Computer Writing and Research Lab

White Paper Series: #030917-2

Creating a Single Authentication System for the CWRL

Ryan Starck
University of Texas at Austin
ryguy@www.cwrl.utexas.edu

17 September 2003

Keywords: LDAP, authentication, single login, unified login, CWRL login, open source

Abstract: The methods and rationale behind creating a single authentication system for all client and server machines in the CWRL.

What's "Authentication" and Why Does the CWRL Need to Consolidate It?

AUTHENTICATION is the act of users identifying themselves to a computer, server or application. For example, a user must supply a valid username and password to login to one of the CWRL machines. Rather than storing usernames and passwords on each CWRL machine, the machine queries a server for that information. This informs the server that:

- the user is a valid user of the system
- the user's password is correct
- the user has access to the data being requested

If the user has supplied a valid username/password combination, then he/she will be able to use the machine, otherwise access is denied.

This setup generally works well for a single-server system with a small user base. All user information is kept in one place for easy administration and users only have one password to remember. However, the CWRL is much more complex than this; there are five different servers, two client platforms (Mac and PC) and scores of applications that require the authentication of users. All of these different logins can make for a frustrating experience for someone setting up accounts for the first time. A consolidated login scheme

for all servers and applications would:

- simplify the login process for teachers and students
- allow more time for teaching and require less time for account setup
- allow for easier systems administration in that only one database of user information would need to be updated

Why Not Use "Labman" Provided by Information Technology Services (ITS)?

"Labman" is a client/server system capable of authenticating users on Macs and PCs from one central database.[1] "Labman" has been successfully used in the CWRL for authenticating users for many years but is no longer the simplest solution.

[1] <http://www.utexas.edu/its/ds/labman>.

While "Labman" support from ITS is friendly and efficient, the application itself lags far behind current operating system technology and tends to frustrate some administrators:

- no UNIX "Labman" server is being developed
- only Mac and PC logins are supported
- there is no way to authenticate any other machine (Linux, Solaris etc.) to the "Labman" server
- login interface is unattractive, unconfigurable and unfriendly to the user
- bypasses built-in login functions of Mac OS X and Windows

Solution: LDAP Authentication Using SSL/TLS for Encryption

See Figure 1 for a graphical representation of the LDAP authentication system described below.

LDAP (Lightweight Directory Access Protocol) was developed to store and retrieve large amounts of user information quickly and efficiently. LDAP is generally considered to be the standard directory system for institutions around the world. OpenLDAP is the Open Source distribution of LDAP.

Benefits of using this system in the CWRL:

- all directory information (usernames, passwords) encrypted over the wire using SSL/TLS

- software is open source and free of charge
- easy for systems administrator to update and add entries into directory
- OpenLDAP is constantly updated and improved
- supported by Windows XP/2000 login via a plugin (pGina)[2]
- supported by Mac OS X login via "Directory Services"
- supported by all flavors of UNIX (Linux, Solaris, etc.)

[2] <http://pgina.xpasystems.com>.

Drawbacks of using this system in the CWRL:

- difficult to implement for UNIX novice
- sparse documentation
- no support from ITS
- doesn't currently support MOO[3], phpBB forums[4] and CorporateTime calendar system[5]

[3] <http://lingua.utdallas.edu>.
[4] <http://phpbb.com>.
[5] <http://www.oracle.com>.

While the drawbacks are significant, they are outweighed by the benefits of a single authentication system supported by so many applications, clients and servers.

Requirements for Deployment

Hardware and software configuration requirements:

- *NIX server (Mac OS X, Linux, FreeBSD, Solaris)
- server must be able to handle thousands of authentication requests per day
- OpenLDAP[6] configured to allow access over SSL/TLS only
- Windows and Mac OS installations that take advantage of authentication over LDAP
- configure all servers to use LDAP for primary authentication (slatin, acker, gibson, babbage2)
- configure all server applications to authenticate via LDAP
- configure "Teacher Folders" to so that teachers and students see their own folders only, not a list of all folders
- design a secure web utility for user update of passwords
- develop scripts to populate LDAP database with usernames and passwords at the beginning of each semester

[6] <http://www.openldap.org>.

