Abstract

In recent years, Attribute-Based Access Control (ABAC) has emerged as the desired access control model for many organizations. ABAC provides the most fine-grained access control as compared to the contemporary access control models and supports dynamic decision making through the inclusion of environment conditions. However, the successful deployment of ABAC in an organization largely depends on the process of policy engineering that involves the construction of an appropriate set of rules called an ABAC policy. In this thesis, we present a collection of novel techniques for policy engineering that facilitates the development of an ABAC policy in varying situations. First, we present a method that enables an organization to use an existing policy from another organization having similar attributes and their values. The proposed method eliminates the need for ab-initio development of an ABAC policy. Next, we discuss two different policy engineering approaches. The first is a bottom-up approach that is suitable for scenarios where all the permitted accesses in the organization are known. Here, we use Gini impurity to form the authorization rules from the given accesses. The second is a hybrid approach that constructs an ABAC policy with the help of the security officer of an organization and only a fraction of the organizational accesses. Finally, we propose a technique that intuitively represents the permitted accesses in an organization and forms authorization rules using it. The intuitive representation facilitates an easy understanding of the access patterns in the organization and also helps in detecting unauthorized accesses. We have performed the complexity analysis of all the proposed methods. Also, experimental evaluation of all the proposed methods on various synthetically generated data sets is carried out to ensure their applicability in different scenarios.

Keywords: Access Control Models, Attribute-Based Access Control, ABAC Policy, Policy Engineering, Policy Adaptation, Policy Mining, Hybrid Policy Engineering.