Subject: Re: RBAC and LDAP
Posted by dennisj on Thu, 02 Nov 2006 07:16:29 GMT
View Forum Message <> Reply to Message

Tony,

Thanks for the response.

I have minimal experience with LDAP and Web applications.

1/. Moodle http://moodle.org a php MySQL learning management system. If you turn on LDAP authentication, and point the Moodle application at your LDAP server, then, when a user clicks to logon, it takes the entered credentials and asks the LDAP server, over an LDAP connection, whether that user is allowed to proceed.

2/. An apache server can have the mod_auth_kerb module installed http://modauthkerb.sourceforge.net/ . "Mod_auth_kerb is an Apache module designed to provide Kerberos authentication to the Apache web server. Using the Basic Auth mechanism, it retrieves a username/password pair from the browser and checks them against a Kerberos server as set up by your particular organization." The Kerberos connection can talk to an LDAP server.

Because there is a bit of pressure to centralise identity and permissions management in an LDAP server, it would be great if there was some way for your security system to interact with LDAP.

As I said in my original post I'm not a coder. There is a general article here on this topic...
http://www.list.gmu.edu/confrnc/ifip/i01-kluwer01-jpark.pdf
ROLE-BASED ACCESS CONTROL ON THE WEB USING LDAP

The abstract reads...
This paper gives a framework for how to leverage Lightweight Directory Access Protocol (LDAP) to implement Role-based Access Control (RBAC) on the Web in the server-pull architecture. LDAP-based directory services have recently received much attention because they can support object-oriented hierarchies of entries in which we can easily search and modify attributes over TCP/IP. To implement RBAC on the Web, we use an LDAP directory server as a role server that contains users' role information. The role information in the role server is referred to by Web servers for access control purposes through LDAP in a secure manner (over SSL). We provide a comparison of this work to our previous work, RBAC on the Web in the user-pull architecture.

Dennis