ROLES IN INFORMATION SECURITY - A SURVEY AND CLASSIFICATION OF THE RESEARCH AREA

L. FUCHS, M. FERSTL, and G. PERNUL

Department of Information Systems, University of Regensburg, Germany

AND

R.S. SANDHU

Institute for Cyber Security, University of Texas at San Antonio, USA

Since the publication of a seminal paper on "RBAC – role based access control models" in 1996 (IEEE Computer) a huge amount of work has been published on the application of sociological role theory in Information Security. Theoretical role models and interpretations as well as several commercial products are for instance based on the role concept and use them as their underlying access control paradigm. A conducted scientific literature collection revealed 866 publications dealing with roles in the context of Information Security. Although there is an ANSI/NIST standard and an ISO standard proposal there are a variety of competing models and application scenarios available and based on their different concepts and interpretations there is lack of consensus and clarity. Additionally, in practice several interpretations of the role concept have developed, dealing with the usage of theoretical findings on roles to improve existing security technologies. Because of the current situation there is need for a comprehensive article surveying the different proposals and streams of research on roles in Information Security. The goal and major contribution of this survey are a categorization of existing research into different classes following a three-level classification methodology. Based on a well-defined methodology a general categorization of the complete underlying set of publications, including general statistical data is provided. The main part of the work is investigating 30 identified research directions, evaluating their importance, and analyzing research tendencies and trends. An electronic bibliography including all surveyed publications together with the classification information is provided additionally. As a final contribution of the paper future trends in the area of role -research based on the data collected and own personal interpretations are predicted.

Categories and Subject Descriptors: A.1 [Introductory and Survey]; K.6.1 [Project and People Management] – Systems analysis and design; K.6.5 [Security and Protection] – Authentication, Unauthorized Access; K.6.m [Miscellaneous] – Security.

General Terms: RBAC, role concept, role theory, Information Security

Additional Key Words and Phrases: Survey, research areas, adaption of role theory

Authors' addresses: L. Fuchs, Department of Information Systems, University of Regensburg, Regensburg, Germany. E-mail: Ludwig.Fuchs@wiwi.uni-regensburg.de; G. Pernul, Department of Information Systems, University of Regensburg, Regensburg, Germany. E-mail: guenther.pernul@wiwi.uni-regensburg.de; R. Sandhu, Institute for Cyber Security, University of Texas at San Antonio, USA. E-mail: ravi.sandhu@utsa.edu;

---

1. MOTIVATION

The increasing use of the Internet, international competition, inter-organizational networks together with the constantly growing diffusion of IT technologies within all areas of human society have increased the importance of information technology as critical success factor in the modern world. Information processing systems are vulnerable to many different kinds of threats that can lead to various types of damage resulting in significant economic losses. The field of Information Security has thus grown and evolved over the last decades. In its most basic definition, Information Security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction. The aim of Information Security in particular is to minimize risks related to the three main security goals confidentiality, integrity, and availability - usually referred to as "CIA" [Pfleeger and Pfleeger 2006]. Access control (AC), i.e. the management of admission to system and network resources is known as one of the most important and challenging areas of Information Security. It is the most fundamental and pervasive security mechanism in use, showing up in virtually all systems and imposing great architectural and administrative challenges at all levels of enterprise computing [Ferraiolo *et al.* 2007] .

Research on access control started in the 1960s and 1970s. During these first years two models were prevalent. Discretionary Access Control (DAC) assigns privileges explicitly to security subjects. In short, it regulates access at the discretion of the resource owner. Mandatory Access Control (MAC), on the other hand, not only controls access but furthermore regulates the information flow between objects and subjects. Since the 1990s both traditional models are dominated by the Role-based Access Control (RBAC) model. Role-based Access Control nowadays marks the de facto standard in enterprise systems involving large numbers of users with different rights and obligations. The fundamental idea of RBAC is the removal of the direct linkage between user and permission. Following this paradigm roles are created for the various job functions in an organization and users are assigned to roles based on their responsibilities and qualifications. The roles themselves are connected with access rights to certain resources (see Figure 1). This simplifies management of permissions: Users can be easily reassigned from one role to another. Roles can be granted new permissions as new systems are incorporated, and permissions can be revoked from roles as needed.

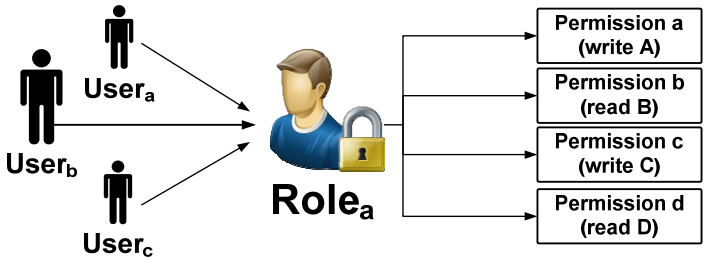


Figure 1: Roles as intermediates between users and permissions

After the introduction of the term *RBAC* in 1992 [Ferraiolo and Kuhn 1992] and the publication of the RBAC model family in 1996 ([Sandhu *et al.* 1996]) a rapid increase of the scientific output in this area took place. As a result of its practical and theoretical relevance, a complex and vivid research community deals with the adaption of role theory in Information Security since the mid-1990s. Up to now more than 1300 researchers contributed to this area, investigating new application areas, providing formal

foundation frameworks, combining role theory with other technologies, or providing insight into practical usage scenarios – to mention only selected research fields. However, not all of them focus on roles in Information Security. The different interpretations of the role concept in the computing world besides Information Security comprise fields like *Artificial Intelligence*, *Social Psychology and Organizations Management*, as well as *Human-Computer-Interaction* [Zhu 2006]. The following article only focuses on the interpretation of roles in the context of Information Security. In order to avoid homonym- and interpretation conflicts the term *roles* is used in respect to Information Security.

Up to now there is no structured and comprehensive overview over the huge amount of publications and competing research directions on role-research available. Only few meta-analysis and review articles have been published, however, they only provide a very limited overview, being commonly based on about 25 surveyed publications. This work provides a comprehensive survey, embracing not just several tens but 866 identified scientific publications in the field. A detailed statistical analysis of those publications combined with a classification scheme allows for the identification and interpretation of research directions and their importance for the overall field. As not all surveyed publications can be listed in the reference section of this paper, the complete publication set is provided in an electronic database including all classification information used in the survey paper[1]. Hence authors and researchers can use this bibliography for their own work – and even can update and extend it. Additionally, this work provides insight into possible research directions in the future. For the detailed analysis and combination of available research results such a scientific analysis contributes to the future development of the field.

We are aware that the provided analysis does not represent a standard survey paper due to the large number of surveyed publications. Such a broad survey of significant value for the field of IT- and Information Security needs to be based on a well-founded survey methodology focusing on the specific requirements arising due to the large amount of investigated publications.

The rest of the work is organized as follows: In Chapter 2 preliminaries and a short introduction of different role concepts and understandings are presented. Furthermore, a brief overview of existing review and meta-analysis articles dealing with roles in Information Security is given. Afterwards the research methodology is explained detailed in chapter 3. General statistical findings and high-level results are presented in chapter 4, forming the basis for the further classification and thorough analysis of the different research directions in chapter 6 and 7. Finally, an outlook and conclusion dealing with the development of the research field in the future is given in chapter 8.

2. PRELIMINARIES AND RELATED WORK

This citation from Shakespeare's play "As you like it" underlines that the concept of role theory has been prevalent on the stages for more than 400 years. As the term role suggests, the theory began life as a theatrical metaphor.

> "All the world's a stage, and all the men and women merely players; they all have their exits and entrances; and one man in his time plays many parts." (As You Like It, 1598-1599, Act II, Scene 7)

[1] http://www-ifs.uni-regensburg.de/Roles

Scientists in the 1930s began to compare social life with the theatre in which actors played predictable *roles*. According to Biddle ([Biddle 1986]) role theory in sociology concerns one of the most important characteristics of social behavior - the fact that human beings behave in ways that are different and predictable depending on their respective social identities and the situation.

Researchers like Ralph Linton (anthropology), George H. Mead (social philosophy), or Jacob Moreno (psychology) contributed to the foundation of the role theory. Linton defined role theory a means for analyzing social systems. He conceived roles as the dynamic aspects of societal recognized social positions ([Linton 1936]). In contrast, George Herbert Mead viewed roles as the coping strategies that individuals evolve as they interact with other persons. In his main work "Mind, Self and Society" ([Mead 1934]) he characterized *role taking* as a prerequisite for effective social interaction. Finally, Jacob Moreno saw roles as the tactics that are adopted by persons within primary relationships, and argued that imitative behavior was a useful strategy for learning new roles ([Moreno and Jennings 1934]). Over the time, the notion of roles has become a construct that has been widely adapted to the knowledge base and the environment of fields such as sociology, psychology, anthropology, organizational theory, and, lately computer science. This broad range of applications underlines the feasibility of role theory for research areas that deal with behavioral aspects of humans.

2.1 The History of Roles in Information Security

Up to the year 1996 two different phases of the adoption of role theory in Information Security can be distinguished: Since the development of computing technology and its usage in organizations above all different software vendors selectively dealt with usage of roles in a so called *pre-RBAC* phase. With the beginning of the formalization process of role-based access control the *early RBAC* phase started in 1992. It was finalized in 1996 with the publication of the RBAC models [Sandhu *et al.* 1996].

Pre-RBAC efforts until 1992

The concept of roles has been used in software applications for at least 30 years. Indeed, different products already started to integrate enterprise roles in the beginning of the 1970s, including RACF developed by IBM or Computer Associate's CA-ACF2 and CA-TOP SECRET. These roots of RBAC include the use of groups in UNIX and other operating systems and privilege groupings in database management systems.

In the early days of adaption Heckman and Galletta analyzed the application of role theory in the computing world in ([Heckman and Galletta 1988]) and ([Galletta and Heckman 1990]). They state that stabile, shared patterns of expected behavior which are associated with positions become the basic fabric for organizational roles. The *pre-RBAC* phase is heavily influenced by the interpretation of roles in organizational theory and management. This stems from the historic relationship between today's *Information Systems* and its roots in MIS[2]. In traditional organizational theory roles are used to express the position of an employee within an organizational structure. As they represent job functions and tasks as well as the organizational structure they are sometimes referred to as the DNA of an organization. Roles are determined by factors like the company type, the branch, and the life phase of the enterprise (e.g., foundation, reorganization, internationalization, or renovation). However, at that time during the *pre-RBAC* phase there was no general-purpose model defining how access control could be based on roles and that there was only little formal analysis of the security of these systems.

[2] Management of Information Systems

Early RBAC efforts between 1992 and 1996

As already mentioned, the *pre-RBAC* phase lacked a well-founded formal theoretical basis and understanding of a role-based security mechanism. An important milestone improving that situation was the work of Ferraiolo and Kuhn ([Ferraiolo and Kuhn 1992], introducing the term *RBAC*. Within the scope of a study carried out by NIST[3], systems MAC- and DAC-based systems were analyzed and a draft for a formal interpretation of the role concept was given. A role basically was seen as a collection of authorizations. Furthermore, the idea of a role hierarchy stating that authorizations can also be inherited from senior roles was presented. In addition a regulation of the restrictions of the role membership, namely constraints, was identified. This first model and its properties were studied and formalized more detailed in ([Ferraiolo *et al.* 1995]).

The interpretation of a role-based security mechanism by Nyanchama and Osborn also provided a concept of integrating roles within the scope of access control. Their work ([Nyanchama and Osborn 1993, Nyanchama and Osborn 1993]) underlines the growing meaning of roles in security-critical applications. The interaction of the involved entities was closely investigated in order to integrate information flow control into the administration mechanisms in role-based security and access control. These efforts later resulted in the so called *role-graph model*.

Additional results also contributed to the early RBAC efforts. Mohammed and Dilts [Mohammed and Dilts 1994]), for instance, presented the URBS[4] paradigm, using a user-role definition hierarchy called URDH to identify user classes, user types, user roles and user privileges. In [Sandhu *et al.* 1994] and [Sandhu and Feinstein 1994] RBAC was seen as a multidimensional architecture with three dimensions adapting the 3-level database architecture from ANSI/SPARC. It contains an external view of users as well as an internal view which shows the real system including the authorizations. The conceptual view serves as intermediate which corresponds to the roles in the RBAC model.

The phase of *early RBAC* efforts resulted in the publication of the initial RBAC96 family ([Sandhu *et al.* 1996]) in 1996. Sandhu et al.'s article and the simultaneous start of the *ACM Workshop on Role-Based Access Control* series represent the core milestone concerning adaption of role theory in Information Security. Both, the *pre-RBAC* phase and the consecutive *early RBAC* efforts are seen as preliminary work for the development of the field as only a relatively small number of publications have been published up to 1996. Due to this reason the survey conducted in this work focuses on the research area and its development from 1996 up to the beginning of 2009.

2.2 Review & Meta-Analysis Articles

Due to the scientific interest and the resulting diversity of research foci, a number of review and meta-analysis articles have been published. The early contributions provided shortly after the initial introduction of the RBAC models focus on the identification of future research areas and developments while later survey articles commonly analyze the historical development of specific role-related research issues. For a complete list of those publications search the provided electronic bibliography database for the research area *Review & Meta-Analysis*. In this chapter, the content of existing meta-analysis and review articles is described briefly.

The first meta-analyses already appeared in 1996 ([Ferraiolo and Kuhn 1996], [Giuri 1996]). The authors classified the RBAC research and tried to derive trends. Focusing on access control, they identified the refinement and development of the nature of RBAC as

[3] National Institute of Standards and Technology (http://www.nist.gov/)
[4] User-Role Based Security

well as the practical implementation of RBAC as major research areas. A marketing survey of Smith et al. ([Smith *et al.* 1996], [Smith 1997]) identified customer requirements regarding their security needs for information processing systems. In 1998 Sandhu ([Sandhu 1998]) recapitulated, amongst others, the RBAC96 models ([Sandhu *et al.* 1996]) and the ARBAC97 administration models ([Sandhu *et al.* 1997]). Furthermore, he noted that the discipline of role development needs considerable work to fully realize the potential of RBAC.

In ([Rhodes and Caelli 2000]) RBAC characteristics and policies were reviewed. The advantages of RBAC have been analyzed in combination with an overview of existing RBAC models and architectures. However, Rhodes only described a limited selection of role models, providing insight into RBAC usage and implementation. In [Ferraiolo 2001], Ferraiolo summarized and classified 25 role-related publications. He recognized role models, role concepts, role relations, and former efforts on integrating roles in access control as research directions. In the same year Sandhu ([Sandhu 2001]) identified three major classes of RBAC research: The development of a consensus standard model, a deeper theoretical understanding of RBAC, and a contextual understanding of the practical purpose of role models. Aspects of RBAC models, the authorization of administration of RBAC and related paradigms, a comprehensive RBAC administrative model, and applications of RBAC to business-to-business and business-to-consumer electronic commerce were considered future research directions. Again, this work enlightened only a segment of the whole research area as only 19 publications were cited.

In 2002 ([Gallaher *et al.* 2002]) describe the NIST RBAC efforts and evolution and analyzed the economic impacts of RBAC. On basis of a case study the benefits and costs per employee managed by RBAC systems are quantified. Another overview of RBAC Models can be found in ([Bertino 2003]). In this work the concepts of flat, hierarchical and constrained RBAC models are explained. Furthermore, advise for some research efforts in implementing RBAC features are given. In 2004 Essmayr et al. ([Essmayr *et al.* 2004]) presented an overview over security models in general and an additional survey on RBAC. The authors summarized RBAC entities, properties, constraints, administration in RBAC, and the coexistence with DAC and MAC. Discussions on the review and further development of methodologies that support the definition of roles have been carried out in a panel at the SACMAT[5] conference series in 2008.

In contrast to the previous meta-analysis and review articles a higher number of publications are referenced in ([Zhu and Zhou 2008]). However, the authors are only partly focusing on roles in Information Security and mainly present different kinds of roles in information systems in general. They provide a short classification including the evolution and the applications of *RBAC-roles*, without giving a detailed analysis: The authors only investigate 13 RBAC-related publications, leading to a very limited overview over the research area.

Fuchs recently provided an evaluation of different role development approaches in [Fuchs *et al.* 2009]. However, this survey also only covers a limited part of the overall research area. Note that over the years also a number of textbooks have been published, reviewing and summing up the scientific results of specific research directions. Examples are [Ferraiolo *et al.* 2007] or [Coyne and Davis 2007]. These books are not included as scientific publications in the survey process itself as they recapitulate existing knowledge in the field.

In the following, Table 1 sums up the different review and meta-analysis articles together with the number of surveyed publications and contrasts to this work. It

[5] ACM Symposium on Access Control Models and Technologies

underlines the need for an all-embracing survey on roles in Information Security as all the existing publications only survey a very limited number of articles and thus do not provide a comprehensive overview over the research area. Theoretical and practical research tendencies were identified by most of these publications as main application areas of research. However, so far, no comprehensive portrait of scientific RBAC literature that systematically profiles the large set of existing Information Security publications has been given. Up to now no detailed identification and classification of research tendencies is available. Hence, the material presented in this paper forms a significant contribution to the existing knowledge base of roles in Information Security research.

TITLE	AUTHOR	YEAR	PAPERS CITED
Future Directions in Role-Based Access Control	Ferraiolo and Kuhn	1996	5
Role-Based Access Control: A Natural Approach	Giuri	1996	9
A Marketing Survey of Civil Federal Government Organizations to Determine the Need for a Role-Based Access Control (RBAC) Security Product	Smith et al.	1996	23
Issues in RBAC	Sandhu	1996	0
Role-Based Access Control	Sandhu	1998	30
A Review Paper: Role Based Access Control	Rhodes and Caelli	2000	35
An Argument for the Role-Based Access Control Model	Ferraiolo	2001	25
Future Directions in Role-Based Access Control Models	Sandhu	2001	19
The Economic Impact of Role-Based Access Control	Gallaher et al.	2002	32
RBAC Models - Concepts and Trends	Bertino	2003	13
Role-Based Access Controls: Status, Dissemination, and Prospects for Generic Security Mechanisms	Essmayr et al.	2004	24
Panel on Role Engineering	Atluri	2008	18
Roles in Information Systems : A Survey	Zhu and Zhou	2008	99 (13 on RBAC)
Different Approaches to Identity Management – Justification of an Assumption	Fuchs et al.	2009	17
Roles in Information Security – A Survey and Classification of the Research Area	Fuchs et al.	2009	866

Table 1: Review and Meta-Analysis publications

3. RESEARCH METHODOLOGY

In order to achieve a detailed and correct classification of a large amount of publications a well-defined research methodology is of critical importance. This chapter points out the cornerstones of the underlying methodology used in this survey and explains and reasons about the overall survey process considering possible alternative approaches.

In chapter 3.1 a detection strategy for the identification of the relevant publications is presented and evaluated against possible alternative approaches. The outcome is a comprehensive result set consisting of 866 publications dealing with the research on role theory. In chapter 3.2 the used classification methodology is outlined. Again, alternative

approaches are considered and evaluated. The central outcome of this second process step is the complete classification of all publications included in the previously derived result set into 30 different, hierarchically aligned research areas. On the basis of the classification results in-depth analyses of research tendencies, statistical analysis of the results, and future research directions can be given. These tasks represent the major contribution of this work and are carried out in chapter 4 to 7 of this survey.

3.1 The Detection of Relevant Publications

In order to conduct a comprehensive survey the detection techniques that lead to the derivation of relevant publications have to be considered and evaluated carefully. A straightforward approach would be a manual check of references given inside publications. Starting from few core publications a complete reference analysis iteratively leads to the identification of further scientific contributions that are added to the investigation basis. Another possibility for a manual approach could be the content analysis of significant and well-established conferences and journals in the field. However, both manual approaches have drawbacks. On the one hand a fully mashed cross-referencing among the scientific publications is required. Additionally conference and journals based identification is heavily subjective and based on the individual knowledge of the investigator. Nevertheless, the biggest drawback stems from the high expected number of publications to be analyzed. Hence, a manual identification process would be time-consuming, error-prone, and inefficient.

As a result, an automatic search based on a bibliographic database needs to be carried out. Due to the fact that automated search facilities do not always lead to appropriate results categorically, it is essential to include a subsequent manual verification process. The derived final set of publications represents the basis for identifying research areas and -tendencies and is called result set in the following (RES_{RBAC}^{+} = result set). It consists of all publications that are either listed in one of the major computer science journals and proceedings, have been referenced in one of them, or were contained in one of the major Information Security journals and proceedings.

The used methodology to conduct a comprehensive survey of the research area is depicted in Figure 2. It consists of four major steps, bibliography selection, query selection and search, result reviewing, and result extension. These steps are described in the following.

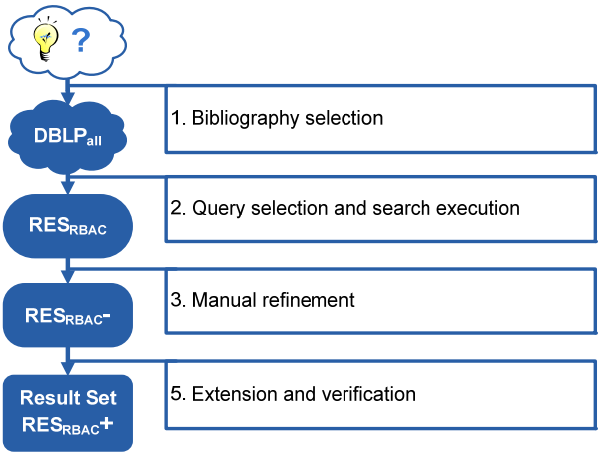


Figure 2: The detection of relevant publications

Bibliography selection

As the research area is broad and complex only electronic and automated search for publications is a reasonable means to ensure an adequate overview over the field. Characteristics like the investigated scientific discipline, the amount of included publication types and the offered search-capabilities must be considered.

