Usage and Impact of Model-Based User Authorization

Martin Juhrisch, Dresden University of Technology, Germany
Gunnar Dietz, Dresden University of Technology, Germany

ABSTRACT

Identity management projects are often a great challenge for organizations. This is not due to the technical complexity of these projects, but due to the fact that managing access to resources and services involves a deep understanding of organizational responsibilities, workflows, and processes. The presented approach aims at enabling domain experts to deal with that complexity without the support of external expertise. To accomplish this, the approach involves the organizational dimension of role engineering. The integration of the organizational layer is achieved by seamlessly integrating model data from process optimization projects. Conceptual models carry knowledge about the structure of an organization and its processes. The role engineering process is driven by the information in these models. The presented approach is not limited to the technical level and thus allows a high degree of automation. This research deals with – in addition to a practical illustration – a theoretical answer to the question whether it is even possible to integrate semi-formal models in an automated transformation process of transformation and requirements for such a process. The aim of this paper is to give a first positive answer to this question and to provide a way to automatically generate a useful setting for configuring identity management systems based on semi-formal models.

Keywords: Authorization, Conceptual Models, Description Kit Approach, Identity Management, Role-Based Access Control

INTRODUCTION

The need to raise the level of automation of development and configuration of application systems fosters the discussion about a more effective usage of conceptual models as one well established instrument in the field of information management. What is missing is a deeper understanding of the specific requirements of a purely model-based approach. In the literature there is little agreement about the problems that exist in dealing with semi-formal models when trying to analyze them automatically – to compare or to integrate them, respectively.

Model-based methods are often used in situations, where management processes are highly manual and cause extensive efforts, like in quality management, business process management, or system simulation. They serve as an essential instrument in the administration, configuration and improvement of the enterprise. An increased efficiency could be achieved if the necessary activities are solved completely model-based.
The wide field of service management, especially in service-oriented architectures (SOA) (for a good overview see Demirkan, Kauffman, Vayghan, Fill, Karagiannis, & Maglio, 2008) contains the management of the underlying security layer, namely the access rights for the services within a SOA. However, nowadays many identity management (IdM) solutions still only address application access control and lack support for a fine-granular SOA with a lot of possible access rights.

The role based access control (RBAC) paradigm (Ferraiolo & Kuhn, 1992) was the beginning of a shift from creating simple bundles of access rights in the form of groups towards creating bundles of persons with similar access rights — the so-called roles. Most IdM solutions implement a certain interpretation of RBAC to create a connection between users and their corresponding rights (to access resources and services).

The management of these roles, however, often remains a difficult task. Also underestimated is the definition of resources and their (access) rights, especially their granularity (access to an application system as a whole versus access to certain functions or services within an application). This is a problem one encounters not only when thinking about rights, but already when thinking of workflow and process optimization within an organization. The granting of access to a certain resource should reflect the necessity of using these resources within certain workflows. The question “who is responsible for what within the company and why?” needs to be answered (possibly also including a “when”).

A detailed process analysis aims at answering this question and often yields a huge amount of information. This information is often prepared, summarized, and visualized in conceptual models. A natural question would be: Is it possible to use these models to at least semi-automatically generate a configuration for an identity management? This would include a useful set of roles as well as rules and policies to assign them to users and resources.

This paper aims at answering this question positively. After this introduction our research methodology is presented. A background section introduces fundamental concepts before stating the research problem. Some barriers for solving the problem are discussed, especially integration conflicts in modeling, which motivate the use of a certain modeling approach, the so-called Description Kit Approach (DKA). This approach creates the necessary foundation for delving into the problem of model-based authorization, which includes the two parts model-based access control and model-based role identification. The applicability of this approach in real projects is discussed before finishing with future research and concluding remarks.

**RESEARCH METHODOLOGY**

The need for explication of a research design is the obligation of transparency about the steps on the way to the developed research results. Thus, in our case the explication serves as a first result in the presentation of the design rationale for the developed artifact. Its validity largely depends on the appropriateness of the selected research method. Conclusions may be drawn already here about the usefulness and quality of the obtained results.

We follow a technology-oriented, constructivist position of the research process (Hevner, March, Park, & Ram, 2004). Similar to the engineering disciplines, research is understood as the process of understanding a problem and constructing an appropriate artifact in the form of (descriptive, explorative etc.) models, algorithms and/or objects. We do not claim to explore the socio-technical cause-effect relationships of the use of the artifact in IS. Rather, the understanding of the domain is achieved during a solvation process of an isolated problem. Becker, Holten, Knackstedt, and Niehaves (2004) describe such processes on various levels, graded on their practical implications from theoretical to technological and/or abstract to domain-specific.
Relationship of Skill Expectation Gap Between IS Employees and Their Managers with User Satisfaction
www.igi-global.com/article/relationship-skill-expectation-gap-between/1321?camid=4v1a

Information Technology & FDA Compliance in the Pharmaceutical Industry
www.igi-global.com/article/information-technology-fda-compliance-pharmaceutical/44546?camid=4v1a