UAB Middleware Team & Support

IT Academic Computing
- David L. Shealy
- Jill Gemmill
- John-Paul Robinson
- Jason Lynn
- Zach Garner
- Ramesh Puljala
- Rajani Sadasivam
- Aditya Srinivasan
- Pravin Joshi
- Silbia Peechakara
- Yiyi Chen

Other IT Divisions
- Sheila Sanders
- Landy Manderson
- David Green

Acknowledgement of Support
- UAB Office VPIT
- NSF ANI-0123937 via SURA-2002-103 NMI Testbed Participant Shealy, Gemmill
- NSF EPS-0096193 Alabama EPSCoR Cooperative Agreement: Internet2 Initiative Griffin (PI), Cordes, Gemmill, Graves, Hancock, Shealy
- NSF ANI-022710 ViDe.Net: Middleware for Scalable Video Services for Research and Higher Education. Gemmill (PI), Chatterjee, Johnson, Verharen
UAB Benefits from NMI

- Enhanced Integrated Directory Services, based on eduPerson, eduOrg, LDAP Recipe
- WebLogin service is rolling out, based on Pubcookie
- Grid Computing service is rolling out, based on Globus
OUTLINE

- Integrated Directory Services
- WebLogin using Pubcookie
- Grid Computing using Globus
Historical Background

1983-90:
- Implemented Access Control Facility (ACF2) security software on mainframe & database of eligible users
- Campus Directory
- BITNET; SURAnet; Internet mailhost

1991-99:
- UIUC/CCSO qi directory online for “alias@uab.edu” e-mail forwarding with web page registration where information provided from merge of employee and student databases
- Setup LDAP directory to mirror qi directory
- Phonebook alias used for web sign-in to authenticate SMTP relay
Historical Background

2000-02:

- Dr. Clair Goldsmith hired as CIO / VPIT
- LDAP committees formed; and then recommendations from LDAP and Win2K Task Force were implemented
- UAB Alias => BlazerID
- VPN implemented with qi authentication
- Library’s Virtual Desktop interfaced to qi
- ResNet online using qi authentication
UAB LDAP Committees

- Propose useful attributes
- Define “continuums of association” and when to add, remove, or inactivate people in LDAP directory

<table>
<thead>
<tr>
<th>Employees</th>
<th>Students</th>
</tr>
</thead>
<tbody>
<tr>
<td>Job applicant</td>
<td>Admissions applicant</td>
</tr>
<tr>
<td>Job offer extended</td>
<td>Accepted for enrollment</td>
</tr>
<tr>
<td>Hired</td>
<td>Enrolled</td>
</tr>
<tr>
<td>On leave</td>
<td>Not taking classes</td>
</tr>
<tr>
<td>Terminated</td>
<td>Dropped out</td>
</tr>
<tr>
<td>Retired</td>
<td>Graduated</td>
</tr>
</tbody>
</table>
How NMI Helped

- Existing UAB LDAP schema was arbitrary, out-of-date, and did not have important attributes useful to educational institutions, such as, courses taught or enrolled in.

- NMI eduPerson gave opportunity to add additional data to campus LDPA for support of new applications.
LDAP Milestones – Aug 2002

- New schema put into production
- Passwords sync in real-time between qi and LDAP
- Follow eduPerson and Recipe 1.0, which were LDAP Committee recommendations
- Group local attributes under uabPerson based on eduPerson, such as, courses taken or taught
- Provide for non-person (entity) look-up
- Implement new base root per Recipe, but old still works
- Include passwords & “unlisted” users so that WebCT and other applications can use LDAP directory
LDAP 2002 - 03

- Created BlazerID Central
- New web screens sync BlazerID and password between qi, LDAP, AD, Novell.
- All authentication done through secure services
- Strong passwords enforced
- Microsoft Active Directory synchronization
- Central Exchange 2000 mail service
- Oracle HR/Finance sign-on
- Unix authentication (PAM)
- Wireless sign-on
- Class e-mail distribution & bulk/broadcast e-mail
Where UAB is Today

- Single authoritative directory
  - Single management point for
    - Creating BlazerID
    - password resets
    - user account creation/deactivation

- Implemented Groups, commObject, latest NMI schema recommendations
  (eduPerson, eduOrg, LDAP Recipe)

- Even more applications use LDAP
UAB Authoritative Directory

- Employee Hired
- New Student
- Student Entered at Admission
- 1-30 Days for Employee Record Entry
- HR System
- Once Every 24 Hours
- LDAP/BLAZERID RECORD
- Cycle Dependent on User
  - User goes to Web site and creates BlazerID and password
  - Wireless (Realtime)
  - WEB CT
  - Virtual Desktop (Realtime)
  - ResNet (24 Hours)
  - AD Account (Realtime)
  - STEPS (One Hour?)
More on LDAP-enabled Apps…

- Authentication & Authorization Services
  - Authentication – Identifying people
  - Authorization – Allow proper access
- Download Software Licensed to UAB Community
- Unix Account Management
Application: Download Software
Licensed to UAB Community

