2009 Third International Conference on Emerging Security Information, Systems and Technologies

# Extending Role-based Access Control for Business Usage

Heiko Klarl[1, 2], Korbinian Molitorisz[3], Christian Emig[1, 3], Karsten Klinger[1] and Sebastian Abeck[3]

[1]iC Consult GmbH, Keltenring 14, 82041 Oberhaching, Germany
[2]Media Computing, University of Regensburg, Germany
[3]Cooperation & Management, University of Karlsruhe (TH), Germany

## Abstract

*Role-based access control (RBAC) is used for managing authorisation in IT systems, by utilising the concept of roles. Existing approaches do not clearly define the term "role" in its different contexts as well as not considering the relation between roles and business process modelling. Therefore this work introduces business and system role-based access control (B&S-RBAC). Established role-based access control models are extended with a business perspective and the term role is defined from a business and from an IT perspective, resulting in business and system roles. The relation between them is shown in a meta-model and the usage of business roles for secure business process modelling is explained.*

***Keywords:*** *RBAC, Roles, Business Process Modelling, Identity Management, Access Control, Business-IT Alignment.*

## 1 Introduction

Nowadays nearly every business process is extensively supported by IT systems. Globalisation and hard competition led to short reaction times in adapting business processes and mergers and acquisitions are still challenges for every enterprise. Due to these conditions, demands for the companies' IT systems, business processes and their security architecture arise [10]. Business process modelling [17] tries to cope with those needs as modelled business processes are easier to understand, better to redesign and executable codes can be generated by model-driven techniques. As not everyone is allowed to execute particular business processes, *identity management* (IdM) ensures that only authorised persons may do so. In order to achieve this, role information can be assigned to activities within the business process. In order to accomplish authorisation of the business processes' activities within the supporting IT systems, *role-based access control* (RBAC) may be used. But different views and definitions of "roles" complicate the RBAC approach enormously. Within the business process information on roles consists of job functions or business tasks and roles are often more or less just descriptive information. In contrast, RBAC roles within IT systems encapsulate permissions but do often not have any relation to the business perspective of roles. Generally, the term *role* used in RBAC does not distinguish between business and IT. In order to unify these two different concepts of roles, an error prone coordination process between business and IT department arises [2], when business focused roles have to be transferred to the technological-focused RBAC roles. A first step to overcome this weakness is to extend existing business and IT role models and to link them in a comprehensive way in order to gain a direct relation between business and IT.

In this paper we present *business and system role-based access control* (B&S-RBAC), a model for business focused role-based access control which overcomes the weakness of existing business role definitions and RBAC models. Our contribution is to extend existing RBAC models with a business perspective to allow the mapping of business roles deduced from job profiles to system roles abstracting permissions of IT systems. We illustrate the relation of B&S-RBAC with business process modelling where our novel approach can be utilised for securing business processes with the help of business roles without loosing their connection to underlying IT systems.

The paper is organised as follows: Section 2 discusses different existing role models for role-based access control and gives a short introduction to identity management and business processes. Our enriched RBAC model for business usage B&S-RBAC is introduced in Section 3 explaining the concept of business and system roles and their relation to business process modelling. The application of B&S-RBAC is illustrated by a loan application within the banking domain in Section 4. The paper concludes with a summary and an outlook on future work in Section 5.

978-0-7695-3668-2/09 $25.00 © 2009 IEEE
DOI 10.1109/SECURWARE.2009.28



IEEE computer society

## 2 Background and related work

### 2.1 Identity management and business process modelling

The importance of business processes models became obvious with the idea of business process reengineering [4] in the 1990s and with the development of the service-oriented architecture paradigm [11]. The nearly arbitrary combination of single sub-processes or loosely coupled services to business processes in the sense of service-orientation is only possible on the base of meaningful and executable models. This enables enterprises to cope with market challenges and new business regulations in a flexible and agile way. The focus lies on the optimal support of the business process whereas the IT plays a supporting role in the background. The modelling of business processes can be done using different notations like *Event-driven Process Chains* (EPC) [6], the *Business Process Modeling Notation* (BPMN) [12] or the behaviour diagrams of the *Unified Modeling Language* (UML) [13]. The concept of roles is not unknown in *business process modelling* (BPM) (cf. [16, 17]). Roles are assigned to activities "indicating that all members of the role are capable of performing the respective activity instances" [17]. For example, BPMN supports a role concept utilising so-called *lanes*, which "are often used for such things as internal roles (e.g., Manager, Associate)" [12]. As the meaning of lanes is not defined and up to the modeller [12], the modelling of roles in business processes is often more or less descriptive information.

