

DAC, MLS, Chinese wall, ORCON, object-based SoD constraints, etc.). In addition, basic application services can be provided through configuration to include those services offered by workflow management, email, and database management applications. This is in contrast to the “hard-wiring” of policy into the mechanism.

[0179] Additionally, the system **20** provides policy combinations. Resources, (objects) regardless of their type, can be selectively protected under one or more configurable policies (e.g., DAC only, or DAC and RBAC combined).

[0180] The system **20** also provides comprehensive enforcement. All user and subject (process) access requests, and all exchange of data to and from and among applications, between sessions, all exportation of data outside the bounds of the PM can be uniformly controlled under the protection policies of the objects of concern.

[0181] The system **20** also provides assurance. Configuration strategies can render malicious application code harmless, prevent unlawful leakage of data, and all enforcement could be implemented in the client module **28** but outside the user applications, e.g., at the operating system kernel level.

[0182] The system **20** also provides for policy libraries. Standard configurations for a variety of policies may be made available and new configurations can be created for immediate policy instantiation, testing and deployment. This reduces the burden on administrators in specifying and configuring policies. In addition, basic application services can be provided through configuration to include those services offered by workflow management, email, and database management applications.

[0183] The system **20** features as described herein could be provided through a number of architectural deployments to include implementation within a single operating system environment. Our reference implementation provides centralized policy configuration and decision-making within a local user environment. This kind of deployment affords still additional benefits, such as single enterprise-wide scope of protection for one administrative domain vs. policy management on an OS-by-OS and application-by-application basis. Access control policies are uniformly enforced over resources that are physically stored on a multitude of heterogeneous systems.

[0184] The system **20** also provides a true single-sign on. By virtue of the single scope of control and a personal object system that includes the ability to reference and open any resource accessible to a user (e.g., email messages, work items, files, records and fields within records), the system **20** eliminates the need for a user to authenticate to a multitude of applications and hosts.

[0185] The system **20** also provides logical access. Any accessible resource could be securely accessed through any PM compliant OS with access to an application to process the resource.

[0186] The system **20** also reduces the need for OS vendor support. To be PM compliant, all an OS vendor needs to do is implement a standard set of enforcement functions (i.e., PM authentication, user resource presentation, session management and reference mediation), and does not need to be concerned with the management of access control data, or performing access control decisions.

[0187] Although a combination of features is shown in the illustrated examples, not all of them need to be combined to realize the benefits of various embodiments of this disclosure. In other words, a system designed according to an embodiment of this disclosure will not necessarily include all of the features shown in any one of the Figures or all of the portions schematically shown in the Figures. Moreover, selected fea-

tures of one example embodiment may be combined with selected features of other example embodiments.

[0188] The preceding description is exemplary rather than limiting in nature. Variations and modifications to the disclosed examples may become apparent to those skilled in the art that do not necessarily depart from the essence of this disclosure. The scope of legal protection given to this disclosure can only be determined by studying the following claims.

What is claimed is:

1. A general attribute-based access control system, comprising:

at least one resource server that stores and retrieves computer-accessible resources referenced by objects to and from resource repositories;

at least one client module that authenticates human users, executes programs as processes on behalf of authenticated users, requests access to the computer-accessible resources referenced by the objects, and enforces access policies with respect to the objects;

an access control database including basic data sets and basic relations between the basic data sets, the basic data sets including data corresponding to users, user attributes, objects, object attributes, operations, policy classes, and the processes, wherein the objects are names for the computer-accessible resources to which access by processes is controlled and which may be stored on the at least one resource server, and each object is also an object attribute, the operations are actions that can be performed on the computer-accessible resources and also include administrative operations that create, delete, and update elements of the basic data sets and the basic relations, and a process is an instance of a computer program being executed on behalf of any of the users, has a unique identity, and issues access requests, and the basic relations including assignments, prohibitions, and obligations, wherein the assignments collectively are representations of the capabilities of the users to perform operations on the objects, the prohibitions are representations of the capabilities of the users that are denied to the users or the processes, and the obligations are representations of conditions under which the basic data sets and the basic relations are obligated to change in a manner also prescribed in the obligations; and

at least one server module including an access decision sub-module that computes a decision whether to grant or deny access to the computer-accessible resource referenced by any of the objects to any of the processes, an event processing sub-module that processes events, and an administrative sub-module that creates, deletes, and modifies elements of the basic data sets and the basic relations.

2. The general attribute-based access control system as recited in claim 1, wherein the at least one client module includes a user authentication sub-module configured to establish an association between the human users and the data corresponding to the users of the basic data sets through an authentication scheme, a user space sub-module that executes programs as processes that issue access requests on behalf of any authenticated user, and a policy enforcement sub-module that enforces access control decisions with respect to the access requests issued by the user space sub-module, and wherein any access request issued by any of the processes is a pair composed of any of the operations and any of the objects.