2

The Use of Business Process Models for Security Design in Organisations

R. Holbein,
S. Teufel,
K. Bauknecht
Department of Computer Science
Winterthurerstr. 190, 8057 Zurich, Switzerland
+41 - 1 - 257 43 11; {holbein, teufel, bauknecht}@ifi.unizh.ch

Abstract

This paper introduces a security design method for information exchange in organisations. The method supports security authorities in the design of individual security models. An individual security model is a fully customised specification of access control information for information exchange within a particular business environment. We introduce transaction based business process models (BPMs) and utilise these models to specify need-to-know authorisations. Therefore, we allocate information from BPMs which can be transformed to access control information and derive a specification of an organisation's individual security model. Our method provides transparency of security design because a security model is directly related to the business. Moreover, security effort and costs will be reduced because BPMs must not be specified for security reasons. BPMs are a result of management activities and therefore, existing resources from a security point of view.

Keywords

Access control, business process modelling, business transaction, need-to-know, security policy, role based access control, security design, security modelling

1 INTRODUCTION

Information security in organisations must be designed and implemented according to individual needs. Unfortunately, specifying an individual security model which is suitable for implementation with IT security mechanisms is a tremendous and extensive engineering task. Security design effort depends on the organisational environment as well as the complexity of security mechanisms which must be applied in order to implement a security policy, e.g. access control mechanisms. Specification of authorisation structures, for example, is part of security design and may require more than a year of work [Pohl et al., 1993]. We will introduce a security design method for information exchange in organisations in order to decrease the effort

S. K. Katsikas et al. (eds.), *Information Systems Security*

for individual *security design*[1]. With this method we will bridge the gap between development of powerful and complex access control mechanisms and the systematic application of these mechanisms concerning individual organisational needs [Holbein et al., 1995a]. We aim to reduce complexity and to increase transparency within the specification of individual security models [Neumann, 1992]. At the same time, a customer point of view demands for traceability concerning how access rights come into being: "It is a major defect of most current models of security, such as that of Bell and LaPadula, that while they well express (one view of) security as a matter of who can do what to whom, they are powerless to express the social procedures by which the access rules come into being and which ascribe authority and security attributes to the subjects and objects of which they treat." [Dobson, 1990, p. 164].

Several approaches concerning security design have been proposed in the past [Dobson, 1990] [Steinke et al., 1992] [Pottas et al., 1992] [Ting et al., 1992] [Martin et al., 1990]. Mostly, these approaches are directed/restricted to access controls but refer to specific organisation models that must be specified within the security design process. Such models provide an intermediary layer between real world and a security implementation [Bhaskar, 1993]. In this paper, we will introduce a method for comprehensive security design dealing with global authorisation for information exchange. We use transaction based business process models (BPM) to derive an organisation's individual security model for information exchange. Transaction based BPMs result from management activities. Therefore, these models are existing resources from a security point of view and not part of security effort. The remainder of this paper is structured as follows: In chapter 2 we introduce business process modelling with respect to security design and establish a comprehensive understanding of the principles that we will use subsequently. In chapter 3 we give an overview on the security design method. Finally, we draw some conclusions and provide an outlook for our future research.

2 BUSINESS PROCESS MODELLING

2.1 Business Processes and Security Design

Business processes take place in and between organisations. Business processes are directed to an organisation's goals and consist of well defined and coordinated business activities suitable to reach these goals. Information exchange takes place within the business activities and therefore, business processes define the context of information exchange in organisations [Abdallah et al., 1993]. "The relevance of business processes as a major asset of an enterprise is more and more accepted: business processes prescribe the way in which the resources of an enterprise are used, i.e., they describe how an enterprise will achieve its business goals." [Leymann et al., 1994, p 326].