From an IdM perspective, these types of role information can also be used to derive requirements for restricting access to activities. Therefore we introduced in [9] a meta-model for modelling access control requirements at the business process level, using business roles to describe the acting subject. The meta-model combines the business process model and its IdM requirements in one model. This enables the business department to define its own or compliance-driven IdM requirements, using their specific domain knowledge in business process modelling. With the help of a model-driven development process these models are transformed to product specific access control policies. But as the roles in BPM often have just a descriptive nature, e.g. names of job functions or business tasks, it is not easy to find out which IT systems' authorisation is related to the assigned role in the business process models. This missing definition of the role concept and its IT relation hinders the usage of a full model-driven generation of access control policies out of a business process.

### 2.2 Role-based access control models

Much research has been done on role-based access control since the 1990s. The basic idea that "users are assigned to roles, permissions are assigned to roles, and users acquire permissions by being members of roles" [3] of the proposed concepts was the same, but diversity existed in the details. This diversity enormously complicated the usage of RBAC approaches, as each implementation was based on a slightly different concept. To overcome this weakness Ferraiolo et al. proposed the *NIST standard for role-based access control* (NIST RBAC) [3] containing the "fundamental and stable set of mechanisms" [3] of RBAC. NIST RBAC includes hierarchy concepts "whereby senior roles acquire the permission of their juniors, and junior roles acquire the user membership of their seniors" [3]. Static and dynamic *separation of duties* (SoD) ensures that roles leading to a conflict of interests may be either not assigned to the same user or that the conflicting roles may not be used together within the same user session.

The main lack of NIST RBAC is the missing definition of the term *role*. Depending on the perspective, the term *role* is interpreted with different meanings. From a business perspective, a role reflects job functions and business tasks (cf. 2.1), e.g. *clerk* or *loan officer*. It is expected that the role *clerk* contains all permissions for serving a customer at the cashier's desk, regardless of the IT system required for fulfilling this tasks. These IT systems e.g. may comprise a *credit system* and a *banking system*. From the IT perspective a role may be seen as a bundle of the system's permissions reflecting a certain task which can be accomplished in this system, e.g. 'scoring management' or 'securities management'. These roles contain only the permissions of the respective system, e.g. the *banking system*. Comparing the business and IT perspective, the scope of the role is totally different: one point of view contains information about roles across systems, the other only from a certain IT system. As NIST RBAC has no definition of the term *role*, communication problems between business and IT will arise. There is a need to define *role* from both perspectives including each others relation.

Kern et al. presented ERBAC in [8] which tries to overcome the described weakness of RBAC. They define the term role explicitly as *enterprise role* consisting "of permissions in one or more target systems" [8], where permissions "are specific to the target system and can be of various natures" [8]. With the term *enterprise role* they established a definition of *role* to a have clear understanding in the enterprise. With the overarching concept of *enterprise roles* they took into mind, that for one job function, support from one or more IT systems could be necessary. But the approach has the disadvantage that very technological and IT-focused permissions of any kind, which may comprise roles, groups,

policies or system permission, are directly combined with job profiles in its definitions as *enterprise roles*. The advantage of role concepts to encapsulate permissions of an IT system used for doing a certain task is not considered anymore, thereby neglecting the basic idea of RBAC. *Enterprise roles* containing the authorisation for executing the same business tasks will include the same bundles of permissions. This is redundant and should be avoided by the abstraction of system specific roles.

In [18] Wortmann presented a method for enterprise-wide authorisation. He proposed a model which is based on ERBAC and which is divided in a three layer architecture. The first layer represents decentral *authorisation components*, whereas the second layer stands for the system overarching *authorisation component*. The third layer is not explained but seems to be a human-centric virtual construct for reflecting the business side. On the first layer he introduced *resource* representing a system specific bundle of permissions, which could be seen as a system role. The term *role*, an element of the second layer, reflects the concept of ERBACs' *enterprise roles* which bundle *resources* across different systems. On the third layer *process roles* are introduced, being the organisational bundle of *roles* needed for processing tasks or activities. In this meta-model the relation from *process roles* to business process modelling is not explained, although the name indicates such a relation and it is not argued which benefits are gained by the use of *process roles*. Basically the third layer seems to be more or less an indirection which should ease understanding by making a reference to the business perspective, which is not worked out in detail. Wortman refines the idea of ERBAC in that *resource* and *enterprise roles* reflect the concept of system and business roles. But the work lacks a defined relation between roles and business process modelling.