A careful analysis of available electronic library databases and associated search options is the starting point for the investigation. Existing bibliographic databases including the ACM Digital Library[6], AIS Electronic Library[7], IEEE Digital Library[8], CiteSeerX Scientific Literature Digital Library[9], Google Scholar[10], Springer Link[11], and DBLP[12] (Digital Bibliography and Library Project) were investigated for usage throughout this work. An evaluation revealed the DBLP as the best bibliographic source for the purpose of this survey. This database firstly is not limited to a certain publisher like Springer Link. Secondly the library service returns the found publications along with a number of distinguishing facets, e.g. the publication date, authors, or conferences. Thirdly, it provides bibliographic information on major journals and proceedings in the field of computer science, including most results that can be obtained with other bibliographies. The majority of information technology journals and proceedings are embraced in DBLP. All in all over 2^{20} records are included ($DBLP_{all}$ in Figure 2)[13]. In order to ensure a high result quality, the IEEE library has been facilitated in addition to the DBLP service in a second retrieval step as not all publications listed in the IEEE bibliography are listed in the DBLP. Both results were compared and combined to obtain a set union of both publication sets.

The DBLP provides two different search mirrors: the complete search and the faceted search[14]. The faceted search option was used during this survey as it allows searching for publications on basis of one or more keyword(s) in the title, the venue, and the annotated metadata. A BibTeX entry for each publication was derived consecutively. BibTeX is a tool for formatting lists of references on basis of a text-based file format. The availability of those entries in combination with reference management software (e.g. the open-source solution JabRef[15] used for this research) is mandatory as the number of identified publications is in the several hundred.

Query selection and search execution

The second step after the selection of the search engine is the consideration of appropriate query terms. For this survey one promising term is *role*. However, due to homonym conflicts it is not suitable for identifying relevant publications. Using *role* as search term a total of 17080 records was returned by the DBLP service (retrieval date 01/01/09). Only a small number of those publications deal with the term *role* in terms of

---

[6] http://portal.acm.org/dl.cfm
[7] http://aisel.aisnet.org/
[8] http://www2.computer.org/portal/web/csdl
[9] http://citeseerx.ist.psu.edu/
[10] http://scholar.google.de/
[11] http://www.springerlink.com/home/main.mpx
[12] http://dblp.uni-trier.de/, former known as “DataBase systems and Logic Programming”
[13] A comprehensive list of included sources can be obtained at http://www.informatik.uni-trier.de/~ley/db/.
[14] maintained by Jörg Diederich, Chief Information Officer at the University of Hildesheim
[15] http://jabref.sourceforge.net/

Information Security. Therefore the idioms *RBAC*, *role based*, and *role-based access control* as synonyms for the adaption of role theory in Information Security were selected. Authors publishing in the investigated research field are most likely to mention these terms in the title, the keywords, or the metadata of their publication. If this is not the case they at least refer to the initial RBAC models in the reference section. The investigation of the obtained results in terms of a cross-checking with the results of other search terms underlined the reasonability of our approach. The DBLP query resulted in the extraction of 996 records based on the cutoff date 01/01/09. The additional search of the IEEE library provided returned another 65 publications which have not yet been included in result set returned by the DBLP search engine. The set union (RES_{RBAC}) hence consisted of 1061 publications.

Manual refinement

A detailed investigation of the returned results revealed that not all displayed entries were relevant for the objective of this survey. As already mentioned in the introduction to this article, several related research areas exist, not all of them dealing with roles in respect to Information Security. Examples for those areas are agent systems or modeling roles as investigated in [Zhu and Zhou 2008]. Due to the focus of this survey, only publications which fulfill at least one of the following criteria have been kept in the result set: The term *RBAC*, *Role-Based Access Control*, or *role* in terms of Information Security is included in the title, the keywords, in the venue-title, or the abstract of the publication.

This, e.g., excluded publications focusing on *agent systems* or *modeling roles*. These publications commonly use roles in respect to software components and agent behavior neither involving human interaction, nor dealing with Information Security. However, note that there is no clear differentiation among the mentioned related areas. Thus several borderline publications had to be investigated in detail to determine their primary focus and decide upon their inclusion in the result set. This manual review process reduced the amount of publications to 881 (RES_{RBAC}^{-}).

Extension and verification

Even though the DBLP library and the IEEE library span a large number of publications and publication types, a full coverage of all relevant scientific publications cannot be ensured automatically. To improve the quality of the preliminary result set, manual and recursive reference checking of the 881 publications was conducted. The references listed in every publication included in RES_{RBAC}^{-} were investigated for their inclusion. If a listed reference dealing with roles in Information Security was not yet incorporated it was added to the result set. This refinement step ensured that the significant publications (i.e. those which are referred to by other authors) have been considered during the survey. Note that dissertations have not been considered as they are usually published (at least partly) in one of the investigated venues. Again, books are also not included as they recapitulate existing knowledge in the field.

The fact that possibly a temporal delay may exists in the DBLP library may lead to the special circumstances that not all relevant publications from the year 2008 are integrated into DBLP on 01/01/2009. Due to that reason, all significant conferences and journals were re-checked manually to identify further relevant publications. Additionally, the previous search has been repeated in early 2009, filtering late 2008 publications. Both these step ensure the inclusion of recent publications, above all, those included in the most significant conferences and journals. After this manual result extension the amount of scientific publications resulted in 866 (RES_{RBAC}^{+}), representing the final result set used as basis for the consecutive classification process and thus the identification of research areas.

3.2 The Classification of Relevant Publications

The essential challenge of the conducted survey is discovering a suitable and meaningful structure for the identified publications. The elements included in the previously derived result set need to be classified and clustered into appropriate research fields and –tendencies during the subsequent and final classification process. This work made use of a hierarchical n-level clustering approach as shown in Figure 3.

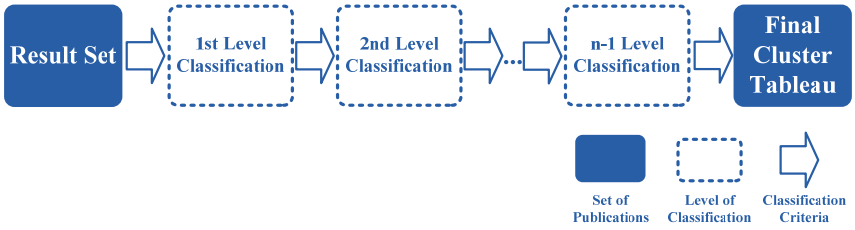


Figure 3: The classification methodology

Several classification criteria have been considered to reach a stable hierarchy of clusters representing the various research directions. During the classification process entities in RES_{RBAC}^{+} have been assigned to exactly one cluster in the resulting class hierarchy. Each of the individual papers has been weighted equally. Without these restrictions no meaningful structuring of the large number of publications would have been possible.
The most important indicators for cluster definition and assignment were the

- title of the paper and the content presented in the abstract,
- structure of the paper, in particular the captions of the sections,
- author(s) and research group the paper originates from,
- results of existing review and meta-analysis papers (see chapter 2.2),
- references given in the publication, or
- exhaustive reading of the content.

In the following alternative ways to solve the classification task are discussed shortly to justify the decision for hierarchical clustering as pragmatic classification approach. Firstly, it would be possible to carry out a sophisticated weighing of publications. For example, the more often a publication is referenced, the more important the publication is considered. Such an approach would take the subjective significance of the different publications into account. Another option would be to remove the limitation of hierarchical clustering and the resulting assignment of publications to only one cluster by applying an allocation based on a specific percentage. For example a publication P belongs to a research area A1 (90%) and to another research area A2 (10%). Furthermore, it would be possible to draw a references graph that considers the reference relationships among publications. A scientific paper represents a node and a reference link is represented by edges, essentially revealing groups or clusters representing a special research area. However, due to the fact that only limited space for references is given and that additional publications are referenced which do not belong to the same area, this graph-based approach is controversial. With the high number of publications in the result set RES_{RBAC}^{+}, the alternative approaches are not applicable because of the rapidly increasing complexity. We recommend these alternative classification techniques for smaller survey settings. However, it would be interesting to extend and refine this work by facilitating the weighted allocation of publications to multiple clusters.

4. GENERAL FINDINGS

Considering the large amount of 866 publications included in RES_{RBAC}^{+}, the research area concerning roles in Information Security seems to be confusing and diverse. This chapter provides a first impression and analysis of the complete area on basis of a statistical analysis. This supports the development of a general insight into the development of the field. The result set is examined and split up depending on general characteristics of publications including the year of publication, the venue-title, and the actively involved authors in publishing papers concerning roles in Information Security.

4.1 Publications According to Year of Publication

The amount of publications according to the year of publication is illustrated in Figure 4. The vertical axis represents the year of publication while the horizontal axis represents the amount of scientific work that has been published in the corresponding year. Underneath, the corresponding absolute amounts of publications are given and summarized.

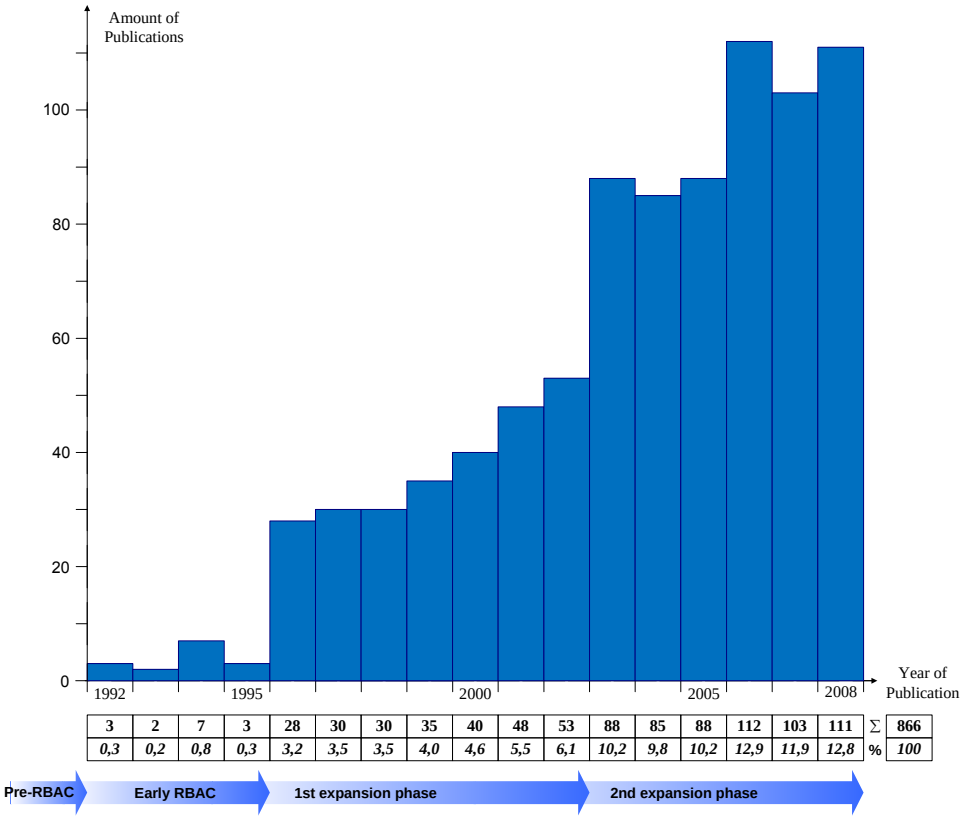


Figure 4: Publications according to year of publication

The visualization is characterized by overall constantly growing publication numbers. A closer examination reveals four major development phases of the research area. They are heavily influenced by the three ground-laying publications [Sandhu *et al.* 1996], [Ferraiolo *et al.* 2001], and [ANSI/INCITS 2004].

Several authors in the area of Information Technology and Information Security dealt with role theory before 1992. As aforementioned, these research efforts were summarized as *pre-RBAC* phase and excluded from the following analysis. In 1992 the term *RBAC* was introduced ([Ferraiolo and Kuhn 1992]). This phase of *early RBAC* efforts until 1996 resulted in the publication of the initial RBAC96 family ([Sandhu *et al.* 1996]). This contribution and the simultaneous start of the *ACM Workshop on Role-Based Access Control* series represent the probably most significant milestone for the development of the research area. Based on this work, the efforts of researchers have increased over the following years and reached at a constant level until 2002 with about 30 to 40 publications per year. During this time RBAC developed to a widely used access control paradigm. It evolved from a NIST Standard in 2001 ([Ferraiolo *et al.* 2001]) to an ANSI[16]/INCITS[17] Standard in 2004 ([ANSI/INCITS 2004]). This standardization process marks the second and third milestone. During that time the amount of publications attained new heights at approximately 100 publications per year. The frontiers of the research area were expanded into various directions with the focus on the discovery of new application areas and improvements to the original role model and -theory.

4.2 Publications According to Venue

Table 2 presents the examination of the result set according to the venue in which the respective articles appeared. The publications were mostly published in the proceedings of various conferences, Journals, and tech-reports. A total of more than 200 different venue-titles were identified during this investigation. Note that due to space restrictions Table 2 illustrates only venue-titles with a minimum of six published papers. The largest number of articles on roles in Information Security appeared either in the *ACM Symposium on Access Control Models and Technologies* (71) or in the *ACM Workshop on Role-Based Access Control* (70). These workshops played a decisive role in the development of a scientifically proven and reputable adaption of role theory in Information Security. Since 2001 the scope of interest has been broadened and the *ACM Workshop on Role-Based Access Control* has evolved into the *ACM Symposium on Access Control Models and Technologies*. Analyzing the proportion of published papers according to the venue-title reveals that more than 16% of all identified scientific works were published in either one of those two venues

At least ten publications each have been published in other Journals and conferences, including the *Annual IFIP WG 11.3 Working Conference on Data and Applications Security* (28), the *Annual Computer Security Applications Conference* (25), the *ACM Transactions on Information and System Security* (22), the *Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises* (17), the *International Workshop on Database and Expert Systems Applications* (14), the *NIST-NCSC National Computer Security Conference* (13), the *ACM Symposium on Applied Computing* (12), and the *International Conference on Advanced Information Networking and Applications* (11).

Even though nearly 35% of all identified works have been published in the major venues mentioned above, the rest of about 65% appeared in a wide diversity of other venues. The total number of more than 200 different venue-titles reveals that there are a large number of conferences and journals that contain only a small number of publications. This fact underlines the multi-layered diffusion and dispersion of the role concept in nearly all areas of information technology.

[16] American National Standards Institute
[17] InterNational Committee for Information Technology Standards

VENUE-TITLE	ABSOLUTE	% OF ALL
ACM Symposium on Access Control Models and Technologies (SACMAT)	71	8.20 %
ACM Workshop on Role-Based Access Control[18]	70	8.08 %
Annual IFIP WG 11.3 Working Conference on Data and Applications Security (DBSec)	28	3.23 %
Annual Computer Security Applications Conference (ACSAC)	25	2.89 %
ACM Transactions on Information and System Security (TISSEC)	22	2.54 %
Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE)	17	1.96 %
International Conference on Database and Expert Systems Applications including Workshops (DEXA)	14	1.62 %
NIST-NCSC National Information Systems Security Conference[19]	13	1.50 %
ACM Symposium on Applied Computing (SAC)	12	1.39 %
International Conference on Advanced Information Networking and Applications (AINA)	11	1.27 %
International Conference on Information and Communications Security (ICICS)	8	0.92 %
IFIP TC-11 International Information Security Conference (SEC)	8	0.92 %
IEICE Transactions	7	0.81 %
IEEE International Workshop on Policies for Distributed Systems and Networks (POLICY)	7	0.81 %
ACM Conference on Computer and Communications Security (CCS)	7	0.81 %
IEEE International Conference on Computer and Information Technology (CIT)	7	0.81 %
International Conference on Availability, Reliability and Security (ARES)	7	0.81 %
International Working Group on Computer Supported Cooperative Work in Design (CSCWD)	7	0.81 %
Australasian Conference on Information Security and Privacy (ACISP)	6	0.69 %
IEEE Symposium on Security and Privacy (S&P)	6	0.69 %
OTM Conferences/Workshops	6	0.69 %
Grid Computing Conference (GCC)	6	0.69 %
International Conference on Trust, Privacy & Security in Digital Business (TrustBus)	6	0.69 %
Hawaii International Conference on System Sciences (HICSS)	6	0.69 %

Table 2: Publications according to venue

[18] evolved into SACMAT
[19] discontinued

4.3 Authors involved in the area

In addition to the timeline- and the venue analysis, Table 3 lists authors actively involved in conducting and publishing on roles. Due to space limitations only authors who have been involved in at least five publications are listed.

AUTHOR	INV. PUBL.	AUTHOR	INV. PUBL.
Ravi S. Sandhu	55	Ken Moody	8
Elisa Bertino	34	BongNam Noh	8
Gail-Joon Ahn	33	HyungHyo Lee	8
Sylvia L. Osborn	22	Matunda Nyanchama	7
James B. D. Joshi	22	Mark Strembeck	7
Arif Ghafoor	18	Indrakshi Ray	7
Jason Crampton	15	Rafae Bhatti	7
Makoto Takizawa	14	David M. Eyers	7
Chang N. Zhang	14	T. C. Ting	7
Cungang Yang	13	Jonathan D. Moffett	6
David F. Ferraiolo	13	Emil Lupu	6
Tomoya Enokido	13	Jinli Cao	6
Joon S. Park	12	Trent Jaeger	6
David W. Chadwick	12	A. Belokosztolszki	6
D. Richard Kuhn	11	Luigi Giuri	6
Seog Park	11	Chang-Joo Moon	6
John F. Barkley	11	Vijay Varadharajan	6
Sejong Oh	11	Gustaf Neumann	5
Steven A. Demurjian	11	Morris Sloman	5
Ninghui Li	10	Steve Barker	5
Hua Wang	10	Michael Hitchens	5
Vijayalakshmi Atluri	9	Axel Kern	5
Edward J. Coyne	9	Basit Shafiq	5
Günther Pernul	8	Maria Luisa Damiani	5
Jean Bacon	8	Charles E. Youman	5
R. Chandramouli	8		

Table 3: Involved authors in the research field

The methodology considers all authors and co-authors of a selected publication. The researcher on top of leads this list with 55 publications. This amount of articles approves his general acceptance as one of the core authors in the field. Above all the acceptance of ([Sandhu *et al.* 1996], [Ferraiolo *et al.* 2001]) as milestones of RBAC research underlines this assumption. It is additionally supported by the fact that almost publications in the result set reference at least one of his scientific contributions. Positions 2 and 3 follow with 34 and 33 publications respectively. Altogether 22 authors contributed to more than ten publications. Be aware that several authors like Pierangela Samarai, Sushil Jajodia, Bhavani M. Thuraisingham, Elena Ferrari, or Eduardo Fernandez – to mention only selected – did extensive research on access control. Throughout their work they dealt with roles and related issues, however, their main contribution lies in the area of access control in general. Thus, their work is not included in this survey by design.

As already pointed out during the evaluation of the venue-titles, the author-based analysis also proves the huge diffusion and multi-layered spreading of RBAC. More than

1300 different (co-)authors have been identified in this investigation. Besides the core scientists listen in Table 3 there are a lot of authors using and integrating RBAC for their special and individual needs. This result shows that the draft of RBAC and a more general role-based security mechanism has been disseminated into many areas of Information Security research.

5. IDENTIFYING RESEARCH AREAS – CLASSIFICATION RESULTS

The statistics given in chapter 4 demonstrated the overall development of a role-based security paradigm and the research area. The amount of publications according to the year of publication (see Figure 4) showed that the research development can be divided into major phases and that the amount of articles per year has been rapidly increasing after 1996. Furthermore, both the investigation of venue-titles and the involved authors (see Table 2 and Table 3) underline the multi-layered spreading and dispersion of the role concept the field of Information Security.

However, besides this statistical analysis, the essential challenge of the conducted survey is the discovery of a suitable and meaningful classification structure for the identified publications. Based on the predefined methodology, hierarchical clustering has been conducted. The identified sets of publications allocated to a cluster are called *areas* or *research areas* of a certain *level of classification*. The classification process resulted in a three level classification scheme which ensures appropriate classification of all publications on the one hand combined with simplified understanding and readability on the other hand. Using more than three levels of classification led to too small and specific research areas while using less than three levels leads to large and generic clusters. The classification process allocated each of the 866 scientific publications to one of 30 identified different research directions.

The following chapter presents overall classification results focusing on the main research areas. It thereby provides the basis for a detailed analysis of the 2nd and 3rd level classification results in chapter 6 and 7.

5.1. Main research areas

The 1st level classification analysis depicted in figure 4 reveals three major groups of publications (research areas): *Early RBAC* publications, publications with *theoretical focus*, and publications with *practical focus*. This finding is in alignment with the core outcome of several existing review articles investigated in chapter 2.2.

The smallest cluster consists of the *early RBAC* efforts between 1992 and 1995 which were already mentioned during the introduction of this chapter. This collection of publications deals with the RBAC research activities before the introduction of the RBAC model family. Besides this small cluster, publications can be differentiated according to their *theoretical*- or *practical focus*. While theoretical publications deal with the investigation, extension of existing concepts surrounding roles, the practical publications apply the gained findings in real world scenarios or in prototypical and experimental settings. Note that almost every theoretical work has a practical part and every practical work mentions its theoretical foundation. The final assignment to one class thus was based on the predominant affiliation. The statistical analysis of cardinalities (Figure 5) reveals that both classes consist of about half of the investigated scientific publications (theoretical: 451; practical: 400).

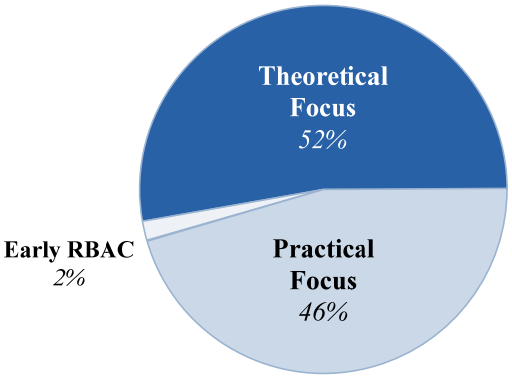


Figure 5: 1st level classification analysis

A timeline analysis shown in Table 4 underlines that the respective yearly publication count of articles with theoretical and practical affiliation is roughly equal. This shows the importance of the role theory for Information Security not only in respect to theoretical research issues, but also for practical research as well as implementation needs. Table 4 again points out the growth of the area starting with only few publications during the *early RBAC* phase, ending up with approximately 100 publications per year after 2005.