Our basic understanding of business processes refers to principle differences of process types and process descriptions depending on the resources that are being studied. A classification was proposed by Winograd and Flores [Medina-Mora et al., 1992] and is illustrated in Figure 1: Material processes refer to the tradition of factory automation where nothing happens without physical things moving and changing state. Information processes shift to "information work" [Medina-Mora et al., 1992, p.281] and effective information processing. Finally, business processes address an important lack of the information perspective: "... information in itself is uninteresting. Information is only useful because someone can do something with it, and we

[1] The OSI Access Control Framework refers to security design as allocation of security information for an establishment of access control policy representations. It is characterised as "... an engineering design activity that necessarily precedes the other access control activities ..." [ISO, 1991, p. 6].

can't define "do something" circularly as just the handling of more information. What do people do that matters? Here we find the domain of business processes, in which people enter into language actions that have consequences for their future activities. ..." [Medina-Mora et al., 1992, p.282]. Certainly, business processes include information as well as physical processes but human interaction is of major concern regarding what happens in real world and therefore, must be taken into account for understanding business processes.

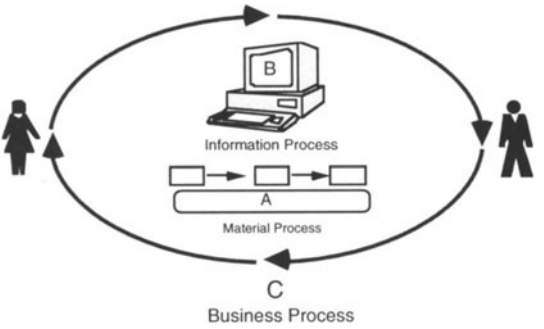

Figure 1: Process types and descriptions

Curtis et al. confirm this notion of business processes. They characterise business process modelling as [Curtis et al., 1992]: "... is distinguished from other types of modelling in computer science because many of the phenomena modelled must be enacted by a human rather than a machine..... Rather than focusing solely on the user's behaviour at the interface or the flow and transformation of data within the system, process modelling also focuses on interacting behaviours among agents, regardless of whether a computer is involved in the transaction." (p. 75).

Business process models (BPM) result from management activities where BPMs are of paramount and still increasing importance regarding strategy and business planning [Davenport, 1993]. Consequently, a BPM is a particular model of the organisation. However, it may be specified on different levels of abstraction and aggregation. Granularity of a process description depends on the purpose of the model and the complexity of agents that perform the process steps. The more knowledge about the process, the more details can be included in the process description [Curtis et al., 1992].

BPMs can be used for a number of different purposes, e.g. information system development (automation and control of business processes), analysis of process states, deadlocks, flow controls etc. [Medina-Mora et al., 1992]. Overall use ability depends on the specification method and the granularity of the process description. For example, investigations in modelling of software development processes were introduced in [Curtis et al., 1992]. The authors characterise software development processes as abstract life cycle descriptions and they define a number of different goals which can be supported by the process models: decomposition and refinement of processes in order to define detailed guidelines for software development, support of process automation to enforce process integrity rules etc.

We will utilise *BPMs for security design* concerning information exchange in organisations. As mentioned above, use ability of BPMs for different purposes depends on the specification method. Therefore, we have selected a prominent and well established approach for business process modelling so called transaction based business process modelling which is suitable to

support security design for information exchange. This approach combines issues of process and organisation with a special emphasis on interpersonal relationships of agents which are established during task fulfilment. Hence, it provides a wide range of information suitable for security design - *security information*. Consequently, our security design method is based on a process oriented view on the organisation instead of considering static organisational structures. From a security point of view BPMs are existing resources in organisations which will not be developed for security reasons but provide a security added-value. In other words, BPMs can be used as intermediary layer for security design but there is no modelling effort within security activities. Moreover, security design can be traced back to the business and may even be partially automated because a formal transformation of model attributes is possible.

In summary, BPMs are suitable to support the application of security mechanisms within security design and to increase transparency of a resulting security model. Process orientation allows to consider information flow as well as establishment of interpersonal relationships and obligations during task fulfilment for comprehensive security design.

