Mac OS X Authentication

Case Study

Darren R. Davis
M.S. Computer Science
Macintosh Specialist
University of Utah
Student Computing Labs
Presentation Overview

• Goals and History
• Authentication System Components
  – Student, Faculty and Staff Database
  – University Network ID System
  – Authentication with Kerberos
  – Enterprise Directory
• Client Setup and Operation
Definitions

• Authentication
  – Process of verifying the identity of a user

• Authorization
  – Determining what the user can access

• Kerberos
  – A network authentication protocol

• Enterprise Directory
  – A network database optimized for searching and used to store identity
Definitions

- **KDC**
  - Kerberos Key Distribution Center
- **LDAP**
  - Lightweight Directory Access Protocol
- **NID**
  - Network Identification for user
    - name
    - password
Student Computing Labs

- Provides Computers for Student Use
  - Macintosh OS X Clients
  - Macintosh OS 9 Clients
  - Windows 2000 and XP Clients
Authentication Project Goals

• Need users to authenticate
  – Control access to computing resources
  – Problems with non-authorized use.

• Need to manage user information
  – Single identity and password

• Need to use existing University infrastructure
  – Campus NID (Network ID) system
Potential Issues

- Authenticated Classrooms
- Guest Users
- Network Disruption
- User Privacy
  - FERPA (Family Education Rights and Privacy Act)
- Integration with campus infrastructure
Timeline

- Project Started December 2001
  - Test environment to work out issues
- Student Computing Labs
  - Several lab locations
  - Set dates to convert labs
- Production Deployment
  - Gradual and incremental roll-out
  - Labs and one classroom Jun - Aug 02
Support Issues

• Consulting Staff Primary Support
  – Aided by full-time staff

• Documentation
  – web based

• Training

• Tools
Staff Tools

- Password Reset
  - people forget their passwords
- Guest Accounts
  - Need to support temporary accounts
User Tools

• Do I have an account
  – NID Discovery

• Account Administration
  – Get NID Password
  – Change NID Password
Network ID Tools

Network ID Tools

Help
- What is a Network ID?
- Login Problems
- Help Desk

Students
- Web Based Email
- Class Registration & Schedules
- WebCT
- Bookstore
- Academic Calendar
- More Student Resources

University
- Home Page
- Colleges & Departments
- Calendar of Events
- Campus Directory
- Campus Map
- Search
- Disclaimer

Need to set up an account?
Forgot your Network ID or password?

Questions, problems, and/or comments please contact the Campus Help Desk at (801) 581-4000 or helpdesk@utah.edu Department of Network & Communication Services, 601 Black Hill Way, SLC, UT 84108. — University of Utah —
Network ID Discovery Tool

Identification

Last Name: 

U of U ID Number: 

PIN: 

The PIN is not the same used to access the Campus Information Systems (student records or employee web systems). Please call the Campus Help Desk at 581-4000 for a PIN that you can use.

Continue  Quit

Questions, problems, and/or comments please call the Campus Help Desk at (801) 581-4000
Department of Network & Communication Services, 606 Black Hawk Way, SLC, UT 84108
--- University of Utah ---
Publicity

- Signs
- Web Pages
- FAQs
- Complaint Handling
System Implementation

- Existing Infrastructure
  - Faculty, staff and student database
    - PeopleSoft
  - University Network ID system (NID)
    - Active Directory
- Kerberos
- Microsoft Active Directory
- Mac OS X Client Setup
PeopleSoft Managed by HR

User Added to PeopleSoft
NID Data Migrates to SCL
SCL Authentication Overview

Kerberos Server

Kerberos

Active Directory

Directory Server

Clients

KERB

KERB

LDAP

AD API

KERB

X

Window

Mac

9
Guest System

- Kerberos Server
- Directory Server
Guest System

• To provide for one-day lab use

• MySQL Database
  – Management and Tracking
    • Account Status
    • Date and Time Data

• Data Migrates
  – Active Directory
  – Kerberos
Ticket based authentication developed at MIT (many web sites)
Many applications support it for authentication and authorization
Realm = UTAH.EDU
Three KDCs
- Secured and replicated
- Configured for fail-over
Why Kerberos?

