COMPUTERS & SECURITY 30 (2011) 748–769

available at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

Roles in information security – A survey and classification of the research area

L. Fuchs [a,*], G. Pernul [a,1], R. Sandhu [b]

[a] Department of Information Systems, University of Regensburg, Germany
[b] Institute for Cyber Security, University of Texas at San Antonio, USA

ARTICLE INFO

Article history:
Received 12 April 2011
Received in revised form
20 July 2011
Accepted 2 August 2011

Keywords:
Role-based access control
RBAC
Role theory
Information Security
Survey

ABSTRACT

The concept of roles has been prevalent in the area of Information Security for more than 15 years already. It promises simplified and flexible user management, reduced administrative costs, improved security, as well as the integration of employees' business functions into the IT administration. A comprehensive scientific literature collection revealed more than 1300 publications dealing with the application of sociological role theory in the context of Information Security up to now. Although there is an ANSI/NIST standard and an ISO standard proposal, a variety of competing models and interpretations of the role concept have developed. The major contribution of this survey is a categorization of the complete underlying set of publications into different classes. The main part of the work is investigating 32 identified research directions, evaluating their importance and analyzing research tendencies. An electronic bibliography including all surveyed publications together with the classification information is provided additionally. As a final contribution potential future developments in the area of role-research are considered.

1. Motivation

The growing diffusion of information technologies within all areas of human society has increased their importance as a critical success factor in the modern world. However, information processing systems are vulnerable to many different kinds of threats that can lead to various types of damage resulting in significant economic losses. Consequently, the importance of Information Security has grown and evolved in a similar manner. 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 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 areas of Information Security and the most fundamental and pervasive security mechanism in use (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 also 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. RBAC nowadays

* *Corresponding author*. Tel.: +49 941 9432952.
E-mail address: ludwig.fuchs@wiwi.uni-regensburg.de (L. Fuchs).
[1] Tel.: +49 941 9432952.
0167-4048/$ – see front matter © 2011 Elsevier Ltd. All rights reserved.
doi:10.1016/j.cose.2011.08.002

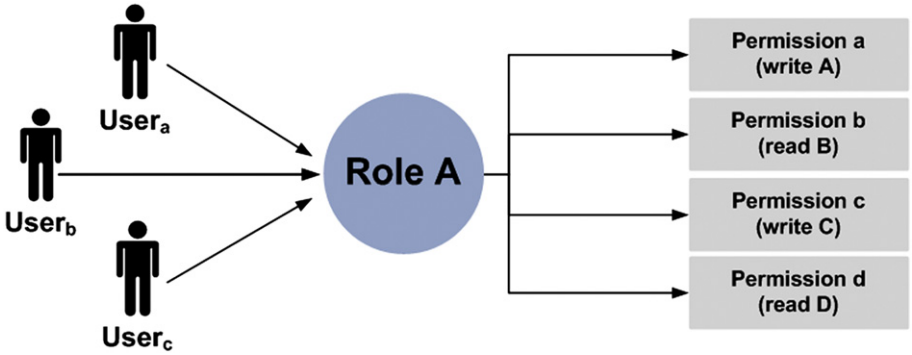

Fig. 1 – Roles as intermediates between users and permissions.

marks the de facto standard in enterprise systems involving large numbers of users with different rights and obligations. The fundamental idea is the removal of the direct linkage between the user and his permissions. Following this paradigm roles are created for the various job functions and users are assigned to roles based on their responsibilities and qualifications. The roles themselves are connected with access rights to certain resources (see Fig. 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.

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 vivid research community deals with the adoption of role theory in Information Security. Up to now more than 1300 publications contributed to this area, investigating new application areas, providing formal foundation frameworks or combining role theory with other technologies in practical usage scenarios – to mention only selected research fields.

Up to now there is no structured and comprehensive overview over the huge amount of publications and competing research directions on role-research available. This work provides such a survey, embracing 1361 identified scientific publications. A detailed statistical analysis combined with a classification scheme allows for the identification and interpretation of research directions and their importance. 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 throughout the survey.[2] 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 further development of the field.

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

2. Preliminaries and related work

"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).

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 to think of life as a theatrical metaphor. Scientists in the 1930s began to compare social life with the theatre in which actors played predictable roles. If performances in the theatre were differentiated and predictable because actors were constrained to perform parts for which scripts were written, then it seemed reasonable for them to believe that social behaviors in other contexts were also associated with parts and scripts understood by social actors (Biddle, 1986).

Researchers like Ralph Linton (anthropology), George Herbert Mead (social philosophy), or Jacob Moreno (psychology) contributed to the foundation of the role theory. Linton defined role theory as a means of analyzing social systems. Roles were conceived as the dynamic aspects of recognized social positions (Linton, 1936). In contrast, Mead saw roles as the coping strategies that individuals develop as they interact with other people. In his main work "Mind, Self and Society" he characterized role taking as a prerequisite for effective social interaction (Mead, 1934). Finally, Moreno regarded roles as the tactics that are adopted by people within primary relationships, and argued that imitative behavior was a useful strategy for learning new roles (Moreno and Jennings, 1934). According to Biddle, the role theory in sociology concerns one

[2] http://www-ifsresearch.wiwi.uni-regensburg.de/Roles.

of the most important characteristics of social behavior – the fact that human beings behave in ways that are predictable depending on their respective social identities and the situation (Biddle, 1986). Over time, this notion of roles has been widely adopted to the environment of fields such as sociology, psychology, anthropology, organizational theory, and, lately, Information Security.

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 several software vendors selectively dealt with the 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.

2.1.1. Pre-RBAC efforts (-1992)

The concept of roles has been used in software applications for at least 30 years. Different products have 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 operating systems and privilege groupings in database management systems. In the early days of adoption, 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 stable, 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. In traditional organizational theory roles are used to express the position of an employee within an organizational structure. Roles are determined by factors like the company type, the branch, and the life phase of the enterprise. 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 there was only little formal analysis of the security of these systems.

2.1.2. Early RBAC Efforts (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 (1992), introducing the term *RBAC*. Within the scope of a study carried out by NIST,[3] MAC- and DAC-based systems were analyzed and a draft for a formal interpretation of the role concept was given. This first model and its properties were 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 AC (Nyanchama and Osborn, 1993a,b). These efforts later resulted in the so called *role-graph model*.

[3] National Institute of Standards and Technology (http://www.nist.gov/).

The phase of *early RBAC* efforts resulted in the publication of the initial RBAC96 family (Sandhu et al., 1996) in 1996. 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 (15) have been provided 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 end of 2010.

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 since 1996.[4] Early contributions focus on the identification of future research areas and developments while later articles commonly analyze the historical development of specific role-related research issues. The first meta-analyses identified the refinement and development of the nature of RBAC as well as the practical implementation of RBAC as major research areas (Ferraiolo and Kuhn, 1996; Giuri, 1996). A marketing survey of Smith et al. (Smith, 1997; Smith et al., 1996) focused on customer requirements regarding their security needs for information processing systems. In 1998 Sandhu (1998) recapitulated, amongst others, the RBAC96 models and the ARBAC97 administration models (Sandhu et al., 1997).

In Rhodes and Caelli (2000) RBAC characteristics and policies were reviewed. However, Rhodes only described a limited selection of role models. In Ferraiolo (2001), Ferraiolo summarized and classified 25 role-related publications. In the same year 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 the economic impacts of RBAC have been described in Gallaher et al. (2002). 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. In 2004, Essmayr et al. (2004) presented an overview over security models in general and an additional survey on RBAC. Further discussions on the review and methodologies that support the definition of roles were 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. They provide a short classification including the evolution and the applications of so called

[4] For a complete list of those publications search the provided electronic bibliography database for the research area *Review & Meta-Analysis*.

[5] ACM Symposium on Access Control Models and Technologies.

Table 1 – Review and Meta-Analysis publications.

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	–
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
The role mining process model – underlining the need for a comprehensive research perspective	Fuchs and Meier	2011	37
Roles in information security – a survey and classification of the research area	Fuchs et al.	2011	1361

RBAC-roles, without giving a detailed analysis. Fuchs et al. provided an evaluation of different role development approaches in Fuchs et al. (2009) and Fuchs and Meier (2011). However, those surveys also only cover a limited part of the overall research area, focusing on the task of defining roles for an information system.

Note that over the years also a number of textbooks have been published, reviewing and summing up the scientific results of research directions. Examples are Ferraiolo et al. (2007) or Coyne and Davis (2007). These books are not included in the survey process itself as they recapitulate existing knowledge in the field.

Table 1 sums up the different review and meta-analyses together with the number of surveyed publications and contrasts to this work. It 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 applied 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.

3. Research methodology

This section points out the cornerstones of our underlying survey methodology. In Section 3.1 a detection strategy for the identification of the relevant publications is presented while Section 3.2 outlines the used classification methodology. The central outcome is the complete classification of 1361 publications included in the derived result set into 32 hierarchically aligned research areas.

3.1. *The detection of relevant publications*

In order to conduct a comprehensive survey the detection techniques that lead to the identification of relevant publications have to be evaluated carefully. A straightforward approach would be a manual and iterative check of references given inside publications pointing to further relevant scientific work. Another possibility could be the content analysis of conferences and journals in the field, requiring a fully mashed cross-referencing among the scientific publications. However, the high expected number of publications to be analyzed makes a purely manual identification process time-consuming and error-prone. As a result, an automatic search based on a bibliographic database needs to be carried out in combination with a manual verification process. The used survey methodology consists of the four major steps, bibliography selection, query selection and search, result reviewing, and result extension (Fig. 2). These steps have been executed for each year starting from 1996 to 2010 resulting in the compilation of the complete result set RES^{+}_{RBAC}.

