CAMP Identity Management Workshop
Management Track
Putting it all together: Identity management on your campus

Presenters: Thomas J. Barton, A. Michael Berman, Amy K. Brooks, Bret L. Ingerman

Date: Tuesday, November 16, 2004 at 10:15 a.m. - 11:30 a.m.

Scribe: Todd Piket

Discussion

I. Self Service Password Reset System
   a. The discussion began with self service password reset systems. The common system referenced in this discussion is one that asks the user one or more questions to identify themselves. In general, the questions asked of the user were initially established by the user at an earlier time in case the user forgot his/her password.
   b. The question was asked if it was safe to use such a system.
      i. Difficult to know the answer. Perhaps a risk/benefit analysis could clear it up. It was asked if it was possible to quantify the help desk savings when using such a system. No answer was proffered by anyone in the room. The consensus seems to be that the help desk time recovered by using such a system is worth using the system (i.e., the risk is worth the benefit).
      ii. It was offered by one institution that the self service application could be optional. If a person opts out of using the system then he/she would have to go through a less convenient process for resetting a password, but it would probably be more secure.
   c. Are there “good” questions out there that can be used by default?
      i. Someone offered that the Burton Group has done a study on this very question.
      ii. It is important to answer this question because it is useful to ward off your auditors.
      iii. There is other research out there other than the Burton Group. It may even be satisfactory to look at other web sites that use a question/answer system and using the questions that they do.
   d. If users are allowed to come up with their own question(s), how do we educate them on what a “good” question is?
      i. Put directions on the system that allows them to enter their own question(s).
         1. Put an emphasis on not using yes/no question(s).
      ii. Is this a moot point? The majority of users are already used to using such systems because of ecommerce or other means. Some have been victims of identity theft already and therefore they realize the importance of a “good” question.
   e. Can we keep users from forgetting their passwords?
i. No! However, by providing services that students use all year long will help students remember their password.

f. Can we keep users from giving out their passwords?
   i. Probably not, but as more and more services are tied to a single/central password students will be less apt to give their password to others.
   
   ii. We can send out notifications to users letting them know when a password change occurs. This will let them know if they don’t change their password, someone else will. If someone that is not them is constantly changing their password, it will educate them the hard way that they shouldn’t be giving it out.

II. Id Naming Conventions

a. University of Michigan uses an 8 character userid, but admits that most of the “good” ones are gone, because they have lots of users and they don’t recycle. They do try to use some form of name based userid. They now provide new users with a choice of several generated userids and to choose their own, but they don’t recommend trying to choose your own because it is difficult to find one that isn’t taken.

b. Users like something that is familiar to them (e.g., userid based on name). It’s easier for them to remember.

c. Some recommended using email address because it is unique. This stemmed a brief discussion on email forwarding/aliasing. Some allow it, but ran into closed list posting issues because the list expected the post to come from there local email, but the user was using his/her “actual” email address from MSN, Yahoo!, or whatever.

d. Some use the userid to map to an opaque identifier which is then used to perform the authentication/authorization. These folks do it this way because they feel that userids have less and less semantic meaning.

III. PKI / Stronger Authentication

a. Should we even bother to go down this road? What’s the motivation?

b. Removes userid/password concept and the security problems that come with the concept.

c. It can be prohibitively expensive.

d. It will probably make auditors happy.

e. How many organizations are doing it?
   i. Virginia is doing it for a decent size faculty base (several thousand).
   ii. Most that are using it are doing so with a limited population set.
   iii. It was asked how the population set was determined. No response from the floor.

f. Nathan Dors spoke about the fairly old SecureID system in place at his organization, but they are looking to replace it.

g. It was asked if we should use soft or hard tokens?
   i. Could be a mixture of both. Security level of user makes the decision.

h. Applications may not support the technology yet.
i. In many cases it’s difficult to secure the systems we already have. How do we ramp security up to protect the even more sensitive stronger authentication data?

IV. Making a case for an Identity Management System
a. Can improve automation of account creation which reduces manual steps in creating accounts which can decrease human error significantly.
b. Can help to establish provisioning for more subtle relationships/roles by exposing these relationships/roles through examination of business logic.
   i. Subtlety example: A full time student who is employed vs. a full time employee who is a student.
c. Provisioning can take a long time because of bureaucracy and the paper work that needs to get done, not because of technology. We should be able to use the IdMS to speed things up by reducing the amount of paper signing required to provision.

V. What data goes into an IdMS (the “join” process)?
   a. Enough data to perform reconciliation
   b. Data that is apt to be used frequently and/or broadly.
   c. Watch out for data that is going to need to be protected.
   d. If multiple applications are using similar common data make sure business rules are consistent for the data so “student”, for example, means the same thing to every application.

VI. Should the enterprise directory server be authoritative?
   a. It depends. Most likely it will be for some data like email address.

VII. What’s the difference between a data warehouse and an IdMS?
   a. The refresh cycle on an IdMS should be faster than a data warehouse.
   b. Data warehouses may have more data than is needed in the IdMS.