2.2 Transaction based Business Process Modelling

A BPM is a process oriented representation of an organisation's business. We propose one central construct for business process modelling. This construct refers to a business transaction and therefore, is called a *business transaction construct* or in short transaction construct. Transaction based business process modelling is established in practice due to a number of case studies and successful applications, primarily in US companies, over the last ten years [Ferstl et al., 1993] [Medina-Mora et al., 1992] [Scherr, 1993]. The work of Winograd and Flores in the mid 80s established a theoretical basis for this approach [Winograd et al., 1986] [Winograd, 1988] [Auramaki et al., 1992].

The basic idea behind the concept of business transactions was to describe a business process as transaction(s) between organisational entities. Therefore, a business process is a single or a network of business transaction(s) which define the interactions between the participating organisational entities [Ferstl et al., 1993]. A transaction includes material and/or information exchange between the organisational entities which represent agents with a task responsibility concerning the transaction. Their tasks are directed to particular goals which are subgoals of their overall organisational goals [Davis et al., 1985]. Transaction constructs integrate all the relevant attributes of business processes consisting of business activities, course of events, organisational entities and information exchange but also represent process oriented responsibilities in organisations [Picot, 1994]. Moreover, transaction constructs include task specifications consisting of a number of business activities which build an unit that is delegated to a responsible agent. In contrast to traditional process models which are restricted to a sequential flow of material and data, transaction constructs include the real structure of business processes. Therefore, two aspects are of major concern: the people which are involved in a business transaction as well as the commitments and obligations which are established between them. Hence, transaction constructs describe the interpersonal relationships which are established within business processes.

A transaction construct represents a *customer-supplier relationship* between the two agents within the business transaction. Consequently, a business process is a network of business transactions where agents are responsible for goal oriented task fulfilment within customer-supplier relationships. Customer and supplier are represented by abstract roles describing the responsible agents. Information units which must be exchanged between the customer and the supplier are defined in terms of document types or information objects of a particular type. As these objects must not be distinguished in general, we will also interpret them as documents in

the following. Transaction constructs allow to describe complex business processes as a composition of interrelated customer-supplier transactions. This composition defines a network where the network components have identical structures regarding their *basic course of events* which corresponds to the customer-supplier transaction[2] [Medina-Mora et al., 1992] [Scherr, 1993]. This basic course of events consists of four sequential phases which can have internal iterations and include the particular material and information processes that take place within the transaction (Figure 2). The overall course of events of a business process can be refined by additional customer-supplier transactions which are related to one of the transaction phases. Relationships between a transaction and its sub-transactions can be represented by transaction links which connect particular phases of the related transactions. Different linkage types allow to differentiate between a normal and an exceptional course of events across multiple transactions.

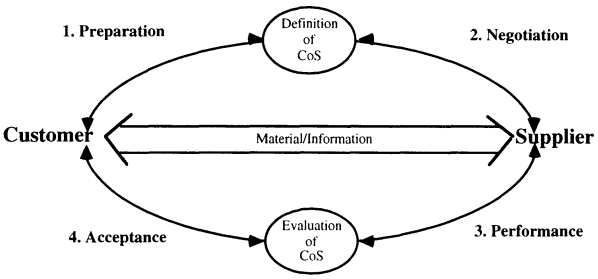

Figure 2: Customer-supplier transaction

1. Preparation: The customer or supplier proposes work to be performed by the supplier.
2. Negotiation: The customer and supplier come to an agreement about the work to be performed, i.e. make commitments about the conditions of satisfaction (CoS).
3. Performance: The supplier performs the work and reports completion.
4. Acceptance: The customer evaluates the work in terms of the CoS and declares satisfaction or declines to accept the result.

In summary, transaction constructs provide extensive information about the information exchange which is necessary to accomplish organisational tasks. This information exchange is embedded in a context of business transactions which define intended purposes for information usage within organisations. Therefore, transaction based BPMs can be used to derive security information. In the following section we will shown that this information is suitable to specify need-to-know security models for implementation with role based access control systems.