3.1.1. *Bibliography selection*

Employing an automated search engine, characteristics like the investigated scientific discipline, the included publication types and the offered search-capabilities must be considered. Accordingly, existing databases including the ACM Digital Library,[6] IEEE Digital Library,[7] AIS Electronic Library,[8] CiteSeerX Scientific Literature Digital Library,[9] Google Scholar,[10]

[6] http://portal.acm.org/dl.cfm.
[7] http://www2.computer.org/portal/web/csdl.
[8] http://aisel.aisnet.org/.
[9] http://citeseerx.ist.psu.edu/.
[10] http://scholar.google.de/.

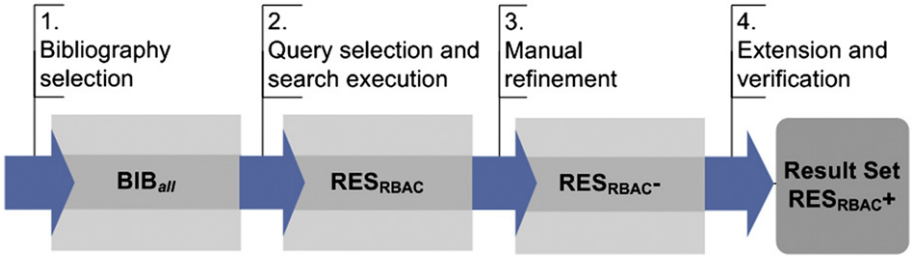

Fig. 2 – The detection of relevant publications.

Springer Link,[11] and DBLP[12] (Digital Bibliography and Library Project) were investigated for usage. An evaluation revealed the DBLP faceted search as the best source for our purpose as it is not limited to a certain publisher and returns identified publications along with a number of distinguishing facets. Moreover, the majority of information technology journals and proceedings are embraced in the DBLP. In order to ensure a high result quality, the IEEE and ACM Digital libraries have been facilitated in a second retrieval step in order to complement the publication set by generating the set union of both publication sets.

3.1.2. *Query selection and search execution*

The second step after the selection of the search engine is the consideration of appropriate query terms. Using *role* as search term a total of 23,644 records was returned by the DBLP service (retrieval date 03/09/11). However, due to homonym conflicts only a small number of those publications deal with the term *role* in terms of Information Security. Therefore *RBAC*, *role based*, and *role-based access control* as synonyms for the adoption of role theory in Information Security were selected as query terms. 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 publications in the reference section. The investigation of the obtained results in terms of a cross-checking with the results of other search terms for each year from 1996 to 2010 underlined the reasonability of our approach.

3.1.3. *Manual refinement*

A detailed investigation of the returned results revealed that not all displayed entries were relevant for the objective of this survey. The different interpretations of the role concept in the computing world comprise fields like Artificial Intelligence, Social Psychology and Organizations Management, as well as Human–Computer-Interaction (Zhu, 2006). Due to the focus of this article, the term *role(s)* is used exclusively in respect to Information Security. Consequently, 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 scientific work focusing on social sciences, role playing, or agent systems.[13] However, note that several borderline publications had to be investigated in detail to determine their primary focus and decide upon their inclusion. Only if a direct link to the field of Information Security was obvious, the publications remained in the result set.

3.1.4. *Extension and verification*

To verify the quality of the preliminary result set, a manual reference checking was conducted. For each year the references listed in every publication included in RES$_{RBAC96\text{-}10}^{-}$ were investigated. If a listed reference dealing with roles in Information Security was not yet incorporated it was added to the result set. Even though this proved to be a cumbersome task, it underlined the feasibility of our methodology as only a low number of publications had to be added or excluded. Exclusions covered books and dissertations. Dissertations are not considered since they are usually published (at least partly) in one of the investigated venues while books recapitulate existing knowledge in the field. Due to the fact that a temporal delay exists in the digital libraries not all relevant publications from the year 2010 are likely to be retrievable on 01/01/11. Therefore, conferences and journals already included in the electronic database from previous years were re-checked manually up to 01/03/11. For the year 2010 this extension process revealed 18 additional papers.

The complete set of scientific publications collected in RES$_{RBAC96\text{-}10}^{+}$ (=RES$_{RBAC}^{+}$) consisted of 1361 publications including 15 early publications from 1992 to 1995. This set has been used as basis for the consecutive classification process.

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. This work made use of a hierarchical 3-level clustering approach as shown in Fig. 3. Several classification criteria have been considered to reach a stable hierarchy of clusters representing the 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

[11] http://www.springerlink.com/home/main.mpx.
[12] http://dblp.uni-trier.de/, former known as "DataBase systems and Logic Programming".
[13] Publications on agent systems commonly use roles in respect to software components and agent behavior neither involving human interaction, nor dealing with Information Security.

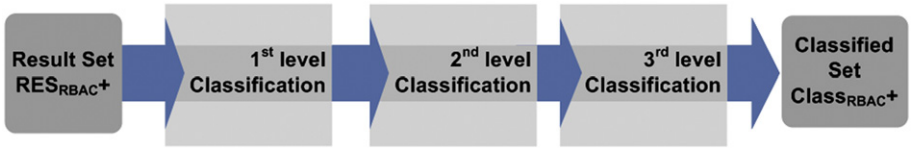

Fig. 3 – The classification methodology.

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 Section 2.2),
- references given in the publication, or
- exhaustive reading of the content.

At this point, alternative ways to solve the classification task are discussed briefly to justify the decision for hierarchical clustering as a pragmatic approach. Firstly, it would be possible to carry out a 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 a percentage-based allocation. For example a publication *P* is assigned to a research area *A*1 (90%) and to another research area *A*2 (10%). However, the weighting process would be heavily subjective and a quantitative comparison of the importance of a publication is hardly possible. Furthermore, it would be possible to draw a references graph that considers the 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

This section provides a first characterization of the research area on the basis of a statistical analysis. The result set is examined depending on general characteristics of publications including the year of publication and the venue of publication.

4.1. *Publications according to year of publication*

The amount of publications according to the year of publication is illustrated in Fig. 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.

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; ANSI/INCITS, 2004). Several authors dealt with role theory before 1992. These research efforts were summarized as *pre-RBAC* phase and excluded from this analysis. This phase of *early RBAC* efforts until 1996 resulted in the publication of the RBAC96 family and the simultaneous start of the *ACM Workshop on Role-Based Access Control* series.

Based on this work, the efforts of researchers have increased over the following years and reached at a constant level until 2002 with about 30–60 publications per year. During this time RBAC developed to a widely used access control paradigm. It evolved from a NIST Standard in 2001 to an ANSI[14]/INCITS[15] Standard in 2004. This standardization process marks the second and third milestone. During the time between 2003 and 2005 the amount of publications attained new heights at approximately 100 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. This resulted in a further increase of yearly publications to more than 140 since 2006. The growth has since then been continuing, resulting in about 160 publications per year. A more detailed analysis in the following sections is going to point out the research areas which are the most vivid and emerging ones.

4.2. *Publications according to venue*

Table 2 presents the examination of the result set according to the venue in which articles appeared (mostly proceedings of

[14] American National Standards Institute.
[15] InterNational Committee for Information Technology Standards.

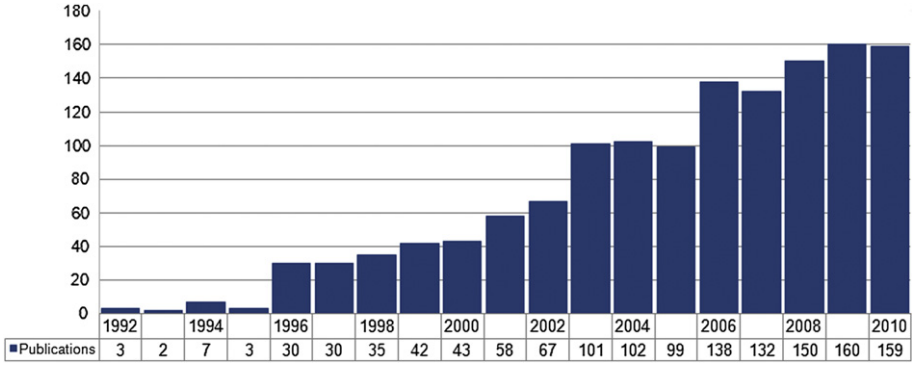

Fig. 4 – Publications according to year of publication.

conferences and journals). A total of more than 450 different venue-titles were identified during this investigation. Due to space restrictions Table 2 illustrates only venues with a minimum of ten publications.

The largest number of articles on roles in Information Security appeared either in the *ACM Symposium on Access Control Models and Technologies* (99) or in the *ACM Workshop on Role-Based Access Control* (73). This venue played a decisive role in the development of a scientifically proven adoption of role theory in Information Security. Since 2001 the scope of interest has been broadened and it has evolved into the *ACM SACMAT*. Nearly 13% of all identified scientific works were published in either one of those two venues.

Following those two main venues, a large amount of academic work has been published in the *Annual IFIP WG 11.3 Working Conference on Data and Applications Security* (38), the *ACM Transactions on Information and System Security* (33), the *Annual Computer Security Applications Conference* (30) and the *International Workshop on Database and Expert Systems Applications* (29). Those venues have experienced a steady growth of the number of publications over the years. Other venues, for instance the *Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises* (18) or the *NIST-NCSC National Computer Security Conference* (13), the *ACM Symposium on Applied Computing* (13), or the *International Conference on Advanced Information Networking and Applications* (11) have experienced a decrease of importance for the field of roles in Information Security. Their number of publications has been stable or has only slightly extended since 2008. Our analysis in Table 2 furthermore points out the applied or theoretical focus of the different venues. While the *SACMAT*, *CCS* or *TISSEC* mainly

Table 2 – Conferences with ten or more relevant publications.

