A Method for Constructing Enterprise-wide Access Views on Business Objects

Sabine Buckl, Florian Matthes, Sascha Roth,
Christopher Schulz, Christian M. Schweda

Lehrstuhl für Informatik 19 (sebis)
Technische Universität München
Boltzmannstr. 3, 85748 Garching
{sabine.buckl, matthes, sascha.roth, christopher.schulz, schweda}@in.tum.de

Abstract: Modern application landscapes consist of a multitude of inter-connected business applications exchanging data in manifold ways. These business applications are used by employees who take on several organizational roles. However, when broadening the scope to an enterprise-wide perspective, lack of clarity and uncertainty prevail regarding the questions which roles have access on which business applications as well as the business objects managed by them. In contrast to alternative approaches, e.g. single sign on, this paper focuses on the enterprise-wide availability of business objects. Motivated by a case study from the car manufacturing industry, this article describes a method to analyze and justify an enterprise-wide access matrix. Respective viewpoints are presented facilitating a business object access management on enterprise level. The method and concepts are further substantiated by means of the case study.

1 Introduction and motivating example

Nowadays, an enterprise's typical application landscape is characterized by a plethora of *business applications* which are interlinked via interfaces used for data exchange. In the course of time, the amount of data stored in these business applications continuously increases, among others as a result of the broadening business support. While the provision of business support inevitably means that employees get access on data that 'they need to know', access to further data has to be restricted. Role-based access mechanisms allow distinctive read and write permissions, while grouping access rights to logical units, so called *roles*. Against the background of an increased interconnectivity of business applications, the mechanisms of role-based access control deserve in-depth analyses. Especially the question, whether a role may transitively access confidential information is of high interest.

The need for a matrix describing the access permissions of a role in a comprehensive manner is confirmed by one of our industry partners acting in the automotive industry. Recent economic development has encouraged this partner to construct a car production plant in the United States to assemble and sell products right on site. From an IT perspective, this means that 170 business applications hosted in Germany will also provide business support for the new plant. Due to *Federal Rules of Civil Procedure*[1] as well as the amendments made

[1] see http://www.uscourts.gov/rules/newrules4.html for details.

on federal state level[2], an attorney filing a lawsuit possibly gets access to electronically stored information retrievable by making use of business applications. In case of the car manufacturer, claims considering specific automotive parts (e.g. front brakes, or gear drive) may allow the plaintiffs counsel in some circumstances to conduct detailed on-site investigations to find additional evidence. These investigations, which are subsumed by the term *eDiscovery* [Gei08], may also encompass data about parts which are not in the focus of the lawsuit. From the perspective of the industry partner, these parts are denoted *critical products*. Translated into the terminology of *business objects*, a critical product is mapped to a business object which in turn is stored within an business application. Hence, if a product is deemed critical since it may be subject to a litigation, the according business object in addition to the storing business applications are marked as critical, too.

The problem motivating the development and usage of a business object access matrix for the industry partner can be stated as follows: In the event of *substantiated suspicion*, a lawyer investigating on a critical product may legally have the right to undertake the role of those employees, who were dealing with the according business object. This in turn may allow the legal representative to gain access on additional business objects and related business applications which originally were not in scope of the litigation. Once access is granted to a business application, the lawyer could retrieve data in neighboring systems possibly leading to further claims. As a consequence, concrete links between roles, business objects, and business applications should be identified and later on adjusted, mitigating the risk which would be emanated by a lawyer who has comprehensive access rights.

In this respect, an enterprise-wide business object access matrix should address the following question: *Which role has permissions to access business objects stored in business applications?* The question is taken further by differentiating between direct and transitive access on business objects besides the distinction of the actual and desired access matrix. Whereas former refers to the possibility that a role manipulates business objects whose according data are not directly stored in a business application but which may be accessed transitively through the connection to a second business application, latter picks up the thought of distinguishing between current and target access state. The presented method addresses the above question is complemented with a set of relevant viewpoints visualizing the relations between role, business object, and business application, and allow to identify:

- Which business objects are stored in specific business applications?
- Which roles have access to which specific business applications?
- Which business applications are connected with other business applications?
- Which roles have access to which specific business objects?

2 Related work

In [JE07], Johnson and Ekstedt discuss models and analyses to support information system decision making on an enterprise level. Thereby, security is identified as one major aspect

[2] see http://www.uscourts.gov/rules/EDiscovery_w_Notes.pdf for details.

which is understood as consisting of the topics confidentiality, integrity, and availability. In respect to our example, especially the aspect of confidentiality, which considers the degree to which a business application protects data from being accessed by unauthorized users, is of interest. While Johnson and Ekstedt mentioned main causalities for security, like e.g. "quality of security policies" or "quality of organizational aspects of information security", no detailed method how to address confidentiality issues, is presented.