3 TRANSFORMATION OF BUSINESS PROCESS MODELS ONTO ROLE BASED ACCESS RIGHTS

The following *transformation of BPMs onto role based access rights* is an overview on a major part of the security design method. It based on the fact that transaction constructs provide extensive information to define global access rights on an abstract level. For more details on a

---

[2] More traditional approaches which are based on procedures and activities result in arbitrary structures because there is no basic course of events and activities may be combined in any way [Scherr, 1993].

formal description of this method we refer to [Holbein et al., 1995b]. In general, role based access rights define relationships between an abstract authorisation unit which represents a set of active entities within a system, a protection object and an operation that can be executed on the protection object. This is considered as discretionary 3-tuples (authorisation unit, protection object, operation). Obviously, a role based specification of authorisation units makes use of abstraction and implies mandatory properties within discretionary access rights. Authorisation units are not restricted to identities of system users, but include roles which represent sets of active entities within a system [Jonscher et al., 1993]. In the following, authorisation units will be allowed to represent any set of active entities within a system. For that reason, we introduce subject expressions in order to specify authorisation units of different type referring to single active entities as well as sets of active entities within a system. Subject expressions provide means of abstraction as well as aggregation and refer to any active entity of a system which is assigned to the abstract expression at a particular time. We even allow authorisation units to be tuples of subject expressions (combined subjects) which refer to any active entity of a system that is assigned to both abstract expressions at a particular time.

Further more, an abstract specification of access rights requires to specify sets of objects within single access rights. Hence, we will specify protection objects using protection object expressions which allow to represent object instances as well as object classes which refer to particular sets of protection objects. Additionally, operations will be represented by the name of a corresponding type of activity concerning the protection object and we extend the 3-tuple with an additional component that allows to define access conditions which must be valid for evaluation of access requests during system operation. The access right holds true for every active entity within a system which is assigned to the subject expressions at a particular time as well as every object of a system which is assigned to the protection object expression.

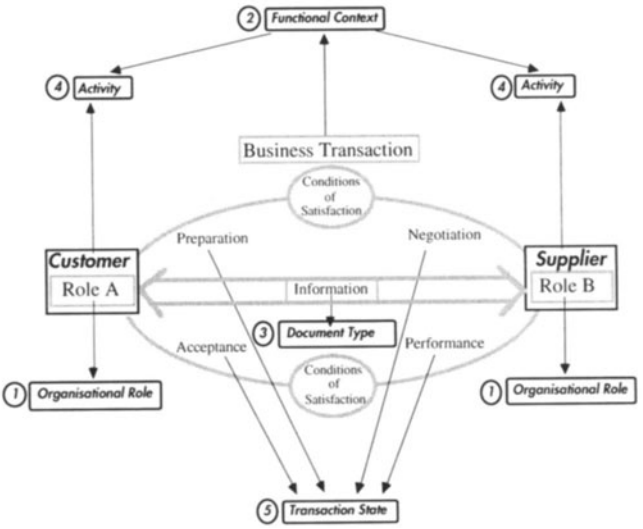

Figure 3: Transformation of attributes from a business transaction construct to a security model

In the following we explain the transformation steps which derive security information from transaction based BPMs. Figure 3 shows a transaction construct. The numbered items (1)-(5)

declare BPM information which we will now transform onto a need-to-know specification for role based access controls:

- organisational roles and functional contexts concerning business processes (1),(2),
- document types concerning information exchange within business processes (3),
- activities concerning the document types (4) and,
- transaction states as access conditions that must be valid during access control (5).

Customer and supplier within a business transaction construct represent a particular set of organisational entities which are specified by role names. These entities are responsible agents and therefore, need to have access to information objects concerning the business transaction, i.e. have a need-to-know. Further on, customer and supplier role names will be associated with different types of business transactions and therefore, describe an agent's overall context of activity within an organisation, i.e. a job type. In other words, the overall association of an organisational role with different types of business transactions defines a scope of responsibility referring to a number of tasks within an organisation. Therefore, customer and supplier roles will be transformed to *organisational roles* (1) within the need-to-know model. These roles can be used as authorisation units if overall need-to-know access rights concerning the overall associated business transactions must be specified.