Venue	∑	%	Theoretical	Practical
ACM Symposium on Access Control Models and Technologies (SACMAT)	99	7.27	74	25
ACM Workshop on Role-Based Access Control (RBAC)[a]	73	5.36	40	33
Annual IFIPWG 11.3 Working Conference on Data and Applications Security (DBSec)	38	2.79	19	19
ACM Transactions on Information and System Security (TISSEC)	33	2.42	26	7
Annual Computer Security Applications Conference (ACSAC)	30	2.20	19	11
International Conference on Database and Expert Systems Applications Series (DEXA)[b]	29	2.13	15	14
Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE)	18	1.32	10	8
International Conference on Availability, Reliability and Security (ARES)	17	1.25	7	10
ACM Conference on Computer and Communications Security (CCS) inc. ASIA CCS	16	1.18	13	3
IEEE International Workshop on Policies for Distributed Systems and Networks (POLICY)	16	1.18	10	6
International Working Group on Computer Supported Cooperative Work in Design (CSCWD)	15	1.10	3	12
International Conference on Advanced Information Networking and Applications (AINA)	14	1.03	8	6
IEEE International Conference on Computer and Information Technology (CIT)	13	0.96	4	9
NIST-NCSC National Information Systems Security Conference	13	0.96	6	7
ACM Symposium on Applied Computing (SAC)	13	0.96	6	7
IFIPTC-11 International Information Security Conference (SEC)	13	0.96	8	5
International Conference on Information and Communications Security (ICICS)	11	0.81	6	5
International Symposium on Information Assurance and Security (IAS)	10	0.73	9	1
Hawaii International Conference on System Sciences (HICSS)	10	0.73	2	8
IEEE International Conference on Systems, Man and Cybernetics (SMC)	10	0.73	1	9
∑	491	36.08	286	205
			58.25%	41.75%

a Evolved into SACMAT.
b Incl. Trustbus, EC-Web, E-Gov.

Table 3 – Composition of the result since 1992.

Result set	'92	'93	'94	'95	'96	'97	'98	'99	'00	'01	'02	'03	'04	'05	'06	'07	'08	'09	'10	∑
Early RBAC	3	2	7	3	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	15
Theoretical focus	–	–	–	–	15	17	13	13	24	29	37	57	51	57	76	66	82	91	76	704
Practical focus	–	–	–	–	15	13	22	29	19	29	30	44	51	42	62	66	68	69	83	642
∑	3	2	7	3	30	30	35	42	43	58	67	101	102	99	138	132	150	160	159	1361

provide a platform for the publication of theoretical research work, the *CSCWD*, *ARES*, *CIT* or *SMC* can be interpreted as practically oriented venues.

Even though more than one-third (36.08%) of all identified works have been published in the major venues mentioned above, the rest appeared in a wide diversity of other venues. The total number of more than 450 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.

5. Identifying research areas – classification results

The statistics given in Section 4 demonstrated the overall development of a role-based security paradigm and research area. The amount of publications according to the respective year (Fig. 4) showed that the research development can be divided into major phases. The investigation of venues (see Table 2) underlined the multi-layered dispersion of the role concept in the field. However, besides this statistical analysis, the essential challenge of the survey is the discovery of a suitable classification structure for the scientific work. The derived clusters of publications are called (*research*) *areas* of a certain *level of classification*. The classification process resulted in a three level classification scheme which ensures appropriate grouping of all publications combined with simplified understanding. 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 1361 scientific publications to exactly one of 32 identified different research directions.

5.1. *Main research areas*

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

The smallest cluster consists of the *early RBAC* efforts between 1992 and 1995 dealing 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 *applied focus*. While theoretical publications deal with the investigation, extension of existing concepts surrounding roles, the applied 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 focus.

A timeline analysis (see Table 3) reveals that both classes consist of about half of the investigated scientific publications (theoretical: 704; applied: 642). It underlines that the respective yearly publication count of articles with theoretical and applied 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 applied research as well as implementation needs. Table 3 again points out the growth of the area ending up with more than 150 publications each year since 2008. Another interesting fact is that applied research work has outpaced its theoretical counterpart in 2010 for the first time since 2004. The reason is an increase of practically related publications during the last year while at the same time a decrease of theoretical publications took place. Future analysis has to reveal if that is a long-term trend.

5.2. *Detailed classification results*

The 1st level classification has revealed applied and theoretical focus as first distinction criteria. Due to the large number of publications assigned, a 2nd level classification needs to be carried out. The 642 publications with applied focus can be differentiated into *industry* and *technology* efforts. The industry-related publications deal with the adoption of roles in 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.[16]

The 704 publications with theoretical affiliation are divided into a large group of *Role Model and Design* including research activities dealing with role models, their elements, the relationships among those elements, and their administration. Additionally a larger group of publications that analyze the relation of *Roles and Security Technologies* like cryptography, information flow, UML or protocols like XACML were identified. Another large cluster deals with *Role Development* comprising publications that deal with the initial definition of roles in specific environments. Several smaller areas deal with *standardization efforts*, the relationship of *RBAC and DAC/MAC*, or *Review and Meta-Analysis*.

[16] Enterprise Security Management.

The pie chart diagram given in Fig. 5 reveals the quantitative constitution of the 2nd level research areas since 1996.[17] The results show that the applied research field (grey colored) is heavily dominated by publications investigating the adoption of roles in different security technologies. The theoretical research field (blue colored) is dominated by publications investigating the framework of role models and design of role-based systems to a large extent. After this presentation of the first classification levels the full classification tableau is provided in the following.

Fig. 6 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 sub-areas 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 clusters represent specific research areas which are investigated in the remainder of this paper.

Note that the 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. Theoretical findings, e.g., concerning roles and their usage in security technologies are for instance usually adopted in practical scenarios. Hence the allocation was carried out based on the main focus of the publication. Additionally, several research areas are related to each other. In the area of web- and network-based application of role theory in practice a new class of research papers dealing specifically with grid computing and cloud computing has for instance evolved over the last years. The amount of publications and their specific focus thus led to the definition of a new research class.

This final classification tableau (Fig. 6) is consecutively explained in detail in Sections 6 and 7. In order to provide readability and consistency, the investigation scheme remains identical during the presentation of all research areas: Before a specific area is explained, it is defined briefly in the first step. The definition shapes the research area and reasons for the assignment of the respective publications. In a second step the development of the area in terms of quantitative research output is interpreted. Consecutively, the refinement of a research area in sub-areas (if applicable) is provided. Representative papers are explained briefly in case the research class has been assigned more than 50 publications.

6. Publications with theoretical focus

After the presentation of the general classification, this section is going to analyze research efforts with a theoretical focus, i.e. the upper part of the classification tableau in Fig. 6. Publications with theoretical focus deal with the investigation and extension of existing concepts surrounding role theory adoption. The quantitative development of the field according to the year of publication is depicted in Fig. 7. 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 significant rise of researchers' interest can be identified. One reason for this development might be the establishment and increasing diffusion of the role concept and RBAC in the Information Security community. Simultaneously, practical usage led to new theoretical research questions. One prime example is the extension of existing role models over the years where 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.

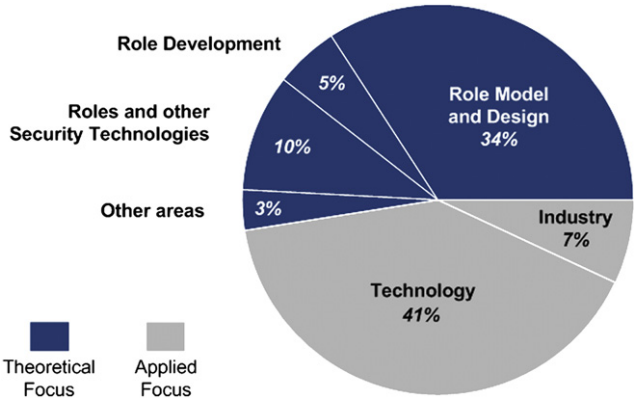

Fig. 5 – 2nd level classification analysis.

The composition of the research area (Table 4) 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* (468). 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* (129) as well as *Role Development* (63) are additional vivid and important research areas. The areas *Review and Meta-Analysis* (16), *Roles and other AC Technologies* (20), and *Roles and Standards* (8) form the minor research areas. The detailed inspection shows that the area of role development is the only area with a steady increase of publications over the last five years. The adoption of data mining technologies to define roles in existing AC infrastructures has attracted a great deal of attention in the community during these years. At the same time the amount of work carried out in the two major theoretical research areas *Role Model and Design* and *Roles and other Security Technologies* decreased slightly.

In the following the 2nd level classification areas are briefly analyzed. For each research area a result interpretation is provided on the basis of plotting diagrams focusing on the most important areas (in terms of publications) *Role Model and Design, Roles and Other Security Technologies* as well as *Role Development*.

6.1. Role model and design

Every role system has to be based on a well-defined theoretical basis. The area of *Role Model and Design* shapes the basic

[17] The early RBAC phase (15 publications) has been excluded.

