

# Lightweight Directory Access Protocol (LDAP)

CISS – 150 William Jojo

The LDAP protocol in its simplest form allows users to authenticate against a common database of knowledge. This knowledge is typically a set of username and password pairs. LDAP, however is not just a warehouse of users and their respective passwords.

This is, of course, a gross simplification of LDAP and the database that supports the protocol. The database back end is usually some form of BerkeleyDB (bdb). It is a database whose data is setup in 2-tuple key and data pairs. If you provide a key to the database, it will return the value for that key. Inversely, you can provide a data value and the database can return the key(s) that match the data value.

OpenLDAP is the LDAP implementation we will be using in the lab. It is built on BerkeleyDB. The LDAP protocol identifies *attributes*. An attribute can be any name and can be defined to hold an form or type of data. However, attributes must be associated with an *objectclass*.

An objectclass defines the rules under which attributes may be used. Some attributes will be defined as MUST, other as MAY. This simply means that you must have attributes and values defined if they are listed in the MUST section. In addition, you may include attributes and values if they are listed in the MAY section. Finally, attributes not listed for a given objectclass simply cannot be used, unless you assign an additional objectclass to a database object.

Now, this discussion has been a bit backward for a reason. Attributes define data, objectclasses define rules for assembling data and now we can talk about how to associate that data with an object – a *distinguished name* or a *dn*.

The distinguished name of a LDAP database object is the unique representation of person, place or thing. The dn could represent a username, a network printer or the name of a business.

The details of the database and the `ldapsearch` command for use with the lab will be discussed during class.

LAB (10 points):

Install the `ldap-utils` package on the Ubuntu guest.

Configure the `/etc/ldap/ldap.conf` file so that it will default to the domain `ciiss150.net`. This is done by setting a specific value for `BASE`. You will also need to set the `URI` value for the appropriate server

Write queries to do the following:

1. Search for all users in the `ou=people` container.
2. Search for all groups in the `ou=groups` container.
3. Search for all users whose second to last character is a '1'. Only return the `uid` values.
4. Search for the users that end in 10 through 15 but not 13 (that is, not `remuser13`). Return only the `uidNumber` and `gidNumber` values.
5. Search for all database entries that have `loginShell` defined. Return only the `dn` values.