LDAP related development at Carnegie Mellon

- OpenLDAP and SQL
- LDAP everywhere
- Cyrus SASL development
Currently, **metadir.andrew.cmu.edu** is an OpenLDAP 2.0 with ldbm

- Slurpd replication is used to ~4 identical replicas
- No foreign key constraints, LDAP interface is “hard” for certain users
- Plus, we have an Oracle site license
LDAP and SQL (2)

• Problems with SQL backend
  – How to do replication if we want to write directly to the database
  – How to make the database schema good for LDAP but also usable for other access

LDAP everywhere

• Administrative applications need information from data stores

• How many access protocols should any one programmer need to use?

• Lots of applications have inherent lists of resources (users, mailboxes, machines, etc.)

• Privilege delegation/authorization
  – we want help desk people to be able to check quotas, but not modify them
LDAP everywhere

• PTS backend is an example we've implemented
  – Exports AFS users and groups, read-only
  – Hopefully will ease our group transition
• Where do we run the LDAP server?
• How tightly do we integrate the backend to the instrumented application?
Cyrus SASL development

• Bug fixes, bug fixes, bug fixes
  – DIGEST-MD5 DES fixed (finally!)
  –

• SASL API standardization
  – Allow interactions in server API to support async programming models
  – Library/application interaction changes?
  – Move sasl_set_alloc() into callbacks?
Cyrus SASL auxprops

- SunONE (Chris Newman) fixes to code
- auxprop API not well understood
  - Server-side API for retrieving user attributes
  - Most popular is “userpassword”--cleartext password
  - More general so that expensive lookups can get everything a server might need
- Currently, the “sasldb” plugin is the only auxprop plugin we ship
An LDAP auxprop plugin?

- OpenLDAP ships with one possible auxprop implementation
- Lots of interest in an LDAP auxprop for things like Cyrus IMAP (get passwords, groups, etc.)
- Generic auxprop plugin that communicates to a separate process
- Process caches connections, handles uid/dn mapping
Cyrus SASL

- I'll take any questions
- ... compliments
- ... complaints
- ... abuse
- ... whatever