

EDUCAUSE Center for Applied Research

Research Bulletin

Volume 2006, Issue 21

October 10, 2006

Campus IT Security: Leveraging Identity Management Technologies

Richard Boes, California State University, Fresno

Tom Cramer, Stanford University

Vicky Dean, Cornell University

Roger Hanson, University of Wisconsin–Madison

Nan McKenna, Stanford University



Overview

Increasing complexity in campus information technology (IT) environments has increased higher education's attention to maintaining acceptable levels of security and data protection. Many people with multiple affiliations, together with large numbers of centralized and distributed systems run by multiple IT groups, reflect the diversity and decentralization on campus.

The data in IT systems are themselves valuable university assets. Not only are IT professionals the stewards of a huge and ever-increasing store of personal and financial information about students, faculty, and staff, but university systems and repositories also hold priceless and irreplaceable research data, analyses, and findings. Access to this information should be treated as seriously as access to physical assets, with the same attention to ensuring that only authorized people and systems can access the information.

Security technologies available today provide various types of protection to the campus. These include technologies that secure the network, control access, encrypt data, facilitate backups, provide virus protection, and supply enterprise directory services. Choosing the right solutions for your institution is a complicated task, involving trade-offs among risk, cost, and functionality.

A broad solution to IT security, in some cases, is likely to mean a less-than-optimal solution for individual groups and departmental systems. Careful analysis up front and a keen awareness of the politics and culture of the institution and its component parts are critical. Governance will be a key factor in a successful security implementation.

Managing IT security becomes exponentially more complex as the numbers of technical layers and institutional boundaries grow. In a distributed environment with multiple boundaries, it is sometimes unclear who should be responsible for solving security issues.

When a security issue or problem is found or defined, there is not always a technical solution that can be implemented without affecting service delivery. Solutions to security problems are sometimes not well tested because of the urgency of getting a solution implemented quickly. Complex solutions frequently offer the best security but are prone to errors resulting from poor configuration, unknown service and system interdependencies, or user misunderstanding. Sometimes the solution presents more risk than the problem.

In this research bulletin we pay particular attention to the emerging set of technologies that fall under the broad category of identity management. In addition to the more technical security solutions, all systems rely on accounts, authentication, authorization, and access to a common set of attributes about people, groups, and organizations. It is becoming increasingly important to provide central infrastructure (middleware) that can handle these functions for all systems—central and distributed, administrative and academic—and relieve individual application providers from the responsibilities of maintaining current and strong systems for authenticated logins, access control, and so forth.

A new breed of systems and new models of integration are emerging to address these needs. To successfully integrate them into a distributed campus environment, the prerequisite is to identify the particular requirements of a given institution so that technologies can be matched to requirements. Whatever approach or technology is chosen, a common set of basic principles can be applied to optimize security and manageability.

This bulletin is a companion to *Campus IT Security: Governance, Strategy, Policy, and Enforcement* (Boes, Cramer, Dean, Hanson, & McKenna, 2006) and is based on a literature review, campus interviews, and the firsthand experience of the authors. Intended to be a survey of issues rather than a solutions guide, this bulletin is both an introduction and a reference for IT stakeholders. It does not provide any specific prescription for solutions to the security problems of any individual college or university.

Highlights of Key IT Security Technologies

This section contains a brief discussion of security technologies in use in higher education, with a focus on technologies related to identity management.

Security Technologies in Use in Higher Education

As shown in Table 1, ECAR's research study *Information Technology Security: Governance, Strategy, and Practice in Higher Education* identified a variety of security approaches in use at U.S. colleges and universities (Kvavik & Voloudakis, 2003). Generally, no one specific solution should be relied on for security needs; a spectrum of solutions, working together, will be more effective.

