Identity and Access Management and Security in Higher Education

It is 9:30 a.m. Do you know who your users are?

By **Mark Bruhn, Michael Gettes,** and **Ann West**

In June, a person identifying herself as a recently hired faculty member calls an academic department to ask that her e-mail and course management system access be enabled early. Logging in to the account management system to add the new information, the assistant notices the department chair coming in and explains the situation. The chair quickly grabs the phone and hangs up, saying, "We haven't hired any new faculty this year."

Respondents to this year's EDUCAUSE Survey of Current IT Issues ranked security and identity management as critical issues not only because of their strategic importance but also because of the high staff requirements in both the management and technical areas. The preceding scenario illustrates how some of the elements that go into security and identity management affect a campus's ability to deal with challenges to the integrity of its security processes and policies.

A key component of security plans is well-managed access to services that protect online resources and user privacy while enabling ease of use. Centralizing the management of user identity and related information not only reduces the staff required to manage appropriate access and monitoring, but also allows better service through automatic granting (or revoking) of services based on institutional roles.

This article discusses the drivers for an identity management system (IdM), the components of such a system, and the role it plays within a security strategy. We close by offering deployment suggestions and resources.

Basic Access Management

Identification, authentication, authorization, and accountability (or IAAA) are essential functions in providing the required services. Working together, these systems answer questions like

- Are the people using these services who they claim to be?
- Are they members of our campus community?
- Do they have permission to use these services?
- Is their privacy being protected?

Identification is the act of pre-assigning a unique marker or a token (for example, a "username") to an individual, program, script, application, or database ("entities"), such that the entities can be distinguished from each other. The identity token is seldom, if ever, a confidential bit of data. These tokens are also called identifiers.

Authentication is the act of validating that an entity producing a token (or identifier) is the one to which the token was assigned. Authentication generally takes three forms. When protecting resources considered most sensitive, combining two of the three forms is reasonable practice. To authenticate the entity, the system may require

- Something the entity knows, like a password.
- Something the entity carries, like an identity card.
- Some physical attribute of the entity, like a fingerprint or retina pattern.

Authorization is the act of ensuring that the entity is afforded access only to the services and data required to support allowed tasks. Authority can be associated with an entity explicitly on its authority record or implicitly to groups or roles to which the entity belongs.

Accountability flows from appropriate administration of identification, authentication, and authorization, ensuring that only the authorized entity can exercise its individual authority. Ensuring that authentication is commensurate with the data or function being accessed and that an unauthorized person cannot assume an authorized active session are examples of maintaining accountability. Sharing identities among multiple entities eliminates accountability. Permitting entities to choose easily guessed passwords reduces accountability.

Clearly, the security of functions and data rely on well-managed IAAA processes. If it is easy to gain unauthorized access to sensitive data via flaws in the implementation of IAAA, securing the host computer counts for naught. Intruders wouldn't have to identify a security flaw in an operating system, write a program to exploit that flaw, find computers with the flaw, and execute the program to gain access—they would merely have to co-opt already authorized credentials.

Requirements for Access Management

Four general drivers pressure campuses to ensure that their users are eligible to access services: funding, ethics, legal requirements, and prudent stewardship.

Funding sources (students paying

tuition, state governments appropriating funds, and friends/alumni donating gifts) expect that monies will be used to support the campus missions. In some circumstances, they dictate specific purposes. For example, allocating student fees to support a particular facility or service would likely dictate that only students be permitted to use that facility or service.

Legal pressures stem from statutory requirements, mostly related to student records, health information, tax records, and classified research data. Among the regulations affecting access in higher education are the Family Educational Rights and Privacy Act (FERPA), the Health Insurance Portability and Accountability Act (HIPAA), and the Gramm-Leach-Bliley (GLB) Act. Service associations also enforce rules under which members must operate, such as those established by the Electronic Payments Association.

Ethical obligations involve protection of privacy, research protocols, intellectual property, and "strategic" information. Disclosing some of these data could result in identity theft, premature release of research conclusions, or other negative consequences. While some of these areas have established practices, others are emerging as concerns.

Prudent stewardship involves access to data not protected by statute or without formal standards, such as information that can be combined to provide fodder for stalkers or that can cause embarrassment to individuals or institutions. These data might illuminate variances in compensation for faculty, for example. Logs of Web sites visited by administrators might be of concern—the nature of the sites visited could imply things the individual wants kept private. Open data access policies and open records laws will affect decisions made about protecting these data.