In [Win08], enterprise-wide information logistics (IL) is defined as a process of planning, implementing, as well as controlling cross-unit data flows in addition to the storage and provisioning of the respective data. While pointing out its general scope and characteristics, [Win08] also presents managerial challenges for an enterprise implied by IL and compares the concept to approaches like data warehousing, business intelligence, and management support systems. By centering around information which is spawned, processed, and used in an enterprise-wide context, the article motivates the fundamental necessity to manage information on an enterprise level in a holistic manner. In contrast to [Win08] who remains on a rather general point of view, we address a real-life case explicitly in proposing a solution.

The work of [DMR$^+$05] thoroughly examines enterprise-wide data management, acting on the assumption of six distinct stages of development, i.e. isolated applications, usage of DBMSs, standardization of data, distinct responsibilities for data, information as enterprise resource, combination of information to knowledge. Covering the role and importance of data for a modern enterprise in detail, [DMR$^+$05] also presents a matrix depicting which business function accesses and manipulates which specific entity. While the viewpoint is only briefly sketched by the authors, the approach presented in this article goes further in proposing a concrete method for designing enterprise-wide access views. Our matrix-based viewpoints consider three main concepts (role, business object, business application) including also transitive relations due to the reference to a concrete use case.

In his work, [Jun06] copes with the integration of data by elaborating different integration architectures which are divided in a typology, replication, transaction type, and synchronization control dimension. The work analyzes the management of information in an enterprise context by differentiating between business and technical perspectives. Thereby, the concept of a *information object type* as specified in the book can be directly mapped on the business object used in our work. However, while focusing on data integration, [Jun06] does not tackle the issue of access management through roles on business objects which are stored in different information systems, i.e. business applications.

Control Objectives for Information and related Technology (COBIT) represents a prominent framework for IT management created by the Information Systems Audit and Control Association in cooperation with the IT Governance Institute [IT 09]. The framework is focused on what is required to achieve adequate management and control of IT, and is positioned at a high level. Besides structuring IT in four core domains which are subdivided into 34 IT processes, COBIT suggests illustrative examples of those processes. Thereby, each example contains generic inputs and outputs, key activity goals, metrics, as well as activities and guidance on roles and responsibilities reified in a *Responsible, Accountable, Consulted and Informed* (RACI) chart. RACI charts, which are presented via matrices within the framework, identify who, i.e. which function, is responsible, accountable, consulted, and/or informed when a specific IT process activity is performed. While the viewpoint structure in the form of a matrix is identical to the one presented in this article, its content and field of application is different.

3 Enterprise-wide access control on relevant business objects

The initial step in constructing an enterprise-wide access model is the creation of an *information model*, i.e. a conceptual model containing the relevant concepts of the problem domain. Figure 1 presents the model developed in cooperation with the industry partner – it contains the three main concepts of our problem description: role, business application, and business object. As described in the model, roles have access to business applications storing different business objects. Furthermore, business applications are connected via interfaces to other business applications, whereas interfaces may constitute of database dumps of another business applications, i.e. business objects are transfered without any access control leading to transitive access for roles as claimed in the Section 1.

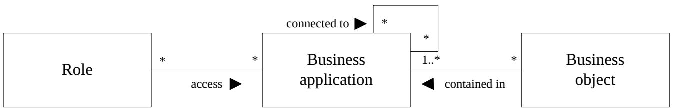

Figure 1: Information model for an enterprise-wide access management

A method for constructing enterprise-wide access views on business objects is shown in Figure 2 using the Business Process Modeling Notation (see [OMG08]). In the following, the method steps are explained in detail.

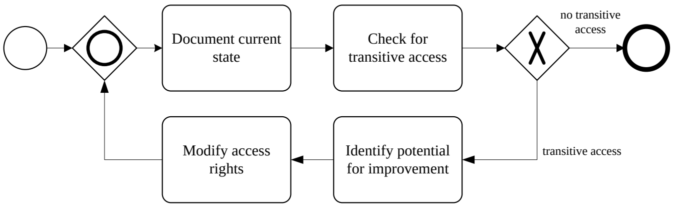

Figure 2: A method for creating enterprise-wide access views on business objects

Document current state gathers information about current access rights, hence documenting which business objects are stored in a business application which in turn may be accessed by one to many roles. Thereby, viewpoints making use of a table form can be used. The resulting views (cf. Figure 3) have to be filled with information gathered from different business units within the enterprise which have information on the access permissions. This documentation task can be performed in various ways, e.g. interviewing the respective stakeholders in the business units or observing actors during their IT-supported work. While the former methods are top-down, hence from a user's point of view, bottom-up approaches from a business application perspective can also be applied.

First, the car manufacturer documents which roles have direct access to which business applications, see Figure 3(a), and the stored business objects, see Figure 3(b). Afterwards, the car manufacturer documents which business application accesses other business applications (cf. Figure 3(c)). For instance, system administrators reported that they send a nightly database dump of the *CRM* to the *ERP* business application.