Result Set	´92	´93	´94	´95	´96	´97	´98	´99	´00	´01	´02	´03	´04	´05	´06	´07	´08	∑
Early RBAC	3	2	7	3	-	-	-	-	-	-	-	-	-	-	-	-	-	15
Theoretical Focus	-	-	-	-	15	16	12	12	22	26	30	53	40	47	62	55	61	451
Practical Focus	-	-	-	-	13	14	18	23	18	22	23	35	45	41	50	48	50	400
∑	3	2	7	3	28	30	30	35	40	48	53	88	85	88	112	103	111	866
%	*0,3*	*0,2*	*0,8*	*0,3*	*3,2*	*3,5*	*3,5*	*4,0*	*4,6*	*5,5*	*6,1*	*10,2*	*9,8*	*10,2*	*12,9*	*11,9*	*12,8*	*100*

Table 4: Composition of the result set

5.2. Detailed classification results

The 1st level classification has revealed practical and theoretical focus as first distinction criteria of the area. Due to the large number of publications assigned, a 2nd level classification needs to be carried out. The 400 Publications dealing with practical RBAC and role-related issues can be differentiated into *industry* and *technology* efforts. The industry-related publications deal with the adoption and usage of roles in certain types of industries like health care or the banking sector. The group of technology-based publications is much larger and investigates the adoption of RBAC and role theory in various existing technologies, e.g. operating systems, databases, the internet, software engineering, or middleware and ESM[20]. The cluster definition was carried out manually and subjectively based on the predefined methodology introduced in chapter 3.

The 451 publications with theoretical affiliation are divided into a large group of *Role Model and Design* and several smaller clusters dealing with *Role Development*, *Roles and Standards*, etc. *Role Model and Design* as the largest cluster includes research activities dealing with role models, their elements, the relationships among those elements, and their administration. *Role Development* comprises publications that deal with the initial definition of roles in specific environments like a software engineering project. Several

[20] Enterprise Security Management

smaller areas deal with *standardization efforts*, the relationship of *RBAC and DAC/MAC*, or *Review and Meta-Analysis.* Additionally a group of publications that analyze the relation of *Roles and Security Technologies* like cryptography, information flow, or protocols like XACML were identified.

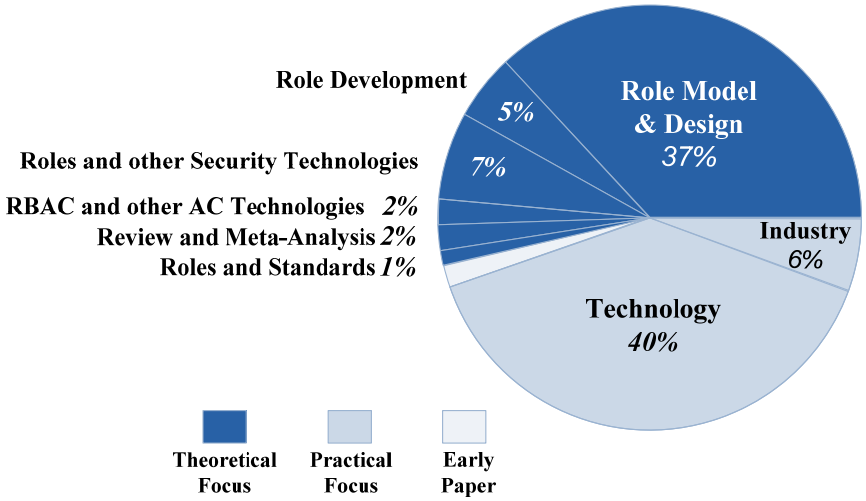


Figure 6: 2nd level classification analysis

The refined pie chart diagram depicted in Figure 6 reveals the quantitative constitution of the 2nd level research areas. The results show that the practical research field is heavily dominated by publications investigating the adaption of roles in different security technologies. The theoretical research field is dominated by publications investigating the formal framework of role systems to a large extent. After the identification and explanation of the first classification levels is finished, the full classification tableau is provided in this chapter of the survey. Figure 7 provides a holistic recapitulation of the hierarchical clustering results. One can identify the three levels of classification from the left to the right. The identified 1st level research areas are divided into the smaller subareas derived during the 2nd classification process. The cardinality of a majority of the 2nd level research areas requires a 3rd level classification. As aforementioned, the specific clusters represent specific research areas.

Note that the classification process is based on several criteria mentioned in chapter 3.2. However, class definition itself is a subjective and iterative refinement process. While many research areas are homogenous, several publications cannot be easily assigned to one specific class. Hence the allocation was carried out based on the main focus of the publication. Additionally, several research areas are related to each other. Theoretical findings, e.g. concerning roles and their usage in security technologies are usually adapted in practical scenarios. In order to avoid misunderstandings a clear definition of the respective research areas is needed

This final classification tableau (Figure 7) is consecutively explained in detail in chapter 6 and 7. The constitution and development of the single research areas is analyzed and interpreted. In order to provide readability and consistency, the investigation scheme remains identical during the presentation of all research areas:

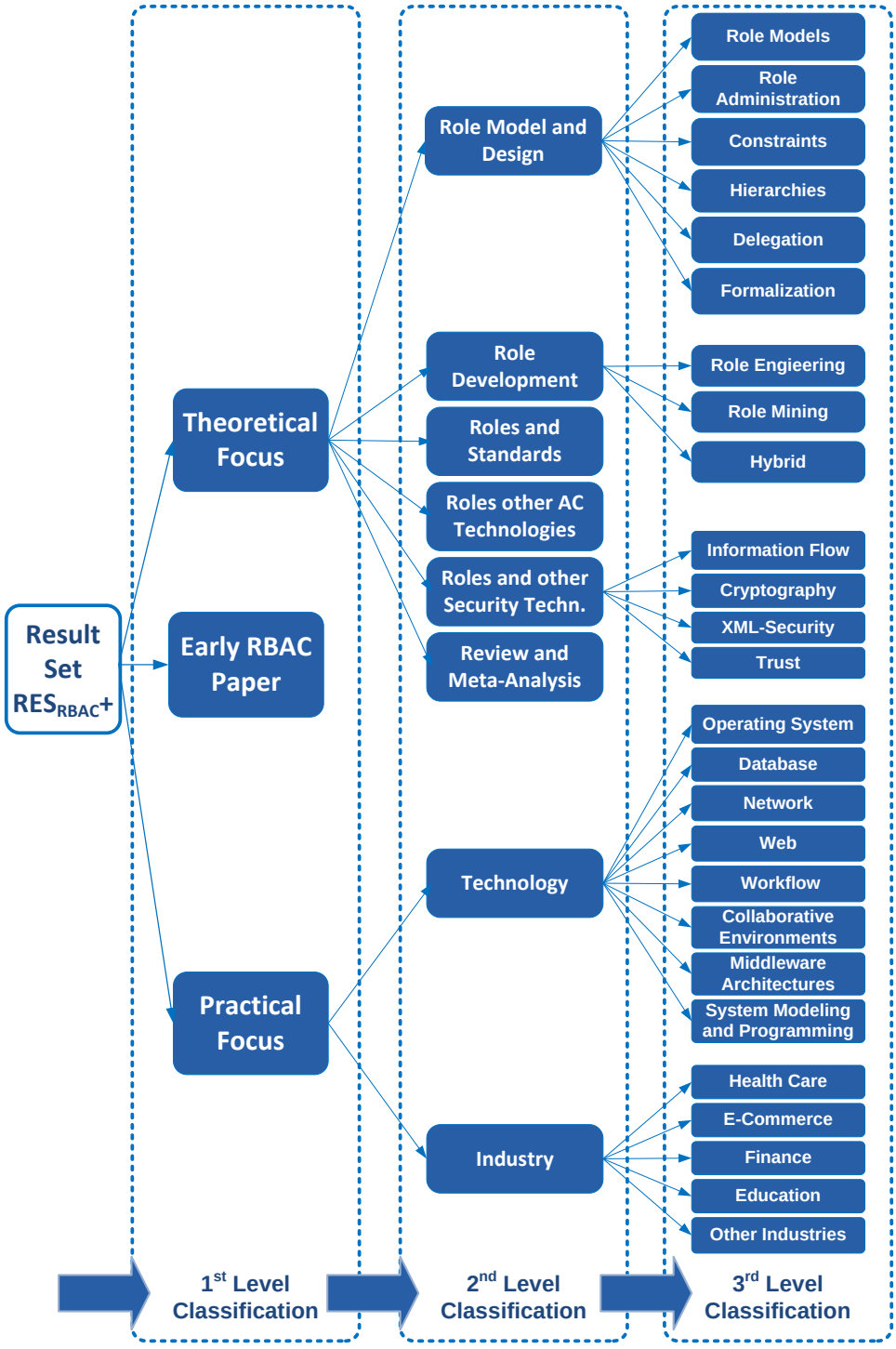


Figure 7: Final classification tableau

Before a specific area is explained, it is defined in the first step. The definition shapes the research area and reasons for the assignment of the respective publications. In a second step (*plotting of an area*) the timeline analysis representing the development of the area in terms of quantitative research output is shown and interpreted. The amount of papers is plotted against the year of publication in order to show variations and allow for the deduction of research tendencies. For the 1st level classification additional percentage values are depicted. Consecutively the refinement of a research area in sub-areas (if applicable) is provided in a third step (*classification of an area*). Supporting and reasoning the classification, representative papers are explained shortly in the last sub-chapter of chapter 6 and 7. Note that not all papers which belong to an area can be mentioned explicitly because of space limitations. Though, only a selection is presented based on the importance of a research area or its current development.

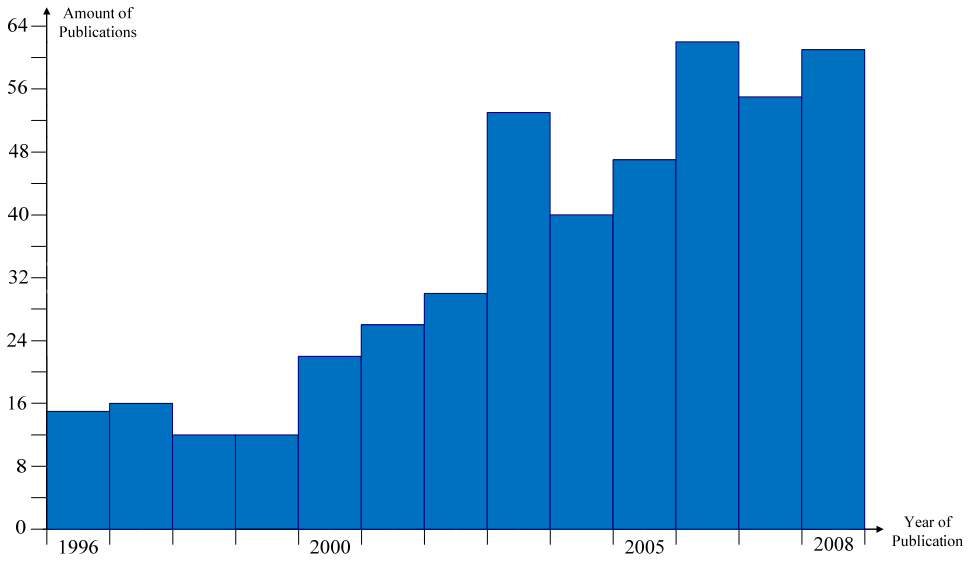
Again, note that due to the high number of publications surveyed and the resulting space conflicts not all applicable publications are referenced in the text and the reference section of this survey. If necessary, the provided electronic database[21] is referred to in the text. The reader is provided with the necessary information to look-up the appropriate publications in the database. The literature itself includes not only the reference information, but also the complete classification information. Therefore the reader can browse research areas and investigate only the scientific work in those specific areas of interest.

6. PUBLICATIONS WITH THEORETICAL FOCUS

After the presentation of the general classification, this chapter is going to analyze research efforts with a theoretical focus, thus the upper part of the classification tableau in Figure 7. Due to space restrictions not all sub-areas can be investigated to the same extent. In the following a short overview and definition of the 2nd level research areas is given before a detailed analysis of selected areas is carried out in the consecutive subchapters.

Publications with theoretical focus deal with the investigation and extension of existing concepts surrounding role theory adaption. The quantitative development of publications with theoretical affiliation according to the year of publication is depicted in Figure 8. In 1996 the publication count has already been relatively high with 15 papers, remaining at a constant level over the next years until 1999. After that a steady rise of researchers' interest in the field between 2000 and 2005 can be identified. One reason for this development is likely the establishment and increasing diffusion of the role concept and RBAC in the Information Security community. Simultaneous, practical usage led to new open theoretical research questions. One prime example is the extension of existing role models over the years (detailed presentation is presented in the following sub-chapter). Practical requirements led to the upcoming of several, slightly adapted role models usable in specific application scenarios. Additionally, the ongoing standardization process supported the development of the research area.

[21] http://www-ifs.uni-regensburg.de/Roles



15	16	12	12	22	26	30	53	40	47	62	55	61	Σ	451
3,3	*3,5*	*2,7*	*2,7*	*4,9*	*5,8*	*6,7*	*11,8*	*8,9*	*10,4*	*13,7*	*12,2*	*13,5*	%	*100*

Figure 8: Plotting of publications with theoretical focus

6.1. Composition of the area

The composition of the research area is presented in Table 5. It lists the various subclasses and their quantitative development. The results underline that most of the publications are assigned to the area of *Role Model and Design* (316). This research area and its sub-areas are the most significant research fields in terms of theoretical role-based security research. *Roles and Other Security Technologies* (60) as well as *Role Development* (39) are additional vivid and important research areas. The areas *Review and Meta-Analysis* (14), *Roles and other AC Technologies* (14), and *Roles and Standards* (8) form the minor research areas.

Theoretical Focus	´96	´97	´98	´99	´00	´01	´02	´03	´04	´05	´06	´07	´08	∑
Role Model and Design	8	11	8	9	12	19	19	38	29	38	49	40	36	316
Role Development	1	2	1	1	3	1	3	5	3	4	1	4	10	39
Roles and Standards	-	-	-	-	2	1	-	-	1	-	1	2	1	8
Roles and other AC Technologies	2	2	2	1	1	1	-	-	-	-	-	2	3	14
Roles and other Security Techn.	-	-	-	1	3	2	7	9	6	5	11	7	9	60
Review and Meta-Analysis	4	1	1	-	1	2	1	1	1	-	-	-	2	14
∑	15	16	12	12	22	26	30	53	40	47	62	55	61	451
%	*3,3*	*3,5*	*2,7*	*2,7*	*4,9*	*5,8*	*6,7*	*11,8*	*8,9*	*10,4*	*13,7*	*12,2*	*13,5*	*100*

Table 5: Composition of publications with theoretical focus

In the following the 2nd level classification areas are shortly analyzed. The areas Role *Model and Design* and *Role Development* are investigated in detail in chapter 6.2. For all other research areas a basic result interpretation is provided on basis of plotting diagrams.

Role Model and Design

Every role system has to be based on a well-defined theoretical basis. The area of *Role Model and Design* provides formal models for the definition and administration of a role system. It shapes the basic understanding of roles in a certain environment by defining the valid properties of roles and the valid mechanisms used to define, use, and manage them. Publications assigned to this research area are developing theoretical role- or administration models as well as publication focusing on different concepts used in these models, e.g. hierarchies, delegation, or constraints. The plotting diagram (Figure 9) underlines the importance of this research area and its subareas. After an initial phase between 1996 and 1999 a steady grown of the scientific output until the year 2004 can be identified. After the year 2006 the number of publications approximately remained at a high level of about 60 publications per year. A general consensus in basic RBAC structures and properties is potentially found. However, special situations and environments are still requiring a theoretical discussion of *Role Model and Design* concepts.

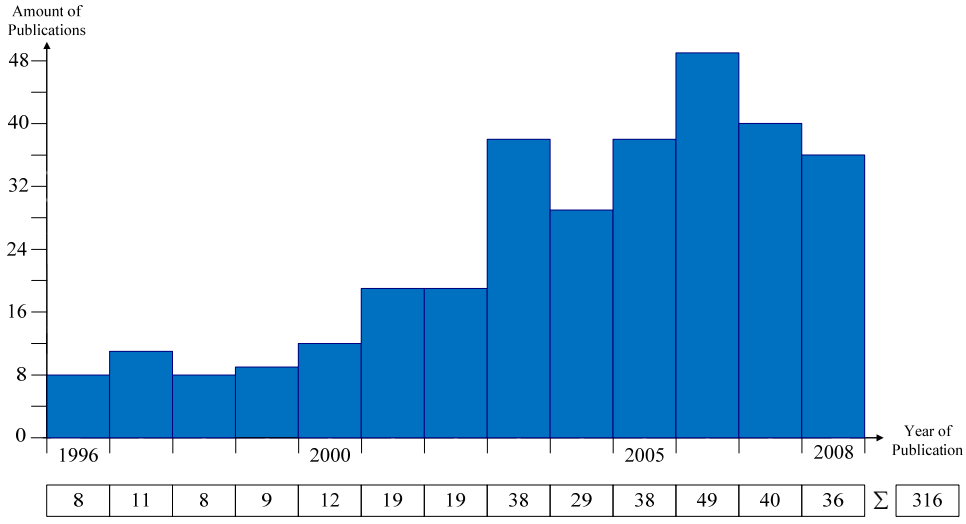


Figure 9: Plotting of *Role Model and Design*

Due to the large amount of publications in that research area a 3rd level classification was needed in order to further reveal well-differentiated research directions. The identified subclasses are depicted in a separated composition table shown in Table 6. Consolidated findings may be obtained by comparing the sub-areas directly. It becomes evident that the major part of 316 publications is belonging either to the area of *Role Models* (105) or to *Role Administration* (92). The other sub-areas are characterized by a smaller amount of papers (*Constraints* (42), *Delegation* (31), *Formalization* (27), and *Hierarchies* (19)). Furthermore, the tableau reveals that the development of the smaller research areas in general did not start immediately after the publication of the RBAC model in 1996.

Role Model and Design	´96	´97	´98	´99	´00	´01	´02	´03	´04	´05	´06	´07	´08	∑
Role Models	5	2	1	1	2	9	8	9	10	13	16	15	14	105
Role Administration	2	6	3	4	4	4	6	12	8	12	14	9	8	92
Constraints	1	2	1	2	2	2	-	8	4	5	4	7	4	42
Hierarchies	-	-	3	1	-	1	2	2	-	3	3	1	3	19
Delegation	-	-	-	-	3	2	2	5	5	2	7	3	2	31
Formalization	-	1	-	1	1	1	1	2	2	3	5	5	5	27
∑	8	11	8	9	12	19	19	38	29	38	49	40	36	316

Table 6: Composition of *Role Model and Design*

The last four specialized subareas are concentrating on specific aspects of *Role Model and Design*. They comprise publications that do not introduce new role (-administration) models but rather analyze specific issues like the possible inclusion of *hierarchical relationships* among roles and their dependency on existing organizational structures. Additionally, several publications deal with *delegation* concepts and their inclusion into a role system. Delegation in this context is the assignment of authority and responsibility to another person to carry out specific activities. The most popular subarea bundles publications that deal with the usage of *constraints* to control elements of the role system and its information flow. Above all the integration of basic security principles like the Separation of Duty (SoD) have traditionally been investigated by several researchers. In its simplest form, the principle states that a sensitive task should be performed by two different users acting in cooperation. The last subarea *Formalization* particularly consists of publications that try to express the role models, role concepts, and other theoretical issues using a formal language. Formalization is defined as the process or result of defining special circumstances or theoretical concepts with the help of special description languages.

Role Development

Before the benefit of a role system can be realized the initial task is the definition of valid roles in the respective environment. The task of identifying roles and their associated permissions in an enterprise is an extremely large and onerous one and needs to be carried out on basis of a predefined methodology. Several authors in the research area have published different approaches to solve the problem of role definition. Publications assigned to this research field hence either provide a structured approach for the development of roles or investigate mechanisms used to address specific role development – related issues.

The plotting diagram (Figure 10) shows that role development has been a research area since the very first days of RBAC in 1996. Due to industry's interest in fast and automated role system deployment the area has gained importance over the last years. Above all the automated role development approaches gained considerable importance. The significant increase of publications in 2008 underlines this development.

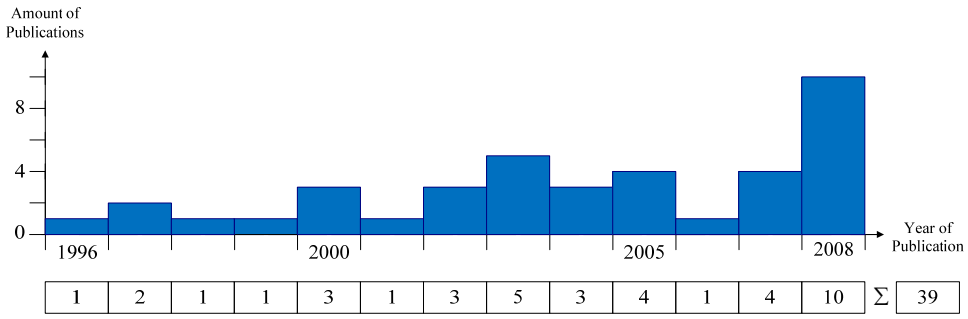


Figure 10: Plotting of *Role Development*

Roles and Standards

Missing standards for role-based access control resulted in inconsistencies and irritations during the development and usage of a role system. Over the years a need for a universally valid and accepted standard became obvious. The small research area of *Roles and Standards* consists of those publications that contributed to the standardization process. It also includes critical evaluation and discussions of the proposed standardization efforts. Figure 11 depicts the publications included in this area with the first publications appearing in the year 2000.

