Identity Management for Educational Portals

Tom S. Chan, Southern New Hampshire University, USA; E-mail: t.chan@snhu.edu, tomschan@verizon.net

INTRODUCTION

Identity management (IDM) is a broad administrative task that includes identifying users in a system, controlling their access to resources, and associating user privileges with the established identity. It is a crucial aspect in a portal's design (Emigh, 2002). Enterprises everywhere are undergoing transformations to enhance the value they deliver to the business while reducing costs. A properly designed portal brings together a range of disparate tools and information sources, providing an effective channel between the business and its stakeholders (Stone, Roof & Lonsdale, 2006). For an educational portal, it must provide equal level and quality of access to applications, from both main campus and satellite centers, and for both on and off campus users. Students and faculty should not have to memorize multiple user ID/password pairs as they use different resources, though access privileges for the same user may be different (Levinson, 2002).

SINGLE SIGN-ON & STRONG AUTHENTICATION

Authentication is the bedrock in a portal as it bridges access privilege and user identity together. By verifying a user's identity, access is correctly granted or denied. Organizations pursue a variety of strategies to simplify and consolidate multiple sign-on, as it betters user experience, reduces costs and improves compliance. Typically, a user authenticates once when accessing a protected resource. The IDM issues the browser a cryptographically protected cookie, which maintains authentication state across applications. Apart from convenience, single sign-on (SSO) externalizes application security. Security externalization results in simpler policy maintenance as authentication no longer maintained within every application. It also improves compliance, as externalization forces the school to take a holistic view on security for all of its applications.

While user ID/password is most commonly used, it is weak and insecure with countless security problems. Stronger authentication can be achieved by using two factors. Two-factor authentication is any protocol that requires two independent ways to validate identity. Commonly, it uses "something you know" (password) as one factor, and either "something you have" (tokens, smart cards and digital certificates) or "something you are" (biometrics) as the other factor. Two-factor authentication enhances security, but each business scenario must dictate the authentication mechanism (Bowers, 2006). As a rule of thumb, schools should consider which regulations impact them, and conduct a risk assessment to balance between vulnerability, cost and impact. They can then decide the most appropriate way to strengthen authentication so that sensitive resources are protected while meeting regulatory requirements without going overboard.

ACCESS CONTROL & AUTO-PROVISIONING

As operating environment expanded to include more distributed applications and growing complexity in user relationship, managing user access is becoming enormously expensive and challenging for any organization (Jacknis, 2005). Access Control List (ACL) is the mechanism for defining security that limit access between users and network resources using filter rules. When a data packet arrives at a firewall, ACLs trigger a filtering process based upon predefined rules. IDM uses ACLs to assign access rights for users to resources. For example: professor A is allowed to access student records, while student X is denied access; student X is allowed to access the distance learning servers while guests are prohibited.

While commonly deployed, rule-based ACs are attached to objects. They are advisable only when options are few. Too much alternatives can complicate the policy to unmanageable and impede performance. In role-based ACs, access privileges are grouped into roles, and users are attached to roles as a way to manage their access (NIST, 2006). Role-based AC is more appropriate for Web services as access are assigned against a specific user's role and asserted to requesting applications. While simpler and more flexible, role-based AC does raised privacy concerns. In practice, both roles and rules are used to determine access rights. While inflexible and complicated, rules can provide fine-grain control and limit role proliferation.

Provisioning refers to the deployment of digital access rights for employees, business partners and customers across multiple applications and resources based on business policies. Resource provisioning includes the creation of user IDs and credentials. Conversely, de-provisioning deactivates accounts and reallocates resource when an employee leaves an organization. Apart from security, self-service auto-provisioning greatly increases an organization's operation efficiency. Auto-provisioning, for example, can automate account creation for new hires and account shut-off when employees leave the company. Self-service allows users update their accounts such as password reset, freeing up an enormous amount of staff and resources. Educational institutes are mandated to be in compliance with privacy legislations such as HIPAA and FERPA. Provisioning can be extremely helpful when it is time for the school's audit (Tynan, 2005).

CONCLUSION

For an educational portal, the hardest part of IDM does not lay in its development and deployment. Documenting business processes and defining who gets access to what resources can be a monumental task. While implementing IDM in the portal can be expensive, complex, and time-consuming, it can also lead to greater efficiencies and cost savings over time. More importantly, IDM is vital for any educational portal in this age of concern for privacy.

REFERENCES

- Bowers, Tom (2006). Two-factor Authentication Options, *Information Security,* 9(8) pp.30-35.
- Emigh, Jacqueline (2002). Portal Management - Do You Know What It Takes? *Enterprise Networking Planet*. Retrieved 9/22/06 from http://www.enterprisenetworkingplanet.com/netsysm/article.php/1478751
- Jacknis, Norman (2005). A Question of Identity, IT Architect. 11/2005 issue, p. 94.
- Levinson, Meridith (2002). Case Files: Knowledge Management, Portal U. CIO Magazine Retrieved 9/22/06 from http://www.cio.com/archive/110102/portal.html
- NIST (2006). Role Based Access Control, *NIST*, Retrieved 9/22/06 from http://csrc.nist.gov/rbac/
- Stone, J., Roof, J. & Lonsdale, D. (2006). The IT Portal - A Platform for Service Management, *Insight on IT Service Management*. Retrieved 9/22/06 from http://www.itsmwatch.com/itil/article.php/3613771
- Tynan, Dan (2005). Identity Management in Action, *InfoWorld*, 27(41), pp 23-26.