	Business application		
Role	*CRM*	*ERP*	*Portal*
HR	●	○	●
Sales	●	○	●
R&D	○	●	○

(a) Role ⇒ Business application

	Business application		
Business object	*CRM*	*ERP*	*Portal*
Customer	●	○	●
Construction plan	○	●	○
Contract	○	○	●

(b) Business object ⇒ Business application

	Business application		
Business application	*CRM*	*ERP*	*Portal*
CRM	●	○	○
ERP	●	●	○
Portal	○	○	●

(c) Business application ⇒ Business application

Legend	
●	access
○	no access

Figure 3: Enterprise-wide access matrices

Check for transitive access performs an expert-based analysis for transitive access on business objects. In a first step, the access rights of roles via intermediary business applications on corresponding business objects are computed and visualized using a tabular viewpoint. The according view is in a second step enriched with information on transitive access, i.e. with information on business objects that may be reached from a role via exploiting the interrelations between the business applications.

Figure 4 depicts the results of the step checking for transitive access. This view is taken into account by experts from the car manufacturer, who assess the criticality of the corresponding direct and transitive access permissions.

	Business object		
Role	*Customer*	*Construction plan*	*Contract*
HR	●	○	●
Sales	●	○	●
R&D	○ [●]	●	○ [●]

Legend	
●	access
○	no access
[●]	transitive access

Figure 4: Role ⇒ Business object

Identify potential for improvement is conducted by experts, who analyze transitive access relations, and identify the subset violating enterprise policies or legal rights. In using the views and the therein contained knowledge, concrete action items can be derived which aim at restricting access on business objects.

Access violations are identified by the legal department at the car manufacturer, i.e. the role *R&D* accessing the *ERP* business application is also allowed to read the business objects *Customer* and *Contract* violating enterprise policies. According to Figure 4 the documented transitive properties represent access violations since the role *R&D* should not be allowed to read the *Customer* and *Contract* business object. Consequently, a root cause analysis is performed at the car manufacturer, revealing that the connection between *CRM* and *ERP* causes this access violations. Since business processes were improved, the *ERP* system required information on the business object *Customer*, and for this reason, a nightly database dump of the *CRM* is transfered to the *ERP*.

Modify access permissions calls on well-known methods ranging from location-based restrictions of network access to role-based application layer access control. Thus, access permissions are modified in order to incorporate the improvements identified by experts. Afterwards, a new current state of the access permissions is documented (cf. Figure 2).

While the business object *Customer* is not categorized as *critical product*, the business object *Contract* is. Thus, the car manufacturer immediately restricts access to the *CRM* business application and contacts the owners of the *ERP* and *CRM* business applications in order to conjointly work out a solution which prevents the *ERP* business application to access the data of the *CRM* while bewaring business functionality.

4 Outlook

This article presented a method to construct enterprise-wide access views in order to obtain a holistic knowledge which roles have permissions to access business objects stored in specific business applications. Motivated by a real-world problem stated by one of our industry partners from the German car industry, this article suggests viewpoints in terms of matrices helping to identify role-based access rights on an enterprise level.

We are currently implementing the approach at the industry partner, where first results demonstrate its suitability. Nevertheless, we are aware of further challenges tying in with the presented method. To complete the proposed matrices with real data and therefore allow a reliable estimation about the business objects and business application instances a certain role may have access to, a huge amount of data has to be collected. Since the concrete information is spread out in either the business but also in the different IT units, a common terminology understandable by both sides has to be defined in advance.

References

[DMR$^+$05] Rolf Dippold, Andreas Meier, André Ringgenberg, Walter Schnider, and Klaus Schwinn. *Unternehmensweites Datenmanagement - Von der Datenbankadministration bis zum modernen Informationsmanagement*. Vieweg, 4rth edition, 2005.

[Gei08] Ivo Geis. eDiscovery und Datenschutz. Website, 2008. http://www.ivo-geis.de/veroeffentlichungen/eDiscovery_und_Datenschutz.pdf, visited on April 20th, 2010.

[IT 09] IT Governance Institute. Framework Control Objectives Management Guidelines Maturity Models. Website, 2009. http://www.isaca.org/Knowledge-Center/cobit; visited on June 27th, 2010.

[JE07] Pontus Johnson and Mathias Ekstedt. *Enterprise Architecture – Models and Analyses for Information Systems Decision Making*. Studentlitteratur, Pozkal, Poland, 2007.

[Jun06] Reinhard Jung. *Architekturen zur Datenintegration: Gestaltungsempfehlungen auf der Basis fachkonzeptueller Anforderungen*. Vieweg+Teubner, Wiesbaden, Germany, 1st edition, 2006.

[OMG08] OMG. Software & Systems Process Engineering Meta-Model Specification (formal/2008-04-01), 2008.

[Win08] Robert Winter. Enterprise-wide information logistics: Conceptual foundations, technology enablers, and management challenges. In *30th International Conference on Information Technology Interfaces (ITI 2008)*, pages 41–50. IEEE Computer Society Press,U.S., Juni 2008.