



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

Implementing LDAP for Single-Password Access to Campus Resources

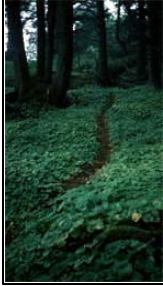
Layne Nordgren
 Director of Multimedia Services/Library Systems

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



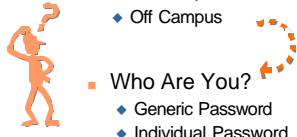

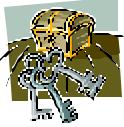
About

- 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

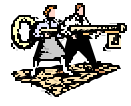




Problems to Address

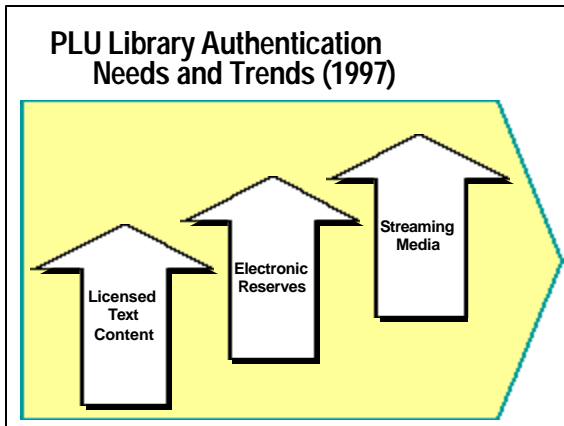
- Selection of UID data source
- Mechanism for UID adds, deletes, updates
- Distribution of UID and passwords for each resource to every user
- Preventing sharing of UID and passwords
- Maintaining publisher-defined authentication schemes for each service



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

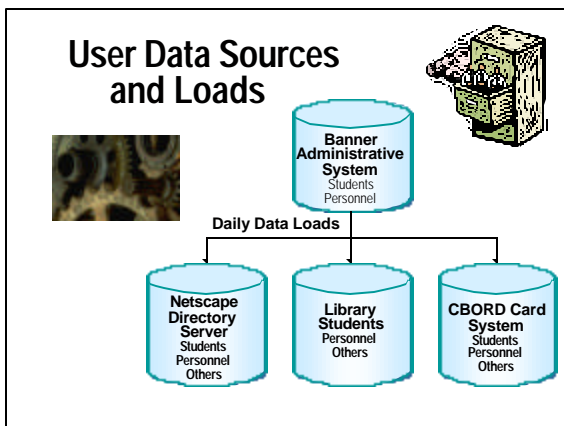
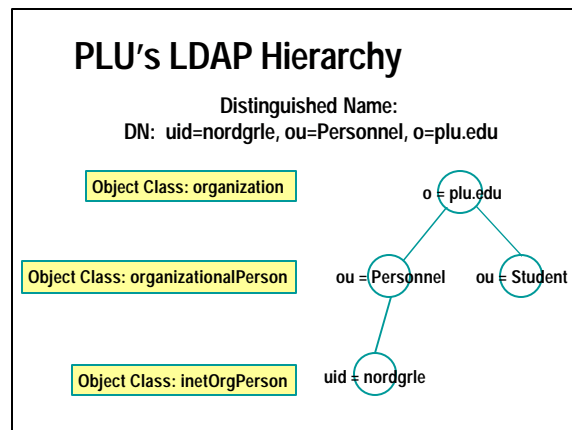
LDAP Lightweight Directory Access Protocol

Recipe*

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

- Open standard for storing and retrieving directory information (RFC's 1777 and 1778)
- Client queries LDAP server and if authenticated allowed to retrieve, store, or update information based on level of access rights
- Uses fast-access object-based hierarchies of entries

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




Toward the Goal of One Password... ePass.


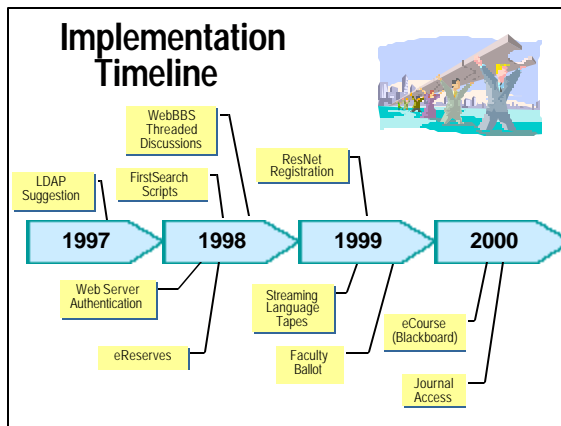
Maintaining and Updating User Data

- ◆ 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



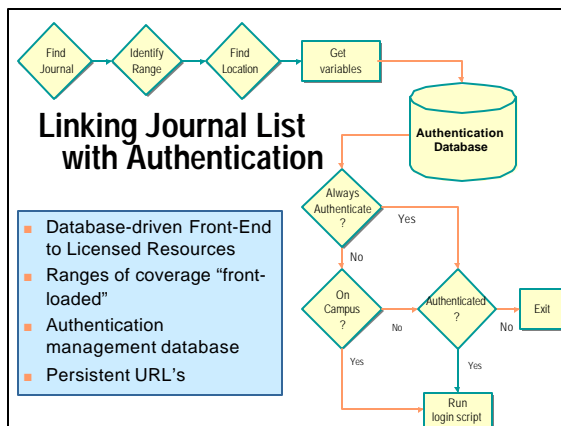
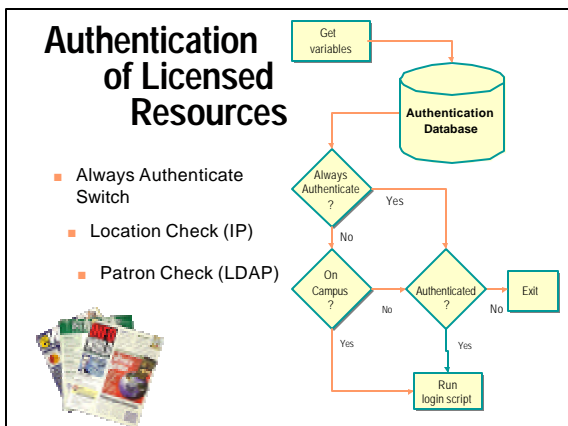
- LDAP groups created and populated with users from Banner
- Restricted access on Netscape Enterprise Server via administrative server
 - .../protected directories
 - .plu file extensions
- When browser requests a restricted file or directory, user is queried for LDAP username/password

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

Streaming Media



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

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

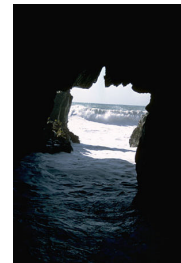
Example:

- ◆ 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/giia/internet2/ldap-recipe/>
- *PerlLDAP*
http://developer.netscape.com/docs/articles/directory/perlldap_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>

eReserves:

<http://www.plu.edu/~ereserves>

Journals at PLU:

<http://www.library.plu.edu/journals>

Presentation Handout:

<http://www.plu.edu/~libr/asisnational2000/handout.pdf>