CAMP: Identity Management Workshop  
Panel: The Overlap of Technology and Policy

Date:    Tuesday, November 16, 2004   4:00 p.m. - 5:00 p.m.

Presenters:  Thomas Barton, A. Michael Berman, Michael Gettes, Paul Hill

Scribe:  Todd Piket

Discussion

I. Should the identity management system allow multiple password policies?
   a. No one specifically said “no” to this question or even disagreed that it
      would be a good idea for the system to, at least, support the concept.
   b. It was suggested that those with higher privileges should require separate
      expiration policies, longer passwords with more non-alphanumeric
      characters, etc.
   c. The question was asked if policies were enough or if the technology
      should enforce the policies. The answer, as usual, “it depends”.
   d. A handful of people have actually, deliberately gone through the process
      of defining multiple policies.
      i. How did the process work?
      ii. Lessons learned?
   e. Has anyone done risk assessment on the effectiveness of having longer
      passwords, or forcing password changes more often?
      i. Nobody indicated that they did.
      ii. Would this be something to indicate where a security risk is
          created because users start writing down their passwords because
          they’re too hard to remember? That could be one thing the
          assessment helps to determine.

II. The “other” problem / sponsored user accounts.
   a. Who should be entitled to use your systems?
      i. Some university libraries are a good example. The problem is that
         they are public so anyone has access. Who is “anyone”, and how
         should this access be granted?
      ii. The concept of sponsored accounts is a good one. “Trusted”
          university members can sponsor someone who is no way affiliated
          with the university, whether the person is a university librarian or a
          departmental system administrator.
          1. This is what MIT does and MTU is headed this way.
          2. A good reason for doing this is to help stop the sharing of
             passwords, a faculty member giving his/her password to
             family members for example.
      iii. Anyone can get an account at Duke and nothing is validated.
      iv. What should the time to live on a sponsored account be?
          1. At MIT the default is 1 year with a maximum of 2 years.
          2. Of course, “it depends”.
v. How does a sponsored account migrate? Should the user of the account become affiliated with the university?
   1. At U of Chicago, the user would get a new account at his university.
   2. At MIT the account migrates through a process, but a new username may be assigned.
vi. What if the sponsor goes away?
   1. At MIT the account gets deactivated, eventually.
   2. It seems that the sponsored user should be notified so that he/she can try and find another sponsor.
vii. What if a user needs multiple IDs for an application? Like a faculty member who wishes to have a WebCT account to be a designer and one to test the design with a user account.
   1. Allow trusted users to create testing accounts?
viii. Should there be another core system specifically for “other” users?
   1. The consensus was that the identity management system (IdMS) should handle this case similar to “regular” accounts.
   2. Perhaps there would be a separate authorization system.
   3. Delegated administration can help by permitting others to grant access to others whether they are sponsored or not.

III. ID Card Replacement for universities
a. At one university, the ID card was replaced because it was based on SSN.
b. At MTU the chip card was replaced because the chip was used too infrequently to justify the significantly more expensive chip cards.
c. Can we map a card ID to the IdMS so we can then provide access to various systems through this mapping?
d. One university has a very interesting card with multiple capabilities: a barcode, multiple magnetic (mag) stripes and a proximity card to handle all sorts of situations.
e. Is security an issue?
   i. How easy is it to modify the mag stripe or card’s chip? Those of us at technical institutions do find this to be a problem.
   ii. How easy is it to read the mag stripe and can sensitive information be obtained by reading the stripe.
   iii. Can a proximity card’s transmission be intercepted and replayed?
      1. This happened at MIT.