Table 1. Status of Security Approaches Used

Security Technology	Implemented	In Progress	Piloting	In 12 Months	In 24 Months	Not Being Considered
SSL for Web transactions	73.2%	12.9%	3.1%	5.0%	3.1%	2.6%
Centralized data backup	71.0%	10.7%	2.8%	4.2%	5.4%	5.8%
Network firewall (perimeter)	70.9%	11.0%	2.6%	4.4%	3.3%	7.9%
Network firewall (interior)	50.0%	18.6%	3.8%	9.4%	8.3%	9.9%
Enterprise directory	48.2%	24.1%	4.9%	9.1%	7.6%	6.1%
VPN for remote access	45.4%	17.8%	8.8%	12.4%	8.1%	7.6%
Intrusion detection	42.8%	15.1%	10.4%	13.7%	15.6%	2.4%
Intrusion prevention tools	33.1%	15.3%	10.9%	16.1%	18.0%	6.6%
Encryption	31.8%	19.5%	9.9%	9.9%	16.6%	12.3%
Content monitoring/filtering	31.6%	10.9%	4.9%	5.9%	10.9%	35.8%
Standards for application and system development	30.0%	21.6%	4.1%	14.8%	12.2%	17.3%
Electronic signature	6.5%	7.8%	8.5%	10.3%	30.5%	36.5%
Shibboleth	1.1%	3.5%	4.9%	7.1%	24.7%	58.7%

Firewalls are probably the best-known and most common solution for network security. They offer a simple, straightforward way to control access to the institution's perimeter and/or interior networks. Because an institution's mission is to educate and share information, security implementations at universities frequently accept higher risk from providing increased access to information. To mitigate the increased risk, firewalls are commonly supplemented with intrusion detection and prevention technologies that allow increased access while helping to detect and prevent malicious behavior.

These technologies and others provide security layers to ensure the confidentiality, integrity, and availability of information, but they are not the only tools. Identity management provides an additional security layer that facilitates application security through user authorization.

Identity Management

A common repository of information about users, accounts, and profiles, such as an enterprise directory, can greatly facilitate the flow and management of identity and account information across all systems. The seemingly simple task of moving, sharing, and synchronizing this information among disparate systems represents a challenge in and of itself. If a student changes her e-mail address or a staff member changes his name, either might be required to update that attribute in a half dozen or more places if each system relies on its own, nonintegrated data store.

Identity management principles and technologies are fast emerging as a critical component of any security strategy. Burton Group defines identity management (IdM) as "the set of business processes, and a supporting infrastructure, for the creation, maintenance, and use of digital identities." (Blum, 2005)

At a basic level, identity management is simply the answer to two questions: What do I say about myself, and what do others say about me? For most organizations, identity management is directory-centric. Access to resources is granted by providing a username and password (or some other secret associated with the individual). Directory-centric identity management has several shortcomings, however. It is opaque, it is based on a single authority, it is not portable, and it is not based on any credential. Most identity transactions involve the presentation and verification of some type of credential (photo identification, driver's license, passport, photo credit card, and so forth). In addition, the acceptance of the credential implies a trust relationship with the credential provider—we implicitly trust certain authorities.

Identity management systems are evolving from directory-centric toward identity management suites (offered by major vendors) and, in the future, user-centric systems that mimic familiar credential-based systems.

Who Are You, and What May You Do?

Authentication systems ask and answer the question, Who are you? They confirm your identity, most commonly through usernames and passwords. Once your identity is

confirmed, you are granted access and other privileges that have been assigned to you. Authentication systems enable appropriate use of networked services or applications.

When authentication systems are tied to specific applications or machines, users must create and maintain multiple usernames and passwords. Typically, this leads to weaker passwords that are easier to remember (and crack), shared passwords, and greater exposure to attacks by hackers.

Authorization systems answer the question, What are you allowed to do? Authorization systems determine each user's level of access to a system or application. Authorizations can be tied to individual users, or individuals can belong to groups or "roles" that carry predetermined permissions.

Regardless of the way authorization works, when roles shift, corresponding changes in system privileges are frequently not well coordinated. Closing this gap requires both good administration practices, such as regular audits, and IT systems that automate privilege management.

Benefits of an Identity Management Solution

Respondents to a recent ECAR survey on identity management, primarily chief information officers and director-level IT officers, clearly see a broad set of benefits to implementing identity management solutions. Table 2, which shows benefits rated on importance and the capability to implement them, is from ECAR's research study *Identity Management in Higher Education: A Baseline Study* (Yanosky, 2006). The table shows that security-related identity management components are generally considered to be important to implement, with tracking unauthorized access and disabling accounts for persons no longer affiliated with the institution occupying the top slots. Perhaps more interesting than these findings, however, is the perceived gap between the importance of identity management benefits and an institution's capability to implement solutions that provide those benefits. In every case, capability ranked lower than importance, with reduced or single sign-on rated the benefit with the largest gap.

