RBAC in Practice

Virginia N. L. Franqueira and Nelly Condori Fernandez

University of Twente
Enschede, The Netherlands
{FranqueiraV,N.CondoriFernandez}@ewi.utwente.nl

1 Introduction

Since the Role-Based Access Control (RBAC) model was first introduced [2], it evolved into probably the most discussed and researched access control model in academia. It became the basis for hundreds of textbooks, research prototypes and theoretical studies. Specially after the NIST (National Institute of Standards and Technology) standard for RBAC [4] was officially approved by the American National Standards Institute [1], RBAC features also gained a lot of attention of high profile commercial products. Its basic feature, which decouples the assignment of users to permissions via roles (illustrated in Figure 1), together with additional features are claimed to allow an efficient management of permissions, an effective enforcement of the need-to-know principle, and a scalable assignment of permissions to users. However, it is unknown to what extent the efforts put into RBAC research and development make true their promise in practice. Are they really aligned with the needs of the practitioners? Requirement engineers should be the first to know the answer!

Fig. 1. RBAC basic feature: assignment of users to permissions via roles [3]

In an earlier literature study, we collected: (a) a set of core features of RBAC, (b) its assumptions and strengths, and (c) a set of phenomena which may limit these strengths in practice. This study revealed that roles can be used to control access to information in: *support applications*, with operating system-specific roles; *stand-alone business applications*, with application-specific roles; *enterprise-wide applications*, with roles shared among several applications; and *cross-enterprise applications*, with roles shared among several enterprises. This empirical proposal builds upon our initial study and aims to verify to what extent these features, assumptions, strengths and phenomena are recognized and important in practice, and also aims to complement our knowledge with additional strengths and phenomena, collected from practitioners.

2 Wanted from Industry

To achieve our goal, we are seeking to gain a broad instead of a deep knowledge of RBAC in practice, i.e. we look for a large number of organizations of any size (e.g., small to multinationals) and from any sector (e.g., banking, government, telecom). One professional per organization experienced with *role engineering* ("the process of defining and implementing roles" [5]) and/or *role management* would be ideal. However, we impose no restriction on how this experience has been acquired. Therefore we welcome, e.g., system administrators, consultants, risk managers, information security officers, IT architects, decision makers, Identity and Access Management experts.

3 Work Plan

Our research strategy includes two steps. The first step is an online survey (requires 0.5 hour) to do a quick scan of the use and experience with RBAC across organizations. The second step will build up on the survey and will include one in-depth interview per organization (requires 1.5 hour) to understand reasons behind choices and get any other background information relevant to the use of RBAC. In the end, the participants will receive a summary report of the results which can help them either to improve the use of RBAC in their organization, or can help them to learn if pitfalls of RBAC they experienced in practice are echoed by the experience of other organizations. We expect the whole process will take three months to complete, after the survey is launched.

References

1. ANSI/INCITS_359: Information Technology - Role Based Access Control. American National Standards Institute (ANSI), International Committee for Information Technology Standards (INCITS) (February 2004)
2. Ferraiolo, D.F., Kuhn, D.R.: Role-Based Access Controls. In: Proc. of the 15th NIST-NCSC National Computer Security Conference. pp. 554–563 (October 1992)
3. Ferraiolo, D.F., Kuhn, D.R., Chandramouli, R.: Role-Based Access Control. Artech House, Inc., Norwood, MA, USA (2003), ISBN: 1-58053-370-1
4. Ferraiolo, D.F., Sandhu, R.S., Gavrila, S.I., Kuhn, D.R., Chandramouli, R.: Proposed NIST Standard for Role-Based Access Control. Information and System Security 4(3), 224–274 (2001)
5. Gallaher, M.P., O'Connor, A.C., Kropp, B.: The Economic Impact of Role-Based Access Control. Tech. Rep. RTI Project Number 07007.012, National Institute of Standards and Technology (NIST) (March 2002)