Approaches like team-based access control (TMAC) [15] or organisation-based access control (ORBAC) [5] do not define concepts like business roles and are therefore not discussed in detail.

### 2.3 Summary

In summary there is a lack of a role concepts' definition that fits the reality of present or modern enterprises, aligning the business and the IT world in a holistic role model. Either there is a total lack of definition of the term *role* [3] or the idea behind business roles is identified [8] but established RBAC concepts on the IT systems' side are ignored. Both gaps were avoided in [18] but the relation of the role model to business process modelling is just indicated and not worked out. Whereas business focused roles (cf. 2.1) cover the business domain well, they do often not have any relation to roles defined in the IT domain on the basis of RBAC models (cf. 2.2). Several problems arise when this relation between business and IT is not considered: The business side is not able to make real use of its domain-specific knowledge in the handling of roles in business process modelling, as its role definitions have no relation to those roles defined in a certain IT system. The IT side is not able to achieve a holistic view on which roles from an IT system are needed for representing a role definition from a business point of view – often resulting in too less or far too many privileges assigned to users. Those role models which do not consider the coherency between business and IT side might have been adequate in the 1990s, where IT support for business processes was in its beginning, but they do definitively not cope with present demands evolving from business process management [17], service-oriented architecture [11] and compliance requirements [1].

## 3 A role model for business and IT

In order to cope with this situation, existing RBAC models have to be enriched with an explicit role definition for the business as well as for the IT side. Therefore we introduced *business role-based access control* (B&S-RBAC), a role model containing *business roles* which represent job profiles and business tasks from the business perspective and *system roles* which bundle different types of permissions in IT systems. The following sections will describe both terms and give an overview of the B&S-RBAC meta-model.

### 3.1 Business roles and business process modelling

Common business terms reflecting an organisational order are business task and job profiles. A business task is an activity which is performed regularly in daily business, e.g. billing or transferring wages. Job profiles are organisational classifications, grouping employees with the same skills and responsibilities, e.g. clerk, manager or software developer. Whereas business tasks and job profiles are pure business concepts, the idea of business roles should lay the fundament for a relation to the enterprises' IT. Therefore we define business roles as follows:

- Business roles represent business tasks or job profiles within enterprise.
- An employee is assigned one or more business roles.
- Business roles are not specific for one IT system, they are an enterprise-wide concept.
- Business roles have a relation to system roles (cf. 3.2) reflecting all IT systems involved in acting on behalf of a business role.

As one or more business roles can be assigned to an employee, the total amount of the employee's business roles determines what he is allowed to do. Some business roles may not be assigned together as they will conflict with *separation of duties* (SoD) concepts e.g. approving and disbursing a credit application.

With a well-defined concept of business roles which are no longer only descriptions, the business department is able to model business processes with role-based access control. Having a role model like B&S-RBAC distinguishing between business and system roles, the business department has a set of business roles which can be assigned to activities, stating which role is allowed to execute them. The selection and application of business roles can be supported by tools for BPM. Without B&S-RBAC the business department had to know which kind of role from an IT system (within B&S-RBAC called *system role*, cf. 3.2) has to be assigned or it just used undefined and descriptive job profiles (cf. 2.1). It is obvious, that this is complicated and error prone. B&S-RBACs' business roles abstract this completely, as they are representing all capabilities necessary for performing a certain business task without lacking a relation to the underlying IT systems.

## 3.2 System roles

For performing a certain action in an IT system, a permission is needed. A permission grants an operation on an object and is assigned to a subject, normally a user or another interacting IT system. As an IT system consists of a huge amount of operations and objects, it is difficult to handle single permissions assigned to subjects, as a subject has steadily changing permissions over time. Therefore we introduce system roles, encapsulating permissions from an IT system, which leads to an abstraction of the permission levels' technological details and to a reduction of complexity. This complies with the classical RBAC approaches proposed in [3, 14] but extends them by defining the term *role*. Summing up, we define system roles as follows:

- System roles encapsulate permissions for doing related tasks within one single IT system.
- System roles are assigned to business roles and not directly to users.
- System roles are organised according to known RBAC concepts like NIST RBAC [3].