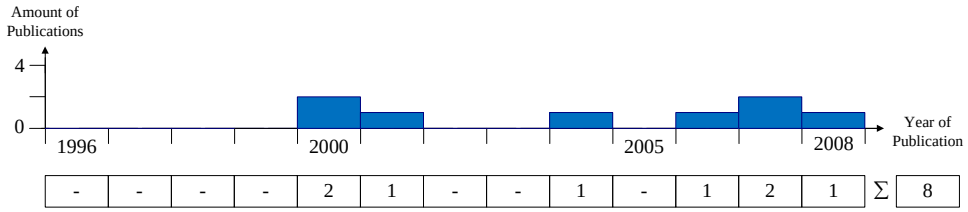


Figure 11: Plotting of *Roles and Standards*

Roles and other Access Control Technologies

Before RBAC, DAC and MAC were the most popular access control concepts. As RBAC became more and more used for access control within organizations, its relationship to the conventional access control mechanisms needed to be investigated. The research area consists of all publications that contributed to this investigation. The plotting of publications (Figure 12) shows that scientists were interested in this area in the early years of role theory research and that this field is basically finalized until the year 2006. Recently, discussion on the relationships between RBAC and models like the Bell-LaPadula model has revived.

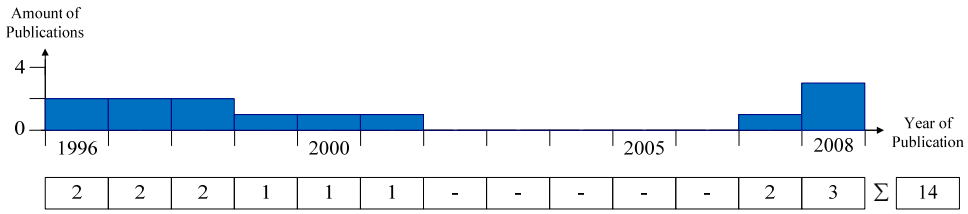
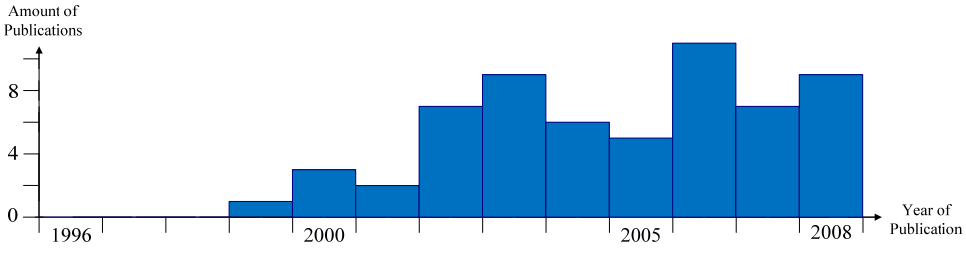


Figure 12: Plotting of *Roles and other Access Control Technologies*

Roles and other Security Technologies

With the increasing relevance of RBAC in both research and practical scenarios, several publications dealt with the relations between roles and other security standards and technologies. Publications assigned to this class can be seen as scientific efforts to harmonize and combine RBAC and other Information Security concepts in a theoretical way. The plotting of publications included in the area *Roles and Other Security Technologies* as shown in Figure 13 shows that research in this field started in 1999 with a steadily growing interest since then.



-	-	-	1	3	2	7	9	6	5	11	7	9	Σ	60

Figure 13: Plotting of *Roles and other Security Technologies*

As a result of the practical relevance of the role concept in Information Security it is no wonder that a harmonization with modern security technologies takes place. In contrast to related publications that investigate the practical usage of role theory in combination with other security technologies, the scientific contributions assigned to this class in particular focuses on theoretical issues. Due to the number of publications a 3rd level classification was necessary (see Table 7). The fields of interest include the usage of roles in combination with cryptography, information flow control, trust mechanisms, and XML (-Security) dialects. Research in those areas did not start before the year 1999. Lately, investigating issues and relationship between trust management and the role concept became more and more popular.

Roles and other Security Techn.	´96	´97	´98	´99	´00	´01	´02	´03	´04	´05	´06	´07	´08	∑
Cryptography	-	-	-	1	2	1	4	3	2	4	5	2	1	25
Information Flow	-	-	-	-	-	1	3	2	-	-	2	3	3	14
XML-Security	-	-	-	-	1	-	-	3	3	-	2	-	1	10
Trust	-	-	-	-	-	-	-	1	1	1	2	2	4	11
∑	-	-	-	1	3	2	7	9	6	5	11	7	9	60

Table 7: Composition of *Roles and other Security Technologies*

Review and Meta-Analysis

The review and meta-analysis publications define the last research field within the section of theoretical research work on roles. As chapter 2.2 already provided detailed insight into this field, no additional investigation is carried out at this point. The plotting diagram (Figure 14) reveals that a high number of meta-articles were published in the early days of RBAC. Over the years, other authors selectively dealt with reviewing a portion of the research area. Overall, as expected, this research area remains quite small.

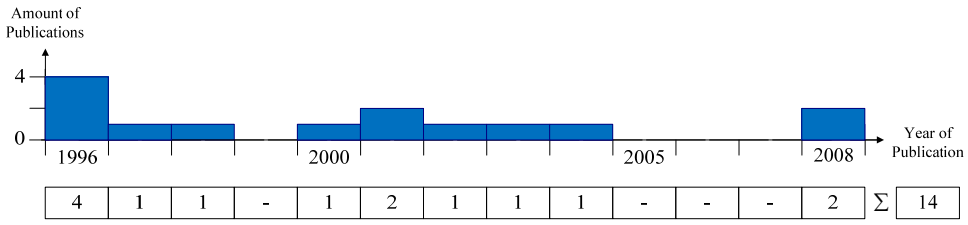


Figure 14: Plotting of *Review and Meta-Analysis*

6.2. Selected Research Areas

This chapter aims at an in-depth and content-specific analysis of selected research directions derived from the publications with theoretical affiliation. Due to their relevance the following subchapter specifically focuses on role models, role administration models, and role development approaches. The last chapter has shown that theoretical research on roles is heavily dominated by the *Role Model and Design* area. Additionally, the area of *Role Development* has recently gained importance among researchers and practitioners. It is the research area that has experienced the largest growth in terms of publication numbers after the year 2007.

Role Models

Role models are one core element of a role system and define the formal understanding of roles, related attributes, and entities. The overall development of the area *Role Models* is plotted in Figure 15. In the year of the first *ACM workshop on role-based assess control* (1995), five articles already were dealing with the content of a role model including RBAC96 ([Sandhu *et al.* 1996]). They were published in 1996, even though the workshop took place in 1995. This fact underlines the importance of this research area as constitutional element of the whole research area. After the year 2000 a newly gained interest of researchers in extending role models can be identified. Practical and theoretical requirements have led to the extension of existing role models for specific scenarios.

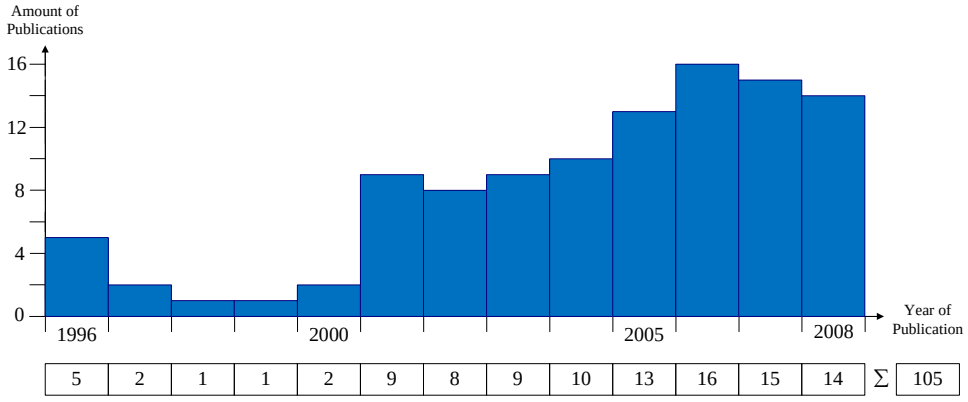


Figure 15: Plotting of *Role Models*

This sub-chapter presents several role models with their different role properties and interpretations of the role concept accordingly, starting with the basic RBAC96 model. The extended role models then are ordered depending on the year of publication. Each one introduces a slightly adjusted interpretation of the role concept. The presented

models have been selected as a result of their importance for the research community. For a detailed analysis and formal description this work refers to the original publications. The models are ordered on basis of their publication date, starting with the oldest models, moving on to recent publications.

RBAC96 [Sandhu *et al.* 1996]. The initial RBAC96 model is seen as the core model for roles and is primarily referenced by subsequent scientific works. RBAC96 exists of four partial models that are closely linked with each other. In its core, it is divided into four sub-models, which embody different subsets of the functionality:

- Core RBAC: Covers the essential RBAC features such that permissions are assigned to roles and roles are assigned to users.
- Hierarchical RBAC: Adds the notion of role hierarchies and inheritance.
- Constraint RBAC: Adds constraints to implement static separation of duty (restriction of the user-role membership) and dynamic separation of duty (restriction of the role activation by users).
- Consolidated Model (Figure 16): Combined Hierarchical and Constraint RBAC

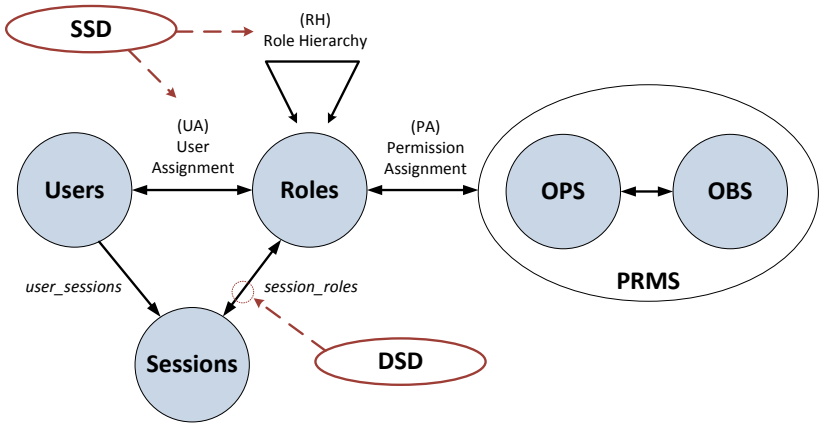


Figure 16: Consolidated RBAC model (drawing based on [Sandhu *et al.* 1996])

After the introduction of the standard RBAC model researchers discussed its limitations in several application scenarios. A large number of extended, slightly altered role models have evolved as result of practical needs. The naming of those following the *xRBAC*-scheme already shows their close relation to the original RBAC model: All of them build upon the data elements known from the RBAC standard. A comparison of the models is provided in [Fuchs and Preis 2008]. This subchapter only presents selected role models and does not claim completeness.

TMAC – Team-based Access Control [Thomas 1997]. In 1997 Thomas presented an approach to apply RBAC in collaborative environments. Thus, the central property of TMAC is the notion of a TEAM. A team is defined as a collection of users in specific roles with the objective of accomplishing a specific task or goal. The motivation of TMAC was the need for a hybrid access control model that incorporates the advantages of having broad role-based permissions across object types, the need to recognize the context associated with collaborative tasks, and the ability to apply this context to decisions regarding permission activation.

T-RBAC - Task-Role-Based Access Control [Oh and Park 2000]. Oh and Park proposed T-RBAC as an extended RBAC model for enterprise environment through integration of role-based access control and activity-based access control. The biggest difference between TRBAC and the original RBAC model is that the access rights are assigned to task rather than to roles. The property TASK represents job functions. T-RBAC defines three different classes of tasks: Supervision oriented tasks, workflow oriented tasks, and private tasks.

TRBAC - Temporal Role Based Access Control [Bertino et al. 2001]. The incorporation of time-dependency into RBAC was first proposed by Bertino et al. and has gathered significant attention since then. In many companies and organizations functions are not permanent. TRBAC addresses this challenge by applying a time limitation to when a given role can be activated for a given access control subject or object. TRBAC includes so called Periodic Expressions to represent a pair {[begin, end], P} where P is a periodic expression denoting an infinite set of periodic time instants, and [begin, end] is a time interval denoting the lower and upper bounds.

dRBAC - Distributed Role Based Access Control [Freudenthal et al. 2002]. Distributed Role-Based Access Control introduced initially by Freudenthal et al. is a scalable, decentralized trust-management and access control mechanism for systems with heterogeneous instances that span multiple administrative domains. It distinguishes itself from previous approaches by providing third-party delegation of roles from outside a domain's namespace, relying upon an explicit delegation of assignment. Additionally it supports modulation of transferred permissions using scalar valued attributes and continuous monitoring of trust relationships over long-lived interactions.

ERBAC - Enterprise Role Based Access Control [Kern 2002]. In 2002, Kern et al. introduced the concept of Enterprise Roles which is centrally built around the notion of organizational structure. Enterprise Roles are capable of spanning all IT systems in a company. The covered permissions can be of various natures, e.g., a group in UNIX, a role in Oracle, or a group in RACF with authorizations for updating a dataset and reading a database table. ERBAC is permission-based and does not incorporate tasks, positions, or job functions of employees. One difference between ERBAC and the RBAC standard lies in the notion of sessions. In an enterprise-wide administration concept, all systems in the enterprise are administered, but without control of the actual user sessions.

OrBAC - Organisation-based access control [Kalam et al. 2003]. The Organization-based access control model defines permissions that apply within an organization to control the activities performed by roles on views. The ORBAC model allows the administrators to specify more complex dynamic permissions since permissions only apply in some given contexts. The core entity in OrBAC is the organization. An organization is seen as an organized group of subjects, playing a certain role. Roles on the one side are related to activities and views while subjects are related to actions and objects on the other side. Context is introduced as a ternary relation between the properties subject, object and action. The views help structuring objects by bundling objects according to characteristics. Moreover, the actions and activities are introduced. An activity bundles a couple of actions like read and write.

Geo-RBAC - a spatially aware RBAC [Bertino et al. 2005]. With the extensive use of mobile computing devices and wireless, users frequently access resources anywhere and

anytime, through mobile terminals. GEO-RBAC, introduced in 2005, is a model that directly supports location constraints, e.g. in real mobile application scenarios. It is based on the notion of spatial role (schema) that is a geographically bound organizational function and location-based information. Spatial entities are used to model objects, user positions, and geographically bounded roles. The boundary of a role is defined as a geographic feature, such as a city, or bank – and specifies the spatial extent in which the user has to be located in order to use the role. Similar to the RBAC family, GEO-RBAC encompasses a variety of different model extensions (core-, hierarchical-, constrained-GEO-RBAC).

PARBAC - Privacy-Aware Role Based Access Control [He 2003]. The introduction of a privacy property into RBAC has been a vivid research area over the last years. PARBAC is one of the first models dealing with that issue, providing support to privacy enforcement by combining access control and privacy management. It provides system security from an organization's perspective and protects consumer privacy from a consumer´s standpoint. The family of privacy-aware RBAC extensions recently has been enlarged with the P-RBAC models introduced in 2007 by [Ni *et al.* 2007].

W-RBAC - A workflow security model [Wainer and Barthelmess 2003]. The W-RBAC model family (W0-RBAC and W1-RBAC) originally introduced by Wainer in 2003 provides an access control model for workflow management systems. It focuses on the definition of task execution rights. In W-RBAC the permission systems is defined separately from workflows. In addition, constraints are split in static and dynamic constraints, which can be overwritten (W1-RBAC). Recently, Wainer published an extension of the model dealing with delegation in workflow systems (Wainer et al. 2007). The inclusion of workflow structures into RBAC has in general gained significant attention among researchers and remained popular in the last years from 2007 on.

GTRBAC - Generalized Temporal Role Based Access Control [Joshi et al. 2005]. As TRBAC only addresses the role enabling constraints, the GTRBAC model family extends this notion and is capable of expressing a wider range of temporal constraints. Joshi et al. proposed this model capable of expressing a wide range of temporal constraints. As its name already suggests, is based on TRBAC ([Bertino *et al.* 2001]) and was further extended by Bhatti et al ([Bhatti *et al.* 2005]). Bhatti et al.'s extension X-GTRBAC allows specification of all the elements of the GTRBAC model capturing them through a context-free grammar called X-Grammar. GTRBAC enables the expression of periodic as well as duration constraints on roles, user-role assignments, and role-permission assignments. In an interval, activation of a role can further be restricted as a result of numerous activation constraints.

TrustBAC [Chakraborty and Ray 2006]. TrustBAC extends the standard RBAC model with the notion of trust. This property helps to differentiate between different security levels. Users are assigned to trust levels instead of roles based on a number of factors like user credentials, user behavior history, user recommendation etc. Trust levels are assigned to roles which are assigned to permissions as in the original RBAC model. The TrustBAC model thus incorporates the advantages of both the RBAC model and credential-based access control models. Formally a trust level is introduced as real number between -1 and +1.

Role Administration

After a role system has been deployed on basis of one of the existing theoretical role models, the administration of the system is the central duty. Operative and strategic management of roles and the role system in general are essential tasks to keep the implemented role definitions usable. Operative Role Management includes routine administration duties like user-role-assignment or role-permission-assignment according to the given administration model. In general, administration includes activities such as creating user accounts, managing roles, and assigning access rights to user accounts. Various authors investigated this area proposing several role administration publications as well as role system lifecycles. A number of well-accepted administration models that can be used in combination with several role models have developed. Their main objectives include the following principles: The decentralization of administrative competence, the autonomy of administration, and the control of irregularities.

The development of publications per year (plotted in Figure 17) reveals that role system administration has been a vivid research field from the early days of the overall research area already. Aside from the six publications in the year 1997, the amount of publications remained at a quite constant level until 2001. Afterwards, the paper count increased, eventually as a result of the high number of simultaneously published role models. Researchers responded with administration concepts for the newly introduced role model elements. Additionally, in the course of the growing interest and importance of RBAC the general increase of scientific output in this area is not surprising. As long as new role-based systems and their models are defined, open questions concerning the management of roles and their properties have to be answered. Following this argumentation the slight decrease of number of publications can be related to the simultaneous decrease in the publication of role models.

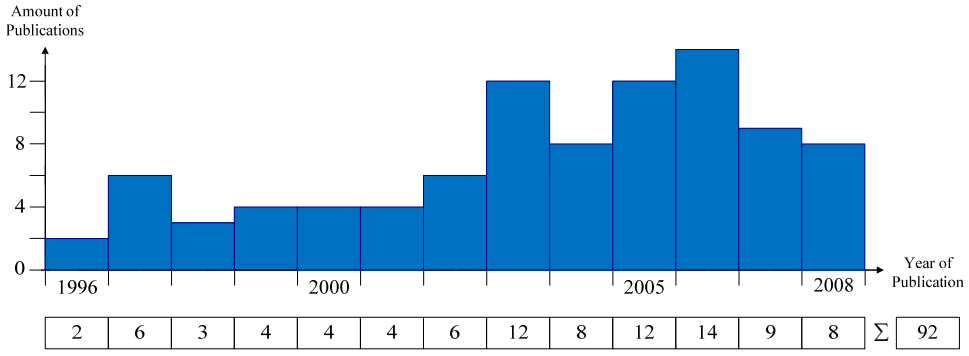


Figure 17: Plotting of *Role Administration*

In the proposed administration models administrative roles carry out the administration of user roles with the help of administrative permissions. This principle was adopted in subsequent works within this research area. Several authors have contributed to the field by analyzing specific administration issues. In the following three models that matured in the area of role administration are presented: The ARBAC family of models, the SARBAC family of models, and the Role-Graph model from Nyanchama and Osborn. All of them have been investigated in a series of scientific efforts, again underlining their acceptance and importance for the research field.

Role-Graph Models. The first administrative research efforts root in the *early RBAC* efforts presented in chapter 2.1. As mentioned in the early RBAC efforts (chapter 2.1) a

research group around Nyanchama and Osborn investigated the integration of information flow control into the administration mechanisms of role systems. Focusing on the administration of roles they formalized the organization of roles with the help of a so-called role graph in 1994. Graph theory was used to model role relations. Furthermore, properties like minroles, maxroles, privileges, authorization, and policies were newly introduced ([Nyanchama and Osborn 1996]). Other related publications concentrated on the evolution of the role-graph model. For instance, delegation issues and conflicts of interest in the model have been investigated. In general, the graph-based approach is also facilitated by several other authors in the field of administrative models. Browse the literature database[22] for *role graph* to retrieve a list of publications dealing with the mentioned issues. Alternatively, browse the class *Role Administration* in the database.

ARBAC Models. The first ARBAC[23] model was proposed in 1997 by Sandhu et al. [Sandhu *et al.* 1997]. It is based on RBAC96 and adds administrative roles and an administrative role hierarchy for RBAC administration. ARBAC97 is composed of three components: URA97 for user-role assignment, PRA97 for permission-role assignment, and RRA97[24] for role-role assignment. This components enable to authorize administrative roles based on the so-called *role range* and *prerequisite conditions* that both resulted from a given role hierarchy. URA97 uses can-assign relations for describing the authority range assigned to security officers. PRA97 has similar relations to URA97. RRA97 has more complex integrity rules for role creation/deletion and edge addition/deletion in a role hierarchy ([Sandhu and Munawer 1998]). The aim of URA97, PRA97, and RRA97 is to assign administrative authority to security officers and to prevent them from executing illegal activities. The first model extension was published in 1999 ([Sandhu and Munawer 1999]), introducing the concept of mobile and non-mobile users. In a consecutive step the ARBAC02[25] ([Oh and Sandhu 2002]) model was proposed. ARBAC02 moves the user/permission pool from role hierarchy to organizational structure. It adopts two-separated organizational structures for the user pool and the permission pool. Furthermore, the authors presented a bottom-up method for the permission-role assignment which is contrary to the top down method in ARBAC97.

Zhang and Joshi ([Zhang and Joshi 2007]) recognized the need for an adaptation of the ARBAC family for the use of hybrid hierarchies in the context of role administration. Such hierarchies are mainly needed in the procedure of the implementation of fine-grained policies. They included this functionality and proposed the so called ARBAC07 model as the latest addition to the ARBAC model family.