Table 2. Identity Management Benefit Importance and Capability to Deliver

Identity Management Benefit	Descriptor	Importance		Capability		Importance-Capability Difference
		Mean	Std. Deviation	Mean	Std. Deviation	
Directly track illegal or unauthorized network activity back to the person responsible	Track unauthorized activity	4.32	0.757	3.24	0.946	1.08
Immediately disable all services and user IDs when a user is no longer affiliated with the institution	Immediate deprovisioning on user departure	4.32	0.711	3.12	1.077	1.20
Prior to issuing credentials (e.g., user account, ID card, etc.), have the appropriate level of confidence (based on type of constituent) that a user is who he or she claims to be	Appropriate ID proofing confidence	4.18	0.750	3.47	0.924	0.71
Reduced or single sign-on (one electronic identity used to access most or all institutional services)	RSSO	4.10	0.836	2.72	1.035	1.38
Have a single authoritative source of information for all persons affiliated with the institution (as an institutional asset)	Single affiliations source	4.05	0.890	2.91	1.043	1.14
Provide self-service functions (e.g., password reset, profile management)	Self service	4.05	0.810	2.94	1.043	1.11
Immediately enable all authorized services for a new user	Immediate new-user enablement	3.93	0.803	2.87	0.931	1.06
Immediately change authorized services for a user who changes roles	Immediate role change	3.89	0.810	2.74	0.959	1.15
User authentication and authorization processes that are scalable (e.g., as enrollment grows)	Scalable authN and authZ	3.89	0.955	3.24	0.944	0.66
Allow institutional users to access off-campus resources that require their own authentication and authorization (e.g., licensed library content)	User access to off-campus resources	3.85	0.922	3.10	1.045	0.75
Strong authentication (e.g., strong passwords, two-factor authentications)	Strong authentication	3.83	0.950	2.77	1.115	1.06
Give visitors/guests only the specific access they require and disable that access at the correct time	Appropriate guest access	3.62	0.969	2.61	1.017	1.01
Allow non-institutional users access to institutional resources for which we require authentication and authorization (e.g., sharing course materials with other institutions)	Non-institutional user access to our resources	3.02	1.038	2.39	0.932	0.63
Decentralize user account management and authorization of services (e.g., to deans of schools, managers of business units)	Decentralize account management	2.70	1.232	2.17	1.050	0.53

(1 = very low, 2 = low, 3 = medium, 4 = high, 5 = very high)

Account Provisioning

Account provisioning systems can automatically create, modify, and terminate user accounts in disparate systems for campus individuals based on their identity and the life cycle of their relationship to the institution. Deprovisioning accounts rapidly, reliably, and appropriately is essential to maintaining the security and integrity of campus systems and data. In addition to the business need for effective account management, the hidden cost of account administration can be significant: managing accounts in independent systems (creating, updating, removing usernames and passwords) is expensive and time-consuming. Significant application administrator and help-desk time can be consumed on this basic task.

When combined with an identity management system, automated account provisioning (and deprovisioning) provides a powerful, efficient way to grant and revoke access to the online applications that community members need to fill their roles. When new students, faculty, or staff arrive, creating a single account for them in the appropriate system of record can trigger the creation of accounts in the other systems that they will use. For instance, when new students are registered in the student administration system, they automatically receive e-mail, calendar, campus portal, course management, library, and student financial systems accounts as well.

From user and system administrator perspectives, this is an obviously elegant and appealing solution; new community members get full and immediate access to every system they need without the need for further human intervention. Just as significantly, from an IT security perspective, this creates three significant benefits. First, IT and business offices almost always do a better job of creating new accounts than of turning off old ones. Tying account revocation to changes in a community member's status (graduation, termination) provides a more reliable mechanism to avoid having old accounts left open—a common security vulnerability. Second, automated account creation reduces the likelihood of human error. Third, it reduces or eliminates the need for administrators to manually create accounts, as well as creating an auditable trail.

