INTRODUCTION

Access control is part of the basic security mechanisms. It affects a wide area of applications including operating systems, database systems, enterprise resource planning systems, workflow systems, Information Technology systems, and many more security sensitive applications. In the last decades, the “Role Based Access Control model” (RBAC) (Sandhu, Coyne, Feinstein, & Youman, 1996; Ferraiolo, Sandhu, Gavrila, Kuhn, & Chandramouli, 2001) has become the dominant model for access control in both commercial and research fields. By structuring and simplifying the access control management, the RBAC model has proven its ability to bring a substantial enhancement of performance and
productivity and has become essential to large enterprises.

Nonetheless, the configuration and deployment of the RBAC model into the organization is still a major difficulty. “Role engineering” refers to the task of structuring the different organization actors into roles and assigning authorizations to them. This task has been fully manual for years. The first approach to role engineering, known as the top-down approach, relies on top-down information and defines roles by decomposition. Security experts have to consider the different use cases, and conduct interviews with business experts and users in order to deeply understand the semantics of business processes. Then, they define the roles by carefully analyzing the business processes and decomposing them into smaller units in a functionally independent manner. The second and less used approach to role engineering is the bottom-up approach. The available bottom-up information, consisting of the deployed access control rules prior to RBAC adoption, is involved. Roles are built by manual aggregation, often in conjunction with the top-down decomposition.

The manual approach to role engineering suffers from several limits. First, it is very expensive. According to a NIST report (Gallaher, O’Connor, & Kropp, 2002), role engineering is estimated to consume 60% of RBAC framework set up and exploitation costs. Second, it is a long process that may last several months. Third, it usually requires the involvement of security access control advisors in the internal business process, which may raise serious security issues. Forth, it does not fully leverage the existing access control framework, since the usage of the bottom-up information remains limited. Finally, it suffers from scalability limits. In a context of dozens of business processes, tens of thousands of users and millions of authorizations, the operation may become unfeasible, and has seldom been done successfully. Thus, relying only on manual role engineering has revealed to be insufficient, not viable, and constitutes a limit to the deployment of the RBAC model in enterprises.

In this context, “role mining” (RM) has presented as the best alternative to traditional role engineering approaches. Indeed, when Kuhlmann et al. (2003) have first suggested automating the bottom-up role engineering approach by using existing data mining techniques to extract the roles from the deployed user permission assignments, this has been a very attractive idea. In fact, it promises to drastically reduce the process cost and complexity. The required time to perform role engineering is likely to decrease from several months with the manual approach to few seconds/hours with the automatic role mining approach. Moreover, the guarantee to take into consideration the existing user-to-permission assignments is an argument that could encourage organizations to move to the usage of RBAC more confidently. Thus, this has been the beginning of intensive research work on role mining.

Role mining is a vivid research field. It has inspired a number of solutions and has showed important advances in a relatively short time. Most of the proposed solutions are trials to adapt different existing data mining techniques to the extraction of roles from the deployed user to permission assignments. It becomes difficult to discern the interesting solutions, and to understand the difference between them in the absence of standardized evaluation metrics and clear objectives. Moreover, fully automating the role definition process, basing only on bottom-up information has raised the problem of the interpretability of the generated roles. Indeed, relying only on the deployed access control rules results usually in roles that are neither intuitive nor meaningful. This is why, more recently, the trend has become to combine top-down role engineering techniques with bottom-up role mining techniques, which is known as the “hybrid role mining.” However, hybrid role mining also raises new problems such as how to combine top-down information within the data mining process, and which top-down information is to be retained. Likewise, role mining techniques output a long list of roles and leveraging them manually is very laborious. This task needs to be assisted by further automatic tools for role
A Study on the Intention to Adopt Third Generation (3G) Wireless Service on a Small Community with Unique Culture: The Use of Hofstede Cultural Dimensions in Predicting the Interaction between Culture and the Technology Acceptance Model on Guam
Kevin K.W. Ho (2012). International Journal of Systems and Service-Oriented Engineering (pp. 57-77).
www.igi-global.com/article/a-study-on-the-intention-to-adopt-third-generation-3g-wireless-service-on-a-small-community-with-unique-culture/89388?camid=4v1a

A Method for Detecting Bad Smells and its Application to Software Engineering Education
www.igi-global.com/article/a-method-for-detecting-bad-smells-and-its-application-to-software-engineering-education/122789?camid=4v1a

Ubiquitous IoT in the Automotive Domain: Decentralized Adaptation
www.igi-global.com/chapter/ubiquitous-iot-in-the-automotive-domain/186900?camid=4v1a