Crampton-Louizou Model (SARBAC). Another model focusing on the administrative requirements of an RBAC system was initially developed in [Crampton and Loizou 2002]. Following the basic idea of the ARBAC family it specifically focused on making the administration more flexible. The Crampton-Loizou model is also known as RHA[26] model or SARBAC[27] model. The SARBAC model consists of three parts: the Role Hierarchy Administration (RHA) model, the User Role Assignment (URA) model, and the Permission Role Assignment (PRA) model. It is based on the idea of *administrative*

[22] http://www-ifs.uni-regensburg.de/Roles
[23] Administrative Role-Based Access Control 1997
[24] The RRA97 model was formalized in [Mun00] subsequently.
[25] Administrative Role-Based Access Control 2002
[26] Role Hierarchy Administration
[27] Scoped Administrative Role-Based Access Control

scope. Every role has an administrative scope, which defines the set of roles that can be modified by a role. This concept can be used to constrain delegations to evolve in a natural progression in the role hierarchy. Similar to ARBAC97, SARBAC uses role hierarchies to define administrative domains. In case some operation may affect existing administrative domains, ARBAC97 restricts the operation, while SARBAC allows it, handling it by changing the existing administrative domains. The administrative model for role hierarchy in the Crampton-Loizou model has been refined and improved in [Crampton 2005]. RBAT[28] formalizes the interaction between the role hierarchy operations and the administrative scopes by having the operations preserve certain aspects of administrative scopes.

The work of Zhang and Joshi ([Zhang and Joshi 2007]) also belongs to this family of administration models. It redefined the concept of administrative scope to develop a scoped administration model for RBAC with hybrid hierarchy (SARBAC07) to administer RBAC systems that support these hybrid hierarchies.

Role Development

The initial role definition is the central challenge after having decided to implement roles in an IT infrastructure of -system. It is a complex task in particular because very often the functions, tasks, and positions of employees in an organization are not formalized and documented at all – or only to a limited extent. The importance of the definition of a valid role catalogue based on a predefined methodology was first mentioned by Edward Coyne in [Coyne 1996]. Several approaches have been published to address this problem since the upcoming of the original RBAC model in the mid-90s. The recent panel on role engineering at the SACMAT conference in 2008 furthermore underlines the importance of this field and its recognition within the research community.

Based on the used input data (input information), the general approach, and various techniques a three-step differentiation of existing RDMs can be recognized. Historically, RDMs can be classified into two approaches (Figure 18), forming the two subareas of research Role Engineering and Role Mining which can be further differentiated according to the used approach and techniques.

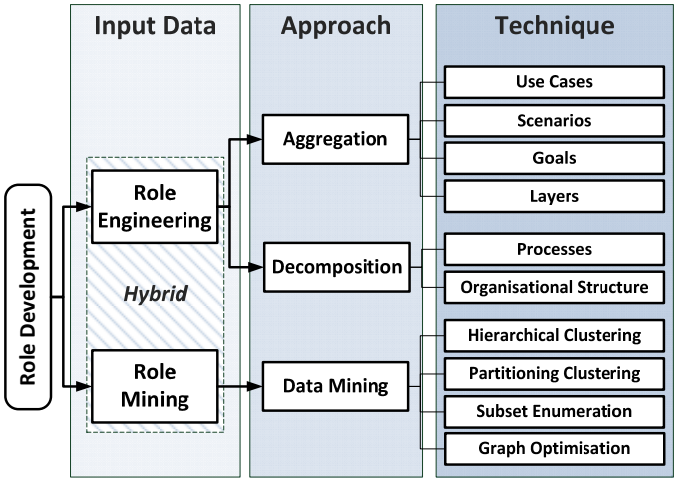


Figure 18: Classification of role development methodologies

[28] Role-Based Administration Template

Role Engineering is considered as the theoretical way of developing roles where roles are derived based on information from organizational and operational Structures within an enterprise following an aggregation (bottom-up) or decomposition (top-down) approach. This includes knowledge about hierarchical structures, process- or workflow definitions, or employees' task bundles. *Role Mining*, on the contrary, is the tool-based approach discovering roles using existing identity information and access rights from user repositories and directories by means of aggregation (bottom-up). It in general investigates users and their existing access rights and is usually based on clustering algorithms. For clustering statistical clustering, graph optimization, or neuronal networks have been proposed.

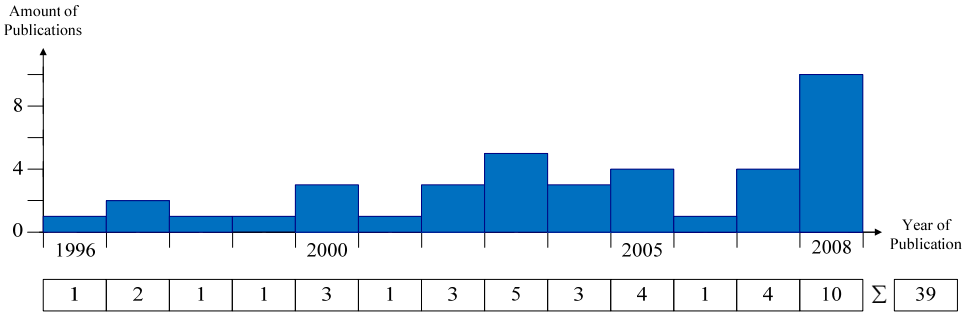


Figure 19: Plotting of *Role Development*

The plotting diagram (Figure 19) underlines the growing interest in this research area. All together, 38 papers have been assigned to the area. While the amount of publications per year remained constant between three and five for a long time, there was a significant increase in 2008 with nine publications. The quantitative analysis in Table 8 reveals a remarkable discrepancy in terms of the development of the subareas. Role Mining gained remarkable interest from 2005 on – mainly due to its automation capabilities. Currently there is an integration trend stating that only a hybrid combination of engineering and mining techniques results in a well-defined role catalogue that is usable in practical scenarios. Most authors from the Role Engineering- as well as Role Mining sector have agreed that hybrid role development offers the chance to minimize the failure risk. A justification for this assumption has been given lately bye [Fuchs *et al.* 2009].

Role Development	´96	´97	´98	´99	´00	´01	´02	´03	´04	´05	´06	´07	´08	∑
Role Engineering	1	2	1	1	3	1	3	4	3	3	-	1	1	24
Role Mining	-	-	-	-	-	-	-	1	-	1	1	3	8	14
Hybrid Role Development	-	-	-	-	-	-	-	-	-	-	-	-	1	1
∑	1	2	1	1	3	1	3	5	3	4	1	4	10	39

Table 8: Composition of *Role Development*

Role Engineering. Role Engineering as defined above is considered as the theoretical and original way of developing roles. The first theoretical publications in the field were role engineering approaches (e.g. [Thomsen *et al.* 1998]). Recently, Coyne and Davis published a textbook on role engineering, presenting some of the available role engineering approaches and their usage [Coyne and Davis 2007]. Role Engineering can follow an aggregation or decomposition approach. The latter defines roles and decomposes them into permissions needed while aggregation works the opposite way.

Both approaches offer the chance to define a role catalogue that is closely aligned to the business perspective within an enterprise. Following a decomposition approach valid positions within a hierarchical element can be split into associated task bundles and in turn single tasks. The necessary access privileges can then be assigned to those single tasks. Following an aggregation approach on the contrary, those tasks would be bundled and assigned to positions which in turn are assigned to specific hierarchical elements within an organization.

Role Engineering following the *decomposition approach* involves an in-depth analysis of business processes, functional structures and existing organizational charts in order to break down these elements to system-specific features needed to fulfill certain tasks. Representatives of this class of approaches like [Roeckle *et al.* 2000] relate the definition and usage of roles to organizational theory and distinguish between organizational and functional roles. Using existing business structures as input information they are able to define so called structural roles ([Ferraiolo *et al.* 2007]). Such system-independent roles are relating employees with access rights to applications on an abstract level depending on their specific job function. They do rather grant or deny access to an application in terms of a user account without dealing with the local access control within the target applications.

While decomposition is used mainly for defining system-independent roles, *aggregation approaches* are mostly adopted in the process of developing an application-specific role model. They are based on use case- or scenario descriptions, goals, or other input information. In general, aggregation approaches like [Thomsen *et al.* 1998] or [Neumann and Strembeck 2002] use this information to define the way of interaction with an application and the bundles of permissions needed to fulfill certain tasks within this application. In order to streamline the mainly manual aggregation process, Strembeck et al. presented a tool-based approach for the definition of scenarios ([Strembeck 2005]) and the automatic extraction of RBAC-models from BPEL4WS processes ([Mendling *et al.* 2004]).

Role Engineering significantly depends on the amount and quality of input information available. Above all in settings where the quality of organizational charts, job descriptions, or position definitions is high, Role Engineering is a promising approach to find role candidates. However, it is primarily a requirements elicitation task for identifying the best roles for a given application scenario. Due to this fact it has several shortcomings like the high complexity related to the labor-intensive engineering tasks, missing tool-support, cost and time issues, collection and preparation of input information, as well as the neglecting of existing access rights. These shortcomings lately led to a decrease in scientific publications in the area of role engineering. Researchers gained interest in the complementary role mining approaches and their potential to overcome the mentioned shortcomings. The timeline analysis (Figure 20) underlines this assumption. The development of roles was recognized as the initial task for setting up a role system very early. Thus, there were a constant number of publications proposing role engineering methodologies over the years. Although two contributions were published in 2007 and 2008, there was a decrease in publishing papers concerning role engineering in the last years (2006-2008).

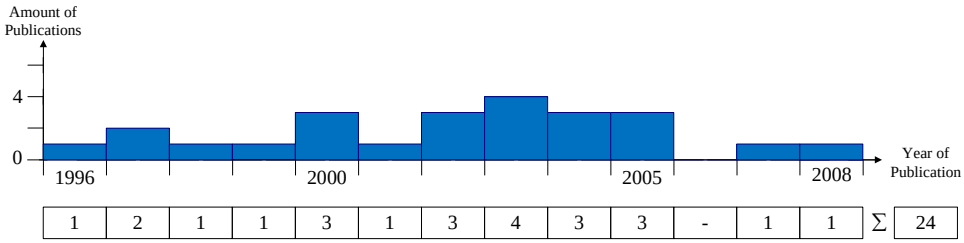


Figure 20: Plotting of *Role Engineering*

Role Mining. As a result of the presented shortcomings of Role Engineering, Role Mining has over the last years evolved as the pragmatic approach to rapidly define adequate roles. Researchers and practitioners have realized that relying solely on Role Engineering for defining company-wide roles is not feasible. This led to a rapid increase in research activities in this area between 2005 and 2009. The timeline analysis (Figure 21) underlines this statement: Research in this area did not start until 2003. After that a steady increase of scientific output can be noticed. It is remarkable, that this research direction gained in importance for developing roles in such a short period of time. This mainly stems from the various adaption possibilities from the well-shaped area of data mining. The various concepts are investigated and evaluated for possible usage to solve the role development problem in the following.

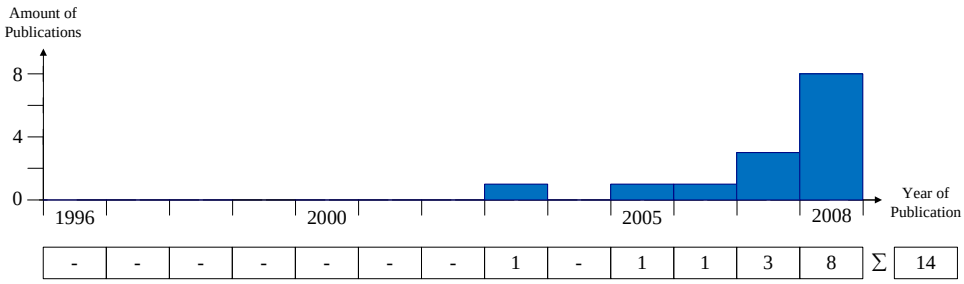


Figure 21: Plotting of *Role Mining*

Role Mining as a new paradigm specifically focuses on the usage of data mining technology for definition of system-independent roles. Existing access rights are aggregated by means of data mining technologies. The derived clusters of employees with similar privileges are refined into possible role candidate. They consecutively are used for the final role definition. Role Mining automates the development process by using tools to identify potential roles. In contrast to Role Engineering, Role Mining is based on the assumption that the actual roles already exist within the IT infrastructure. The central paradigm is that a role is nothing but a set of permissions in case no semantics are available. Hence the task of role mining is essentially that of grouping users that have same (or similar) permissions.

Different data mining techniques are used. Vaidya et al. surveyed existing Role Mining approaches that mostly present heuristic ways to find a set of role candidates ([Vaidya *et al.* 2007]).[Kuhlmann *et al.* 2003]), [Kern *et al.* 2002])), [Schlegelmilch and Steffens 2005] and [Vaidya *et al.* 2006] are identified as the most important publications in that area. Role Mining publications mostly provide an investigation of possible new algorithms for automatically extracting practical sets of roles for existing heterogeneous enterprises.

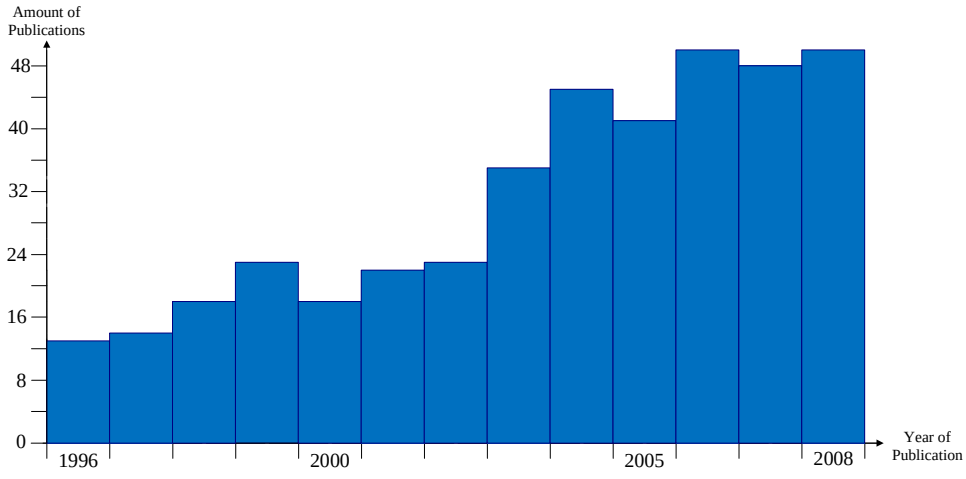
Traditionally, the first heuristics for Role Mining have used clustering techniques (statistical clustering carried out hierarchical or partitioning). In terms of Role Mining groups of permissions are commonly placed into clusters based on user similarity. Following this approach, permissions can only belong to one role candidate. Representatives of this class of approaches are [Kuhlmann *et al.* 2003] and [Schlegelmilch and Steffens 2005]. Kuhlmann et al. propose a clustering technique closely related to the k-means algorithm. Schlegelmilch et al. facilitate an agglomerative hierarchical clustering based algorithm, which discovers roles by merging permissions appropriately. However, unlike the traditional applications of data mining that ideally require identification of non-overlapping clusters, roles are likely to have overlapping permission needs. Vaidya et al. [Vaidya *et al.* 2006] address this issue and propose FastMiner and CompleteMiner, two Role Mining algorithms based on subset enumeration.

In 2008 several publications have presented specific improvements, integrating cost and performance decisions as well as semantics into Role Mining (e.g. [Colantonio et al. 2008] or [Molloy et al. 2008]). Even though providing a high degree of automation, Role Mining has several serious unaddressed drawbacks like error propagation of incorrect input data, performance issues, and low abstraction level.

As a result of those shortcomings, most researchers in that area have already agreed upon the fact that business-related semantics need to be integrated by the hybrid use of Role Engineering techniques to complement Role Mining. Recently the first hybrid role development methodology was published in [Fuchs and Pernul 2008]. As this publication to the best of our knowledge represents the first publication in the subarea of hybrid role development, a separate research area has been newly defined. A number of new follow-up methodologies are expected in that area. Future development is going to prove if hybrid role development establishes itself as separate area.

7. PUBLICATIONS WITH PRACTICAL FOCUS

After research with theoretical focus has been investigated in the previous chapter, the aim of the following chapter is to explore the identified research areas exhibiting a practical affiliation. The overall development of research with practical characteristics along a time line is shown in Figure 22. The tableau reveals that scientists tried to use role-based security for practical needs from the very first days since the development of the field. In the first four years, the amount of publications rose steadily up to 23 in 1999. After a stable period a steep increase of scientific output after the year 2002 can be noticed. This growth can be related to the growth of the overall research area. As more theoretical concepts were provided new possibilities for practical adaption were given. However, even though the research output in main theoretical areas like *Role Models and Design* or *Role Administration* decreased slightly over the last years, the number of publications with a more applied practical focus is constantly growing. This development might be explained with the increasing spreading and adaption of RBAC in organizational context.



13	14	18	23	18	22	23	35	45	41	50	48	50	Σ	400
3,3	*3,5*	*4,5*	*5,8*	*4,5*	*5,5*	*5,8*	*8,8*	*11,3*	*10,3*	*12,5*	*12*	*12,5*	%	*100*

Figure 22: Plotting of *Publications with Practical Focus*

7.1. Composition of the area

As already mentioned in chapter 5, publications with practical affiliation can be differentiated according to their either technology-specific- (*Roles in Technology*) or industry-specific focus (*Roles in Industry*). Technology-specific adaption of theoretical findings on role theory is mainly industry-independent. Nevertheless it usually also provides a share of insight into a practical application scenario in a certain environment. On the other hand each industry-specific publication is to a certain extent related to the usage of a technology. This mutual relationship complicated the assignment process. Still, the comparison with various alternative classification approaches showed that the distinction between Roles in Technology and Roles in Industry is suitable.

The composition of the research area is presented in Table 9. It reveals that in the first years researchers were only publishing in the area *Roles in Technology*. Industry-specific research did not start until 1998. Analyzing the amount of publications, a discrepancy between both sub-areas can be identified. 347 of 400 papers inside this research area were published with the primary focus on combining the RBAC concept and different information technologies. In contrast, only few papers were published dealing with the adaption of RBAC for a special industrial sector. This might change in the future when a larger number of best practices or industrial reports are provided. Nevertheless, the main obstacle for this development is the resistance of organizations to provide detailed insight into their IT projects and possible challenges or failures.

Practical Focus	´96	´97	´98	´99	´00	´01	´02	´03	´04	´05	´06	´07	´08	∑
Technology	13	14	14	20	14	16	17	28	41	35	46	44	45	347
Industry	-	-	4	3	4	6	6	7	4	6	4	4	5	53
∑	13	14	18	23	18	22	23	35	45	41	50	48	50	400
%	*3,3*	*3,5*	*4,5*	*5,8*	*4,5*	*5,5*	*5,8*	*8,8*	*11,3*	*10,3*	*12,5*	*12*	*12,5*	*100*

Table 9: Composition of *Publications with Practical Focus*

7.2. Role-based Security in Technology

In the following both practical research directions are investigated in detail. At first the technology-specific research tendencies are presented. Consecutively the existing industry-specific contributions are analyzed. Due to space limitations only references of main publications are given in the reference section of this article. The publications can be found in the provided electronic database[29].

Roles have been used as underlying paradigm in software of different kind since the 1970s at least. The usage of roles in computer systems started within the area of groups in UNIX and other operating systems and privilege groupings in database management systems. It has spread over different kinds of information technologies.

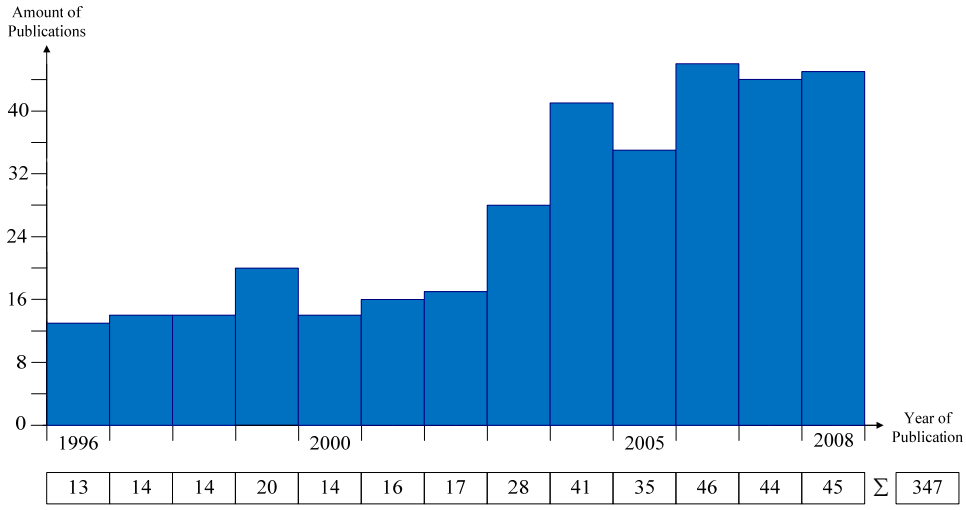


Figure 23: Plotting of *Roles in Technology*

Two phases of development in this research area can be identified based upon the quantitative analysis given in Figure 23. An average of about 15 publications per year can be noticed between 1996 and 2002. After 2002 a significant increase of scientific output took place. More than 40 published contributions yearly underline the ongoing diffusion of role theory in practical scenarios. Based on the RBAC standardization process, this development shows that the usage of the role concept bears potential for improving other security technologies in the field of networks, middleware, or system modeling – to mention only selected. Above all the rapid development of online technologies and inter- as well as intra-organizational networks might be the main reason for this development. This is another evidence for the spreading of RBAC beyond its primary research origins like databases and operating systems.

