Fuzzy Approach to Role Based Access Control

Name

Introduction

The goal of access control is to allow only authorized users to access sensitive information. Role based access control (RBAC) is emerging as a generalized approach to security and has been shown to be applicable to a wide range of security requirements of organizations and applications [3]. Possibility of using RBAC approach to an environment with multiple policy domains further justifies the tremendous momentum seen in RBAC research in the recent years. However, with the increasing size of the problem domain represented by today's huge information systems that cross organizational boundaries, the issue of management and complexity of security and providing its assurance poses daunting challenges. A fuzzy approach to addressing the issue of security can provide a pragmatic and promising new direction in this area.

RBAC approach is based on the premise that authorizing a particular user to access organizational information and to make modifications to it is generally based on the roles and responsibilities the user has within the organization. However, precise categorization of information in order to build an access policy, particularly in today's systems, becomes futile because of the enormity of the information space. In many cases, human decision is needed for such categorizations as well as the formulation of security policies, bringing in the fuzziness that is natural in real world. For example, a document may be categorized somewhere between being *top secret* or *secret*. Role definitions vary from organization to organization. This increases the difficulty when systems with different policies and role structures have to interact. Furthermore, the specification of organizational security policies using such roles becomes imprecise highlighting the possibility that a fussy approach may be a more pragmatic way of dealing with such a problem.

Some initial attempts to address the usefulness of fuzzy logic to information security can be found in the literature. In [1], Hosmer highlights the fuzziness inherent in many security policies, particularly in non-

traditional ones such as privacy, integrity and availability. Hosmer further highlights the possible applicability of fuzzy logic approach to multiple policy systems [1]. Kendel uses fuzzy set theory to policy analysis [2].

Proposed Project Tasks

In this project, I propose to carry out the following two tasks:

Task 1: *Development of a Fuzzy-RBAC model*: Under this task, I plan to first investigate the applicability of fuzzy approach to RBAC by identifying access control requirements that are inherently fuzzy in organizational contexts. Then I propose to develop a Fuzzy-RBAC (F-RBAC) model by extending an existing RBAC model with fuzzy parameters to allow imprecise access control policies.

Task 2: *Apply fuzzy approach to integrate two different policy domains*: Once an F-RBAC model has been formally defined, I plan to investigate and develop a methodology to integrate two policy domains that use F-RBAC, to allow secure access across domain boundaries. I will compare the integration result with the one using general RBAC that has no fuzzy parameters, in order to delineate pros and cons of each approach. Use of Guru is expected for this task.

The impact of the result will be significant for two reasons. First, the result will establish the applicability of fuzzy theory to RBAC, whose importance and applicability has been well recognized. And secondly, access across policy domains represents the scenario of current and future information systems, work related to which is limited and pragmatic solutions do not exist. A positive result of the second task can significantly contribute to a relatively new challenge.

References

[1] Hosmer, H. (1993) "Security is Fuzzy!," *Proc. New Security Paradigms Workshop*, pp. 175-184, 1993.

[2] Kandel, "Fuzzy Statistics and Policy Analysis", *Fuzzy Sets: Theory and Applications to Policy Analysis and Information Systems*, ed. By P. Wang and S. Chang, Plenum Press, New York, 1980.

[3] R. R. Sandhu, "Role-based Access Control," *Advances in Computers*, vol. 46, Academic Press, 1998.