To realize the full security benefits of an account provisioning system, business owners and administrators should establish clear policies on privileges for different community members as they progress through different stages of their campus life cycle. Regular audits of accounts should be performed to ensure appropriate activation and deactivation. Creating secure mechanisms for self-service password resets can greatly alleviate the expense of user support.

Authentication Systems

A common authentication, or login, for university systems can be one of the most powerful tools in ratcheting up security in the campus IT environment. Without common authentication, institutions will typically end up with a set of login requirements that range from weak to strong, and users will be forced to create and remember multiple accounts and passwords.

It is almost always easier to deploy a new system that requires its own username and password than it is to integrate system authentication with a campus-wide authentication infrastructure, especially since many out-of-the-box vendor solutions do not support external authentication systems. For those that do, integration represents incremental effort and cost that are often difficult to estimate. The hidden and ongoing costs, the complexity, and the risk of maintaining numerous disparate systems, however, typically mean that a nonintegrated service will be more expensive to maintain and less secure in the long run. Both vendor systems and homegrown applications may have relatively weak authentication mechanisms; some likely won't pass the minimum guidelines required for security on campus. Each authentication system represents a potential breach in system security: the more there are, the more you have to manage.

To reduce the risk and overhead associated with multiple authentication systems, many campuses have a designated single sign-on (SSO) or WebISO (initial sign on) strategy and technology. With these systems, users can sign in once with a strong password, using a secure, appropriately encrypted method, and effectively log in to every networked service available to them.

The first steps to realizing the benefits of a common authentication mechanism are to create a strategy around single sign-on and to adopt a technology or small set of technologies that are secure, relatively easy to integrate with, and match the existing campus technology profile. With that foundation, it is possible to create policy that makes integration with existing authentication/SSO systems a firm requirement for adopting new systems. Staffing a central group of systems developers to assist projects with integration can also provide the extra expertise and resources necessary to ensure that new systems integrate with the login system before they are deployed.

Authorization Systems

Privilege management is essential to maintaining appropriate security and integrity of applications and data. Application authority levels must be assigned to enable people to do their work without exposing the system or its data to compromise.

Maintaining appropriate levels of authority within an application typically requires manual intervention by an application administrator, which introduces overhead, the probability of delay, and the possibility of human error. This complexity is multiplied many times for a campus-wide application, with potentially thousands of users and a highly distributed base of administrators. In this case, controlled and timely assignment of privileges becomes a Herculean task.

Some of the most recent developments in the identity management domain have been the creation of authorization middleware. By defining and codifying privileges within applications at an abstract level, an authorization system can assign privileges in other systems based on a user's role as defined by an identity management solution. So, when Jane Doe joins the university as an HR manager for a given department, she automatically receives the appropriate level of privileges in the HR system for that department. When she transfers to finance in a different department, her HR privileges

are automatically revoked at the right time and she receives a new set of privileges for the appropriate accounts in the finance system.

As with identity management and account provisioning, the first step in moving toward authorization middleware is to define and agree upon a set of privileges corresponding to each role a person might have. Once this upfront analysis has been accomplished, it can be manifested technically in a number of emerging systems.

What is a CIO or provost to do? How can you manage this complexity and diversity in a secure, scalable, yet streamlined way that also lets people use the systems to do their work? A suite of middleware and enabling technology has emerged and is evolving to better address this diverse set of needs.

What It Means to Higher Education

Although higher education is starting to adopt a security framework that uses identity management, most institutions rely primarily on traditional approaches. These include the use of firewalls (both perimeter and internal), VPN for remote access, and intrusion-detection systems. The ECAR study *Information Technology Security: Governance, Strategy, and Practice in Higher Education* indicated that size of the institution correlates to the adoption of security technologies—larger institutions provide more comprehensive solutions—but higher education still lags behind most business organizations in this area.

While higher education is adopting a set of technologies to improve security, a pattern of gaps exist. Very large institutions (those with more than 100,000 devices) do not use perimeter firewalls. Rodney Peterson, in the ECAR study on IT security, noted that many institutions need to develop a strategy in the area of encryption/authentication for wireless services (Kvavik & Voloudakis, 2003).

