NCSU Use Cases

Background

NCSU developed a home-grown facility for management of privileges within its Peoplesoft-based HR and financial systems some time ago, using as its basis the privileging mechanisms provided natively by Peoplesoft. Over time, the cost of maintaining that privileging system coupled with the perceived need for the additional capabilities of a true IDM system led to the university's deploying Sun Microsystems' Identity Management product, and negotiating with a Sun partner to re-implement the privileging system within the Sun IDM environment. The new solution relies heavily on automated approvals and workflows, and relies extensively on Peoplesoft's native role management and security mechanisms. It provides a great deal of flexibility in some areas, but lacks some granularity the university would find useful in some situations.

The resulting solution has some idiosyncratic properties, perhaps best elucidated through a pair of contrasting scenarios - one that highlights the solution's strengths and one that highlights its weaknesses. These scenarios are arbitrary, but reflective of real-world situations in which (in the first case) the NCSU system provides a particularly effective solution, and (in the second case) has some unexpected and potentially very undesirable consequences.

Use Case I - Interdepartmental Privileging Approvals

Sally is the business manager for the Department of Chemical Engineering within the university's Engineering School. One of her routine job responsibilities is entering into the privilege management system requests for access to fund code information on behalf of PIs within her department. When she took over this responsibility long ago, she was assigned a "requestor" role within the privileging system, and her department Chair approved her being associated with the Chemical Engineering department for purposes of filing requests on the department's behalf.

Following the recent early retirement of Bill, previously the business manager for the Department of Nuclear Engineering, the Nuclear Engineering department determined that with its small staff and faculty (totaling only a dozen individuals) it would no longer need a full-time business manager. The Chair of the Nuclear Engineering department negotiates an agreement with the Chair of the Chemical Engineering department to have Sally take on responsibility for making the infrequent requests for privilege changes on behalf of the handful of PIs in the department. The Nuclear Engineering Chair contacts the Dean's office and has a request submitted into the system to grant Sally access to the Nuclear Engineering data as well as Chemical Engineering data (Sally is not allowed to enter the request on her own behalf, but the Dean's business manager has access spanning the entire Engineering School, and can initiate the request on her behalf).

Because Sally's primary affiliation is with Chemical Engineering, the request first must be approved by the Chair of Chemical Engineering - he must authorize the adjustment of Sally's privileges within the system. The Chair, as a department head, has already been assigned a role allowing him to approve privilege changes staff, and as an affiliate of the Chemical Engineering department, he can exercise that role with employees of the department. Once he provides his approval (through a web interface into the privileging system), the change request is automatically routed to the Chair of the Nuclear Engineering department for his approval. Because the change to Sally's privileges involves granting her access to file requests on behalf of researchers in his department, the Nuclear Engineering Chair must also provide his approval. Like his counterpart in Chemical Engineering, the Nuclear Engineering chair has been granted a role allowing him to approve access requests within the system for "requestor" level access, and exercising that role, he provides his approval through the privileging system's web interface, and Sally is immediately able to file access requests for PIs in his department as well as in her own.

Later, when a new faculty member in the Nuclear Engineering department needs authorization to access financial information pertaining to a grant fund code for which he is the PI, he contacts Sally, who is able to initiate the authorization process within the system on his behalf.

Use Case II - Interdepartmental Privilege Scoping

After the events in Use Case I above, Sally decides that while she enjoys working with the Chemical Engineering department, she would like to return to working in Human Resources, as she did in a previous job. Not wanting to lose her as a business management resource within the department, the Chair works out an agreement with her to have her take on the added role of payroll clerk within the department (a function previously handled by the Chair's administrative assistant, John). The Chair has Sally work with HR to initiate a request to remove the payroll approval role from John's profile within the privileging system and another request to add that role to Sally's profile. Following his approval of both changes, the Chair is able to announce that Sally has taken on the additional job of departmental payroll clerk for Chemical Engineering. Later, while Sally is in the HR system reviewing pending payroll requests, she notices that she's not only seeing Chemical Engineering requests, but she's also seeing Nuclear Engineering requests. Concerned, she contacts the departmental IT manager, who explains that the system can't support her having one role in the Chemical Engineering department a different role in the Nuclear Engineering department without allowing her to exercise both roles within both departments.

Discussion

The first use case above highlights two key features of the current NCSU solution - workflow support for multiple, interlocking approval requirements, and hierarchical scoping of privileges.

In this case, a change is to be made that will affect the privileges of an employee in one part of the organization, but that will affect access to information associated with a different part of the organization. This sort of "interdepartmental" privileging scenario is not at all uncommon, particularly in higher ed environments. The system recognizes that there are actually two separate approvals required for this change to be authorized - one managerial approval, permitting a change (any change) to be made to Sally's profile, and one resource approval, permitting a change that affects access to departmental resources within the system. Because Sally is not part of the Nuclear Engineering department, the system requires approvals from management in both departments before the change is effected. This interlocking approval workflow is somewhat unique, and highlights the need for some privileging systems to consider not only "ownership" of resources to which subjects access is to be managed, but also the management of those subjects as resources themselves.

For purposes of separation of duties (and, I believe, to address specific concerns expressed by internal auditors) the system does not allow individuals to initiate requests on their own behalf, but the system does recognize the hierarchical structure of the organization, and reflects that hierarchy in a way that allows privileges to be "scoped" to specific subsections of the organizational hierarchy. Sally is to be granted rights at a departmental level, but a business manager in the Dean's office with school-level access is able to initiate the request on her behalf. The Dean's business manager is not, however, authorized to approve either Sally's profile being updated or access to the Nuclear Engineering department's fund codes being modified - those approvals must come from individuals with separate approval roles.

The second use case highlights a key limitation of the current NCSU solution - separation of roles and scopes.

Apparently as a direct outgrowth of the Peoplesoft paradigm for privilege assignment, the NCSU solution involves associating two sets of privileging information with each system user - a set of roles (which control the operations the user is authorized to perform within the system) and a set of row-level access rules (which control the resources within the system which the user can manipulate). Significantly, those two sets of information are associated directly with the user, and are **not** linked with one another.

In the second use case above, Sally is assigned an additional role by the Chemical Engineering department which expands the operations she is authorized to perform within the ERP to include approval of HR/payroll changes. That role gives her the ability to perform an additional set of actions **on any resource within the system to which she has also been given access**. Since she was previously given access to resources within the Nuclear Engineering department, she implicitly acquires new rights in **both** departments when she receives the additional payroll approval role. In essence, each of the roles assigned to Sally extends to every scope in which any of the roles extends. When a privileging decision is to be made, the system first determines whether Sally is authorized to perform the requested action, then determines whether her profile allows her to perform actions within the scope in which she is working - there is no allowance within the system, however, or Sally's actions to themselves be scoped. Sally does not have a "Chemical Engineering Departmental payroll approval" privilege, but rather, she has a "payroll approval" role that she can exercise, like her financial access requestor role, in both Chemical and Nuclear Engineering. If the Chair of Nuclear Engineering does not want to extend payroll approval privileges to Sally within his department, he must either have both her payroll approval and her financial requestor privileges revoked (by removing her access to the Nuclear Engineering department within the system), or negotiate with the Chair of Chemical Engineering to have her payroll approver role removed.