User-Centered Authentication: LDAP, WRAP, X.509, XML...

Implementing LDAP for Single-Password Access to Campus Resources

Layne Nordgren
Director of Multimedia Services/Library Systems
Pacific Lutheran University
Tacoma, Washington

Presentation Pathway

- Driving Forces for User Authentication
- Implementing LDAP
- Enabled Applications
  - Campus Online Services
  - eReserves
  - Licensed Content
  - Streaming Media
- Next Steps

About

- Comprehensive Private University
  - 3,550 FTE
  - Liberal Arts
  - Professional Schools
- Residential Campus
  - Off-Campus Students
  - Part-Time Professionals
- Information Resources
  - Major Infrastructure Development Push (1997+)
  - Goal: Populate the Network with Resources

Authentication Dilemmas

- Where Are You?
  - On Campus
  - Off Campus
- Who Are You?
  - Generic Password
  - Individual Password

Problems to Address

- Selection of UID data source
- Mechanism for UID adds, deletes, updates
- Distribution of UID and passwords for each resource to every user
- Preventing sharing of UID and passwords
- Maintaining publisher-defined authentication schemes for each service

Authentication as Enabler for User Services

- Campus Services
  - ResNet Registration
  - Laptop & Kiosk Access
  - Calendar Server
  - Protecting Web Courses
  - Protecting Threaded Discussions
- Library Needs
  - eReserves
  - Access to licensed resources
Imagine adding a variety of information about a new user through a single interface only once, and immediately the user has a Unix account, an NT account, a mail address and aliases, membership in departmental mailing lists, access to a restricted Web server, and inclusion in job-specific restricted newsgroups. The user is also instantly included in the company’s phone list, mail address book, and meeting calendar system. When a user leaves, access can be disabled for all of these services with just a single operation.

Bruce Markey
A System Administrator’s View of LDAP

Lightweight Directory Access Protocol

Recipe*
- 1 Tsp. DIT planning
- 1 Tbsp Schema design
- 3 oz. configuration
- 1000 lbs of data

* Michael R. Gettes, Georgetown University
A Recipe for Configuring and Operating LDAP Directories

PLU’s LDAP Hierarchy

Distinguished Name:
DN: uid=nordgrle, ou=Personnel, o=plu.edu

Object Class: organizationalPerson
ou = Personnel
ou = Student

Object Class: inetOrgPerson
uid = nordgrle

Toward the Goal of One Password...

Maintaining and Updating User Data
- Custom Perl scripts using PerlLDAP
  * Updates LDAP from Banner database nightly
  * Perl-based Server with both Web and UNIX shell interfaces.
- When user changes password...
  * server first changes LDAP entry
  * Netscape Web, Calendar, and ColdFusion servers authenticate via LDAP
  * root-level access changes UNIX password
  * UNIX shell password controls access to POP3/IMAP e-mail
Restricting Access to Web Resources

- LDAP groups created and populated with users from Banner
- Restricted access on Netscape Enterprise Server via administrative server
  - ...protected directories
  - .plu file extensions
- When browser requests a restricted file or directory, user is queried for LDAP username/password

PLU Campus ePass Enabled Services

- Directory Services (Email)
- ResNet (Perl scripts/MySQL)
- Laptop/Kiosk Login
- CorporateTime Calendar
- eCourse (Blackboard)
- Threaded discussions (WebBBS)
- Voting, surveys, order forms (ColdFusion, Access)

eReserves

Authentication of Licensed Resources

- Always Authenticate Switch
- Location Check (IP)
- Patron Check (LDAP)

Linking Journal List with Authentication

- Database-driven Front-End to Licensed Resources
- Ranges of coverage “front-loaded”
- Authentication management database
- Persistent URL’s
Implementing LDAP for Single-Password Access to Campus Resources

Layne Nordgren, Pacific Lutheran University

Technical Glitches
- First password change
  - "Old" users
  - New accounts
- Documentation & Support
  - Computer Support
  - Reference Services
  - Web Support
  - Electronic Reserves
- Different authentication schemes & scripts
- Content Vendor Support
  - Unpredictable vendor URL and authentication changes
  - Spotty technical support

Streaming Media

The Tangled Webs We (They?) Weave...

Example:
- Search EBSCO for ERIC documents
- Follow link to EDRS E*Subscribe via ERIC

Next Steps
- Refine authentication scripts & variables
- Add more vendors
- Implement finer scale web access
  - Web pages
  - Privilege sets
- SSL for authentication check?
- NT domain synchronization with LDAP

References
- A System Administrator’s View of LDAP
  http://people.netscape.com/bjm/whyLDAP.html
- A Recipe for Configuring and Operating LDAP Directories
  http://www.georgetown.edu/gia/internet2/ldap-recipe/
- PerLDAP
  http://developer.netscape.com/docs/articles/directory/perldap_central.html
- OpenLDAP
  http://www.openldap.org/
- OpenLDAP Administrator’s Guide
  http://www.openldap.org/doc/admin/

Contact Information & Links

Layne Nordgren
nordgrle@plu.edu
253-535-7197

Online Services Menu:
  http://www.plu.edu/online
Journals at PLU:
  http://www.library.plu.edu/journals
Presentation Handout: