LDAP and Directories

Jim Leous
leous@aset.psu.edu
http://aset.psu.edu/leous/

Information Technology Services
Penn State University
What LDAP is

- LDAP is the Lightweight Directory Access Protocol, a protocol for accessing on-line directory services. Most vendors implement version 3 or LDAPv3 which is specified in RFC 2251.

- While the term “LDAP Directory” is a misnomer (since LDAP is really just the directory access protocol), it is used often to refer to both the LDAP method for accessing the directory and the directory itself.

- At Penn State, the LDAP server I will be referring to is an IBM SecureWay Directory Server (this name will change ITDS).
What LDAP is NOT

- An Authentication Server/Service
- A phone directory
- A one-to-one replacement for Ph/Qi
What is a Directory?

A directory or more properly directory services organizes information into a logical and accessible structure.

- It provides a database in which to store information about network–based resources.
- This can include printers, servers, networks, filesystems, not just users.
- It is a way of locating network resources.
How Does LDAP Work?

- Directory consists of entries each of which is uniquely referred to by a distinguished name.
- Each entry consists of a set of attributes about that entry.
- Attributes are organized in Object Classes.
- A set of object classes is organized into a Schema or data model or structural description.
- An LDAP query can authenticate to the directory (called a bind) or access it anonymously.
About Attributes

- Attributes are categorized into “Must Have” or “May Have”
- Attributes can be specified to be “Multivalued” or “Single valued”
- Attributes can be protected at different levels
- Attributes are organized into Object Classes
How Do We Get Them?

Much thought went into the processes by which these attributes are collected. Information/attributes are coordinated through the CACTUS system.

- Student Information from Registrar
- Staff Information from OHR
- Account information from ITS Accounts Office
- Hershey Medical Center/College of Medicine
- University Libraries
Which Object Classes?

- psuPerson
- eduPerson
- inetOrgPerson
- organizationalPerson
- person
- top
What is eduPerson?

- **eduPerson** is an Object Class which is specified by the Internet 2 Middleware working group. It consists of a list of attributes which enables inter-institutional cooperation between differing institutions of Higher Ed.

- Penn State people involved in the eduPerson specification include Renée Shuey, Jim Leous, Jim Vuccolo, Bob Fowles, and Bob Walters.

- Penn State had the first instance of eduPerson in our production LDAP directory.
Why eduPerson Matters

- eduPerson uniquely specifies some of the attributes which all Internet 2 schools are migrating toward.
- eduPerson attempts to make uniform descriptions and attributes which vary greatly among institutions.
- eduPerson prevents each institution from “reinventing the wheel”
- eduPerson provides some of the middleware infrastructure which will enable more efficient collaboration and cooperation between schools.
Directory Enabled?

- Directory Enabled Applications use something in the directory to alter or personalize the application.
- Authorization can result based on what someone does rather than who someone is.
- Access can be controlled via a Penn State protected attribute and given to an outside vendor without divulging personal information.
Where Do We Use LDAP?

- Napster
- The Penn State Portal
- Oracle Calendar Manager
- WebMail
- MRI Seminar Registration
- WebAssign
Resources

- http://ldap.psu.edu/
- http://www.psu.edu/ldap/