LDAP and Active Directory: Working Together to Manage Identity

Harold Esche and Jeremy Mortis
Today’s Agenda

2. The Problem in Context
3. Identity and Identifiers
4. Identity Repositories
5. Provisioning
6. Application Interfaces
7. Next Steps
8. Q & A
The One Minute
Identity Management Assessment™
North America
North America
• 5th largest city in Canada
  – Nearly 1 million People
  – 16% population growth in last 5 yrs
• 2nd most Head Offices in Canada
• Highest Education Level in Canada
  – 69% post secondary education
The University of Calgary

- 8th largest University in Canada
- Calgary’s 4th largest employer
- 28K FTE students, 5K faculty/staff
- $781M annual budget,
- $247M sponsored research
- Students from over 80 countries
- 15 Faculties, 53 Depts, 30 Institutes
Academic Plan

Principles

- To enhance the learning experience
- To enhance research, discovery and creativity
- To promote multi-disciplinary inquiry
- To give back to the community

Priorities

- To be leaders and innovators in energy and the environment
- To promote understanding of human behavior, institutions and cultures
- To create technologies and manage information for a knowledge society
- To advance health and wellness
Campus Technology Vision

Connected Campus

“Enabling the learning, research, administrative, and community goals of the UofC, through the effective and efficient use of technology; allowing people to access information they need, at the required time, in the desired location, and in the appropriate format”
Every system had a username/password:

- SIS, HR, Finance, UNIX, linux, email, calendar, portal, labs, desktops, faculty-run systems, telephone, departmental systems, Continuing Education, Campus Recreation, file servers, ...
Symptoms & Outcomes

– Customers were confused and annoyed.
– We spent a lot of time helping people with identity and password problems
– We were fearful that we had significant security risks
– The complexity was impacting implementing our vision!
Nirvana

One easy-to-remember and completely secure identity and credentials that allow a user to access everything they should be able to access.
“Any scheme that depends on a person having one and only one identifier is doomed to fail”
What is identity?

Is your identity:
3. You as a physical person
4. You filling a particular role
5. An arbitrary collection of stuff
Personal Identifiers
Identifier Realms

The world in which an identifier has meaning:

- The payroll system
- The email system
- The portal
- A government agency
- etc.
Identifier Types

• Content based (maxwellj)
• Content free (02039093)
• Self-chosen (bluesky@yahoo.ca)

• Internal versus external
Within a Realm

Multiple identifiers occur due to:

- Weak system role capabilities
- Mistakes in assigning identifiers
- Identity theft
- Need to retain old e-mail address
- Delegation
Realms can overlap or encompass:

- School of Engineering
- School of Medicine
- University of Calgary
- Campus Alberta
- Calgary Health Region
Multiple identifiers occur due to:

- Fear of “Big Brother”
- Different syntactical rules
- Lack of trust
More bad news

“Any scheme to consolidate all identity information into a single system is doomed to fail”
Our approach

• Accept the fact that there will be multiple identities and identifiers associated with a person
• Attempt to link all the identifiers together
• Let applications pick the one they want
• Facilitate access to associated information in other systems
Centralized IAM model

- Application
  - wongd + password
  - Permissions
  - wongd + password
- IAM
- IAM DB
- Payroll DB
- Request
- Result
- Daily loads

- wongd?
- dennis.wong?
- d_wong?
- 03818732?
- wongmeister?
Distributed IAM model

daisy.sanchez + password

Application

Identity

IAM

Payroll IAM

Payroll DB

IAM DB

Request

Result

permissions

dsanchez

identities

daisy.sanchez + password
The Identity Repository

• Built on OpenLDAP
• Links identifiers together (some of which occur multiple times)
• Contains basic personal information synchronized from other systems
• Allows applications to store data
Repository Contents

- Identities and linkages
- Commonly used items
- Stuff not readily accessible
- Stuff with no other home
- Stuff published by applications
LDAP Trees

- **o=ucalgary.ca**
  - **ou=accounts**
    - UNIX/Windows accounts
    - e.g. mortisj
    - 50,000 entries
  - **ou=people**
    - Students, staff, and others
    - e.g. 42003020
    - 800,000 entries
  - **ou=eID**
    - Portal accounts
    - e.g. jeremy.mortis
    - 30,000 entries
Active Directory

```
ad.ucalgary.ca

  dc=campus
    ou=users
    ou=itlabs
      ou=computers
  dc=admin
    ou=users
    ou=chem
    ou=computers
  dc=...
```
LDAP/AD Synchronization

- Same namespace as UNIX accounts
- AD accounts created automatically
- Passwords synced at setup and change
- Other data synced daily
Password Synchronization

• Impossible to copy from LDAP to AD
• Single point of password change
• First sync disables PW changes in Windows
• Ability to exclude users from sync
• Web tool to resync without changing
• Commercial products too expensive
Provisioning

• Anybody can have a portal identity
• Self serve IT account registration
• UCID’s created by business systems

• De-provisioning is a problem at Universities
Linking Identities

Method 1 – Self Registration
• User provides their identifiers themselves
• Ownership confirmed with system data, e.g., password, birthdate

Method 2 – System Owner
• Link new identifiers to eID at time of issue or after the fact
API’s

- LDAP
- Virtual LDAP
- Active Directory
- SSO (Single Signon)
- Authent service
- PAM
- Gina
Application Interfaces

e-mail       UNIX       wireless
uPortal       Blackboard   Peoplesoft
cognos       dialup
.htaccess       Webdisk    DSpace
Windows logon       Citrix
.NET web applications
Java web applications

and others...
Next steps

- Capture additional identities
- Federated identities
- Additional application integration
- Identity equivalence
The Path to Nirvana

“A journey of a thousand miles begins with a single step.”

- Campus Portal is both the glue and the carrot
- Create flexible standards
- Accept that the solution will never be perfect
- You can do a lot to address the problem without having to buy an expensive commercial package
Questions?
Contact Us

Harold Esche (esche@ucalgary.ca)
Jeremy Mortis (mortis@ucalgary.ca)