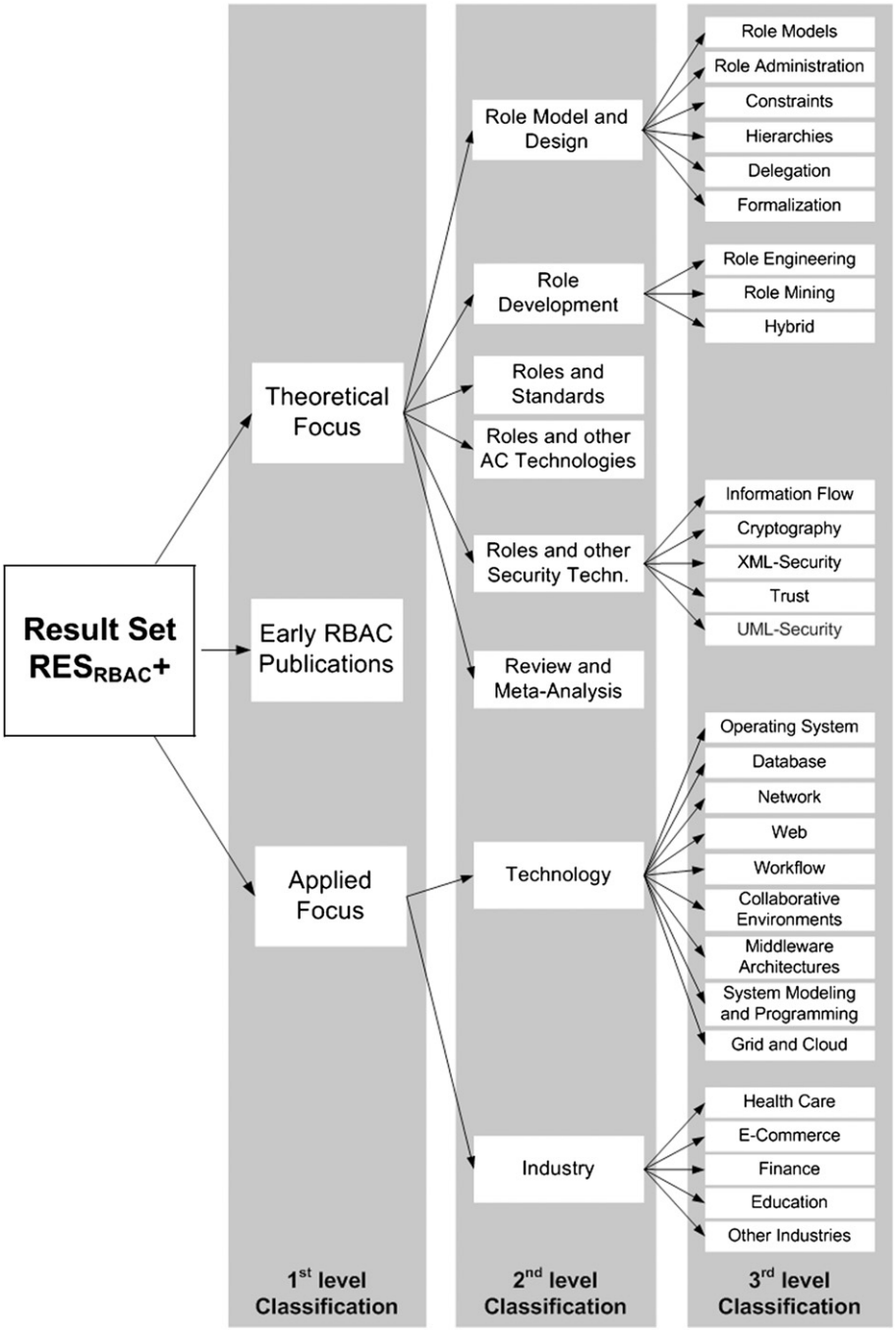

Fig. 6 – Final classification tableau.

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 are developing theoretical role or administration models as well as focusing on concepts used in these models, e.g., hierarchies, delegation, formalization or constraints.

After an initial phase a growth of the scientific output with a peak in the year 2003 can be identified (Table 5). After the year 2005 the number of publications remained at a high level of about 40–50 publications per year. 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. It becomes evident that the major part of 468 publications is belonging either to the area of *Role Models* (165) or to *Role Administration* (120). The other sub-areas are characterized by a smaller amount of papers (*Constraints* (65), *Delegation* (40), *Formalization* (48), and *Hierarchies* (30)). 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.

6.1.1. *Role models*

Role models are one core element of a role system and define the formal understanding of roles, related attributes, and

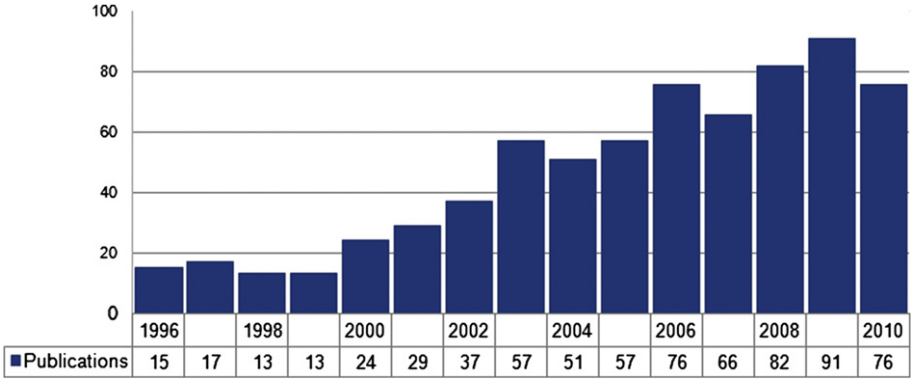

Fig. 7 – Publications with *Theoretical Focus*.

entities. Looking at the research activities reveals that the related field has been a vivid area since 1996 with a total number of 165 published works since then.

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).[18] This 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: Core RBAC covers the essential RBAC features such that permissions are assigned to roles and roles are assigned to users while hierarchical RBAC adds the notion of role hierarchies and inheritance. Constrained RBAC allows for constraints to implement static and dynamic separation of duty policies. A consolidated model (Fig. 8) combines the aforementioned partial models.

After the year 2000, a newly gained interest of researchers in extending role models can be identified. 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 several models has been provided in Fuchs and Preis (2008).

Selected examples are:

- T-RBAC (Task-Role-Based Access Control) integrating tasks representing job functions related to access rights (Oh and Park, 2000);
- OrBAC (Organisation-Based Access Control) defining permissions to control the activities performed by roles on views (Kalam et al., 2003);
- TRBAC (Temporal Role-Based Access Control) and the (X-) GTRBAC family incorporating time-dependency into RBAC (Bertino et al., 2001; Joshi et al., 2005).

Most of the RBAC extensions have been dealt with through several research publications. Due to their specific focus they laid the foundation for practical adoption in different areas as well as for the development of specific administration models. Note that some publications dealing with RBAC extensions are due to their focus allocated to one of the specific research areas considering hierarchies, constraints, delegation and formalization.

6.1.2. *Role administration*

After a role system has been deployed, its administration is the central duty. A number of well-accepted administration models have been developed in order to address this task. Their main objectives include the decentralization of administrative competence, the autonomy of administration, and the control of irregularities.

The development of publications per year reveals that role administration has been a vivid research field since 1996. Aside from the six publications in the year 1997, the amount of publications remained at a quite constant level until 2001. Afterward, the paper count increased, eventually as a result of the high number of published role models to which researchers responded with administration concepts. 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. Additionally, in the course of the growing importance of RBAC the general increase of output in this area is not surprising. In the following, three models that matured in the area of role administration are briefly presented.

6.1.2.1. Role-graph models. The first administrative research work roots in the *early RBAC* efforts (Section 2.1). Nyanchama and Osborn (1996) investigated the integration of information flow control into the administration mechanisms of role systems and later used graph theory in order to model role relations. Several other authors also base their work on the graph-based approach. Browse the literature database[19] for *role graph* to retrieve a list of the (currently 58) publications dealing with the mentioned issues. Alternatively, browse the class *Role Administration* in the database.

6.1.2.2. ARBAC models. The first ARBAC[20] model was introduced in 1997 by Sandhu et al. (1997) and refined in 1999, introducing the concept of mobile and non-mobile users

[18] Those models were published in 1996, even though the workshop took place in 1995.

[19] http://www-ifsresearch.wiwi.uni-regensburg.de/Roles.

[20] Administrative Role-Based Access Control 1997.

Table 4 – Composition of publications with *Theoretical Focus*.

Theoretical focus	'96	'97	'98	'99	'00	'01	'02	'03	'04	'05	'06	'07	'08	'09	'10	∑
Role model and design	8	12	9	10	12	22	22	40	32	42	57	47	49	59	47	468
Role development	1	2	1	–	3	1	3	5	3	3	1	3	10	11	16	63
Roles and standards	–	–	–	–	2	1	–	–	1	–	1	2	1	–	–	8
Roles and other AC technologies	2	2	2	1	1	1	–	–	1	–	–	3	3	3	1	20
Roles and other security techn.	–	–	–	2	5	2	11	11	13	12	17	11	16	17	12	129
Review and meta-analysis	4	1	1	–	1	2	1	1	1	–	–	–	3	1	–	16
∑	8	17	13	13	24	29	37	57	51	57	76	66	82	91	76	704

(Sandhu and Munawer, 1999). In a consecutive step the ARBAC02[21] model was proposed (Oh and Sandhu, 2002), moving the user/permission pool from role hierarchy to organizational structure. Zhang and Joshi (2007a) recognized the need for an adaptation of the ARBAC family for the use of hybrid role hierarchies in their so called ARBAC07 model.

6.1.2.3. Crampton–Louizou Model (SARBAC). In Crampton and Loizou (2002), they defined the RHA[22] or SARBAC[23] model. In this model every role has an administrative scope, which defines the set of roles that can be modified. The administrative model for role hierarchy in the Crampton–Loizou model has been refined and improved in (Crampton, 2005). The work of Zhang and Joshi (2007b) 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.

6.1.3. *Focusing on constraints, formalization, delegation and hierarchies*

The last four sub-areas are concentrating on specific aspects of *Role Model and Design*. They comprise publications that analyze specific role (administration) model 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 sub-area 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) has traditionally been investigated. In its simplest form, the principle states that a sensitive task should be performed by two different users acting in cooperation. The last sub-area *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.

Note that these sub-areas include many publications dealing with RBAC policies (browse the database for *policy* and *policies*) as RBAC policies mainly are concerned with the expression of restrictions on the relationships between role system elements.

Investigating the specialized research areas, one can see that the interest in delegation did not start before the year 2000. The related publications deal with the modeling and verification of delegation policies as well as conflict detection and the application of delegation in the various role models. *Constraints* have been dealt with extensively throughout 65 publications since 1996. Authors investigated constraint modeling and enforcement as well as the application of constraints on role system elements depending on the used role model (e.g., for workflow or temporal-based role systems). Similarly, several authors focused on the investigation of role hierarchies, dealing with the inclusion of hybrid, temporal or multiple hierarchies into role (administration) models. Finally, 48 publications dealt with the formalization of role models. This includes formal languages for expressing RBAC models and entities as well as their relationships.