[29] http://www-ifs.uni-regensburg.de/Roles

Roles in Technology	´96	´97	´98	´99	´00	´01	´02	´03	´04	´05	´06	´07	´08	∑
Operating System	1	3	2	1	-	-	-	-	-	1	1	2	1	12
Database	3	2	3	2	-	2	1	2	1	2	1	2	3	24
Web	-	4	2	3	3	4	5	4	4	8	5	7	5	54
Network	-	1	1	1	1	2	2	5	9	9	12	10	13	66
Workflow	-	1	-	2	2	1	1	2	8	3	2	4	3	29
Collaborative Environment	2	1	1	3	-	2	2	5	8	4	5	6	5	44
Middleware Arch. for ESM	3	1	1	5	5	2	2	7	5	2	8	9	8	58
System Modeling and Programming	4	1	4	3	3	3	4	3	6	6	12	4	7	60
∑	13	14	14	20	14	16	17	28	41	35	46	44	45	347

Table 10: Composition of *Roles in Technology*

The composition in Table 10 shows the diversity of research in the area and again underlines the previous argumentation. Eight different sub-areas can be identified. On the one hand traditional and small fields like *Operating Systems* (12) or *Databases* (24) are settled and well-established. On the other hand a rapid increase in scientific output in larger areas like *Network* (66), *Web* (54), or *Middleware Architectures for Enterprise Security Management* (58) can be noticed. Taking the close relationship between *Web* and *Network* into consideration, even more points out the importance of role theory for the communication area. Additional research areas like *Workflow* (29), *Collaborative Environments* (44) and *System Modeling and Programming* (69) complete the technology-specific research activities. Compared to theoretical research which is dominated by formal *Role Model and Design*, there is no significant difference between the sub-areas in terms of quantitative research output. Hence all areas are shortly investigated in the following.

Again, similar to the previous analysis of theoretical research areas not all publications with practical affiliation can be included in the reference list of this survey. The reader is required to browse the electronic literature database for the respective publications. The easiest way to gather a list of referenced publications is the selection of the research area in question. The classification information, i.e. the structuring in research areas, is included in the database. On basis of this information the detection of a single publication can be achieved. In case one author has published more than one work with the same co-authors the publications are referenced and appear in the reference section of this survey.

Roles in Operating Systems

Adapting role theory in operating systems is a traditional research area. Operating systems manage resources such as memory, input and output devices and control the execution of programs. They are thus responsible for the management and coordination of activities and for the sharing of resources. The first authors dealing with roles in operating system explicitly are Epstein and Sandhu in 1996 [Epstein and Sandhu 1996]. They present NetWare 4 as an example of access control based on roles. Inside the NetWare 4 operating system developed by Novell, Netware Directory Services (NDS) objects are used to represent abstractions such as users, roles, groups, and computers.

Several publications deal with roles in UNIX and UNIX-like computer system. An extension of the Linux ext2 file system with sub domains is e.g. presented in 1997

[Friberg and Held 1997]. In the same year the commercial DG/UX B2[30] operating system is mapped into a simple RBAC emulation [Meyers 1997]. Modeling of permissions granted in a UNIX system as a role graph was carried out in [Hua and Osborn 1998]. In 1998, Sandhu and Ahn dealt with the UNIX group mechanism and proposed two extensions: Hierarchical groups were added to automatically assign the user to all junior groups when the user is assigned to a senior group [Sandhu and Ahn 1998]. Furthermore, the URA97 administration model is used for decentralized user-group assignment.

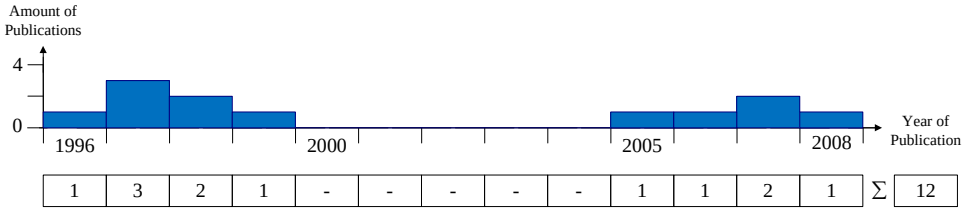


Figure 24: Plotting of *Roles in Operating Systems*

Figure 24 gives information about the number of publications along the time line. Most of the publications belonging to this area were published in the early years of the period under review. Additional five articles were published later, namely between 2005 and 2007, However, due to the fact that operating systems are dealing with access control fundamentally it seemed natural to integrate the concept of roles in the early days of RBAC (including pre-RBAC and early RBAC phases).

Roles in Databases

The second traditional research field that adapted role theory was the protection of databases from unauthorized access requests. The essential task of a database system is to store large amounts of data efficiently, consistently and permanently. As shown earlier, the roots of RBAC prior to 1992 include privilege groupings in database management systems. In 1995, e.g., Essmayr et al. already studied RBAC in the context of federated database systems [Eßmayr et al. 1995]. In 1996, Notargiacomo showed RBAC capabilities of Oracle's basic DBMS in its product version 7.0. The implementation of, e.g., including fine-grained privileges, role definition and management, as well as the ability to control access to both database objects and executable application programs was described [Notargiacomo 1996]. Analyzing and comparing RBAC features in three commercial database management systems was the aim of Chandramouli and Sandhu in 1998 [Chandramouli and Sandhu 1998]. They categorized RBAC features under three areas, including user role assignment, support for role relationships and constraints, and assignable privileges. In 1998, Sandhu and Bhamidipati described the implementation of the PRA97 model in an Oracle environment assigning permission to roles and revoking permissions from roles [Sandhu and Bhamidipati 1998]. One year earlier in 1997 they exclusively focused on user-role assignment [Sandhu and Bhamidipati 1999].

In 2001, [Osborn 2001] provided an algorithm for integrating two database systems whose access control behavior is represented by role graphs. The algorithm helps to merge two role graphs into one. Bertino et al. developed a solution for the detection of intruders in RBAC database systems in their publication [Bertino et al. 2005] in 2005. They addressed the problem of building and maintaining role profiles that represent accurate and consistent user behavior, and how to use these profiles for intrusion detection.

[30] Data General UNIX

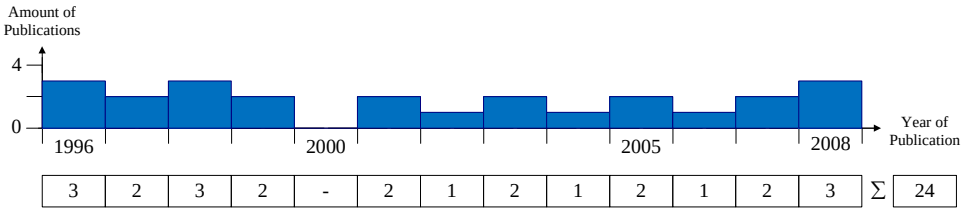


Figure 25: Plotting of *Roles in Databases*

Similar to the Operating Systems research area, databases and database management systems can be recognized as one of the roots of role-based security management. The amount of scientific publications per year (Figure 25) remained relatively constant on a low level with the exception of the year 2000 (0 publications). Note that due to the importance of databases the usage of roles in these environments plays a part in many identified papers of this investigation that are allocated to other research areas. This area only consists of publications exclusively dealing with roles in databases.

Roles in Networks

A network environment in general is a collection of computers connected to each other. Note that this area includes publications dealing with network environments classified as system-level environments. The Open Systems Interconnection Reference Model[31] served as theoretical basis for the decision of classifying publications. In its most basic form, it divides network architecture into seven layers which, from top to bottom, are the Application, Presentation, Session, Transport, Network, Data-Link, and Physical Layers. The lower four layers of this model are more transport-oriented, whereas the higher layers are more application-oriented. In the area of *Roles in Networks*, publications that deal with transport-oriented requirements of computer networks are included. This is the reason why *Roles in the Web* is defined as a separate research area. Also note that modeling roles in areas like sensor technology and networks are excluded from the investigation, following the rational introduced in the motivation for this work.

A first work in this area is [Gustafsson et al. 1997]. The author used the file-sharing technology NFS to introduce the RBAC paradigm in existing computer systems. NFS[32] is a network file system protocol that provides transparent remote access to shared file systems across networks. According to the assignments made in the role database, the user can activate and deactivate roles. Similarly, Ashley et al. developed a security mechanism for NFS using the SESAME security architecture based on the RBAC paradigm [Ashley and Vandenwauver 1999]. In [Bohra et al. 2007] the authors propose FRAC, a framework that enforces RBAC through message transformation. The assignment of users is mapped to roles in a user session. Subjects are mapped to static and dynamic separation of duty constraints.

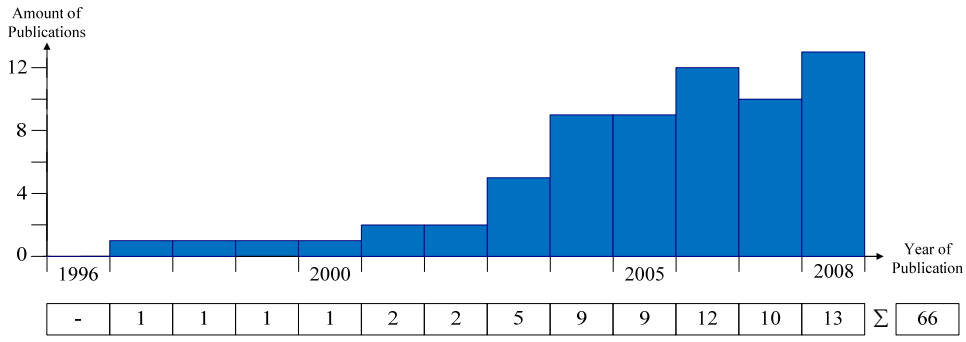
Besides NFS, wireless networking environments are a core part of this research area. In 2003, Park et al. presented contributions for wireless privilege management infrastructures in order to support authorization service for authorized users in wireless environments (e.g. [Park and Lee 2003]). One year later, [Chae et al. 2004] also proposed a realization for combining the RBAC concept for wireless networking. They represent access control by bit patterns which are obtained via neural networks. The system consisted of two Internet services in a wireless terminal such as mobile phone and PDA[33]

[31] http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/osi_prot.htm
[32] Network File System
[33] Personal Digital Assistant

that performs stock trading and remote banking service. [Tomur and Erten 2006] presented an architecture for controlling access to 802.11 wireless networks that can be seen as a realization of temporal and spatial RBAC in 2006. The authors made use of roles, location and time information, using the tested wired network components such as VPN[34]s and Firewalls.

The next research tendency in this field is roles and their usage in peer to peer networks. A Peer to Peer (or P2P) computer network uses mashed connectivity between participants in a network and the cumulative bandwidth of network participants rather than conventional centralized resources. In their 2003 SACMAT contribution Park et al. enforce RBAC for enterprise projects in P2P computing environments. Considering the job functionalities of peers as roles, the authors used those roles for access control decisions [Park and Hwang 2003]. Another approach for implementing RBAC security paradigm in a P2P system is provided by Mathur et al in 2006 [Mathur et al. 2006].

Lately, researchers also dealt with integrating roles in grid computing. Grid computing or the use of a computational grid is the application of several computers to a single problem at the same time. With the recent development of grid computing systems, secure resource-sharing has become more and more important. In 2004 Adabala et al. pioneered combining roles and grid computing. In their publication, the authors presented an approach for Single Sign-On in a deployed functioning grid called In-VIGO [Adabala et al. 2004]. The grid system maps the credentials of a principal to a role, and accesses entities on behalf of the role. Another example for integrating roles in grid computing environment is provided by Chen et al. in [Chen et al. 2005]. Their system modified the user's role and related privileges dynamically by his behavior inside the grid computing environment.



-	1	1	1	1	2	2	5	9	9	12	10	13	Σ	66

Figure 26: Plotting of *Roles in Networks*

The content-specific analysis has shown that a large number of researchers worked on the area of role theory adaption in networks. The development of the research area is shown in Figure 26. It is significant that the amount of publications remained on a low and constant level between 1997 and 2002. In the following, however, scientific output rapidly increased and stabilized on this new level of about 10-13 publications per year. This development is not surprising, taking the growing importance of computer networks for society and organizations into consideration. Access control based on users' roles significantly gained importance in (networked) organizations since 2003. After the theoretical basis had been proposed, researchers began adapting those contributions in practical settings. The spreading of modern network technologies like grid computing and wireless network environments even more pushed scientific output in this research area.

[34] Virtual Private Network

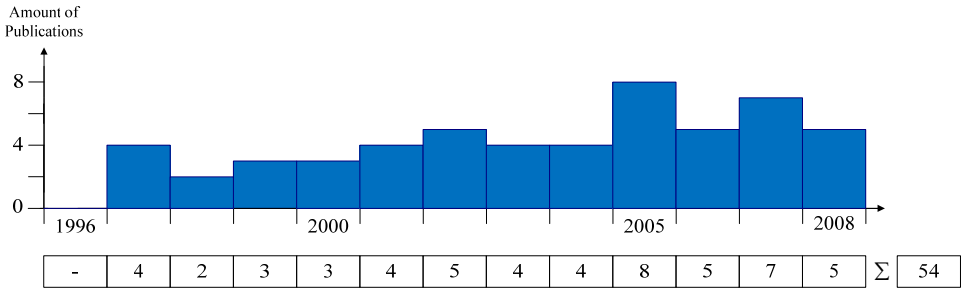
Roles in the Web

Today the World-Wide-Web (WWW) has become a crucial enabling technology for electronic commerce and business on the Internet. The research community consecutively deals with the large number of web security problems. The role concept is a widely used solution to cope with many of those issues. The research area ”Roles and web technologies” comprises of contributions that investigate the use of roles for the purpose of securing web technologies such as web servers, web services, and web applications.

The work of Barkley et al. [Barkley *et al.* 1997] is the first one explicitly dealing with realizing roles in web environment for the purpose of access control. RBAC/Web is proposed as an implementation of RBAC for usage by web servers. The primary purpose of RBAC/Web is to provide a flexible and effective access control for intranet computing environments without any necessary modification to server code.

Publications dealing with Intranets also belong to this research area. An intranet is a private computer network that uses Internet technologies to securely share any part of an organization’s information or operational systems with its employees. Sometimes the term refers only to the organization’s internal website. But often it is a more extensive part of the organization’s computer infrastructure and private websites are an important component and focal point of internal communication and collaboration. In 1997, [Ferraiolo and Barkley 1997] as well as [Tari and Chan 1997] described how to use role theory for securing web-based intranets. The latter propose I-RBAC, a RBAC framework protecting an intranet from intruders. In [Sandhu and Park 1998] the authors investigated the URA97 model for user-role assignment to decentralize the details of RBAC administration on the web without losing central control over the system policy. In contrast, [Giuri 1999] focused on the Java platform and its extension for the support of Web-based server-side applications, i.e. Java Servlets in the same year.

Additionally, a number of authors dealt with the integration of role concepts in web services. With the advent of massively distributed computing systems requiring secure interoperability and the demand for sharing online information content across Internet applications, the security of web services is becoming an increasingly important task.



-	4	2	3	3	4	5	4	4	8	5	7	5	Σ	54

Figure 27: Plotting of *Roles in the Web*

Figure 27 provides an overview over the amount of published papers according to the year of publication. It can be seen from the figures that the amount of publications remained constant between the years 1997 and 2008. Due to the increasing use of the Internet and in the light of web technologies gaining in importance, the figures are not surprising. Note that there is a close content-specific relationship with the area *Roles in Networks*. Investigating the focus of the publications shows that the area is currently dominated by the combination of modern web service technologies with the role concept.

Roles in Workflows

Workflow management systems are computerized systems which support, coordinate and streamline the business processes in various application domains in different industries. Examples of business workflow processes in a manufacturing organization include production scheduling, order processing, or preparing goods. Similar to other research areas, role theory is facilitated for security administration in workflow management systems.

Apart from the aforementioned W-RBAC role model, a number of different articles dealing roles in workflow management security were published. Bertino et al. [Bertino *et al.* 1997], for instance, presented an approach for defining constraints on role assignment and on user assignment to tasks in a workflow. Furthermore, the authors proposed algorithms to assign roles and users to the workflow tasks and to check the consistency of defined constraints. This work was refined and extended in [Bertino et al. 1999]. In 1999, Huang and Atluri presented SecureFlow, a web-enabled workflow management system. The architecture of SecureFlow consists of four major components, namely the workflow design/specification module, workflow execution server, workflow authorization server, and workflow client [Huang and Atluri 1999].

[Kandala and Sandhu 2002] focused on introducing a series of reference models for secure role-based workflow systems in 2002. Sun et al. presented a flexible workflow architecture based on the role concept in order to support dynamic customization and modification of workflow both at design and execution stage. [Sun et al. 2005]. Furthermore, they presented the design and implementation of PRES, a practical system for Property Right Exchange [Sun and Pan 2005].

With BPEL[35] becoming the standard for specifying and executing workflow specifications for web service composition, Xiangpeng et al. in 2006 used the concept of role-based access control for securing workflow requirements [Xiangpeng et al. 2006]. Recently, Wainer et al. showed how delegation can be introduced in a workflow system. They mapped ideas concerning delegation in role-based access control into the workflow domain [Wainer et al. 2007].

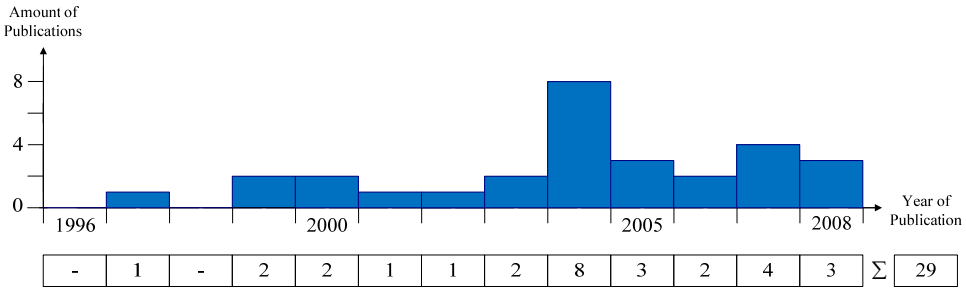


Figure 28: Plotting of Roles in Workflow

The timeline plotting in Figure 28 reveals that research in this area did start in 1997. However, it was not until around the year 2000 when scientists' interest got bigger. In 2004, there was a significant increase of scientific output. In general, there has been a constant output on a low level over the years. Nevertheless, the research area is rather small compared to the two areas presented beforehand (*Roles in the Web*, *Roles in Networks*).

[35] Business Process Execution Language

Roles in Collaborative Environments

Publications are allocated to this research area, if they focus on technologies supporting groups, communities, societies, and especially organizations in their collaborative tasks. This above all includes publications in the field of Computer Supported Cooperative Work[36]. Moreover, articles dealing with document sharing, group communication systems, or some other kind of collaborative characteristics are also allocated to this research area. Note that some authors define workflow environments as an element of CSCW-Systems. However, due to the number of publications explicitly focusing on each of those two areas, they have been kept separate for this survey.

In 1996, Edwards presented a language for role specification in [Edwards 1996]. This language can be used by application developers and system administrators to configure policies and roles for their users in collaborative environments. Lee et al. proposed, AID[37] tag in 2001 [Lee *et al.* 2001], a mechanism simplifying differentiating and merging different versions of various documents. Having analyzed the security needs and access control requirements in group communications systems, Li and Nita-Rotaru define services that allow for coordination and efficient dissemination of messages to multiple parties [Li and Nita-Rotaru 2003]. Recently, Ahmed and Tripathi focused on the goal of creating a programming framework for developing secure distributed CSCW systems. The framework is used for specifying policies concerning role-based user participation, coordination, and security in collaborative environments [Ahmed and Tripathi 2007].

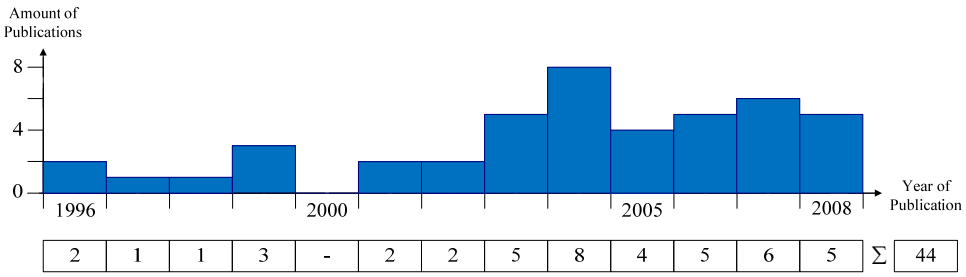


Figure 29: Plotting of *Roles in Collaborative Environments*

The development of the area *Roles in Collaborative Environments* is plotted in Figure 29. The diagram reveals a constant interest of researchers over the years. After the year 2002 an increase of the number of publications can be seen. Similar to the area *Roles in Workflows*, the peak of interest can be identified around 2004. The close relationship between those research areas leads to the interpretation that around this time an increased scientific interest existed.

Roles in Middleware Architectures

Middleware (-Architectures) describe the process of mediating between applications in order to connect software components. Unlike network services, middleware handles the low-level communication between computers. Applications and services in middleware environments are not static but are joined dynamically. Hence, dependency of applications and authentication of users to data objects are significant. In this context the role concept is integrated in order to secure middleware software and middleware architectures.

[36] CSCW-Systems
[37] Activity IDentification

The first presented publications are dealing with roles in the field of the security service of CORBA[38]. The CORBA environment, including the CORBA Security Service was developed by OMG[39] in order to provide a general-purpose infrastructure for developing and deploying distributed object systems. Beznosov and Deng [Beznosov and Deng 1999] presented an approach for implementing the role concept into the access control mechanism provided by the CORBAC Security Service. In [Obelheiro and Fraga 2002] a similar approach, presenting RBAC-JACOWEB, a CORBAC security model integrated with Java and Web security models, is proposed.

In the field of enterprise security management, identity management is particularly dealing with the management and administration of user data. The bigger a company the more identities, privileges, and according access control information have to be managed. Identity management infrastructures composed of software components that manage enterprise identities and their permissions. [Fuchs and Preis 2008] analyzed different role properties and use the notion of business roles that serve as intermediate elements between job-oriented business tasks and resource-oriented IT requirements. In a related publication proROLE, a process-oriented lifecycle model for role systems was proposed [Fuchs and Pernul 2008].