For the next transformation step we refer to business transactions as an agent's context of activity from a process oriented point of view. An agent's scope of responsibility consists of tasks which are assigned to business transactions. For that reason, the agent's task related need-to-know can be specified by referring to types of business transactions. Consequently, we will use business transaction names to define roles that represent a *functional context* (2) within need-to-know modelling. These roles are suitable to specify task related need-to-know access rights concerning types of business transactions. The final step in defining subject expressions consists of combining the previous ones according to business transaction constructs. The result is called combined subject expression and consists of an organisational and a functional role part according to their combination within business transaction constructs.

For further transformation of model attributes we consider the information which agents exchange during a business transaction. Information units are explicitly specified within transaction constructs as part of the agents' task descriptions. Agents of a business transaction communicate these information units as sender-initiated information exchange. Additionally, information units for receiver-initiated information exchange across business transactions or even across business processes (e.g. information retrieval: access to a shared databases) are specified as part of the agents' task descriptions. Hence, these information units will be defined as protection objects. For an abstract specification, the information units are represented by *document types* which define a classification scheme for protection object instances (3). Consequently, document types define the protection object classes concerning a business transaction construct, e.g. a class Contract.

A business transaction construct refers to two agents. These agents are responsible for different tasks within the business transaction. With respect to business transactions, the agents' task responsibilities also define process responsibilities in an organisation [Picot, 1994]. A description of the agents' task fulfilment consists of business transaction activities. These *activities* (4) specify operations concerning objects that will be necessary to accomplish the tasks. Again, it is important to note, that transaction based BPMs are not restricted to information processes. Hence, activities may concern every kind of object even physical ones. Nonetheless, for IT security reasons we will focus on activities concerning information objects. These activities define the document processing operations that must be performed. From an object oriented point of view we will consider these operations as the interface description of an

object model for document processing [Bever et al., 1988]. In general, activities of agents will be directed to an organisation's goals. Therefore, we do not aim to define a generic document processing model because it must be individual and depends on document types and operations which exist within a particular environment [Woo et al., 1985]. Nonetheless, a document processing model will be partially included within BPMs due to the association of objects and activities within business transaction activities. For that reason, the transformation of model attributes will result in a specification of access rights which reflect parts of such a model though, a complete object model for document processing including a hierarchy of object classes will not be provided.

Finally, we will use *transaction states* (5) to define conditions (restrictions) that can be assigned to access rights and must be valid during their evaluation. Up to now, we have defined authorisation units with respect to the agents' scope of responsibility (organisational role) as well as their different tasks concerning business transactions (functional contexts). This task related specification of authorisation units can be refined within access rights by additional access conditions which are specified in terms of logical expressions. If a detailed task specification is available, it will be possible to specify access conditions where single activities are directly associated with transaction states or even the content or processing state of the documents involved. It is important to note that relationships between activities and transaction states allow a more accurate specification of an agent's need-to-know.

Now, we can define need-to-know access rights using the components which have been defined during the previous transformation steps, i.e. we define who needs what kind of access to which information object for what purpose. We use the *organisational role* and *functional context* definitions as subject expressions which represent abstract authorisation units referring to the access context of active entities within a system. A combination of an organisational role and a functional context is necessary to represent the agents' task related context within business transactions, i.e. who and what purpose. Therefore, we combine the corresponding subject expressions with respect to our previous definition of combined subject expressions. The further components of need-to-know access rights will be *document types* which define protection object classes, i.e. which information. *Activities* concerning document processing define what kind of operation and *transaction states* define access conditions.

