker
    - HardwareTokenAssurance-2008-06-10.ppt
- Our next step will be to identify use cases for hardware tokens and two-factor authentication. Dedra Chamberlin and Eric Goodman volunteered to participate.

Shifting Attribute Release Decisions to End-Users

Albert Wu proposed implementing IdP-based software to allow users to access services without contacting their campus identity management office.

- Once the number of SPs increases, it'll be difficult to keep up with ARP maintenance.
- This will give end-users greater control over the release of their identity information, although it's not clear how many users will understand the impacts.
- Work along these lines has been done in Europe and Australia. We should track their progress.

Remote Registration Processes

Albert Wu described UCLA's registration process.

- When employees are hired, they are given a UID and told to register for their campus login.
- When a new employee registers, they are asked for their UID, birth date, and name.
- There was discussion of whether the UID provides enough linkage between identification (hiring) and registration to consider them to be a single process.
    - If it's not a single process, then UCTrust's remote registration rules would apply.
    - A maximum number of days between hiring and registration would help enforce a single process, but it's really a matter of risk tolerance on the campus's part.
    - Password resets are not mentioned explicitly in the UCTrust document. Is a password reset a registration process? Many campuses do not treat it as rigorously.
- The Authentify presentation that was held on May 12 was discussed. There wasn't any interest in pursuing their service.

Next Meeting

The next UCTrust Work Group meeting will be at UC Irvine (in September or October). UC San Francisco volunteered for the following meeting.

Day 2 - Shibboleth 2.0 Training

Tom Poage and Matt Elder led a workshop on the installation and administration of Shibboleth 2.0, based on their experience at the Shib InstallFest.

Attendees

Gordon Adams, UCDHS
Abhinav Admal, UCOP
Kalpa Barman, UCOP
Curtis Bray, UCD
Chris Callahan, UCD
Matt Elder, UCSD
Patrick Flannery, UCDHS
Jannelle Fong, UCSF
Martin Gelbaum, LBNL
Eric Goodman, UCSC
John Harris, UCD
Mike Helm, LBNL
Gary Jellis, UCDHS
Chris Lambertus, UCDHS
Warren Leung, UCLA
Munish Malik, UCOP
Dhiva Muruganantham, LBNL
Kiltesh Patel, UCDHS
Tom Poage, UCD
Brian Roode, UCI
Robert Schwartz, UCDHS
Hampton Sublett, UCD
Freddie Tai, UCSF
Josh Van Horn, UCD
David Walker, UCOP
Albert Wu, UCLA
Mukesh Yadav, UCSF
Kenneth Yip, UCSF
Xiaoling Zhang, UCLA