A typical example is a system role named *securities management* from a *banking system*, which e.g. includes permissions like *record securities* or *edit securities* for administering securities from a loan applicant. With the increasing complexity of IT systems, the number of system roles is exploding tremendously. For example, an application in the banking domain can have some hundred system roles, and several applications exist. Putting this in the big picture of an enterprise's application landscape, sometimes with several hundreds of applications, several thousands of system roles exist. It is obvious, that this huge amount of system roles is difficult to manage and more important not be understood by the business domain, so that business roles encapsulating system roles is a possibility to abstract this complexity.

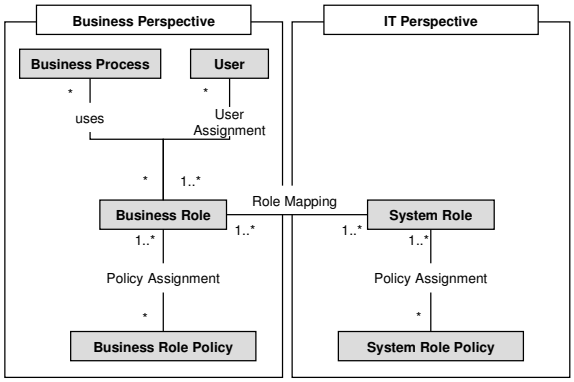


**Figure 1. The B&S-RBAC meta-model**

## 3.3 The B&S-RBAC meta-model

Considering the analysis of business and system roles and state of the art role-based access control concepts, two main problems can be identified: On the IT side a huge amount of system roles exists. Their strong IT focus decouples them from the business domain and their number makes their administration very complicated and complex.

On the business side roles are used to represent business tasks but they lack a relation to the IT systems' roles. To overcome these problems, B&S-RBAC allows a holistic view on roles defined in an enterprise environment. To unify the business and the IT world, business roles and system roles have a *role mapping* relation, depicted in the meta-model in Figure 1. The connection between both enables the usage of business roles and system roles in each's original domain. The business side is using business roles as a description for job profiles without need for technological knowledge of the underlying IT systems. The IT side uses the systems roles, but knows according to the mapping to the overarching business role the business context.

The left part in Figure 1 shows the business-focused part of B&S-RBAC. The user has one or more business roles assigned. Business roles are used in business processes to describe business role owners who are allowed and responsible for performing an activity. To each business role a business role policy is connected, defining its authorisations at a

business level and reflecting its distinction for certain business tasks. Business roles may be structured in hierarchies to allow inheritance, but this is out of the papers' scope.

The IT-focused part on the right side shows the system role and its assignment to system role policies, abstracting the IT systems' permissions. That means, system role policies contain the information what a system role is allowed to do within an IT system. In order to structure the IT systems' permissions and roles, known RBAC concepts (cf. [3, 7, 14]) can be utilised for supporting the building of hierarchies including role-inheritance, generic roles, joker permissions, user-based attributes and constraints or separation of duties (SoD). As these technological aspects of RBAC models are out of the paper's scope, we will not address these concepts in detail.

Both parts are connected by the role mapping between business roles and system roles. Each business role is related to one or more system roles, connecting the business and the IT world together. This is the only connection between the business and the IT perspective, more connections will mix up B&S-RBACs' paradigm of a clear definition and separation of business and IT roles.

## 4 Applying B&S-RBAC in the banking domain

In the banking domain role concepts are very important to ensure a separation of duties and to be compliant with laws and regulations like Basel II or the Sarbanes Oxley Act (SOX) [1]. In this section we apply the concept B&S-RBAC to the roles involved when a loan application has to be checked and approved. Three people with different job profiles are involved in this process. Alice is the contact person to the customer, she creates the act necessary for the loan application and ensures that all required data are collected. For obtaining more knowledge about the creditworthiness of the customer, she may use a scoring service. Bob works in the back office and prepares and approves the loan application. He is able to view and record the securities provided by the customer, may use the scoring service and will create the loan contract and the loan account. Finally Bob values the loan. Chris, the third person involved, is Bob's supervisor with extended permissions. He may value loans exceeding the limit of his subordinates. For performing the loan application process, three different IT systems are used, each system with its own organisation and administration of roles and permissions.