<table>
<thead>
<tr>
<th>Implementation Details</th>
<th>Problems Solved</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client - Browser</td>
<td>Session Management</td>
</tr>
<tr>
<td></td>
<td>Secure Socket layer (SSL) for Authentication but not for download</td>
</tr>
<tr>
<td>HTTP server</td>
<td>Collecting the authenticated user’s group information for making a policy decision</td>
</tr>
<tr>
<td>Application container</td>
<td>Customizable timeout mechanism during login</td>
</tr>
<tr>
<td>Backend connectivity</td>
<td></td>
</tr>
<tr>
<td>Backend</td>
<td></td>
</tr>
</tbody>
</table>

JSP with embedded HTML
Apache
Tomcat version 4.0.3 – JSP, Servlets
JNDI
LDAP

http://www.uab.edu/it/software/index.html
Application: Unix Account Management

- Tools
  - Enterprise LDAP Infrastructure
  - OSF Pluggable Authentication Module (PAM) Architecture
  - PADL Software’s LDAP module for PAM on Unix Systems (pam_ldap)

- [http://www.uab.edu/it/academic/Presentations/presentations/authentication-timgroup.ppt](http://www.uab.edu/it/academic/Presentations/presentations/authentication-timgroup.ppt)
OUTLINE

- Integrated Directory Services
- WebLogin using Pubcookie
- Grid Computing using Globus
What is WebLogin?

- WebLogin allows users with standard web browsers to authenticate to web-based resources across many web servers using a central authentication service with username & password.
- WebLogin is moving towards a production service at UAB
Overview of WebLogin

Features
- Single Sign-On
- Consistent Login Interface and Experience
- User Security
- Independence for Web Server Administrators

Components
- User-Agent (Web Browser)
- Authentication Service (e.g. Campus LDAP Server)
- Uses Pubcookie
  - Application Server (Web Server Plug-in to protect resource)
  - Login Server
… What is it?


- Uses a standalone login server and modules for common web server platforms like Apache and Microsoft IIS.

- Uses these components with existing authentication services (like Kerberos, LDAP, or NIS) into a solution for single sign-on authentication to websites throughout an institution.

- At UAB, pubcookie authenticates username & password (“BlazerID”) with LDAP directory.
Using Pubcookie

- Install a pubcookie Apache or IIS module on each web server to be protected
- Put protected information in a directory protected by this module
- User’s attempts to access the URL
- Pubcookie redirects them to login if they have not today; otherwise cookie credential is checked
Pubcookie Limitations

- All authenticated users are equal; useful for resources available to entire campus only
  - Library materials
  - Licensed software
- Usually, the target population is smaller
  - Students in a particular school or class
  - Faculty, staff, students in School of Engineering
User’s First Login Perspective

1. User tries to access secure webpage/application/document.
2. User is presented with UAB login screen.
3. User supplies BlazerID and Password (over a secure connection).
4. Upon successful credentials, user sees the secured webpage & application doc.
User’s Perspective After Initial Login

1. User tries to access secure webpage/application/document.
2. User sees the secured webpage/application/document.
WebLogin Demonstration

**Servers**
- metric.it.uab.edu (Apache Webserver 1.3.27)
  - Sample 01
  - Sample 02
  - Sample 03
  - Sample 05
- polka.it.uab.edu (IIS Webserver 5.0)
  - Sample 04
  - Sample 04

**Demonstration Webpage**
- http://lab.ac.uab.edu/node/view/145
- http://lab.ac.uab.edu/node/view/145
Modifying Existing Applications

- The Problem
  - Many Web Applications create their own authentication system
  - So, the user needs a username/password for each application

- The Solution
  - Pubcookie-enable those applications to use centralized username/password
Modifying Existing Applications

- Two Pubcookie-enabled two open source applications
  - Bugzilla (Written in Perl)
  - PHPWebsite (Written in PHP)
- Similar changes were required for both applications
Modifications

- Remove old user login/password web form
  - Instead, Pubcookie authenticates the user
  - Authenticated users can proceed if they also have a Bugzilla or PHPwebsite account

- Change behavior of “Log Out” and “Change Password” pages
Future Directions

- Modifying Pubcookie to support Client-Side SSL Certificates
  - Enables authentication of users without a user remembering username/password
- Modifying Pubcookie to support PAM for the authentication mechanism
  - PAM is a standard system for flexibly using a large number of authentication systems.
OUTLINE

- Integrated Directory Services
- WebLogin using Pubcookie
- Grid Computing using Globus
UABGrid Software Infrastructure

- Resource Monitoring: GISS, SCMS, Ganglia...
- UABGrid Services: Globus, MPICH-G2, Condor Pool...

User ID Management

- Shell/GUI Interface
- Proxy Management
- UABGrid Certificates
- BlazerID

Academic Computing Resources
- Computer Science Resource
- Engineering Resource
- Science Resource

UAB DataGrid
UABGrid Architecture

http://uabgrid.uab.edu/
One Time Registration
UABGrid Summary

Web Grid Client Environment → UABGrid Security Infrastructure → Grid Services

Hardware Resource... of others

Other Data Storage Systems

Hardware Resource... of Academic Computing

UABDataGrid Libraries, Applications, User Space, ...

Application Interfaces

GridID Management

Usage Management
Summary of Benefits from NMI

- Enhanced Integrated Directory Services, based on eduPerson and LDAP Recipe
- Campus WebLogin service is rolling out, based on Pubcookie
- Grid Computing service is rolling out, based on Globus