Time-restricted Access

Problem

In many cases, access privileges may not be conferred in an open-ended fashion, but rather, may need to be restricted in time. Institutional policies may dictate that certain individuals are only authorized to perform certain operations or access certain resources during certain times of day, or certain times of year. Likewise, some access rights may be granted to individuals with a fixed expiration time. In any event, access rights need to be managed in a fashion which can permit their restriction in time.

Solution

At least three categories of solution may be applied effectively, depending on the requirements of specific situations and on institutional security preferences.

- If the situation calls for time-limited access **and** the subject of the access is himself a temporary associate of the organization, it may be sufficient to grant access without reference to any time restriction, and instead time-restrict the subject's identity itself. Rather than time-limiting the specific access privilege, arrange for the user (who may likely be a "guest" or other temporary affiliate) to lose the ability to authenticate at a prespecified time. Many authentication mechanisms provide built-in support for time-limiting identity in this way.

- If the situation calls for broad time-limited access that starts immediately and ends at a predetermined time, but the subject is a permanent associate of the organization, it may be advisable to use an existing solution pattern in conjunction with an out-of-band scheduled task designed to revoke access at the appointed time. This has the advantage of requiring no special time-based support from either the target application or the authorization mechanism - so long as an API is exposed through which, eg., the subject's membership in an authorization group can be removed, it can be used.

- If the situation calls for fine-grained time-limited access, such that a permanent associate of the organization should be granted special privileges on a recurring basis during specific windows in time, it may be possible to employ the out-of-band strategy outlined above, but more advisable to seek embedded support within either the target application or the authorization service for actual time restrictions. Few products are known to currently support such fine-grained time limits, however.

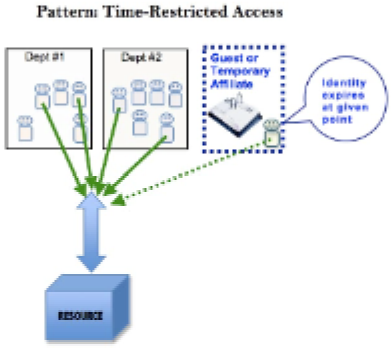
Examples

- A contractor working on a building site on campus needs to be granted temporary access to a number of facilities on campus, but only for so long as the he's engaged in the building project. He's issued a temporary identity that's in turn granted access as needed, but the identity is flagged for expiration at a fixed time agreed upon in his contract.

- A student is to be granted access to his instructor's research web site during the last half of the semester in order to use the instructor's research materials to pursue his final project in the instructor's class. Since other students in the class do not need access to the same materials, the student is added to the instructor's research associate group and a cron task is set up on the student registration system to remove the student from the research group in the campus group management system on the day after classes end.

- Employees in Housekeeping need access to all buildings in order to perform their job responsibilities. One research building on campus contains highly classified material related to DOE research, and access to that building must be restricted tightly. It is agreed that Housekeeping staff should have access to the building during the hours of 8am to 5pm on weekdays only. The campus building access system supports time-limited access controls, so the Housekeeping staff group is granted access to the building in the door control application on an explicit 8-5 weekday schedule only.

Graphic (click on it to view full size)


Pattern: Time-Restricted Access
Dept #1
Dept #2
Guest or Temporary Affiliate
Identity expires at given point
RESOURCE