6.2. *Roles and other security technologies*

With the increasing relevance of RBAC in both research and applied 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. Research in this field started in 1999 with a growing interest since then. 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 analyzing open theoretical issues takes place. Due to the number of publications a 3rd level classification was necessary (see Table 6). The fields of interest include the usage of roles in combination with cryptography, information flow control, trust mechanisms, UML[24] (-Security) and XML (-Security) dialects.

Research in those areas did not start before the year 1999. After an early phase until 2002 an increased need for adapting role theory in different technologies can be noticed, probably stemming from the ongoing standardization process. Overall, the research area can be considered stable since 2002 with in between 11 and 17 publications provided per year with a peak in 2008 and 2009. The five sub-areas are equally important in terms of the number of related publications. While cryptographic- as well as UML-related issues

[21] Administrative Role-Based Access Control 2002.
[22] Role Hierarchy Administration.
[23] Scoped Administrative Role-Based Access Control.
[24] Unified Modeling Language.

Table 5 – Composition of *Role Model and Design*.

Role model and design	'96	'97	'98	'99	'00	'01	'02	'03	'04	'05	'06	'07	'08	'09	'10	∑
Role models	5	2	2	1	3	9	8	10	11	15	18	19	18	24	20	165
Role administration	2	6	3	5	3	4	6	12	8	13	16	10	9	11	12	120
Constraints	1	2	1	2	2	5	1	8	4	5	6	8	8	8	4	65
Formalization	–	1	–	1	1	1	4	3	3	3	7	5	6	8	5	48
Delegation	–	–	–	–	3	2	1	5	6	3	7	3	3	4	3	40
Hierarchies	–	1	3	1	–	1	2	2	–	3	3	2	5	4	3	30
∑	8	12	9	10	12	22	22	40	32	42	57	47	49	59	47	468

have been investigated mainly in between 2002 and 2007, lately, investigating issues and relationship between trust management and the role concept became more and more popular. Additionally, the investigation of XML-related issues experienced a significant increase of interest in since 2003. Most publications deal with the relationship between and the expression of the role concept in XACML.[25] At that time, Wang and Osborn (2004), for instance, proposed a role-based approach to access control for XML databases at the SACMAT conference in 2004.

6.3. *Role development*

Before the benefit of a role system can be realized the initial task is the definition of valid roles. In the course of an increasing importance of RBAC the topic attracted more attention of scientists. Publications assigned to this research field provide a structured approach for the definition of roles or investigate mechanisms used to address related issues. A total of 63 publications dealing with role development issues have been identified. The field initially was dominated by *Role Engineering* techniques. 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. *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. Role Mining has gathered importance from 2005 on, after Kuhlmann et al. (2003) were the first to link role development with Data Mining in 2003. Several algorithms for role mining, for instance the FastMiner family (Vaidya et al., 2006), have been proposed since then. Currently there is an integration trend stating that only a *hybrid* combination of engineering and mining techniques results in a well-defined role catalog.

Due to industry's interest in fast and automated role system deployment in combination with the integration of business knowledge, the area has gained importance over the last years (see Table 7). Since 2008, the first concepts for hybrid role development have been proposed, e.g., by Fuchs et al. (Fuchs and Pernul, 2008). The field has been integrated as a separate research area as 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. Looking at the sub-areas one can see, that Role Mining experienced a significant interest since the year 2008 and has since then evolved to one of the most vivid research areas investigated. 29 out of 37 role development publications since 2008 deal with Role Mining issues.

[25] eXtensible Access Control Markup Language.

6.4. *Further theoretical research areas*

In the following the remaining three smaller research areas dealing with the standardization of the role concepts, with roles and their relationship to other existing AC technologies as well as review and meta analysis issues are presented briefly.

6.4.1. *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.

6.4.2. *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. Scientists were interested in this area in the early years of role theory research and there are no more publications after 2006. Recently, discussion on the relationships between RBAC and information flow models like the Bell-LaPadula model has revived.

6.4.3. *Review and meta-analysis*

The review and meta-analysis publications define the final research field within the section of theoretical research work. As Section 2.2 already provided a detailed insight, no additional investigation is carried out at this point. 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.

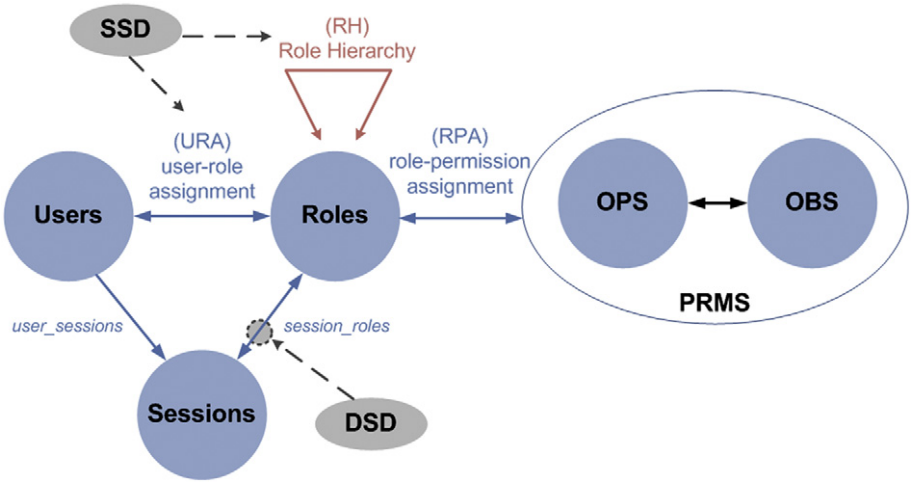

Fig. 8 – Consolidated RBAC model – drawing based on (Sandhu et al., 1996).

7. Publications with applied focus

After research with theoretical focus was investigated in the previous section, the aim of this section is to explore the identified research areas exhibiting an applied affiliation. The overall development of research with applied focus along a time line is shown in Fig. 9. It 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 up to 29 in 1999. After a rather stable period a significant increase of scientific output after the year 2002 can be noticed. This growth can be related to the growth of the overall research area and the initiation and development of the standardization processes. As more theoretical concepts were provided new possibilities for practical adoption were given. However, in contrast to the research output in the main theoretical areas like *Role Models and Design* or *Role Administration*, the number of publications with an applied focus has been constantly growing since 2005. This development might be explained with the increasing spreading and adoption of RBAC in the organizational context.

As already mentioned in Section 5, publications with an applied affiliation can be differentiated according to their either technology-specific (*Roles in Technology*) or industry-specific focus (*Roles in Industry*). Note that technology-specific adoption of theoretical findings 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.

The composition of the research area is presented in Table 8. 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. During the last years the number of both *Technology*-specific and *Industry*-specific publications rose considerably, e.g., for about 20% from 69 to 83 publications in between 2009 and 2010. Analyzing the overall amount of publications, a discrepancy between both sub-areas can be identified. 547 of 645 papers inside this research area were published with the primary focus on combining the RBAC concept and different technologies. In contrast, only few papers dealt with the adoption 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. In the context of roles and the healthcare industry, for instance, the number of publications rose significantly over the last two years. 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.

7.1. *Role-based security in technology*

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

Table 6 – Composition of *Roles and other Security Technologies*.

Roles and other security technologies	'96	'97	'98	'99	'00	'01	'02	'03	'04	'05	'06	'07	'08	'09	'10	∑
Cryptography	–	–	–	1	2	1	5	3	2	4	6	3	1	–	2	30
Information flow	–	–	–	–	–	1	3	2	2	1	2	4	4	2	2	23
XML-security	–	–	–	–	1	–	1	5	5	–	2	–	1	8	3	26
Trust	–	–	–	–	–	–	1	1	1	1	4	3	8	5	5	29
UML	–	–	–	1	2	–	1	–	3	6	3	1	2	2	–	21
∑	–	–	–	2	5	2	11	11	13	12	17	11	16	17	12	129

Table 7 – Composition of *Role Development*.

Role development	'96	'97	'98	'99	'00	'01	'02	'03	'04	'05	'06	'07	'08	'09	'10	∑
Role engineering	1	2	1	–	3	1	3	4	3	2	–	1	1	2	1	25
Role mining	–	–	–	–	–	–	–	1	–	1	1	2	8	8	13	34
Hybrid	–	–	–	–	–	–	–	–	–	–	–	–	1	1	2	4
∑	1	2	1	–	3	1	3	5	3	3	1	3	10	11	16	63

database management systems. Since then it has spread over different kinds of information technologies. Two phases of development in this research area can be identified. An average of about 20 publications per year can be noticed between 1996 and 2002. After 2002, a significant increase of scientific output took place. About 40 or more contributions yearly underline the ongoing diffusion of role theory in applied scenarios. Based on the RBAC standardization process, this development shows that the usage of the role concept bears potential for improving other software-based technologies. Above all, the rapid development of online technologies and inter- as well as intra-organizational networks might be the main reason for this development. Furthermore, current trends, for instance in respect to cloud computing, influence the development of the area.

The composition underlines the diversity of research in the area: Eight different sub-areas can be identified. On the one hand traditional fields like *Operating Systems* (16) or *Databases* (34) are settled and well-established. On the other hand a rapid increase in scientific output in larger areas like *Network* (78), *Web* (80), or *Middleware Architectures for Enterprise Security Management* (74) can be noticed. Additional research areas like *Workflow* (64), *Collaborative Environments* (77) and *System Modeling and Programming* (93) complete the technology-specific research activities. Compared to theoretical research there is no significant difference between the sub-areas in terms of quantitative research output.

7.1.1. *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. Many of the publications were proposed in the early years of the period under review. In 1996, Epstein and Sandhu (1996) explicitly dealt with roles in operating systems. In 1997, the commercial DG/UX B2[26] operating system is mapped into a simple RBAC emulation (Meyers, 1997). In 1998, Sandhu and Ahn (1998) dealt with the UNIX group mechanism and proposed two extensions. Several other articles (8) were published in between 2004 and 2008. 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).

