Abstract

Over the last few years, various types of access control models have been proposed for expressing the growing needs of organizations. Out of these, there is an increasing interest in specification and enforcement of flexible and dynamic decision making security policies using attribute based access control (ABAC). However, it is not easy to migrate an existing security policy specified in a different model into ABAC. Furthermore, no comprehensive approach can specify, enforce, and manage ABAC policies along with other policies potentially already existing in the organization as heterogeneous security policies. In this thesis, our aim is to develop a unified framework for enabling specification and enforcement of heterogeneous access control policies, such as ABAC, role based access control (RBAC), and a combination of both ABAC and RBAC, named as meta-policy based access control (MPBAC). Additionally, we also introduce an administration model for managing heterogeneous access control policies and propose a methodology for performing security analysis of heterogeneous access control policies in the presence of the proposed administrative model.

In this work, we present a unique and flexible solution that enables concurrent specification and enforcement of such security policies by storing and querying data in a multi-dimensional and multi-granular data model. Specifically, we present a unified database schema, similar to that traditionally used in data warehouse design, representing different access control policies and storing relevant policies as in-memory data, thereby significantly reducing the execution time of access request evaluation. We also present an approach for combining multiple access control policies through meta-policies. Extensive experiments on a wide range of data sets have been performed to demonstrate the viability of the proposed approach.

Next, for ease of administration, we introduce a complete role based administrative model for managing ABAC, RBAC and MPBAC, named as RAMHAC. It uses RBAC itself to manage ABAC, RBAC and MPBAC. RAMHAC consists of forty-one administrative relations, commands, pre-constraints, and post-constraints. The administrative relations capture policies that define which administrative role can modify which component of ABAC, RBAC and MPBAC. ABAC, RBAC or MPBAC components define a state of the system that can be changed by commands upon their successful execution under the control of administrative policies, pre-constraints, and post-constraints.

Finally, we introduce a methodology for performing security analysis of ABAC, RBAC and MPBAC in the presence of RAMHAC. In this work, μZ, a fixed-point constraint solver, has been used for analyzing the various security properties, like reachability, safety and liveness. Extensive experiments on a wide range of data sets have been done to study the impact of the components of ABAC, RBAC, MPBAC and RAMHAC on time taken for security analysis.

Keywords: *ABAC, RBAC, RAMHAC, Administrative model, Security analysis, Fixed-point analysis*