Long Term Goals

Current documentation for this approach is fragmented and unclear. A good long term goal would be to develop clear, detailed documentation for the implementation of an LDAP authentication scheme.

This LDAP system can also be utilized in other applications such as the forums, blogs and email lists. Any new applications developed in the CWRL should also work to incorporate the LDAP authentication to simplify the login process for all users.

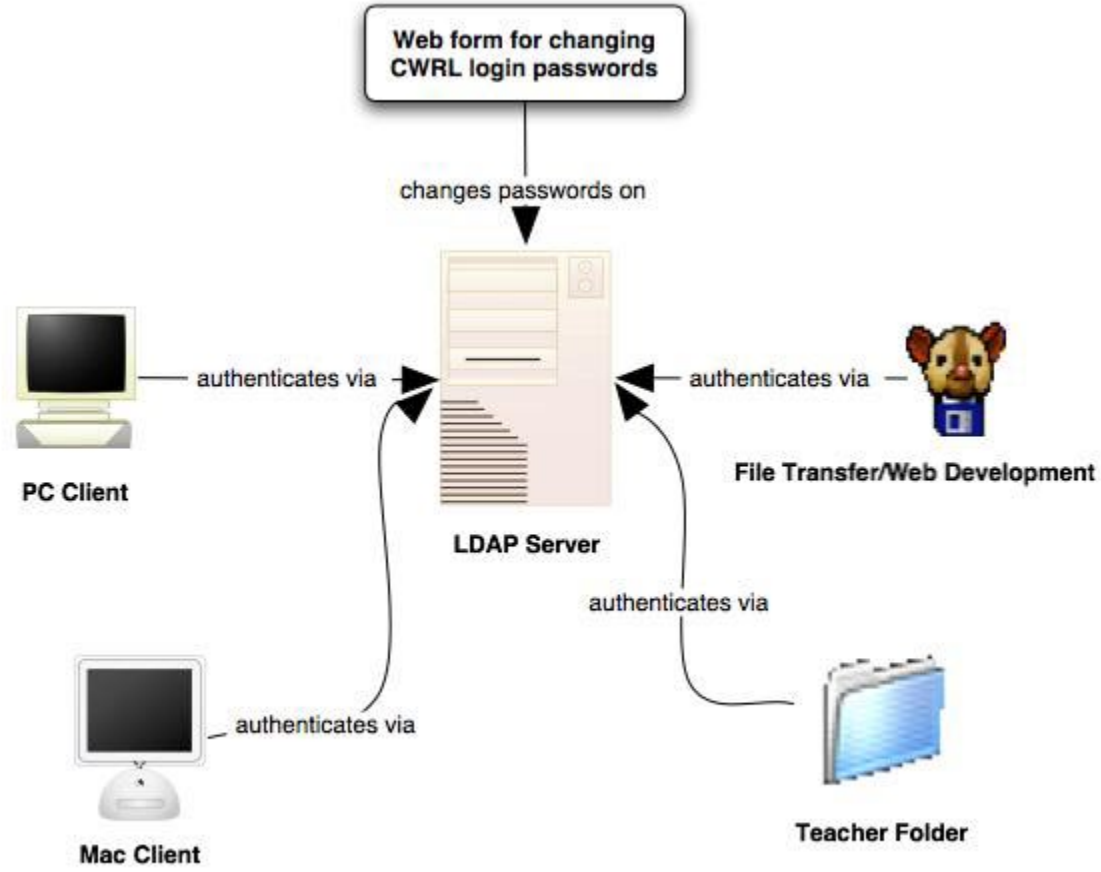

Figure 1: Diagram of Authentication Scheme