7.1.2. *Roles in databases*

The second traditional research field that adopted 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, Essmayr et al. (1995) studied RBAC in the context of federated database systems.

The amount of scientific publications per year remained relatively constant on a low level between 1 and 4 with the exception of 2000. In 1996, for instance, the implementation of fine-grained privileges, role definitions and management in order to control access to both database objects and executable application programs was described in (Notargiacomo, 1996). More recently, intrusion detection mechanisms gained importance in this specific sub-area. Bertino et al. (2005), e.g., developed a solution for the detection of intruders in RBAC database systems in 2005 while Kamra et al. (2008) provided an approach for detecting anomalous access patterns in relational databases in 2008.

Note that due to the importance of databases the usage of roles in these environments plays a part in many of the papers that are investigated throughout this survey. Many of them use database-related knowledge for their research purpose while being allocated to other research areas (i.e. their main focus). This area, however, only consists of publications exclusively dealing with roles in databases.

7.1.3. *Roles in networks*

A network environment in general is a collection of computers connected to each other. The Open Systems Interconnection Reference Model[27] served as a theoretical basis for the classification decision. In its most basic form, it divided 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* or *Grid and Cloud Environments* are defined as a separate research area. Roles in Networks deal with the file-sharing technology NFS,[28] wireless networks or usage of roles in Peer-to-Peer (P2P) networks.

The amount of publications remained on a low and constant level between 1997 and 2002. In the years after 2002, it rapidly increased and stabilized on a new level of about 10 publications per year. This development is not surprising, taking the growing importance of computer networks for society and organizations into consideration.

[26] Data General UNIX.

[27] TCP/IP Distributed System, Vivek Acharya, Laxmi Publications, ISBN 8170089328, 2006.

[28] Network File System.

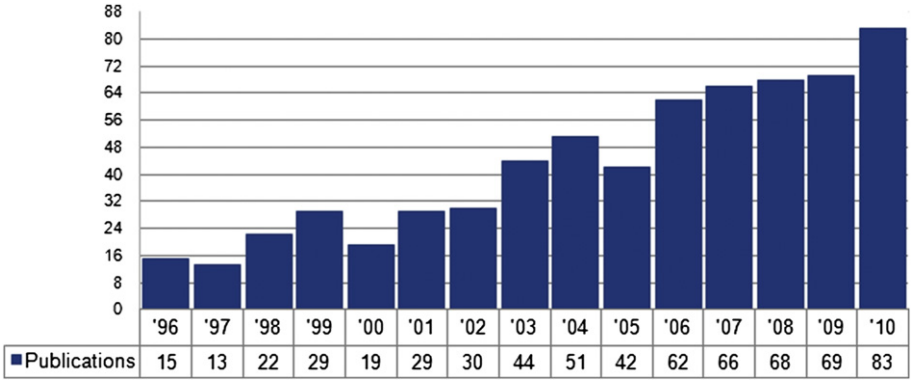

Fig. 9 – Publications dealing with *Publications with Applied Focus*.

Access control based on users' roles significantly has 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 wireless network environments even more pushed scientific output in this research area. In 2003, for example, Park et al. presented contributions for wireless privilege management infrastructures in order to support authorization service for authorized users in wireless environments (Park and Lee, 2003). In 2006, 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. Concerning P2P networks, an approach for implementing RBAC security paradigm in a P2P system is, amongst others, provided by Mathur et al. (2006).

7.1.4. *Roles in the web*

The research area *Roles in the Web* includes contributions that investigate the use of roles for the purpose of securing web technologies such as web servers, web services, and web applications. Furthermore, 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. Additionally, a number of authors dealt with the integration of role concepts in web services.

The amount of publications experienced a relatively constant growth between the years 1997 and 2008. The work of Barkley et al. (1997) is an early example of publications dealing with modeling roles in web environment for the purpose of access control. 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. Investigating the focus of current publications shows that the area is currently dominated by the combination of modern web service technologies with the role concept. Service-oriented architectures are investigated for integrating elements of the role concept. Besides other authors, Sun et al. (2010), for instance, recently provided a conceptual Model for Managing Service-Oriented Authorization.

Note that there is a close content-specific relationship with the areas *Roles in Networks* and *Roles in Grid and Cloud Environments*. This might be the reason for the decline of publications in 2010 as at the same time the number of cloud computing-related publications rose.

7.1.5. *Roles in workflows*

Workflow management systems are computerized systems which support, coordinate and streamline the business processes in various application domains in different industries. Similar to other research areas, role theory is facilitated for security administration in workflow management systems.

Research in this area did start in 1997. Bertino et al. (1997) for instance, presented an approach for defining constraints on role assignment and on user assignment to tasks in a workflow. Starting in the year 2004, an increase of scientific output can be noticed. Sun et al. (2005), for instance, 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.

With BPEL[29] becoming the standard for specifying and executing workflow specifications for web service composition, Xiangpeng et al. (2006) used the concept of RBAC for securing workflow requirements. In 2007, Wainer et al. (2007) showed how delegation can be introduced in a workflow system. Another peak level was reached in 2009 (12 publications) when several new concepts for access control models in workflows were proposed.

7.1.6. *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. Moreover, articles dealing with document sharing, group communication or some other kind of collaborative characteristics are also allocated to this area. Note that some authors define workflow environments as an element of collaborative systems. However, due to the number of publications explicitly focusing on each of those two areas, they have been kept separate for this survey.

[29] Business Process Execution Language.

Table 8 – Composition of Publications with *Applied Focus*.

Applied focus	'96	'97	'98	'99	'00	'01	'02	'03	'04	'05	'06	'07	'08	'09	'10	∑
Technology	15	13	17	25	15	24	24	36	47	38	56	60	59	55	60	544
Industry	–	–	5	4	4	5	6	8	4	4	6	6	9	14	23	98
∑	15	13	22	29	19	29	30	44	51	42	62	66	68	69	83	642

After an initial period with less than five publications per year until 2003 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 and 2009. This underlines the close relationship between those research areas. In 2007, Ahmed and Tripathi (2007), for instance, focused on the goal of creating a programming framework for developing secure distributed CSCW systems. Later, Liu and Huang (2009), investigated the application of RBAC in Distributed Cooperation Environments.

7.1.7. *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. Hence, dependency of applications and authentication of users are significant. In this context the role concept is integrated in order to secure middleware software and architectures.

Several peak phases of the development of this research area can be identified (e.g., 1999, 2003, or 2007). The first publications are dealing with roles in the field of the security service of CORBA.[30] Beznosov and Deng (1999) proposed a related approach for implementing the role concept into the access control mechanism. Identity Management as part of ESM, as one driver for this area, has been a field of emerging interest from 2006 on, dealing with the management and administration of user data. 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. The tendency for implementing organization-wide user management infrastructures requires the development and enforcement of role-based security policies. This might be one reason for the peak in 2007. Another research topic of interest during the last years is Java EE[31] as 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. 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.

7.1.8. *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 as well as quality- and documentation-management. Until the year 2005 a constant research output on a low level can be experienced. In the year 2000, Shin and Ahn (2000) provided a UML representation of RBAC to meet specific security needs of system development requirements. Above all around the year 2006 and 2010 a peak of researchers' interest can be noticed. In 2006, authors investigated the usage of the security architecture JDOSecure for introducing Role-Based permissions to JDO[32]-Based application (e.g., (Merz and Aleksy, 2006)). In 2010, Zarnett et al. (2010) proposed an approach for RBAC in Java via proxy objects using annotations. However, it is surprising that in 2007 the output decreased sharply. The development exhibits a quite fluctuating behavior, thus it cannot be deduced that the trend of 2010 is going to continue in 2011.

7.1.9. *Roles in grid and cloud environments*

Lately, researchers also dealt with integrating roles in grid and cloud computing. Grid computing or the use of a computational grid is the application of several computers cooperating together to solve a single problem. With the development of grid computing systems, secure resource-sharing has become more and more important from 2004 on. Investigating the development of this sub-area, it can be seen that a constant growth during the last years took place. Similar to the field of role mining this area is one of the most vivid research fields surveyed.

Since 2009 a trend toward cloud computing has influenced the efforts of researchers in the field. The first publications investigating potential usage of the role concept in cloud-based environments are provided, amongst others, by Huang et al. (2009). In the near future this trend is going to continue with even more publications focusing on the integration of different aspects of the role concept into cloud computing. Additionally, publications are going to appear at conferences not yet included in the investigation, again underlining a further spreading of the research area and dissemination of research results.

7.2. *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. 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 in form of case studies or reports.

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

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

[32] Java Data Objects.

Table 9 – Composition of *Roles in Technology*.

Roles in technology	'96	'97	'98	'99	'00	'01	'02	'03	'04	'05	'06	'07	'08	'09	'10	∑
Operating system	1	3	2	1	–	–	–	–	1	1	1	3	2	–	1	16
Database	4	1	3	2	–	2	2	3	1	3	2	1	4	2	4	34
Web	–	4	2	4	2	6	4	6	5	8	7	9	8	9	6	80
Network	–	1	1	2	1	2	2	7	10	5	10	11	11	6	9	78
Workflow	–	1	–	3	2	1	1	3	9	5	6	9	6	12	6	64
Collaborative environment	2	1	3	4	–	5	5	5	9	7	4	9	9	10	4	77
Middleware Architectures, for ESM	4	1	1	5	5	2	5	8	7	2	8	10	7	4	5	74
System modeling and programming	4	1	5	4	5	6	5	4	4	4	15	3	9	7	17	93
Grid and cloud environments	–	–	–	–	–	–	–	–	1	3	3	5	3	5	8	28
∑	15	13	17	25	15	24	24	36	47	38	56	60	59	55	60	544

It has already been shown earlier, that the scientific output (98 publications) in this area is small compared to the publications dealing with the usage of roles in technology (544 publications). Research did not start until 1998. Afterward, two stages of development can be identified. At first the publication count was slowly increasing on a low level between 1999 and 2003. One reason might be the refusal of organizations to publish best practices and provide insights into their user administration techniques. During a second stage of development a steady rise of the amount of publications from 2005 on can be noticed. Above all in the healthcare environment legislative restrictions as well as best practices led to a further adoption of role theory and thus to an increasing number of publications. This development cumulated in the years 2009 and 2010 when a growth of about 55% (2008–2009) and 64% (2009–2010) was experienced (Table 9).