The traditional role assignment is depicted in Figure 2. The users are assigned to roles (white boxes within the grey boxes) in different IT systems (grey boxes). Each user has various assignments to the IT systems. Many assignments are redundant information – Bob differs just in two assigned roles from Chris. It can be easily seen, that these assignments are very complex and difficult to maintain. This point is where B&S-RBAC comes into play. The relation between identities and roles in the IT systems is analysed with the help of a so-called role-mining process. The outcome of this analysis is the introduction of business roles and the reorganisation of roles for reducing complexity which is shown in Figure 3. First of all four business roles can be identified *clerk*, *employee*, *loan officer* and *senior loan officer* which aggregate the already known system roles. For example the business role *employee* encapsulates system roles which are used by every employee in this scenario. It is not necessary to assign each employee his basic system roles directly, it is much more logical to combine a set of them in a business role. The business role is then assigned to the identity. Compared with the situation described in Figure 2 the relation between identities and roles is clearer.

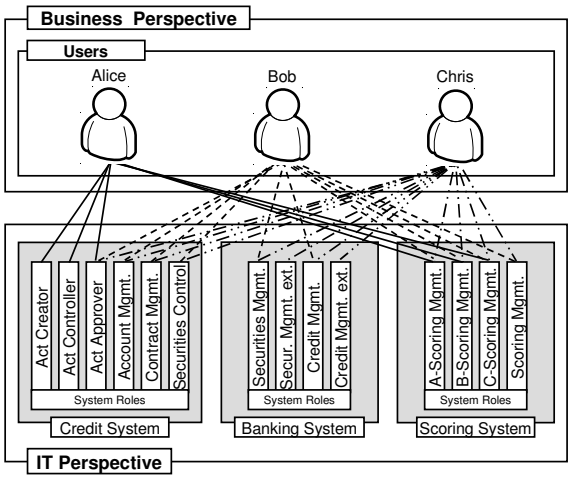


**Figure 2. Traditional role assignment**

The decoupling of system roles and identities by the business role layer enables changes in the IT system without effects on the employees. The assignment of system roles to business roles may change, e.g. new system roles may be added and obsolete ones may be removed without any influence on the relation between business roles and identities. This saves a tremendous amount of work and overhead, considering that in the traditional role assignment every change of a system role has effects on the identities, leading to hundreds or thousands of alterations in the role assignment when common system roles are changing.

## 5 Conclusion and further work

In this paper we proposed B&S-RBAC, a model for business focused role-based access control which overcomes the weakness of existing business role definitions and RBAC models. We have defined business and systems roles and their relation to each other. Business roles represent job

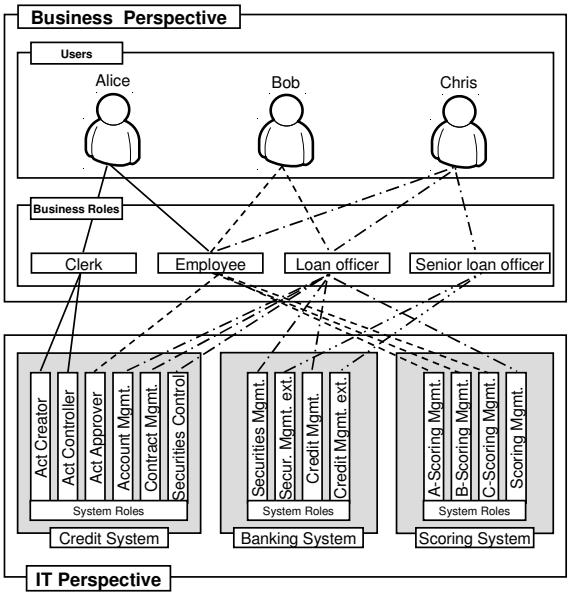


**Figure 3. Role assignment using B&S-RBAC**

profiles and business tasks within an enterprise and are directly assigned to users. System roles encapsulate permissions of certain IT systems and are only assigned to business roles. Within IT systems they may be organised according to known RBAC concepts. Although there has been much research on role-based access control in the past, this explicit definition was still missing. The concept of B&S-RBAC allows the usage of business roles in the modelling of secure business processes [9]. This is novel, as information on roles and owners of activities and tasks was often descriptive nature without an underlying concept or a relation to the supporting IT systems.