Middleware Support for an Access Management System

In the context of identity management systems, middleware, sometimes referred to as core middleware, is an infrastructure that manages security, access, and information exchange on behalf of applications to make the process more secure and easier for people to collaborate and do their work. Middleware allows for the implementation of enterprise class authentication and authorization systems relying upon the data supplied largely from the IdM.

Looking at Figure 1, this IdM architecture can be described left to right by the source systems, data extraction and reconciliation, and consumer systems.

Source Systems

At a technical level, an IdM is usually a database or collection of databases aggregating information from core business systems within the institution to develop a total view of all members of the community. Core business systems include human resources/payroll systems, student information systems, alumni databases, telephone management systems, and patient databases. Asynchronous sources include self-service applications such as student-group membership management delegated to the president of that organization.

Some members of the community are not in any core business system, so the IdM may end up being the source for representing these other affiliates of the community. Wherever possible, the IdM should use information from respective business systems, as they are the "system of record" for that data.

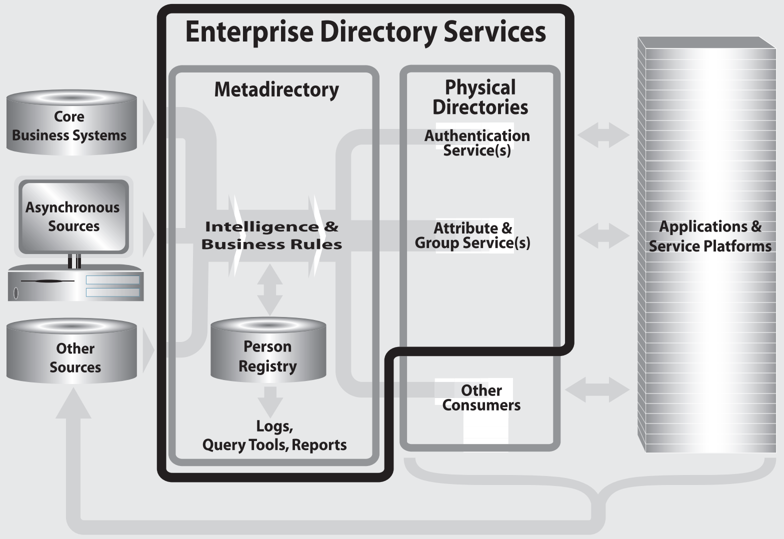
Data Extraction and Reconciliation

The IdM applies a set of business rules to this total view of the community to make a determination about identity for each member of the community. It is in this system that identifier crosswalk tends to happen, so a person expressed by a Social Security number in one system can be determined to be the same person identified in another by an alumni ID, for example. From this integrated view of a person's affiliations with the institution, the IdM can then go about determining what services, capabilities, access, and visibility that person should enjoy.

These business rules are integrated tightly with existing or to-be-created policy to support the business needs of the institution. As a sanity check it is important to consider regular, automated analysis of the contents of the IdM compared to the data in the source systems. All of this processing and the IdM database become a critical component of the enterprise infrastructure.

Figure 1

An Identity Management Architecture


Enterprise Directory Services
Metadirectory
Physical Directories
Core Business Systems
Asynchronous Sources
Other Sources
Authentication Service(s)
Intelligence & Business Rules
Attribute & Group Service(s)
Applications & Service Platforms
Person Registry
Other Consumers
Logs, Query Tools, Reports

Courtesy of Thomas J. Barton, University of Chicago

Consumer Systems

Put this all together and the IdM drives the middleware components by provisioning identity—a collection of attributes—and making this information operationally available to applications and directories. This enables authentication and authorization systems to manage the whole of the institutional electronic identity, including who is allowed access to services and who can perform certain functions. Of course, it can be useful to employ these middleware components to control access and management of the IdM itself and even to the core business systems that feed the IdM.

IdM Implementation Considerations

Myriad issues surround management of good IAAA processes. They include establishing access eligibilities, developing a single namespace, securely distributing credentials, determining the strength of authentication, deciding on authorization mechanism, and developing a logging strategy.

Access Eligibilities

Continuing students and full-time faculty and staff make up the basic constituency of any campus. Sources for data supporting access for these groups are usually current and reliable. However, as the user type strays from these groups, it becomes more difficult to determine eligibility and to manage credentials. Central sources are often no longer reliable. For example visiting faculty might not be required to register with an academic affairs office, and continuing education students may not use central registration. Contractors, conferees, high school students in special programs, affiliate employees, prospects, parents, sponsoring organizations, and alumni are examples of individuals not reflected in central databases who might need the campus to provide some services.