The composition of the research area is shown in Table 10. The major number of papers concerning this research area was published in the health care sector (50). E-Commerce and other industries rank second with 15 publications each. The amount of the sub-areas Education (12) is at a similar level. The output concerning Finance is low (6 publications), potentially due to the reluctance of companies in publishing potentially security-related insights or case studies. As a result of its importance only the health care sector is investigated in detail in the following.

7.2.1. *Roles in health care environment*

Health care systems have proven to be one of the main adoption areas of the role concept. Due to the high security requirements, information technology plays a decisive role not only to increase the efficiency of health care institutions, but also to ensure secure information processing. Research is thus focusing on the realization of complex, sometimes cooperating structures across federated systems of different types of health care providers.

Looking at the development of publications, it can be detected that only two papers have been identified from 1996 to 2000. Mainly driven by regulations of the health care sector (e.g., HIPAA[33]) the amount of publications rose steadily after 2005, reaching new heights in 2010 with 12 publications. In 2009 and 2010, authors investigated the integration of roles in workflow-based, mobile and collaborative health care environments (e.g., Berhe et al., 2009; Steele and Min, 2010).

[33] Health Insurance Portability and Accountability Act.

8. Outlook and future considerations

In this section we give the authors' personal perspective on the principal insights of this study and speculate on the future of RBAC and Information Security research. Fig. 4 gives a compelling visualization of the development of RBAC research. As discussed earlier the 1996 spurt is attributable to the 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. 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 Information Security.

Turning to Table 2 we see that the *ACM Workshop on Role-Based Access Control* series and its successor the *ACM Symposium on Access Control Models and Technologies* series together account for over 12% of the research publications on RBAC. This suggests that the 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 it 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 role-related publications perhaps reflecting their more theoretical emphasis. It is our conjecture that the CCS and S&P papers have likely been less influential with respect to roles in Information Security 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 the 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

Table 10 – Composition of *Roles in Industry*.

Roles in industry	'96	'97	'98	'99	'00	'01	'02	'03	'04	'05	'06	'07	'08	'09	'10	∑
Health care	–	–	1	1	–	2	2	5	3	2	5	5	7	5	12	50
E-commerce	–	–	2	1	2	1	2	1	–	1	–	1	–	1	3	15
Finance	–	–	–	–	2	1	1	1	–	–	–	–	–	1	–	6
Education	–	–	–	2	–	1	1	1	–	1	–	–	1	3	2	12
Other industries	–	–	2	–	–	–	–	–	1	–	1	–	1	4	6	15
∑	–	–	5	4	4	5	6	8	4	4	6	6	9	14	23	98

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 Information Security. Through facilitating the RBAC concept in various practical fields, new research work has been inspired. Practical usage of role models, e.g., has led to the development of new extended role models.

A major result of this paper is the three level classification of RBAC literature shown in Fig. 6. This was developed using the methodology reported in this paper and the classification itself has been discussed at length earlier. 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 applied 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 the 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 Information 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 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 Fig. 6 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 a deep consideration of the underlying application whereas role–permission requires such a 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 both (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).

9. Conclusion

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 limitations of traditional access control have already led to ground breaking models such as Usage Control (Park and Sandhu, 2004; 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.

Acknowledgment

The work carried out in this paper would not have been possible without the help of our students at the University of Regensburg: Manfred Ferstl, Klaus Meisl, Sebastian Herbst and Victor Rebhan. The automated publication identification was supported by their efforts. The work of Ravi Sandhu is partially supported by grants from the State of Texas, NSF and AFOSR.

Electronic bibliography and extended version

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

REFERENCES

Ahmed T, Tripathi AR. Specification and verification of security requirements in a programming model for decentralized CSCW systems. ACM Transactions on Information and System Security (TISSEC) 2007;10:2.

ANSI/INCITS. ANSI INCITS 359–2004, American National Standard for Information Technology – role based access control. American National Standards Institute; 2004.

Barkley JF, Cincotta AV, Ferraiolo DF, Gavrila S, Kuhn DR. Role based access control for the world wide web. In: Proceedings of the 20th NIST-NCSC National Information Systems Security Conference, 1997. pp. 331–340.

Berhe S, Demurjian SA, Agresta T. Emerging trends in health care delivery: towards collaborative security for NIST RBAC. In: Proceedings of the 23rd Annual IFIP WG 113 Working Conference on Data and Applications Security. Springer; 2009. p. 283–90.

Bertino E. RBAC models – concepts and trends. Computers & Security 2003;22:511–4.

Bertino E, Bonatti PA, Ferrari E. TRBAC: a temporal role-based access control model. ACM Transactions on Information and System Security (TISSEC) 2001;4:191–233.

Bertino E, Ferrari E, Atluri V. A flexible model supporting the specification and enforcement of role-based authorization in workflow management systems. In: RBAC'97: Proceedings of the 2nd ACM Workshop on Role-based Access Control. ACM Press; 1997. p. 1–12.

Bertino E, Kamra A, Terzi E, Vakali A. Intrusion detection in RBAC-administered databases. In: ACSAC'05: Proceedings of the 21th Annual Computer Security Applications Conference. 2005. pp. 170–182.

Beznosov K, Deng Y. A framework for implementing role-based access control using CORBA security service. In: RBAC'99: Proceedings of the 4th ACM Workshop on Role-based Access Control. ACM Press; 1999. p. 19–30.

Biddle BJ. Recent developments in role theory. Annual Review of Sociology 1986;12:67–92.

Coyne EJ, Davis JM. Role engineering for enterprise security management. 1st ed. Boston, MA, USA: Artech House; 2007.

Crampton J. Understanding and developing role-based administrative models. In: CCS'05: Proceedings of the ACM Conference on Computer and Communications Security. ACM Press; 2005. p. 158–67.

Crampton J, Loizou G. Administrative scope and role hierarchy operations. In: SACMAT '02: Proceedings of the 7th ACM Symposium on Access Control Models and Technologies. ACM Press; 2002. p. 145–54.

Epstein J, Sandhu R. NetWare 4 as an example of role-based access control. In: RBAC'95: Proceedings of the 1st ACM Workshop on Role-based Access Control. ACM Press; 1996. p. 18.

Essmayr W, Kastner F, Pernul G, Tjoa AM. The security architecture of IRO-DB. In: Proceedings of the 12th IFIP International Conference on Information Security. 1995. pp. 249–258.

Essmayr W, Probst S, Weippl E. Role-based access controls: status, dissemination, and prospects for generic security mechanisms. Electronic Commerce Research 2004;4:127–56.

Ferraiolo D, Kuhn R. Role-based access control. In: Proceedings of the 15th NIST-NCSC National Computer Security Conference, 1992. pp. 554–563.

Ferraiolo D, Kuhn R, Chandramouli R. Role-based access control. 2nd ed. Boston, MA, USA: Artech House; 2007.

Ferraiolo DF. An argument for the role-based access control model. In: SACMAT'01: Proceedings of the 6th ACM Symposium on Access Control Models and Technologies. ACM Press; 2001. p. 142–3.

Ferraiolo DF, Cugini JA, Kuhn DR. Role-based access control: features and motivations. In: ACSAC'95: Proceedings of the 11th Annual Computer Security Applications Conference, 1995.

Ferraiolo DF, Kuhn DR. Future directions in role-based access control. In: RBAC'95: Proceedings of the 1st ACM Workshop on Role-based Access Control. ACM Press; 1996. p. 8.

Ferraiolo DF, Sandhu R, Gavrila S, Kuhn DR, Chandramouli R. Proposed NIST standard for role-based access control. ACM Transactions on Information and System Security (TISSEC) 2001;4:224–74.

Fuchs L, Broser C, Pernul G. Different approaches to in-house identity management – pros and cons and the justification of an assumption. In: ARES'09: Proceedings of the 4th International Conference on Availability, Reliability and Security. IEEE Computer Society; 2009.

Fuchs L, Meier S. The role mining process model – underlining the need for a comprehensive research perspective. In: ARES'11: Proceedings of the 6th International Conference on Availability, Reliability and Security. IEEE Computer Society; 2011.

Fuchs L, Pernul G. HyDRo: hybrid development of roles. In: ICISS'08: Proceedings of the 4th International Conference on Information Systems Security. Springer; 2008. p. 287–302.

Fuchs L, Preis A. 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, 2008. pp. 128–138.

Gallaher MP, ÓConnor AC, Kropp B. The economic impact of role-based access control. Gaithersburg, MD, USA: National Institute of Standards and Technology; 2002.

Galletta DF, Heckman R. A role theory perspective on end-user development. Information Systems Research 1990;1:168–87.

Giuri L. Role-based access control: a natural approach. In: RBAC'95: Proceedings of the 1st ACM Workshop on Role-based Access Control. ACM Press; 1996. p. 13.

Heckman R, Galletta DF. Changing roles in information systems: a role theory perspective. In: ICIS'88: Proceedings of the 9th International Conference on Information Systems. 1988. pp. 265–274.

Huang X, He Y, Hou Y, Li L, Sun L, Zhang S, et al. Privacy of value-added context-aware service cloud. In: CloudCom'09: Proceedings of the 1st International Conference on Cloud Computing. Springer; 2009. p. 547–52.

