Mac OS X Authentication

Kerberos and LDAP Issue

Darren R. Davis
Macintosh Specialist
University of Utah
Student Computing Labs
System Implementation

- Kerberos
- Enterprise Directory
  - Using LDAP to search
- Mac OS X Client Setup
  - Kerberos
  - Directory Access
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
LDAP Directory

- Lightweight Directory Access Protocol
- Directories are special network databases optimized for searching
  - Think of a phone book
  - You have name, search, and find number
  - Used for storing user information
    - SCL does not store passwords in the Directory
Mac OS X 10.2.x Clients

- All Mac OS X clients running Jaguar
- 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
Mac OS X Directory Setup

- Apple supplied utility
- “Directory Access”
- Configure LDAPv3
Mac OS X Login Process

Login passes user name to Directory Server

A default user created just for LDAP is used to authenticate to Directory to get user information.
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
Mac OS X Login Process

Yes! user is authentic
Mac OS X Login Process

Directory searched again for user attributes

LDAP BIND Attempted!
Meaning the Username and Kerberos Password sent to Directory Server.
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
Solutions

• Use SSL for all LDAP information
  - Everything is encrypted so OK

• Configure Directory Access to use AuthenticationAuthority attribute
  - Set to an existing Directory attribute that always has a value!
## Directory Access

### Services

<table>
<thead>
<tr>
<th>Enable</th>
<th>Name</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>AppleTalk</td>
<td>1.0</td>
</tr>
<tr>
<td></td>
<td>BSD Configuration Files</td>
<td>1.1</td>
</tr>
<tr>
<td></td>
<td>LDAPv2</td>
<td>1.5</td>
</tr>
<tr>
<td></td>
<td>LDAPv3</td>
<td>1.5.4</td>
</tr>
<tr>
<td></td>
<td>NetInfo</td>
<td>1.5.1</td>
</tr>
<tr>
<td></td>
<td>NIS</td>
<td>1.0</td>
</tr>
<tr>
<td></td>
<td>Rendezvous</td>
<td>1.0.1</td>
</tr>
<tr>
<td></td>
<td>SLP</td>
<td>1.0</td>
</tr>
<tr>
<td></td>
<td>SMB</td>
<td>1.0</td>
</tr>
</tbody>
</table>

Click the lock to prevent further changes.

Configure the selected plug-in

Configure the selected plug-in
Directory Access

<table>
<thead>
<tr>
<th>Enable</th>
<th>Configuration Name</th>
<th>Server Name or IP Address</th>
<th>LDAP Mappings</th>
<th>SSL</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓</td>
<td>SCL</td>
<td>dc1-mmc.scl.utah.edu</td>
<td>Custom</td>
<td></td>
</tr>
</tbody>
</table>
Directory Access

Configuration Name: SCL

Server Name or IP Address: dc1-mmc.scl.utah.edu

Open/closed times out in: 120 seconds
Connection times out in: 120 seconds

Use authentication when connecting
Distinguished Name: cn=ldapaccess,cn=users,dc=scl,
Password: ************

Encrypt using SSL
Use custom port: 389
Directory Access

Connection:
- Configuration Name: SCL
- Server Name or IP Address: dc1-m...scl.utah.edu
- Open/close times out in: 30 seconds
- Connection times out: 120 seconds
- Use authentication when connecting
- Distinguished Name: cn=ldapaccess,cn=users,dc=scl,
- Password: ********
- Encrypt using SSL
- Use custom port: 636
Directory Access

SCL

Connection

Search & Mappings

Access this LDAPv3 server using Custom

Record Types and Attributes

Map to any items in list

RecordName
UniqueID
RealName
PrimaryGroupID
NFSHomeDirectory
AuthenticationAuthority

uidNumber

Delete
Add...

Search base:

Search in: all subtrees first level only

Write to Server...

Cancel OK
Directory Access

Choose where to search for user authentication information.

Search: Custom path

Directory Node
/NetInfo/root
/LDAPv3/dc1-mmc.scl.utah.edu

Drag directory nodes into your preferred order for searching.

Remove  Add...

Click the lock to prevent further changes.

Revert  Apply
Questions and Answers