Single Namespace

A primary problem in trying to improve IAAA processes is creating a single namespace. The goal is to establish the relationship among identifiers from various systems (library, administrative, e-mail, and so on) such that identity and access information associated with each can be integrated under one primary and unique identifier.

This lengthy and difficult task is critical to ensuring that services validate against one credential and that user authority is consistently applied. Not only do a single authoritative identity database and a single set of authentication services make management of the IAAA processes easier, but application developers can then rely on central common processes, and users and help desks contend with only one set of credentials across a wide variety of services.

Distribution of Credentials

The traditional method for ensuring that the right credentials are distributed to the appropriate users has been to require them to visit a support desk and present a photo ID as proof of identity. However, many users are not on campus or cannot come to a designated location. In these cases, campus mail or e-mail can be used, but neither is secure. An online account management system (AMS) permits users to access an online application and supply some data that only they will (reasonably) know, such as date of birth.

The source data might be gleaned from data collected at employment or enrollment. However, this may not be feasible for nonstandard groups, such as visiting lecturers, because relationships between these affiliates and campuses are most always through a department. In this case, a department representative should manage or sponsor that relationship, as a form of registration authority, and enable the visitors to access the AMS in order to administer their accounts.

Authentication Strength

Most statutes that require access controls are goal oriented and do not dictate technologies. A partnership among technologists, security staff, data stewards, auditors, and legal counselors is critical to choosing the authentication method for various resources.

It isn't difficult to recognize situations that require some form of authentication; deciding on the strength of the method takes some deliberation. Authentication can be as simple as validating a static password or as complicated as password generators, pass phrases, symmetric keys, digitized signatures, and biometrics. (The existence of databases of digitized signatures and biometric patterns makes a lot of users queasy, however.) The chosen method should be commensurate with the sensitivity of the data or functions being accessed.

All authentication databases must be afforded a high level of protection, as these are the keys to the kingdom. Unauthorized access to and decryption of the data would certainly afford potentially disastrous access to a wide variety of data and functions.

Other aspects of authentication include single sign-on, which has to do with users having a single credential for all major network services on campus, and the related "sticky authentication," where the user only has to authenticate once. After that, all applications subsequently accessed trust that authentication.

Authorization Mechanisms

Once the authentication scheme is in place and working, a means to ensure that users gain access to what they need—and only what they need—is important. Network services will authorize access in various ways, using a variety of attributes. It is nearly impossible to develop a central authorization scheme that takes into account every requirement.

Decisions about scope must be made; certain attributes many services should be programmed to care about, including student applications that need to know school and major and employee applications that need to know an employee's department. High-level roles and groups are static and fairly easy to accommodate. Few applications need to know if a student belongs to the Spanish Club. Perhaps a self-service function can be used to manage these granular groupings in the central authorization database.

Attributes about individuals must be stored and passed in order for applications to make authorization decisions. The issue of personal privacy is a concern. For example, an online address book will display standard information about users. Sometimes users have a need to suppress all or some of their data, however. Indeed, FERPA requires that students be afforded the opportunity to suppress the release of attributes otherwise identified by the campus as directory (publicly available) information.

Logging Strategies

Some campuses have chosen to require authentication for access to all network services. In this case, logs can be used to identify when a network service is accessed and by whom. This facilitates investigation following allegations of illegal or inappropriate behavior, using time, date, and device information. The other end of the spectrum is authenticating where tracking access is required for legal or policy reasons and all other access is allowed to be anonymous.

Logging can become controversial and subject to FERPA protection if authentication instances are logged, and definitely if the user's actions during the logged session are also captured. If these logs are kept, the strategy for doing so should be well thought out and publicized so that users can make informed choices about what they will do on the campus network versus using an external service.

For most services, authentication logs need not be kept very long, if at all, and access to logs should be restricted to individuals whose jobs require it. If activities are also logged, along with concerns of individual privacy comes the possibility of increased institutional liability.

If the institution collects activity records, a court could assume that the institution should know about illegal activities and should carry some amount of liability for them. Some legal counselors believe that liability could be heavier if the campus has a policy of using the logs to pursue alleged violators of law or policy and more still if applied inconsistently. Before any authentication and logging scheme is implemented, local legal advice should be sought.

Authentication Between Institutions

Beyond the issues just touched on here, there is a recognized need to authenticate users between institutions. One campus may offer particular courses to which students of another campus want to gain access. Or an organization might have developed information resources that it wants to sell. In these and many other situations, there is a need to ensure that only registered or paid users access these services.

