

1

**AUTHORIZATION DATA MODEL****CROSS-REFERENCE TO RELATED APPLICATIONS**

The present application is related to an application entitled "An Authorization Mechanism," filed in the U.S. Patent & Trademark Office by Cristina Buchholz on Feb. 21, 2003, Ser. No. 10/372,030, which application in its entirety is incorporated by reference herein.

**TECHNICAL FIELD**

This invention relates to information technology security sometimes referred to as e-security, and more particularly to authorization management within the context of information technology.

**BACKGROUND**

The working environment of e-business is characterized by open networks and cross-company business transactions, replacing closed, monolithic systems with intrinsic security mechanisms. In the world of Web services in eCommerce, access will depend more and more on authorization. In this environment, ways of rationalizing the authorization process and authorization status will be key.

Existing solutions for authorization management share a common constraint: they are all tailored to particular applications. Consequently, every time a new application is introduced into the corporate landscape, the user management tool has to create yet another adaptor for it. In most cases, the connection to a central user management tool also requires a plug-in to be installed in the software in order to accomplish the connection. While the user and current role information is centrally kept, because the information has to be prepared by and immediately available to each connected system, there is likely to be redundant storage. For example, where the same users have essentially the same roles and authorizations on different systems, the same user information may wind up being stored separately for multiple systems.

The amount of user information that must be handled is further exacerbated by the need to define and maintain separate roles for each distinct position within the organization, each distinct role being understood as a specific collection of privileges associated with a particular position. While user administration can rely on these roles for administering access rights, the advantages realized by the use of roles, in terms of easier inclusion of new users and grouping of function-related authorizations, are overridden by the huge number of roles to be maintained for even a medium-sized organization. Merely creating derived roles does not solve this problem of proliferation. In the case where the individual's actual role is merely a qualified version of a higher order role, the derived or qualified role merely gives rise to still another discretely defined role associated on an ad hoc basis with a specific privilege set for a specific position. Derived roles thus do not avoid proliferating data to be analyzed and maintained by the user management tools.

**SUMMARY**

The invention is based on an authorization data model that uses generic roles and, if applicable, responsibilities at run-time to complete an authorization process based on

2

non-static privileges associated with the currently defined roles and responsibilities associated with a given user. In one aspect of the invention, when prompted by a user request to access a protected resource, such as a data file, via an application, the application collects information at run-time about the user's currently defined role, e.g., sales manager, and privileges associated with that role, dynamically decides whether the user is authorized to access a given protected resource based on the current variable role-based information, rather than the user's identity, collected at run-time. In a preferred system, the collection of this authorization information is accomplished by querying a central authorization data repository external to the application. The central authorization repository preferably stores and maintains dynamically variable role data defining generic roles that can be associated with multiple users and assigns users to said generic roles, more than one user being assignable to a given role. The role data can be altered from time to time to change a definition of a given role independently of user associations, and preferably independently of the respective responsibilities of users associated with a given generic role or responsibility. The repository associates privileges with said roles based on their current respective definitions. The information collected from said repository by the application includes the current variable value of the privilege status, with respect to the sought-after protected resource or type of resource, associated with the currently defined role assigned to the user requesting access.

In addition to roles, the repository can store and maintain generic responsibilities, e.g., sales territory, in the same manner described for roles, the responsibilities being variable, independently of the roles and users, and assignable to multiple users.

In the preferred system, the users are assigned to roles and responsibilities by decomposing a given user's positional functions and responsibilities into basic actions and objects to which the actions are applied, mapping the actions and objects onto respective generic roles and responsibilities stored in said repository, and assigning the respective roles and responsibilities to the user.

In another aspect of the invention, multiple applications collect current, variable authorization information at run-time from an external central repository that maintains updated generic role and, if applicable, generic responsibility information independent of user identity, thus replacing a fixed authorization structure with a flexible wild-card based model. Upon receiving requests for authorization at a plurality of applications from users seeking access to protected resources, the applications independently collect respective authorization information at run-time from a central repository containing user information, the user information including non-static roles whose definitions and corresponding privileges are variable, independently of the users associated with said roles. The applications base decisions on access to protected resources on the current authorization information collected at run time in response to a given request.

Still another aspect of the invention comprises an authorization information management process comprising storing in a central repository dynamically variable role data defining generic roles that can be associated with multiple users, along with responsibility data in the same manner, if applicable. In this process privileges are associated with the roles or responsibilities based on their current respective definitions. When queried by an external application, the current variable value of the privilege status, with respect to a given protected resource or type of resource, associated