Joshi J, Bertino E, Latif U, Ghafoor A. A generalized temporal role-based access control model. IEEE Transactions on Knowledge and Data Engineering 2005;17:4–23.
Kalam AAE, Benferhat S, Miege A, Baida RE, Cuppens F, Saurel C, et al. Organization-based access control. In: POLICY'03: Proceedings of the 4th IEEE International Workshop on Policies for Distributed Systems and Networks. IEEE Computer Society; 2003. p. 120.
Kamra A, Terzi E, Bertino E. Detecting anomalous access patterns in relational databases. VLDB J 2008;17:1063–77.
Kuhlmann M, Shohat D, Schimpf G. Role mining – revealing business roles for security administration using data mining technology. In: SACMAT'03: Proceedings of the 8th ACM Symposium on Access Control Models and Technologies. Como, Italy: ACM Press; 2003. p. 179–86.
Linton R. The study of man. New York, NY, USA: Appleton-Century-Crofts; 1936.
Liu SL, Huang H. Role-based access control for distributed COOPERATION environment. In: CIS'09: International Conference on Computational Intelligence and Security, 2009. pp. 455–459.
Mathur A, Kim S, Stamp M. Role based access control and the JXTA peer-to-peer framework. Security and Management; 2006:390–8.
Mead GH. Mind, self and society. Chicago: University of Chicago Press; 1934.
Merz M, Aleksy M. Using JDOSecure to introduce role-based permissions to Java data objects-based applications. In: DEXA'06: Proceedings of the 17th International Conference on Database and Expert Systems Applications. IEEE Computer Society; 2006. p. 449–58.
Meyers WJ. RBAC emulation on trusted DG/UX. RBAC'97. In: Proceedings of the 2nd ACM Workshop on Role-based Access Control. ACM Press; 1997. p. 55–60.
Moreno JL, Jennings HH. Who shall survive? Foundations of sociometry, group psychotherapy, and sociodrama. Washington, DC, USA: Nervous and Mental Disease Publishing Co.; 1934.
Naumovich G, Centonze P. Static analysis of role-based access control in J2EE applications. SIGSOFT Software Engineering Notes 2004;29:1–10.
Notargiacomo L. Role-based access control in ORACLE7 and trusted ORACLE7. In: RBAC'95: Proceedings of the 1st ACM Workshop on Role-based Access Control. ACM Press; 1996.
Nyanchama M, Osborn S. Role-based security, object oriented databases and separation of duty. SIGMOD Record 1993a;22: 45–51.
Nyanchama M, Osborn S. Role-based security: pros, cons & some research directions. ACM SIGSAC Review 1993b;2:11–7.
Nyanchama M, Osborn SL. The role graph model. In: RBAC '95: Proceedings of the 1st ACM Workshop on Role-based Access Control. ACM Press; 1996.
Oh S, Park S. 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; 2000. p. 264–73.
Oh S, Sandhu R. A model for role administration using organization structure. In: SACMAT'02: Proceedings of the 7th ACM Symposium on Access Control Models and Technologies. ACM Press; 2002. p. 155–62.
Osborn S, Sandhu R, Munawer Q. Configuring role-based access control to enforce mandatory and discretionary access control policies. ACM Transactions on Information and System Security (TISSEC) 2000;3:85–106.
Park D-G, Lee Y-R. 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; 2003. p. 84–93.
Park J, Sandhu R. The UCON_ABC usage control model. ACM Transactions on Information and System Security (TISSEC) 2004;7:128–74.
Pfleeger CP, Pfleeger SL. Security in computing. 4th ed. Upper Saddle River, NJ, USA: Prentice Hall PTR; 2006.
Pretschner A, Hilty M, Basin D. Distributed usage control. Communications of the ACM 2006;49:39–44.
Rhodes A, Caelli W. A review paper role based access control. Information Security Research Centre; 2000.
Sandhu R, Bhamidipati V. The ASCAA principles for next-generation role-based access control. In: ARES'08: Proceedings of the 3rd International Conference on Availability, Reliability and Security. 2008.
Sandhu R, Munawer Q. The ARBAC99 model for administration of roles. In: ACSAC '99: Proceedings of the 15th Annual Computer Security Applications Conference. IEEE Computer Society; 1999. p. 229.
Sandhu R, Park JS. Decentralized user-role assignment for web-based intranets. In: RBAC'98: Proceedings of the 3rd ACM Workshop on Role-based Access Control. ACM Press; 1998. p. 1–12.
Sandhu R. Role-based access control. In: Advances in computers. Academic Press; 1998. p. 238–87.
Sandhu R. Future directions in role-based access control models. In: MMM-ACNS'01: Proceedings of the International Workshop on Information Assurance in Computer Networks. Springer; 2001. p. 22–6.
Sandhu R, Ahn G-J. Decentralized group hierarchies in UNIX: an experiment and lessons learned. In: Proceedings of 21st NIST-NCSC National Information Systems Security Conference, 1998. pp. 486–502.
Sandhu R, Coyne EJ, Feinstein HL, Youman CE. Role-based access control models. IEEE Computer 1996;29:38–47.
Sandhu R, Bhamidipati V, Coyne E, Ganta S, Youman C. The ARBAC97 model for role-based administration of roles: preliminary description and outline. In: RBAC'97: Proceedings of the 2nd ACM Workshop on Role-based Access Control. ACM Press; 1997. p. 41–50.
Shin ME, Ahn G-J. UML-based representation of role-based access control. In: WETICE'00: Proceedings of the 9th IEEE International Workshops on Enabling Technologies. IEEE Computer Society; 2000. p. 195–200.
Smith C. 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; 1997.
Smith CL, Coyne EJ, Youman CE, Ganta S. A marketing survey of civil federal government organisations to determine the need for a role-based access control (RBAC) security product. Small Business Innovation Research (SBIR) for the National Institute of Standards and Technology: SETA Corporation; 1996.
Steele R, Min K. HealthPass: fine-grained access control to portable personal health records. In: AINA'10: Proceedings of the 24th IEEE International Conference on Advanced Information Networking and Applications. Perth, Australia: IEEE Computer Society; 2010. p. 1012–9.
Sun H, Zhao W, Yang JSOAC. A conceptual model for managing service-oriented authorization. In: SCC'10: Proceedings of the IEEE International Conference on Services Computing. IEEE Computer Society; 2010. p. 546–53.
Sun L, Huang G, Sun Y, Song H, Mei H. An approach for generation of J2EE access control configurations from requirements specification. In: QSIC '08: Proceedings of the 8th International Conference on Quality Software, 2008. pp. 87–96.

Sun Y, Meng X, Liu S, Pan P. Flexible workflow incorporated with RBAC CSCWD'05. In: Proceedings of the 9th International Conference on Computer supported Cooperative Work in Design, 2005. pp. 525–534.

Tomur E, Erten YM. Application of temporal and spatial role-based access control in 802.11 wireless networks. Computers & Security 2006;25:452–8.

Vaidya J, Atluri V, Warner J. RoleMiner: mining roles using subset enumeration. In: CCS'06: Proceedings of the 13th ACM Conference on Computer and Communications Security. ACM Press; 2006. p. 144–53.

Wainer J, Kumar A, Barthelmess P. DW-RBAC: a formal security model of delegation and revocation in workflow systems. Information Systems 2007;32:365–84.

Wang J, Osborn SL. A role-based approach to access control for XML databases. In: SACMAT'04: Proceedings of the 9th ACM Symposium on Access Control Models and Technologies. ACM Press; 2004. p. 70–7.

Xiangpeng Z, Cerone A, Krishnan P. Verifying BPEL workflows under authorisation constraints. Business Process Management Journal; 2006:439–44.

Zarnett J, Tripunitara MV, Lam P. Role-based access control (RBAC) in Java via proxy objects using annotations. In: SACMAT'10: Proceedings of the 15th ACM Symposium on Access Control Models and Technologies. ACM Press; 2010. p. 79–88.

Zhang Y, Joshi JBD. ARBAC07: a role-based administration model for RBAC with hybrid hierarchy. In: IRI'07: Proceedings of the IEEE International Conference on Information Reuse and Integration, 2007a. pp. 196–202.

Zhang Y, Joshi JBD. SARBAC07: a scoped administration model for RBAC with hybrid hierarchy. In: IAS '07: Proceedings of the 3rd International Symposium on Information Assurance and Security, 2007b. pp. 149–154.

Zhu H. 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; 2006.

Zhu H, Zhou M. Roles in information systems: a survey. IEEE Transactions on Systems, Man and Cybernetics Part C, Applications and Reviews 2008;38:377–96.

Ludwig Fuchs studied Business Information Systems at the University of Regensburg, Germany and completed his diploma degree in 2005. During his courses he studied at the Department of Computer Science and the Department of Management Studies at the University of York (UK). After graduation, he lectured and researched at the Department of Information Systems at the University of Regensburg with Prof. Dr. Günther Pernul and at the University of Texas in San Antonio (USA) together with Prof. Dr. Ravi Sandhu. He received his doctoral degree in 2009 (Dr. rer. pol).

Günther Pernul received both the diploma degree in 1985 and the doctorate degree in 1989 from the University of Vienna, Austria. Currently he is full professor at the Department of Information Systems at the University of Regensburg, Germany. His research interests are web-based information systems, new media, information systems security, advanced database applications, and applied cryptography. Günther Pernul is co-author of a database text book, has edited or co-edited more than ten books, published more than 100 papers in scientific journals and conference proceedings on various information systems topics and has participated in European funded research under ESPRIT, ACTS and IST frameworks.

Ravi Sandhu is Executive Director of the Institute for Cyber Security at the University of Texas at San Antonio. Previously he was on the faculty at George Mason University (1989–2007) and Ohio State University (1982–1989). He holds BTech and MTech degrees from IIT Bombay and Delhi, and MS and PhD degrees from Rutgers University. He is a Fellow of IEEE, ACM and AAAS, and has received awards from IEEE, ACM, NSA and NIST. A prolific and highly cited author, his research has been funded by NSF, NSA, NIST, DARPA, AFOSR, ONR, AFRL and private industry.