

## AUTHORIZING A REQUESTING ENTITY TO OPERATE UPON DATA STRUCTURES

### CROSS-REFERENCE TO RELATED APPLICATION

The present application claims priority from co-pending U.S. provisional application Ser. No. 60/275,809, filed Mar. 14, 2001 and entitled "Identity-Based Service Communication Using XML Messaging Interfaces", which provisional application is incorporated herein by reference in its entirety.

### BACKGROUND OF THE INVENTION

#### 1. The Field of the Invention

The present invention relates to the field of network security. Specifically, the present invention relates to methods, systems, and computer program products for authorizing a requesting entity to operate upon data structures in a standard manner that is at least partly independent of the type of underlying data structure being operated upon.

#### 2. Background and Related Art

The success of the information age is widely attributed to the ability to efficiently access data. Data comes in a wide, almost unlimited, variety of different data types. For example, there may be data types corresponding to calendar information, task information, in-box information, word processing documents presence information, favorite web site information, or a host of other different types of information. Often, it is desirable to control who has what kind of access to what kind of data. For example, a user or application might have read/write privileges over a small group of files, while having read-only privileges over another group of files.

Conventionally, this was accomplished by using an Access Control List or ACL associated with each file or directory in a hierarchical directory tree structure. Typically, access control rights for a particular directory are inherited by any descendent directories or files unless expressly overwritten by an access control list at the descendent directory or file. When a request comes in to perform an operation on a particular target file or directory, the total access control for that request is defined by any access rights inherited as well as the express enumeration of access rights indicated in the corresponding access control list for the target file or directory. If appropriate for the total access control permissions corresponding to the target file or directory, the request is then processed.

The use of access control lists thus allows for access control at the granularity of a file or directory. However, often certain parts of a file may be more sensitive than others. Regardless, the conventional use of access control lists provides the same level of access to all parts of a file. In other words, conventional access control lists do not provide for granular access control below the file level. Accordingly, what is desired are methods, systems, and computer program products for providing more refined granular access control than the directory or file level.

In addition, conventional access control lists grant the same level of access regardless of the way the user or application was authenticated. However, there are often a wide variety of authorization methods available, each offering a different level of confidence that a user or application requesting operation is indeed who it purports to be. It may not be appropriate to grant the same level of access to a user or application who used a relatively low security authentication method such as the simple assertion method as

compared to a user or application that used a relatively high level of authentication. After all, it would be fairly easy for an imposter to simply assert that they were a particular authorized user or application. Accordingly, what is further desired are methods, systems, and computer program product for granting appropriate access privileges based on authentication credentials.

### SUMMARY OF THE INVENTION

The present invention extends to methods, systems and computer products for authorizing a requesting entity to have a service perform a particular action in a manner that is at least partially independent of the underlying target data structure that is desired to be accessed. In one operating environment, there are a number of individuals and applications operating through a variety of services on a variety of different types of identity-specific data structures that are organized in accordance with a set or rules. Each service is configured to perform operations on one or more different types of data structures. For example, an identity may have an in-box data structure organized in accordance with an in-box schema and that is managed by an in-box service, a calendar data structure organized in accordance with a calendar schema and that is managed by a calendar service, and so forth.

The principles of the present invention allow for authorization of a requesting entity to occur largely, if not wholly, independent of the type of the underlying data structure that is desired to be operated upon. This allows for a centralized authorization station that performs the entire authorization process for a wide variety of different services. The centralized authorization station may then inform the target service that the requested operation is authorized and provide the service with sufficient information to perform the desired operation on the target data structure. Although only one authorization station is described and illustrated for clarity, there may be more than one (and even numerous) authorization stations that perform the described authorization on behalf of the services.

In one embodiment, the authorization station maintains a number of role templates that each define basic access permissions with respect to a number of command methods. Those role templates may be included within a role map document in which all of the role templates corresponding to a particular service are compiled. The role templates represent coarse-grained access permissions corresponding to permissions that might be of particular use when accessing the particular service. Thus, applications that are not able to implement more fine-grained access control may at least implement these core role templates for coarser-grained control over access permissions. When the authorization station receives a request, it identifies the target service and thereby accesses the appropriate role map that contains the corresponding role templates.

The authorization station also maintains a number of role definitions that each define access permissions for specific requesting entities by using one or more of the role templates. In one embodiment, all of the role definitions that might define access permissions with respect to a particular identity's data are included within a role list document. There may be a role list document corresponding to a particular identity. Each role definition defines access privileges with respect to this identity's data for a requesting entity. The requesting entity is specified by a user identifier, an application-platform combination identifier, and a credential type identifier.