CNS /Update Newsletter Feature

Role-based Security

CNS Document ID: u030904a
Last Updated: 8/28/03

UF Information Technology

UFIT

2046 NE Waldo Rd, Suite 2100
Gainesville Florida 32609-8942
(352) 392.2061
<editor@cns.ufl.edu>
Table of Contents

Role-based Security ..................................................................................................3
Role-based Security

As new systems are put in place and existing systems are retired, the university will be moving to a new approach for securing access to data and applications. Role-based security creates collections of similar access rights called "roles" which can be assigned to user accounts.

Role-based security is fundamentally different from our current methods of assigning access rights. We now use a variety of methods-some are ad hoc, some are based on affiliation, some are based on job title, and some applications are assigned by security administrators directly.

We often assign access rights to data (files, databases) and/or applications (programs we can run) on a one-by-one basis. In some cases we use hierarchical concepts such as files in folders-we authorize access to a folder and all the files and folders within it. In most administrative processes, we assign users access rights to particular programs following a security review and approval process. This is cumbersome and error-prone. In many cases users do not have access to programs they need for their work. In other cases they gain access to programs they should not have access to operate.

By grouping permissions together into roles we can create a manageable collection of assignable "chunks" of permissions. We can ensure that when a user is given a role, they have all the permissions required to perform the work associated with the role. A person with "travel authorizer" role would be able to authorize travel, but would also be able to review travel to be authorized, as well as review travel that had been authorized.

Roles are not affiliations. Affiliations are broad collections of users such as faculty, staff, undergraduate student and so on. When we try to grant access to data and software based on affiliation, we often run into tangles related to exceptions. Using role-based security, we can assign a common set of roles and then manage the role assignments as required by policy to handle the exceptions.

Roles are also not job titles. A person with the job title "administrative assistant" may have the role "directory administrator" allowing them to maintain unit directory entries. But this role may be assigned to others with different job titles and not all administrative assistants maintain directory entries. It may be common for some roles to be held by people with particular jobs, but it is a management decision to assign security roles to individuals.

The my.ufl.edu portal uses role-based security and the roles "author" and "publisher" to permit and control content on the portal. The system has proven to be straightforward to administer and allows many people to provide content and have the content reviewed before publication.

Your Comments are Welcome

We welcome your comments and suggestions on this and all UFIT documentation. Please send your comments to:

UFIT

UF Information Technology