Proxy and Delegation Access

Problem

An individual is granted access to a service through some formal mechanism, however the indivudual would like to delegate that access to one or more individuals who cannot be identified through any authoritative means. For example, a faculty member wishes to delegate a variety of tasks for their course to individuals whose role or membership in the course is not captured as part of the ERP or directory service. Only the faculty member knows the users and their specific roles, so the assignments cannot be managed centrally.

Delegation of the access may be specific and temporary (ie, allow someone to approve purchaes while I am on vacation) or may be permanent (I would like my administrative assistant to be able to act as my proxy.) The nature of the access is such that I cannot delegate more authority than I have myself, and I will still be held accountable for the actions taken on my behalf.

Solution

Proxy and delegation solutions are often application-specific. For example, in the faculty example above, the same application that is used to gather final grades could provide a user-interface for the faculty member to manage the delegation of grading. Wherever possible, capturing delegation or proxy assigments in a central IdM system allows multiple applications to provision based on a single delegation.

Examples

- Professor Smith, by virtue of being the named instructor of a course, is granted access to print photo class rosters, to post course materials on the LMS site, and to enter official grades into the system of record. Professor Smith wishes for her teaching assistant to print the class roster at the beginning of the semester and post materials to the LMS site, and plans to ask her administrative assistant to enter the final grades for the course. In addition, Professor Smith has asked an honors student to view daily blog posts in WordPress, grade them, and enter the grades into the system.
- At the University of Michigan, faculty perform a variety of course-related activities using the PeopleSoft system of record. We built a bolt-on application that allows the faculty to delegate different tasks, and an automated batch process runs each day to grant/remove the PeopleSoft access roles based on the faculty member's choices. The process also interfaces the role assignments to the LMS system, and will soon interface the same information to the central IdM system so that it can be used to provision additional applications, such as WordPress, rather than manage it on and app-by-app-basis.
- For the UM online directory, individuals can grant proxy access to any other member of the UM Community to manage directory attributes on their behalf. Proxy access is stored as an LDAP attribute on the in individual directory entry.

Graphics (click on them to view full size)