Another platform belonging to this research area is Java EE[40] a software architecture for the transaction-based execution of applications programmed in Java. In 2004 [Naumovich and Centonze 2004] focused on EJBs inside the J2EE middleware framework. Points-to graph formalisms and a semi-lattice are used in order to present a static technique for analyzing J2EE access control policies with respect to security-sensitive fields of EJBs. [Bindiganavale and Ouyang 2006], on the contrary, focused on the presentation of access control mechanism that could be integrated into a typical enterprise J2EE application in 2006. Another approach for combining roles and Java EE is provided in [Sun et al. 2008] where the authors presented a role-based proposal for automatic generation of J2EE access control configurations.

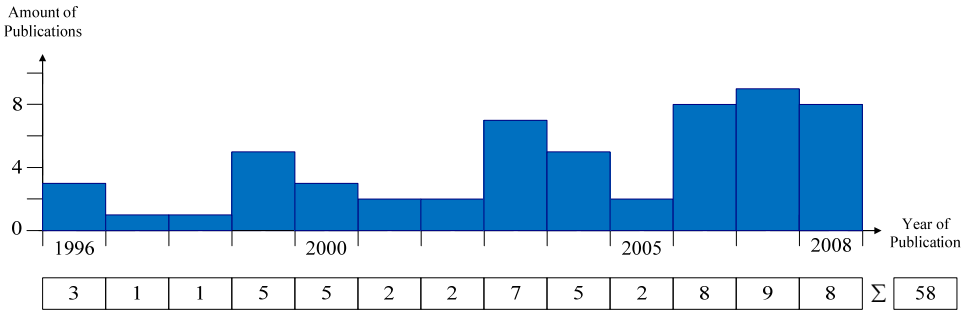


Figure 30: Plotting of *Roles in Middleware Architectures for ESM*

The amount of publications dealing with Roles in Middleware (Architectures) for Enterprise Security Management is illustrated in Figure 30. Several peak phases can be identified (e.g. 1999, 2003, or 2007). Over the last years researchers' interest in this area seems to remain stable at a high level. The tendency for implementing organization-wide user management infrastructures requires the development and enforcement of role-based security policies. Due to the current importance of identity management within organizations this trend is expected to continue.

[38] Common Object Request Broker Architecture, a consortium formed by more than 800 companies

[39] Object Management Group

[40] Java Platform, Enterprise Edition (former known as J2EE)

Roles in System Modeling and Programming

Publications allocated to this research area deal with the engineering of software as well as the development and operation of it. The term software engineering includes fields like planning, analyzing, designing, programming, testing and maintaining software using engineering methods. Additionally, this area focuses on the organization and modeling of systems and associated data structures and quality- and documentation management.

The de facto modeling languages for designing software and software systems is the UML[41] developed and standardized by the OMG[42]. In the year 2000, Shin and Ahn [Shin and Ahn 2000] provided an UML representation of RBAC to meet specific security needs of system development requirements. To achieve their goal, the authors used class diagrams to formulate a conceptual static view, use case diagrams to express a functional view, and a dynamic view of RBAC expressed by object collaboration diagrams. [Ray et al. 2004] can be seen as another approach combining UML and RBAC. The authors incorporated RBAC concepts, above all constraints expressed in OCL[43], into a software design model, presenting a generic RBAC model that is expressed as a class diagram template. Roles are associated with class templates, the relations according to user assignments are modeled with association templates and operation templates are used to grant permissions.

In 2005, [Pavlich-Mariscal et al. 2005] focused on formalizing the concept of role slices assisting in designing and developing software systems. [Basin et al. 2006] presented Model Driven Security, an approach for integrating security into the development process. This approach extends MDA[44] which supports system development by employing a model-centric and generative development process. With the help of Model Driven Security, software engineers are able to meet security requirements when deducing access control infrastructures from UML models.

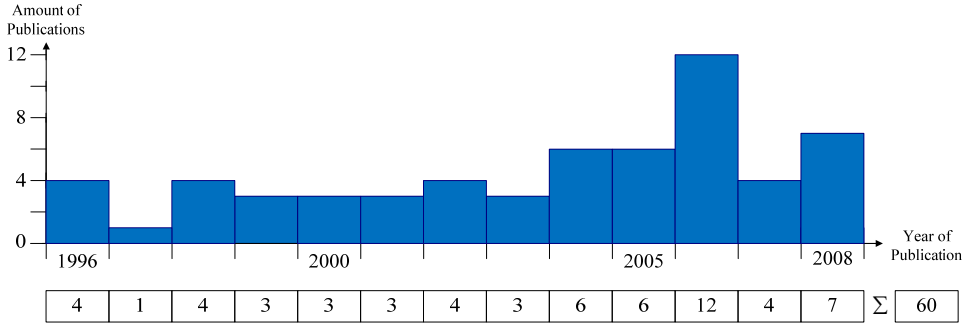


Figure 31: Plotting of *Roles in System Modeling and Programming*

The development of the area *Roles in System Modeling and Programming* is illustrated in Figure 31. Similar to the overall tendency within the practical research areas, a constant growth of scientific output can be identified. Above all around the year 2005 a large number of publications have been presented. It is surprising that in 2007 the output decreased sharply, also because it was followed by another six publications in 2008. This development exhibits a quite fluctuate behavior. However, it must be noted that the general technologies concerning system modeling and programming gain in importance due to the growing complexity of information system infrastructures and its implementation.

[41] Unified Modeling Language
[42] Object Management Group
[43] Object Constraint Language
[44] Model Driven Architecture

7.3 Role-based Security in different industrial sectors

The usage of roles for the purpose of securing information is not only adopted in various technologies, but also inside certain industries. In contrast to the previous chapter, which focused on its use in different types of software, this research area consists of publications which mainly present the adoption process in different application sectors. The findings provide insight into the usage of theoretical findings in a specific real-life environment, e.g. a large bank ([Schaad *et al.* 2001]), in form of case studies or reports.

It has already been shown earlier, that the scientific output (42 publications) in this area is small compared to the publications dealing with the usage of roles in technology (261). Even though the role concept has reached some industries the low aggregate amount of publications is surprising. Figure 32 presents the historic development of the area. It becomes obvious that research did not start until 1998. Afterwards, the publication count remained at a constant, but low level. One reason might be the refusal of organizations to publish best practices that provide detailed insights into their infrastructure or user administration techniques. Note, however, that the market of role-based security management and enterprise security management provides a large number of white papers, best practices, or analyst reports that are not included in this survey as they have not been published in academic Journals or conference proceedings covered in this survey. Other publications have not undergone a thorough review process and might thus be biased (in case of vendors selling their security management products).

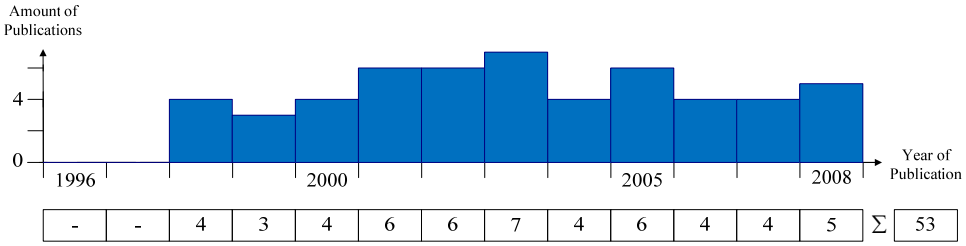


Figure 32: Plotting of *Roles in Industry*

The composition of the research area is shown in Table 11. The available scientific publications show that above all regulated industries are using the role concept to a great extent. The major amount of papers concerning this research area was published in the health care sector (26). E-Commerce and Education rank second with nine publications each. The amount of the sub-areas Finance and other industries is low with 4 and 5 publications respectively. As a result of its importance only the Health Care sector is investigated in detail in the following.

Roles in Industry	´96	´97	´98	´99	´00	´01	´02	´03	´04	´05	´06	´07	´08	∑
Health Care	-	-	1	-	-	2	2	5	3	2	3	4	4	26
E-Commerce	-	-	2	1	2	1	1	1	-	1	-	-	-	9
Finance	-	-	-	-	2	1	1	-	-	-	-	-	-	4
Education	-	-	-	2	-	2	2	1	-	2	-	-	-	9
other Industries	-	-	1	-	-	-	-	-	1	1	1	-	1	5
∑	-	-	4	3	4	6	6	7	4	6	4	4	5	53

Table 11: Composition of *Roles in Industry*

Roles in Health Care environment

Health Care and Health Care systems have proven to be one of the main adaption areas of the role concept. Due to the high security requirements like Separation of Duty enforcement, information technology plays a decisive role not only to increase the efficiency of health care institutions, but also to ensure secure information processing (e.g. in terms of data protection). Research is thus focusing on the realization of complex, sometimes cooperating structures across federated systems of different types of health care providers.

According to [Beznosov 1998], system developers and administrators of heath care facilities need are heavily concerned with access control requirements to secure medical information. Federal regulations, local disclosing requirements of patient information, and different business models in the health care industry are amongst others provided as main reasons for this assumption. The authors identify the role-based decoupling of the application-layer and the authorization-layer as well as a centralized management of access control administration is the most important rules for developing such systems. The primary purpose of [Wilikens et al. 2002] was to describe an extract of the DRIVE[45] project which developed an access control concept for health care business processes based on roles. Furthermore, they presented a trust infrastructure with RBAC functionality applied in the project. According to [Longstaff et al. 2003] an *identity* is a user of an information system that is performing activities. They presented TCM[46] for combining the Identity Based Access Control (IBAC) and the concept of roles for usage with electronic health- and electronic patient records.

In 2004 Coyne et al. provided the report "Role Engineering in Healthcare: Process, Results, and Lessons Learned" [Coyne et al. 2004]. The authors depict the goals, the approach, the results, and the lessons learned from role engineering tasks carried out in connection with the Department of Veterans Affairs Veterans Health Administration. Based largely upon earlier work by Neumann and Strembeck, the scenario-driven role engineering process [Neumann and Strembeck 2002] was formally reviewed and modifications were made.

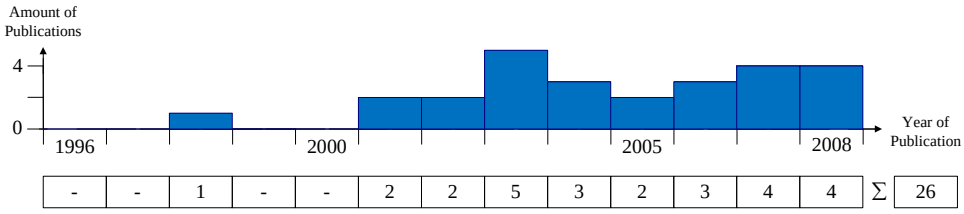


Figure 33: Plotting of *Roles in Health Care*

Figure 33 provides information about the development of publications in area *Roles in Health Care*. It can be detected that only one paper has been identified from 1996 to 2000. Consecutively, mainly driven by regulations of the health care sector (e.g. HIPAA[47]), the amount of publications increased after the year 2000 to a constant level of about 3 publications per year.

[45] Drug in Virtual Enterprise
[46] Tees Confidentiality Model
[47] Health Insurance Portability and Accountability Act

8. OUTLOOK AND FUTURE PREDICTIONS

In this chapter we give the authors' personal perspective on the principal insights of this study and speculate on the future of RBAC and cyber security research. Figure 4 gives a compelling visualization of the development of RBAC research. There are two clear points, in 1996 and 2002, when activity stepped up considerably. As discussed earlier the 1996 spurt is attributable to publication of the RBAC96 model family ([Sandhu *et al.* 1996]) and the founding of the ACM Workshop on Role-Based Access Control series. A second spurt follows publication of a proposed standard model in 2001 ([Ferraiolo *et al.* 2001]). Finally there is a third spurt subsequent to adoption of the proposal in 2004 ([ANSI/INCITS 2004]). Our attribution of the spurts to these specific papers is reinforced by the high citation count these have achieved as well as to the nature of the research that emerged in these spurts. This is an indication that development of models and standards that receive endorsement from the research community can be critical in advancing new research areas within cyber security.

Turning to Table 2 we see that the ACM Workshop on Role-Based Access Control (RBAC) series and its successor the ACM Symposium on Access Control Models and Technologies (SACMAT) series together account for over 16% of the research publications on RBAC. This suggests that creation of a high-quality forum for research publications can also be critical in developing a critical mass of researchers to make up a productive community. Pre-existing established application-focused conferences such as DBSec and ACSAC also include a significant number of RBAC publications. The ACM TISSEC journal was inaugurated in 1998 and has published several RBAC papers many of which grew out of the RBAC and SACMAT conferences. The established ACM and IEEE security conferences, respectively CCS and S&P, have relatively few RBAC publications perhaps reflecting their more theoretical emphasis. It is our conjecture that the CCS and S&P papers have likely been less influential than those published in RBAC, SACMAT and TISSEC.

As we look to the future our expectation is that new areas of cyber security will emerge in response to rapid changes in computing applications, e.g., social networks, and computing infrastructure, e.g., cloud computing. Based on our experience with RBAC we suggest that as these new areas reach a critical mass of interest a few seminal papers along with establishment of high-quality specialized conferences with feeders into high-quality journals could be a recipe that is repeatable. We are not suggesting that this is the only way to approach fostering of a new research area but it is one that has been successful with RBAC and could be inspirational to other security communities in development. Of course, the response from industry in adopting RBAC has also been instrumental and is perhaps the most essential ingredient for success in cyber security.

A major result of this paper is the three level classification of RBAC literature shown in Figure 7. This was developed using the methodology reported in this paper and the classification itself has been earlier discussed at length. Amongst the theoretically focused papers the role model and design papers have plateaued while papers on role development have seen a recent spurt. On the practical focus side there is a smattering of papers across the topic areas without a clear dominance in one area. There has been an overall spurt in this area following publication of the NIST proposed standard in 2001 and its ANSI/INCITS adoption in 2004. This three level classification may serve as a template for classifying literature in other emerging areas of cyber security.

One of the characteristics of the ACM Workshops on Role-Based Access Control was the participation of users of RBAC technology from different verticals such as healthcare and financial services, as well as participation of vendors of RBAC products. As the

discipline has matured there has been a fragmentation, with the academic conferences becoming increasingly more competitive and focused more on theory while the industry oriented practitioner papers have disappeared from the refereed literature. In the early days of RBAC research there was considerable benefit to researchers from interaction with the pragmatic side of the business. It remains a challenge to the RBAC field and to cyber security in general of how to maintain this mutual interaction and influence.

The classification of Figure 7 can help us identify areas where additional work is needed in future to advance RBAC. In the area of role models we have seen a proliferation of models that extend the basic notions of RBAC such as embodied in the RBAC96 family in various different directions as discussed in the body of this paper. Over time some of these may receive the degree of consensus support received by RBAC96 to merit incorporation into an evolved standard. On the administrative side there remains a lack of consensus on a standard model. While a number of administrative models have been proposed and studied none has achieved a dominant level of support. This may be intrinsic in that no single administrative model is applicable to the diverse applications to which RBAC is relevant. Nonetheless a significant step forward in our understanding of RBAC administration would be a major advance. Much of the existing work on RBAC administration has focused on the user-role relationship. The permission-role relationship has not been theoretically investigated to the same degree. This may be a manifestation of the fact the user-role relationship can be discussed to considerable extent without deep consideration of the underlying application whereas role-permission requires such consideration. The role definition papers deal more directly with the permission-role relationship in their approaches to designing roles. With respect to role design we lack meaningful measures for assessing effectiveness of one set of roles over another, as well as notions of how to tradeoff security versus cost versus convenience. These issues plague most security technologies. Perhaps RBAC is the vehicle to show how these conundrums can be effectively addressed in practice, and serve as a "role model" for other security technologies.

At a fundamental theoretical level it still remains unclear what is the essence of RBAC. The essence of mandatory access control (MAC) is generally recognized to be the enforcement of information flow in a lattice of security labels. The essence of discretionary access control (DAC) is generally recognized to be that the "owner" (or custodian) of an object is the one who ultimately determines who is allowed to access it. RBAC has the curious status that it can be configured to do MAC or DAC or [Osborn et al. 2000]. What then is the essence of RBAC? The current best answer seems to be that it is a pragmatic tool that helps security architects design policy that caters to a number of established security principles [Sandhu and Bhamidipati 2008]. Is there a better answer?

We conclude with a few remarks on the future of RBAC and access control research. We believe RBAC is a fundamental aspect of access control that will continue to be used for decades into the future. It has already achieved dominance as the principal form of access control in most commercial systems. At a theoretical level it subsumes MAC and DAC as special cases. This theoretical result notwithstanding it is our considered belief that RBAC will coexist with MAC and DAC in situations where one or both of the latter are intrinsic to the application domain of interest. We anticipate that the access control arena will see significant research and innovation in the near future. The limitation of traditional access control have already led to ground breaking models such as Usage Control [Park and Sandhu 2004] and [Pretschner et al. 2006] which are better suited to the needs of next generation applications. Access control researchers face significant challenges to devise models usable by practitioners that can deal with the uncertain and fuzzy security requirements of emerging multi-party applications while allocating

responsibility for cost, liability and recourse. We anticipate that access control research has an exciting future and that RBAC will be a component of future systems for a long time to come.

ELECTRONIC BIBLIOGRAPHY

Available at: http://www-ifs.uni-regensburg.de/Roles

REFERENCES

ADABALA, S., MATSUNAGA, A., TSUGAWA, M., FIGUEIREDO, R. and FORTES, J. A. B. 2004. Single Sign-On in In-VIGO: Role-Based Access via Delegation Mechanisms Using Short-Lived User Identities. *In IPDPS'04: Proceedings of the18th International Parallel and Distributed Processing Symposium* IEEE Computer Society, 22b.

AHMED, T. and TRIPATHI, A. R. 2007. Specification and verification of security requirements in a programming model for decentralized CSCW systems. *ACM Transactions on Information and System Security (TISSEC)* 10, 2, -.

ANSI/INCITS 2004. ANSI INCITS 359-2004, American National Standard for Information Technology - Role Based Access Control

ASHLEY, P. and VANDENWAUVER, M. 1999. Using SESAME to Implement Role-Based Access Control in Unix File Systems. *In WETICE '99: Proceedings of the 8th Workshop on Enabling Technologies on Infrastructure for Collaborative Enterprises*. IEEE Computer Society, 141-146.

BARKLEY, J. F., CINCOTTA, A. V., FERRAIOLO, D. F., GAVRILA, S. and KUHN, D. R. 1997. Role Based Access Control for the World Wide Web. *In Proceedings of the 20th NIST-NCSC National Information Systems Security Conference*, 331-340.

BASIN, D. A., DOSER, J. and LODDERSTEDT, T. 2006. Model driven security: From UML models to access control infrastructures. *ACM Transactions on Software Engineering and Methodology (TOSEM)* 15, 1, 39-91.

BERTINO, E. 2003. RBAC models - concepts and trends. *Computers & Security* 22, 6, 511-514.

BERTINO, E., BONATTI, P. A. and FERRARI, E. 2001. TRBAC: A temporal role-based access control model. *ACM Transactions on Information and System Security (TISSEC)* 4, 3, 191-233.

BERTINO, E., CATANIA, B., DAMIANI, M. L. and PERLASCA, P. 2005. GEO-RBAC: a spatially aware RBAC. *In SACMAT'05: ACM Symposium on Access Control Models and Technologies*, 29-37.

BERTINO, E., FERRARI, E. and ATLURI, V. 1997. A flexible model supporting the specification and enforcement of role-based authorization in workflow management systems. *In RBAC '97: Proceedings of the second ACM workshop on Role-based access control*. ACM, 1-12.

BERTINO, E., FERRARI, E. and ATLURI, V. 1999. The specification and enforcement of authorization constraints in workflow management systems. *ACM Transactions on Information and System Security (TISSEC)* 2, 1, 65-104.

BERTINO, E., KAMRA, A., TERZI, E. and VAKALI, A. 2005. Intrusion Detection in RBAC-administered Databases. *In ACSAC '05: Proceedings of the 21th Annual Computer Security Applications Conference*, 170-182.

BEZNOSOV, K. 1998. Requirements for access control: US Healthcare domain. *In RBAC '98: Proceedings of the third ACM workshop on Role-based access control*. ACM, 43.

BEZNOSOV, K. and DENG, Y. 1999. A framework for implementing role-based access control using CORBA security service. *In RBAC '99: Proceedings of the fourth ACM workshop on Role-based access control*. ACM, 19-30.

BHATTI, R., GHAFOOR, A., BERTINO, E. and JOSHI, J. B. D. 2005. X-GTRBAC: an XML-based policy specification framework and architecture for enterprise-wide access control. *ACM Transactions on Information and System Security (TISSEC)* 8, 2, 187-227.

BIDDLE, B. J. 1986. Recent Developments in Role Theory. *Annual Review of Sociology* 12, 67-92.

BINDIGANAVALE, V. and OUYANG, J. 2006. Role based access control in enterprise application - security administration and user management. *In 2006 IEEE International Conference on Information Reuse and Integration*, 111-116.

BOHRA, A., SMALDONE, S. and IFTODE, L. 2007. FRAC: Implementing Role-Based Access Control for Network File Systems. *In IEEE International Symposium on Network Computing and Applications*, 95-104.

CHAE, S.-H., KIM, W. and KIM, D.-K. 2004. Efficient Role Based Access Control Method in Wireless Environment. *In IFIP TC6 International Conference on Personal Wireless Communications*, 431-439.

CHAKRABORTY, S. and RAY, I. 2006. TrustBAC: integrating trust relationships into the RBAC model for access control in open systems. *In SACMAT'06: Proceedings of the eleventh ACM symposium on Access control models and technologies*, 49-58.

CHANDRAMOULI, R. and SANDHU, R. S. 1998. Role-based access control features in commercial database management systems. *In Proceedings of 21st NIST-NCSC National Information Systems Security Conference*, 503-511.

CHEN, Y., YANG, S. and GUO, L. 2005. Dynamic-Role Based Access Control Framework Across Multi-domains in Grid Environment. *In GCC: Grid and Cooperative Computing*, 161-165.

