CNS /Update Newsletter Feature

Identity Management

EI&O Document ID: u0607f
Last Updated: 07/01/2006

UF Computing & Networking Services

CNS Information Services

2124 NE Waldo Rd, Suite 2100
Gainesville Florida  32609-8922
(352) 392.2061
<editor@cns.ufl.edu>
Table of Contents

Identity Management ................................................................................................3
Three Questions .................................................................................................3
Identity ................................................................................................................3
Authentication .........................................................................................................3
Authorization ...........................................................................................................4
A Combination of Tools and Technologies .................................................................4
For More Information ..............................................................................................4
Identity Management

By Dr. Michael Conlon, UF Director of Data Infrastructure and PeopleSoft Implementation Officer

Identity Management (IDM) is the collection of processes, procedures and systems used to answer basic questions regarding people and their access to systems and data. IDM is growing rapidly in higher education as institutions grapple with increasing needs to secure their environments, while simultaneously improving service. In this article we’ll see how sound IDM infrastructure can meet these needs.

Three Questions

IDM is concerned with answering three basic questions. First, who are the people in our environment? This is a question of identity and is independent of computer systems. Second, when a computer system receives a credential (typically a username and password), does it represent a particular person? This is a question of authentication. And finally, what is a person authorized to do with an institution’s computer systems? This is a question of authorization.

Identity

Identity is established by associating a person with an identifier. At UF, the identifier is the UFID, a unique 8-digit number assigned to each individual of interest to the university. The university has numbered over 1.5 million individuals, including all former faculty, staff and students as well as a large number of affiliated persons. Authorized individuals can establish identity for new persons by verifying previously established identity documents such as birth certificates and driver’s licenses. Establishing and managing identity helps produce a secure environment by providing authoritative information about people in the environment.

Identity at UF is established by directory coordinators and through student admission processes. Identity is recorded in the UF Directory, a mainframe application which assigns and manages unique UFIDs as well as the affiliations that each person has with the institution. Affiliations such as faculty, staff, student and alumnus are multi-valued—one person may have many affiliations.

Authentication

Authentication is the process of presenting credentials to a computer system. At UF, the enterprise credential is the GatorLink username and password. Each person with a UFID an one or more appropriate affiliations may have one GatorLink username. The GatorLink username and password can be used with enterprise systems, web-based systems and local area networks through a wide range of supporting technologies. Passwords for GatorLinks are managed according to university policy using software implemented in PeopleSoft. Having strong passwords that are not shared raises confidence that the GatorLink presented to a computer system belongs to the person of record. Having a common credential improves service—many people need to use just one credential for all their interactions with UF. A common credential also improves security—passwords can be managed by policy and less passwords means less chance of exposing a credential to another person.
Authorization

Authorization is the process of permitting individuals to access computer systems and information. This is done by associating "roles" with the person’s UFID. Note that it is always the person that is authorized, not the “account” or credential. Roles are the unit of authorization. Various roles control access to various systems. Roles may be assigned automatically accordingly to university policy, based on an individual’s affiliations. Additional roles may be assigned through manual processes. Assignment of roles is sometimes referred to as access control or application security. Managed roles provide a clear view of who has access to systems. This improves security. It also improves service, since the person authorized can view their authorizations and easily take action to insure they are authorized properly.

Authorization at UF is maturing. Many roles are managed in the PeopleSoft system. These roles control access to the PeopleSoft system, as well as to many other systems. Automated assignment is done using processes that synchronize the UF Directory and its affiliations with role information stored in PeopleSoft. Manual assignment is done by department security administrators using the Access Request System, a locally developed PeopleSoft application. The student system, ISIS, also uses role-based access and some of these roles are integrated with enterprise role management. Future work will improve role management and access to role information for department applications.

A Combination of Tools and Technologies

Many vendors sell identity management solutions, but in a heterogeneous and complex environment such as the University of Florida, a combination of tools and technologies is required to insure that all systems can participate in the fundamental identity, authentication and authorization processes.

For More Information

For additional information on identity management, you may wish to see the Educause site on identity management and/or sign up for the identity management LISTSERV [http://www.educause.edu/IdentityManagementDiscussionGroup/9363] which discusses issues and implementations of identity management in higher education.

Your Comments are Welcome

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

CNS Information Services

2124 NE Waldo Rd, Suite 2100
Gainesville Florida 32609-8922
(352) 392.2061
<editor@cns.ufl.edu>
UF Computing & Networking Services

CNS Information Services

2124 NE Waldo Rd, Suite 2100

Gainesville Florida 32609-8922
(352) 392.2061
<editor@cns.ufl.edu>