Institutions must also recognize that success is not based solely on specific technical solutions. Effective governance, strategy, culture, policy, and enforcement are needed to create a consciousness of security within the institution. These drivers can ensure thoughtful and scalable integration into the infrastructure for new technical solutions and demands for identity management.

While the problems of identity management present a challenge to any organization of sufficient size and complexity, they are particularly challenging in higher education, where the organization structure is frequently decentralized, the influx and turnover is rapid, and individuals often perform multiple roles simultaneously.

Due in part to their typically distributed organization of campus IT, departmental and administrative computing groups historically have assigned, built, and supported their own account management systems to meet their business needs. This scattered approach, coupled with the nomadic nature of the higher education population, results in inconsistent levels of service and access as individuals come and go or change their status—termination or modifications made in one account (e.g., removal from payroll

upon termination) don't necessarily cascade to other systems (e.g., removal of the ability to approve purchase requisitions).

These inconsistencies can lead to significant vulnerabilities in the campus computing environment, as well as inefficient and ineffective service to the institution's scholars, students, and administrators. An integrated approach to identity management improves the level of service and security of IT systems as well as their manageability.

Key Questions to Ask

- How do we balance traditional security tools with identity management to provide an acceptable level of risk?
- How much agreement and clarity do we have on cross-system roles, privileges, and authority?
- What are our policies related to identity management?
- Where does our institution fall on the spectrum of authentication sources (i.e. multiple sources versus a single source such as password)
- How have we linked identity to business processes?
- To what degree are key stakeholders engaged in establishing identity management policies and practices?

Where to Learn More

- Cameron, K. (2005). The laws of identity. *Kim Cameron's Identity Weblog*. Available from <http://www.identityblog.com/stories/2004/12/09/thelaws.html>
- Lewis, J. (2006, June). *Identity in context: The evolving business and social infrastructure*. Burton Group Catalyst Conference. Available from http://www.burtongroup.com/research_consulting/doc.aspx?cid=938
- Madelin, J., & Razzell, L. (2006). *Towards the identity society*. Retrieved July 18, 2006, from <http://www.identitysociety.org/files/identitysociety.pdf>

Acknowledgment

This paper is the work of a cross-institutional project team participating in the IT Leaders Program, a leadership development initiative facilitated by MOR Associates, Inc., of Watertown, Massachusetts (<http://www.morassociates.com/itlp.htm>).

References

- Blum, D. (2005, May 25). *Concepts and definitions*. Midvale, UT: Burton Group.
- Kvavik, R., & Voloudakis, J. (with Katz, R. N., Caruso, J., King, P., & Pirani, J.). (2003). *Information technology security: Governance, strategy, and practice in higher education*. (Research Study, Vol. 5). Boulder, CO: EDUCAUSE Center for Applied Research. Available from <http://www.educause.edu/ecar>
- Yanosky, R. (with Salaway, G.). (2006). *Identity management in higher education: A baseline study*. (Research Study, Vol. 2). Boulder, CO: EDUCAUSE Center for Applied Research. Available from <http://www.educause.edu/ecar>

About the Authors

Richard Boes (rboes@csufrenno.edu) is Director of Information Technology Services at California State University, Fresno. Tom Cramer (tcramer@stanford.edu) is Associate Director, Digital Library Systems and Services, at Stanford University. Vicky Dean (vrd4@cornell.edu) is Assistant Director of Systems and Operations at Cornell University. Roger Hanson (rlhanson@wisc.edu) is Assistant Director, Internet Infrastructure Applications at the University of Wisconsin–Madison. Nan McKenna (nmckenna@stanford.edu) is Director of Process and Account Management at Stanford University.

Copyright 2006 EDUCAUSE and Richard Boes, Tom Cramer, Vicky Dean, Roger Hanson, and Nan McKenna. All rights reserved. This ECAR research bulletin is proprietary and intended for use only by subscribers. Reproduction, or distribution of ECAR research bulletins to those not formally affiliated with the subscribing organization, is strictly prohibited unless prior permission is granted by EDUCAUSE and the authors.