Future work will be done on the integration of business roles in secure business process modelling and the generation of security policies with the help of model-driven techniques. In the area of compliance the dichotomy of business and system roles motivates additional research on separation of duties and the roles' life cycle.

## References


[1] M. Burling. The key to compliance. *Database-and-Network-Journal*, 35(3):17–18, 2005.

[2] S. Cormack, A. Cater-Steel, J. H. Nord, and G. D. Nord. Resolving the troubled it-business relationship from a cultural perspective. In *Proceedings of the 12th Australasian Conference on Information Systems*, Coffs Harbour, NSW, Australia, Dec. 2001.

[3] D. F. Ferraiolo, R. Sandhu, S. Gavrila, D. R. Kuhn, and R. Chandramouli. Proposed NIST standard for role-based access control. *ACM Transactions on Information and System Security*, 4(3):224–274, Aug. 2001.

[4] M. Hammer. Reengineering work: don't automate, obliterate. *Harvard Business Review*, 68(4):104–112, 1990.

[5] A. A. E. Kalam, S. Benferhat, A. Miège, R. E. Baida, F. Cuppens, C. Saurel, P. Balbiani, Y. Deswarte, and G. Trouessin. Organization based access control. In *Proceedings of the 4th IEEE International Workshop on Policies for Distributed Systems and Networks*, pages 120–131, June 2003.

[6] G. Keller, M. Nüttgens, and A.-W. Scheer. *Semantische Prozessmodellierung auf der Grundlage Ereignisgesteuerter Prozessketten (EPK)*, volume 89. Universität des Saarlandes, Jan. 1992.

[7] A. Kern. Advanced features for enterprise-wide role-based access control. In *Proceedings of the 18th Annual Computer Security Applications Conference*. IEEE Computer Society, 2002.

[8] A. Kern, M. Kuhlmann, A. Schaad, and J. Moffett. Observations on the role life-cycle in the context of enterprise security management. In *Proceedings of the 7th ACM Symposium on Access Control Models and Technologies*, pages 43–51. ACM, 2002.

[9] H. Klarl, C. Wolff, and C. Emig. Identity management in business process modelling: A model-driven approach. In *9. Internationale Tagung Wirtschaftsinformatik – Business Services: Konzepte, Technologien, Anwendungen, Band 1*, pages 161–170, Vienna, Austria, Feb. 2009. Österreichische Computer Gesellschaft.

[10] T. Neubauer, M. Klemen, and S. Biffl. Secure business process management: A roadmap. In *Proceedings of the 1st International Conference on Availability, Reliability and Security*, pages 457 – 464. IEEE Computer Society, Apr. 2006.

[11] E. Newcomer and G. Lomow. *Understanding SOA with Web Services*. Addison-Wesley, 2005.

[12] Object Management Group, Inc. Business Process Modeling Notation (BPMN) Specification. `http://www.bpmn.org/Documents/OMGFinalAdoptedBPMN1-0Spec06-02-01.pdf`, Feb. 2006.

[13] Object Management Group, Inc. Unified modeling language: Infrastructure – version 2.1.1. `http://www.omg.org/docs/formal/07-02-06.pdf`, Feb. 2007.

[14] R. S. Sandhu, E. J. Coynek, H. L. Feinsteink, and C. E. Youmank. Role-based access control models. *IEEE Computer*, 29(2):38–47, Feb. 1996.

[15] R. K. Thomas. Team-based access control (tmac): a primitive for applying role-based access controls in collaborative environments. In *Proceedings of the second ACM workshop on Role-based access control*, pages 13–19, New York, NY, USA, 1997. ACM.

[16] W. van der Aalst and K. van Hee. *Workflow Management – Models, Methods, and Systems*. MIT Press, 1. MIT Press paperback edition, 2004.

[17] M. Weske. *Business Process Management – Concepts, Languages, Architectures*. Springer, 2007.

[18] F. Wortmann. *Entwicklung einer Methode für die unternehmensweite Autorisierung*. PhD thesis, Universität St. Gallen, 2006.


All web references were checked on March 24th, 2009.