Next Steps

It is safe to assume that an IdM is not strictly a buy or build solution. Some have purchased identity management systems successfully, and others have built their own systems. Each campus has a unique culture, policy structure, and technology environment that inform its IdM implementation. Whatever product you choose will require that you build in your institutional requirements.

In addition to a technological infrastructure, typical outcomes of this deployment include developing new administrative policies and processes to enable online applications and security systems to access and use institutional data. Below are the basic steps for implementing an IdM service:

■ *Educate yourself and get plugged into the middleware community.*
Learn about identity management systems. Discuss campus needs with stakeholders. Move on to the campus data custodians, and begin identifying one or more specific business drivers or applications that would benefit from using this infrastructure.

■ *Develop a person registry.*
Take an inventory of the campus identifiers, such as those used by the campus card, library, administrative, and e-mail systems. Research how people are assigned those identifiers and what services are accessed using them. Work with the custodians of the data to correlate the correct identifiers with each person. Develop a system of assigning a unique identifier as a root for cross-correlation. Store the resulting identity information.

■ *Implement enterprise directory and authentication services.*
Review your institutional, technical, and application requirements and needs. Review higher education and vendor implementations of enterprise directories. Refer to the Enterprise Directory Implementation Roadmap under the Getting Started section of the National Science Foundation (NSF) Middleware Initiative–Enterprise and Desktop Integration Technologies (NMI-EDIT) Web page for more information (see the sidebar).

These are by no means all the required steps for implementing IdM services. Keeping tabs on what's happening with middleware development and talking with middleware-savvy staff from a school similar to your own can help reduce the "reinventing the wheel" syndrome. See the sidebar for more information on identity management systems.

Conclusion

Identity management involves a campus infrastructure requiring design, deployment, and oversight input from stakeholders across the institution. In the big picture, IdM brings together all the information about a school's constituents and enables centralized control of access to and monitoring of critical systems for the institution. They can be complex to implement, and project teams must consider a multitude of policy, operational, and technical decisions to keep an individual's privacy in balance with institutional security.

When all is said and done, system managers will know who their users really are—at any time.

Acknowledgment
This material is based in whole or in part on work supported by the National Science Foundation under the NSF Middleware Initiative—NSF 02-028, Grant No. ANI-0123937.

Mark Bruhn (mbruhn@iu.edu) is Chief IT Security and Policy Officer at Indiana University and Associate Director of the IU Center for Applied Cybersecurity Research. Michael Gettes (gettes@duke.edu) is Senior Technology Architect and Strategist at Duke University in Durham, North Carolina. Ann West (awest@educause.edu) coordinates outreach activities for the National Science Foundation (NSF) Middleware Initiative–Enterprise and Desktop Integration Technologies (NMI-EDIT) Consortium.

More Information on Identity Management Systems

The Enterprise and Desktop Integration Technologies (EDIT) Consortium, part of the National Science Foundation (NSF) Middleware Initiative (NMI), consists of Internet2, EDUCAUSE, and the Southeastern Universities Research Association (SURA). The consortium offers practice documents, software, tools, and directory schemas to facilitate inter-institutional resource sharing and collaboration. For more information on the middleware components in an identity management system, review the following sources:

■ To find out more about the stages involved in IdM implementations, review the resources available on the Getting Started section of the NMI-EDIT Web site, <http://www.nmi-edit.org>.

■ To educate yourself on the specifics and meet colleagues with similar issues, consider attending NMI-EDIT's half- and full-day workshops for CIOs, technical architects, and project managers, covering basic and advanced topics in identity management and related areas. The workshops are held at EDUCAUSE annual and regional meetings, Internet2 meetings, and as announced. Visit the NMI-EDIT Web site for locations, topics, and dates.

■ For additional information and networking opportunities with experienced architects and management, consider attending the Campus Architectural Middleware Planning (CAMP) sessions. Check the NMI-EDIT, EDUCAUSE, or Internet2 Web sites for details.

■ For a current list of tools, documents, software, and schemas available from NMI-EDIT relating to identity management components, visit the Development section of the NMI-EDIT Web site or the Internet2 Middleware Initiative site at <http://middleware.internet2.edu>.

■ To discuss identity management with your colleagues, subscribe to the EDUCAUSE Middleware Constituent Group at <http://www.educause.edu/cg/middleware.asp>.

■ For more information on the NSF Middleware Initiative, visit <http://nsf-middleware.org>.