• Local authentication
• Kerberized applications
  – ssh, fetch, mail, printing, etc.
• Kerberized services
  – AFP, login, print accounting, etc.
• Kerberized OS integration
• Years of experience and use!
Enterprise Directory

• Microsoft Active Directory (AD)
  – Why Active Directory?
  – Because we manage Windows 2000 clients
  – Use the enterprise directory we have
• Could switch to another directory
Setting up Active Directory

- Install Windows 2000 Server
- Applied patches and updates
- Setup domain controller
- Extend directory schema
- Automated adding users
  - PERL script
Extend the Schema

• The schema represents the structure of the directory
  - We needed it to contain Mac OS X (UNIX) information
  - So, we added schema information for UNIX using AD4UNIX, but other schema extensions tools will work
  • Microsoft Windows Services for UNIX
Active Directory Management

• Five domain controllers
  - located adjacent to each lab

• User information updates
  - University NID system
  - Guest account system

• All users are populated in a single container
What is stored in AD?

- Minimally populated
  - User ID ('the-user')
  - UID (Unique ID #)
  - GID (Group ID #)
  - Home Directory Path (/User/Home)

- We DO NOT store passwords in AD
  - For security reasons
  - Password field set to random value
Example Directory Entry

- gidNumber: 500
- loginShell: /bin/false
- msSFUHomeDirectory: /Users/Authenticated User/
- msSFUNName: the-user
- syncNisDomain: scl
- uidNumber: 1234567
Mac OS X 10.2.x Clients

- All Mac OS X clients running Jaguar
  - Currently Mac OS X 10.2.5
- Kerberos client (built in)
- Directory configuration (built in)
  - Apple Directory Access Utility
Enabling Kerberos Login

• Must edit XML document
  – /etc/authorization

• Several configuration options
  – Kerberos authentication required for login
  – Post-login Kerberos authentication

• Apple support documents
  – 107153
  – 107154
Kerberos Extras

- Apple does not include support for Kerberos-using applications like Eudora and Fetch
- Get Mac OS X 10.2 Kerberos Extras from MIT
  - This gives support for some applications to use the Kerberos authentication system
- No support for Screen Saver and Keychain, but coming from Apple
Mac OS X Directory Setup

- Apple supplied utility
- “Directory Access”
Directory Access

The image shows a window for configuring directory access services. The window includes tabs for Services, Authentication, and Contacts. The Services tab is currently visible, showing a list of available services and their versions:

- AppleTalk: 1.0
- BSD Configuration Files: 1.1
- LDAPv2: 1.5
- LDAPv3: 1.5.3
- NetInfo: 1.5.1
- Rendezvous: 1.0.1
- SLP: 1.0
- SMB: 1.0

A check mark indicates which services are enabled. The bottom of the window has options to configure the settings, revert changes, or apply them.
Configure LDAPv2

<table>
<thead>
<tr>
<th>Enable</th>
<th>Name</th>
<th>Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>☑</td>
<td>U of U</td>
<td>dc1-mmcc.scl.utah.edu</td>
</tr>
</tbody>
</table>
LDAPv2 - Identity

Name: U of U
Address: dc1-mmcl.scl.utah.edu

Examples
LDAP-My Company
ldap.example.com
or 192.168.100.12
LDAPv2 - Records

Record Type: Users
Maps to: ou=campus, dc=scl, dc=utah, dc=edu
LDAPv2 - Data

Data Type:
- RealName
- UniqueID
- PrimaryGroupID
- NFSHomeDirectory
- RecordName

Maps to:
- msSFUName
Authentication
Contacts
Mac OS X Login Process

Login passes user name to Directory Server
Mac OS X Login Process

If user is in the Directory, user attributes are returned
Mac OS X Login Process

Kerberos Client has user info, so authenticate

Kerberos Server

Direction Server

Kerberos Client Plug-In to Login

Mac OS X Login
Mac OS X Login Process

Yes! user is authentic

- Mac OS X Login
- Kerberos Client Plug-In to Login
- Kerberos Server
- Directory Server
Mac OS X Login Process

Directory searched again for user attributes
Mac OS X Login Process

Login gets remaining user attributes
Mac OS X Login Process

User is logged in and attributes used for user identity
Future Goals

- Finer Control for Managed Groups
  - Restrict certain software
  - Restrict certain machines
  - Restrict user services

- Pay for Print based on Authentication

- Managed Disk Space for users
  - minimum fixed limit (quota)
  - lease for extra space
Questions and Answers