COLANTONIO, A., PIETRO, R. D. and OCELLO, A. 2008. A cost-driven approach to role engineering. *In SAC '08: Proceedings of the 2008 ACM symposium on Applied computing* 2129-2136.

COYNE, E. J. 1996. Role engineering. *In RBAC '95: Proceedings of the first ACM Workshop on Role-based access control*. ACM, 4.

COYNE, E. J. and DAVIS, J. M. 2007. Role Engineering for Enterprise Security Management Artech House.

COYNE, E. J., PAGE, A. B., DAVIS, J. M. and ROTA, D. D. 2004. Role Engineering in Healthcare: Process, Results, and Lessons Learned.

CRAMPTON, J. 2005. Understanding and developing role-based administrative models. *In ACM Conference on Computer and Communications Security*, 158-167.

CRAMPTON, J. and LOIZOU, G. 2002. Administrative scope and role hierarchy operations. *In SACMAT '02: Proceedings of the seventh ACM symposium on Access control models and technologies*. ACM, 145-154.

EDWARDS, W. K. 1996. Policies and roles in collaborative applications. *In CSCW '96: Proceedings of the 1996 ACM conference on Computer supported cooperative work*. ACM, 11-20.

EPSTEIN, J. and SANDHU, R. 1996. NetWare 4 as an example of role-based access control. *In RBAC '95: Proceedings of the first ACM Workshop on Role-based access control*. ACM, 18.

EßMAYR, W., KASTNER, F., PERNUL, G. and TJOA, A. M. 1995. The security architecture of IRO-DB. *In Proceedings of the 12th IFIP International Conference on Information Security*, 249-258.

ESSMAYR, W., PROBST, S. and WEIPPL, E. 2004. Role-Based Access Controls: Status, Dissemination, and Prospects for Generic Security Mechanisms. *Electronic Commerce Research* 4, 1-2, 127-156.

FERRAIOLO, D. and BARKLEY, J. 1997. Specifying and managing role-based access control within a corporate intranet. *In RBAC '97: Proceedings of the second ACM workshop on Role-based access control*. ACM, 77-82.

FERRAIOLO, D. and KUHN, R. 1992. Role-Based Access Control. *In 15th NIST-NCSC National Computer Security Conference*, 554-563.

FERRAIOLO, D., KUHN, R. and CHANDRAMOULI, R. 2007. Role-Based Access Control, Artech House.

FERRAIOLO, D. F. 2001. An argument for the role-based access control model. *In SACMAT '01: Proceedings of the sixth ACM symposium on Access control models and technologies*. ACM, 142-143.

FERRAIOLO, D. F., CUGINI, J. A. and KUHN, D. R. 1995. Role-Based Access Control: Features and Motivations. *In Proceedings of the 11th Annual Computer Security Applications Conference*.

FERRAIOLO, D. F. and KUHN, D. R. 1996. Future directions in role-based access control. *In RBAC '95: Proceedings of the first ACM Workshop on Role-based access control*. ACM, 8.

FERRAIOLO, D. F., SANDHU, R., GAVRILA, S., KUHN, D. R. and CHANDRAMOULI, R. 2001. Proposed NIST standard for role-based access control. *ACM Transactions on Information and System Security (TISSEC)* 4, 3, 224-274.

FREUDENTHAL, E., PESIN, T., PORT, L., KEENAN, E. and KARAMCHETI, V. 2002. dRBAC: Distributed Role-based Access Control for Dynamic Coalition Environments. *In ICDCS '02: Proceedings of the 22nd International Conference on Distributed Computing Systems (ICDCS'02)*. IEEE Computer Society, 411.

FRIBERG, C. and HELD, A. 1997. Support for discretionary role based access control in ACL-oriented operating systems. *In RBAC '97: Proceedings of the second ACM workshop on Role-based access control*. ACM, 83-94.

FUCHS, L., BROSER, C. and PERNUL, G. 2009. Different Approaches to in-house Identity Management - Pros and Cons and the Justification of an Assumption. *In Proceedings of the The Fourth International Conference on Availability, Reliability and Security*. IEEE Computer Society, Fukuoka, Japan.

FUCHS, L. and PERNUL, G. 2008. PROROLE: A Process-Oriented Lifecycle Model for Role Systems Leveraging Identity Management and Guiding Role Projects. *In ECIS'08: Proceedings of the16th European Conference on Information Systems*, 1322-1333.

FUCHS, L. and PERNUL, G. U. 2008. HyDRo: Hybrid Development of Roles. *In ICISS'08: Proceedings of the 4th International Conference on Information Systems Security*. Springer, Hyderabad, India, 287-302.

FUCHS, L. and PREIS, A. 2008. BusiROLE: A Model for Integrating Business Roles into Identity Management. *In TrustBus '08: Proceedings of the 5th international conference on Trust, Privacy and Security in Digital Business* 128-138.

GALLAHER, M. P., O´CONNOR, A. C. and KROPP, B. 2002.The Economic Impact of Role-Based Access Control. prepared by RTI (Research Triangle Institute) for NIST.

GALLETTA, D. F. and HECKMAN, R. 1990. A Role Theory Perspective on End-User Development. *Information Systems Research* 1, 2, 168-187.

GIURI, L. 1996. Role-based access control: a natural approach. *In RBAC '95: Proceedings of the first ACM Workshop on Role-based access control*. ACM, 13.

GIURI, L. 1999. Role-based access control on the Web using Java. *In RBAC '99: Proceedings of the fourth ACM workshop on Role-based access control*. ACM, 11-18.

GUSTAFSSON, M., DELIGNY, B. and SHAHMEHRI, N. 1997. Using NFS to Implement Role-Based Access Control. *In WET-ICE '97: Proceedings of the 6th Workshop on Enabling Technologies on Infrastructure for Collaborative Enterprises*. IEEE Computer Society, 299-304.

HE, Q. 2003.Privacy Enforcement with an Extended Role-Based Access Control Model. North Carolina State University at Raleigh.

HECKMAN, R. and GALLETTA, D. F. 1988. Changing Roles in Information Systems: A Role Theory Perspective. *In Proceedings of the Ninth International Conference on Information Systems*, Minneapolis, 265-274.

HUA, L. and OSBORN, S. 1998. Modeling UNIX Access Control with a Role Graph. *In Proceedings of International Conference on Computers and Information Technology*.

HUANG, W.-K. and ATLURI, V. 1999. SecureFlow: a secure Web-enabled workflow management system. *In RBAC '99: Proceedings of the fourth ACM workshop on Role-based access control*. ACM, 83-94.

JOSHI, J., BERTINO, E., LATIF, U. and GHAFOOR, A. 2005. A Generalized Temporal Role-Based Access Control Model. *IEEE Trans. Knowl. Data Eng.* 17, 1, 4-23.

KALAM, A. A. E., BENFERHAT, S., MIEGE, A., BAIDA, R. E., CUPPENS, F., SAUREL, C., BALBIANI, P., DESWARTE, Y. and TROUESSIN, G. 2003. Organization based access control. *In POLICY '03: Proceedings of the 4th IEEE International Workshop on Policies for Distributed Systems and Networks*. IEEE Computer Society, 120.

KANDALA, S. and SANDHU, R. 2002. Secure role-based workflow models. *In Das'01: Proceedings of the fifteenth annual working conference on Database and application security*. Kluwer Academic Publishers, 45-58.

KERN, A. 2002. Advanced Features for Enterprise-Wide Role-Based Access Control. *In ACSAC '02: Proceedings of the 18th Annual Computer Security Applications Conference*. IEEE Computer Society, 333.

KERN, A., KUHLMANN, M., SCHAAD, A. and MOFFETT, J. 2002. Observations on the role life-cycle in the context of enterprise security management. *In SACMAT '02: Proceedings of the seventh ACM symposium on Access control models and technologies*. ACM, 43-51.

KUHLMANN, M., SHOHAT, D. and SCHIMPF, G. 2003. Role mining - revealing business roles for security administration using data mining technology. *In SACMAT '03: Proceedings of the eighth ACM symposium on Access control models and technologies*. ACM, 179-186.

LEE, B. G., NARAYANAN, N. H. and CHANG, K. H. 2001. An integrated approach to distributed version management and role-based access control in computer supported collaborative writing. *Journal of Systems and Software* 59, 2, 119-134.

LI, N. and NITA-ROTARU, C. 2003. A Framework for Role-Based Access Control in Group Communication Systems, Purdue University.

LINTON, R. 1936. The study of man, Appleton-Century-Crofts, New York.

LONGSTAFF, J., LOCKYER, M. and NICHOLAS, J. 2003. The tees confidentiality model: an authorisation model for identities and roles. *In SACMAT '03: Proceedings of the eighth ACM symposium on Access control models and technologies*. ACM, 125-133.

MATHUR, A., KIM, S. and STAMP, M. 2006. Role Based Access Control and the JXTA Peer-to-Peer Framework. *In Security and Management*, 390-398.

MEAD, G. H. 1934. Mind, Self and Society, University of Chicago Press, Chicago.

MENDLING, J., STREMBECK, M., STERMSEK, G. and NEUMANN, G. 2004. An Approach to Extract RBAC Models from BPEL4WS Processes. *In WETICE '04: Proceedings of the 13th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises*. IEEE Computer Society, 81-86.

MEYERS, W. J. 1997. RBAC emulation on trusted DG/UX. *In RBAC '97: Proceedings of the second ACM workshop on Role-based access control*. ACM, 55-60.

MOHAMMED, I. and DILTS, D. M. 1994. Design for dynamic user-role-based security. *Comput. Secur.* 13, 9, 661-671.

MOLLOY, I., CHEN, H., LI, T., WANG, Q., LI, N., BERTINO, E., CALO, S. B. and LOBO, J. 2008. Mining roles with semantic meanings. *In SACMAT '08: Proceedings of the 13th ACM symposium on Access control models and technologies* 21-30.

MORENO, J. L. and JENNINGS, H. H. 1934. Who Shall Survive?: Foundations of Sociometry, Group Psychotherapy, and Sociodrama, Nervous and Mental Disease Publishing Co., Washington, DC.

NAUMOVICH, G. and CENTONZE, P. 2004. Static analysis of role-based access control in J2EE applications. *SIGSOFT Software Engineering Notes* 29, 5, 1-10.

NEUMANN, G. and STREMBECK, M. 2002. A Scenario-Driven Role Engineering Process for functional RBAC Roles. *In SACMAT'02: Proceedings of 7th ACM Symposium on Access control models and technologies*, 33-42.

NI, Q., TROMBETTA, A., BERTINO, E. and LOBO, J. 2007. Privacy-aware role based access control. *In SACMAT '07: Proceedings of the twelfth ACM symposium on Access control models and technologies*, 41-50.

NOTARGIACOMO, L. 1996. Role-based access control in ORACLE7 and Trusted ORACLE7. *In RBAC '95: Proceedings of the first ACM Workshop on Role-based access control*. ACM.

NYANCHAMA, M. and OSBORN, S. 1993. Role-based security, object oriented databases and separation of duty. *SIGMOD Record* 22, 4, 45-51.

NYANCHAMA, M. and OSBORN, S. 1993. Role-based security: Pros, cons & some research directions. *ACM SIGSAC Review* 2, 11-17.

NYANCHAMA, M. and OSBORN, S. L. 1996. The role graph model. *In RBAC '95: Proceedings of the first ACM Workshop on Role-based access control*.

OBELHEIRO, R. R. and FRAGA, J. S. 2002. Role-Based Access Control for CORBA Distributed Object Systems. *In WORDS '02: Proceedings of The Seventh IEEE International Workshop on Object-Oriented Real-Time Dependable Systems*. IEEE Computer Society, 53.

OH, S. and PARK, S. 2000. Task-Role Based Access Control (T-RBAC): An Improved Access Control Model for Enterprise Environment. *In DEXA '00: Proceedings of the 11th International Conference on Database and Expert Systems Applications*. Springer-Verlag, 264-273.

OH, S. and SANDHU, R. 2002. A model for role administration using organization structure. *In SACMAT '02: Proceedings of the seventh ACM symposium on Access control models and technologies*. ACM, 155-162.

OSBORN, S., SANDHU, R. and MUNAWER, Q. 2000. Configuring role-based access control to enforce mandatory and discretionary access control policies. *ACM Transactions on Information and System Security (TISSEC)* 3, 2, 85-106.

OSBORN, S. L. 2001. Database Security Integration using Role-Based Access Control. *In Proceedings of the IFIP TC11/ WG11.3 Fourteenth Annual Working Conference on Database Security*. Kluwer, B.V., 245-258.

PARK, D.-G. and LEE, Y.-R. 2003. The ET-RBAC Based Privilege Management Infrastructure for Wireless Networks. *In EC-Web'03: Proceedings of the 4th International Conference on E-Commerce and Web Technologies*. Springer-Verlag, 84-93.

PARK, J. and SANDHU, R. 2004. The UCON_ABC usage control model. *ACM Transactions on Information and System Security (TISSEC)* 7, 1, 128-174.

PARK, J. S. and HWANG, J. 2003. Role-based access control for collaborative enterprise in peer-to-peer computing environments. *In SACMAT '03: Proceedings of the eighth ACM symposium on Access control models and technologies*. ACM, 93-99.

PAVLICH-MARISCAL, J. A., DOAN, T., MICHEL, L., DEMURJIAN, S. A. and TING, T. C. 2005. Role Slices: A Notation for RBAC Permission Assignment and Enforcement. *In DBSec'05: Proceedings of the 19th Annual IFIP WG11.3 Working Conference on Data and Applications Security*, 40-53.

PFLEEGER, C., P. and PFLEEGER, S. L. 2006. Security in Computing (4th Edition), Prentice Hall PTR.

PRETSCHNER, A., HILTY, M. and BASIN, D. 2006. Distributed usage control. *Communications of the ACM* 49, 9, 39-44.

RAY, I., LI, N., FRANCE, R. and KIM, D.-K. 2004. Using UML to visualize role-based access control constraints. *In SACMAT '04: Proceedings of the ninth ACM symposium on Access control models and technologies*. ACM, 115-124.

RHODES, A. and CAELLI, W. 2000.A Review Paper Role Based Access Control. Information Security Research Centre.

ROECKLE, H., SCHIMPF, G. and WEIDINGER, R. 2000. Process-oriented approach for role-finding to implement role-based security administration in a large industrial organization. *In RBAC '00: Proceedings of the fifth ACM workshop on Role-based access control*. ACM, 103-110.

SANDHU, R. and BHAMIDIPATI, V. 1998. An Oracle implementation of the PRA97 model for permission-role assignment. *In RBAC '98: Proceedings of the third ACM workshop on Role-based access control*. ACM, 13-21.

SANDHU, R. and BHAMIDIPATI, V. 1999. Role-based administration of user-role assignment: The URA97 model and its Oracle implementation. *Journal of Computer Security* 7, 4, 317-342.

SANDHU, R. and BHAMIDIPATI, V. 2008. The ASCAA Principles for Next-Generation Role-Based Access Control. *In ARES'08: Proceedings of the 3rd International Conference on Availability, Reliability and Security*.

SANDHU, R., BHAMIDIPATI, V., COYNE, E., GANTA, S. and YOUMAN, C. 1997. The ARBAC97 model for role-based administration of roles: preliminary description and outline. *In RBAC '97: Proceedings of the second ACM workshop on Role-based access control*. ACM, 41-50.

SANDHU, R. and MUNAWER, Q. 1998. The RRA97 Model for Role-Based Administration of Role Hierarchies. *In ACSAC '98: Proceedings of the 14th Annual Computer Security Applications Conference*. IEEE Computer Society, 39.

SANDHU, R. and MUNAWER, Q. 1999. The ARBAC99 Model for Administration of Roles. *In ACSAC '99: Proceedings of the 15th Annual Computer Security Applications Conference*. IEEE Computer Society, 229.

SANDHU, R. and PARK, J. S. 1998. Decentralized user-role assignment for Web-based intranets. *In RBAC '98: Proceedings of the third ACM workshop on Role-based access control*. ACM, 1-12.

SANDHU, R. S. 1998. Role-Based Access Control. *In Advances in Computers*. Academic Press, 238-287.

SANDHU, R. S. 2001. Future Directions in Role-Based Access Control Models. *In MMM-ACNS '01: Proceedings of the International Workshop on Information Assurance in Computer Networks*. Springer-Verlag, 22-26.

SANDHU, R. S. and AHN, G.-J. 1998. Decentralized Group Hierarchies in UNIX: An Experiment and Lessons Learned. *In Proceedings of 21st NIST-NCSC National Information Systems Security Conference*, 486-502.

SANDHU, R. S., COYNE, E. J., FEINSTEIN, H. L. and YOUMAN, C. E. 1994. Role-based access control: a multidimensional view. *In Proceedings of the 10th Annual Computer Security Applications Conference*. IEEE Press.

SANDHU, R. S., COYNE, E. J., FEINSTEIN, H. L. and YOUMAN, C. E. 1996. Role-Based Access Control Models. *IEEE Computer* 29, 2, 38-47.

SANDHU, R. S. and FEINSTEIN, H. 1994. A Three Tier Architecture for Role-Based Access Control. *In In Proceedings of the 17th NIST-NCSC National Computer Security Conference*, 34-46.

SCHAAD, A., MOFFETT, J. and JACOB, J. 2001. The role-based access control system of a European bank: a case study and discussion. *In SACMAT '01: Proceedings of the sixth ACM symposium on Access control models and technologies*. ACM, 3-9.

SCHLEGELMILCH, J. and STEFFENS, U. 2005. Role mining with ORCA. *In SACMAT '05: Proceedings of the tenth ACM symposium on Access control models and technologies* 168-176.

SHIN, M. E. and AHN, G.-J. 2000. UML-Based Representation of Role-Based Access Control. *In WETICE '00: Proceedings of the 9th IEEE International Workshops on Enabling Technologies*. IEEE Computer Society, 195-200.

SMITH, C. 1997. A Survey to Determine Federal Agency Needs for a Role-Based Access Control Security Product. *In ISESS '97: Proceedings of the 3rd International Software Engineering Standards Symposium*. IEEE Computer Society.

SMITH, C. L., COYNE, E. J., YOUMAN, C. E. and GANTA, S. 1996.A Marketing Survey of Civil Federal Government Organisations to Determine the Need for a Role-Based Access Control (RBAC) Security Product. SETA Corporation.

STREMBECK, M. 2005. A Role Engineering Tool for Role-Based Access Control. *In SREIS'05: Proceedings of the Symposium on Requirements Engineering for Information Security*.

SUN, L., HUANG, G., SUN, Y., SONG, H. and MEI, H. 2008. An Approach for Generation of J2EE Access Control Configurations from Requirements Specification. *In QSIC '08: Proceedings of the 2008 The Eighth International Conference on Quality Software*, 87-96.

SUN, Y., MENG, X., LIU, S. and PAN, P. 2005. Flexible Workflow Incorporated with RBAC. *In CSCWD'05: Proceedings of the 9th International Conference on Computer Supported Cooperative Work in Design*, 525-534.

SUN, Y. and PAN, P. 2005. PRES: a practical flexible RBAC workflow system. *In ICEC '05: Proceedings of the 7th international conference on Electronic commerce* 653-658.

TARI, Z. and CHAN, S.-W. 1997. A Role-Based Access Control for Intranet Security. *IEEE Internet Computing* 1, 5, 24-34.

THOMAS, R. K. 1997. Team-based access control (TMAC): a primitive for applying role-based access controls in collaborative environments. *In RBAC '97: Proceedings of the second ACM workshop on Role-based access control*. ACM, 13-19.

THOMSEN, D., O'BRIEN, D. and BOGLE, J. 1998. Role-Based Access Control Framework for Network Enterprises. *In ACSAC '98: Proceedings of the 14th Annual Computer Security Applications Conference*. IEEE Computer Society, 50.

TOMUR, E. and ERTEN, Y. M. 2006. Application of temporal and spatial role based access control in 802.11 wireless networks. *Computers & Security* 25, 6, 452-458.

VAIDYA, J., ATLURI, V. and GUO, Q. 2007. The role mining problem: finding a minimal descriptive set of roles. *In SACMAT '07: Proceedings of the twelfth ACM symposium on Access control models and technologies*, 175-184.

VAIDYA, J., ATLURI, V. and WARNER, J. 2006. RoleMiner: mining roles using subset enumeration. *In ACM Conference on Computer and Communications Security*, 144-153.

WAINER, J. and BARTHELMESS, P. 2003. W-RBAC - A workflow security model incorporating controlled overriding of constraints. *International Journal of Cooperative Information Systems* 12, 0.

WAINER, J., KUMAR, A. and BARTHELMESS, P. 2007. DW-RBAC: A formal security model of delegation and revocation in workflow systems. *Information Systems* 32, 3, 365-384.

WILIKENS, M., FERITI, S. and MASERA, M. 2002. A context-related authorization and access control method based on RBAC: A case study from the health care domain. *In SACMAT'02: Proceedings of 7th ACM Symposium on Access control models and technologies*.

XIANGPENG, Z., CERONE, A. and KRISHNAN, P. 2006. Verifying BPEL Workflows Under Authorisation Constraints. *In Business Process Management Journal*, 439-444.

ZHANG, Y. and JOSHI, J. B. D. 2007. ARBAC07: A Role-based Administration Model for RBAC with Hybrid Hierarchy. *In IRI'07: IEEE International Conference on Information Reuse and Integration*, 196-202.

ZHANG, Y. and JOSHI, J. B. D. 2007. SARBAC07: A Scoped Administration Model for RBAC with Hybrid Hierarchy. *In IAS '07: Proceedings of the Third International Symposium on Information Assurance and Security* 149-154.

ZHU, H. 2006. Introduction to Special Session (R) on Role-Based Collaboration. *In Proceedings of the IEEE Workshop on Distributed Intelligent Systems: Collective Intelligence and Its Applications*. IEEE Computer Society.

ZHU, H. and ZHOU, M. 2008. Roles in Information Systems: A Survey. *IEEE transactions on systems, man and cybernetics. Part C, Applications and reviews* 38, 3, 377-396.