Perl Net::LDAP

1   Aims

The main aims of the activities today are:

- To understand how to write a Perl program to perform directory searches;

- To understand how to write a Perl program to perform modify operations on a directory.

2   Background

In slide §4 from the Perl LDAP slides, and also from slide §?? in the LDAP lecture notes, you can see that a *simple bind* requires:

- A distinguished name, and

- a password.

However, when a application authenticates a user, we usually send a *username* and password, not a DN and password. To work with applications in the way you might expect, the authentication operation is a two-stage process:

- First we perform an anonymous bind and a search for the DN that matches the given username

- We then perform the simple bind operation using that DN the given password.

This tutorial involves writing software to perform this two-stage process.

It is poor practice to hard code passwords into software. There are a number of ways of avoiding this; one way involves putting the password into a file that is protected from access by any other users.

Here is some example code that you could use to read the password from a file /tmp/password.txt:

```
use constant PASSWORD_FILE => '/tmp/password.txt';
sub read_password() {
    open PW, "<", PASSWORD_FILE
        or die "unable to open ", PASSWORD_FILE, ": $!";
    my $pass = <PW>;
    close PW;
    chomp $pass;
    return $pass;
}
```

Here is a bind example using this function:

```
$r = $ldap->bind( $dn, password => read_password );
```

3   Procedure

Refer to the lecture notes about `Net::LDAP` while doing this activity. Refer also to the many manuals for `Net::LDAP` including `perldoc Net::LDAP::Examples`. You may choose either our local ICT server `ldap.tyict.vtc.edu.hk` or the VTC LDAP server `ldap.vtc.edu.hk`; it's up to you.

1. You should have already configured CPAN. If not, refer to the handout on Net::SNMP.

2. Install `Net::LDAP` using CPAN, as described in the notes, with:

   ```
   cpan> install Net::LDAP
   ```

3. Write a program to take your username as a parameter, and which reads your password stored in a file in the `/tmp` directory (note: make the file containing your password have access mode 600, and delete it when you have finished your activities today). The program then does the following:

   - Performs a search for your entry to obtain the DN for your entry;
   - Uses this DN to perform a simple bind to the directory;
   - Prints the `userPassword` attribute for your entry.

     Note that is is *not* a good idea to store your password on your networked home directory. Instead, store it on your local hard disk in the `/tmp` directory and make it readable only by your account. Be sure to delete this file from your hard disk before you leave the laboratory today.

4. Copy this program to a new name, and change it to:

   - Modify the description in your entry to text read from standard input or from a file given on the command line.
   - The program should display your new entry attributes.