Up to now, we have specified need-to-know access rights according to business transaction activities independent from the BPM in which these business transaction activities occur. Usually, a BPM consists of more than one business transaction construct and there may be multiple BPM including the same business transaction constructs, i.e. the same types of business transactions. In this case, business process names which refer to the type of business process as a whole, i.e. the name of the core transaction, can be used within access conditions for further refinement of a process related need-to-know. In general, these logical expressions are means for refinement of access conditions according to individual constraints.

4 Conclusion and Further Work

In this paper we have briefly introduced a security design method for information exchange. The overall goal of this approach is to support security authorities in the design of need-to-know security models and therefore, to reduce an organisation's security related effort. Our method is founded on transaction based business process models that can be transformed onto individual security models which specify the need-to-know of agents within business processes. Transaction based BPMs are suitable to reduce security design effort because these models are existing resources from a security point of view. Transparency of the security

design process results from the direct relationship between a security model and the BPMs of an organisation. Moreover, security design is more efficient and bridges the gap between development of complex security mechanisms and customisation of such mechanisms for individual application in a business environment.

Actually, we are evaluating the security design method within case studies and we are working on a prototype implementation of a security design environment with automated transformation of BPMs onto access controls. This prototype will be implemented with Ingres Windows4GL™. Based on the ActionWorkflow™ business process modelling tools from ActionTechnologies we automatically transform model attributes to a need-to-know security model for implementation with Argos role based access control mechanisms [Jonscher et al., 1993] [Holbein et al., 1995a].

References

Abdallah T. S., Holbein R., Scheidegger P., Schmidt S. (1993): Offene Bürokommunikation - Inner- und zwischenbetrieblicher Informationsaustausch, Institut für Informatik, Universität Zürich, Technical Report, no. 93.33.

Auramaki E., Hirschheim R., Lyytinen K. (1992): "Modelling offices through discourse analysis: the SAMPO approach", Computer Journal, vol. 35, no. 4, pp. 342-352.

Bever M., Ruland D. (1988): "Aggregation and Generalisation Hierarchies in Office Automation", in: Allen R. B. (Eds.): Conference on Office Information Systems, Palo Alto, California, ACM Press, pp. 250-264.

Bhaskar K. (1993): Computer Security - Threats and Countermeasures, NCC Blackwell, Oxford.

Curtis B., Kellner M. I., Over J. (1992): "Process Modeling", Communications of the ACM, vol. 35, no. 9, pp. 75-90.

Davenport T. H. (1993): Process Innovation - Reengineering Work through Information Technology, Harvard Business School Press, Boston.

Davis G. B., Olson M. H. (1985): Management Information Systems. Conceptual Foundations, Structure and Development, McGraw-Hill, New York, USA.

Dobson J. (1990): "A Methodology for Analysing Human and Computer-Related Issues in Secure Systems", in: Dittrich K., Rautakivi S., Saari J. (Eds.): IFIP Sixth International Conference on Computer Security and Information Integrity, IFIP SEC'90, Espoo (Helsinki), Finland, North-Holland Amsterdam, pp. 151-170.

Ferstl O. K., Sinz E. J. (1993): "Geschäftsprozessmodellierung", Wirtschaftsinformatik, vol. 35, no. 6, pp. 589-592.

Holbein R., Teufel S. (1995a): "A Security Service for Role Based Access Controls in Distributed Systems", in: Eloff J. H. P., von Solms S. H. (Eds.): IFIP TC11 Eleventh International Conference on Computer Security IFIP/SEC95, Cape Town, South Africa, Chapman & Hall, pp. 270-285.

Holbein R., Teufel S., Bauknecht K. (1995b): "A Formal Security Design Approach for Information Exchange in Organisations", in: IFIP WG11.3 Ninth Annual Working Conference on Database Security, Aug. 1995, Rensselearville, N.Y., USA.

ISO (1991): ISO 10181-3: Information technology - Open Systems Interconnection - Security frameworks in open systems - Part 3: Access Control, International Organisation for Standardization ISO, DIS, no. ISO/IEC DIS 10181-3.

Jonscher D., Dittrich K. R. (1993): A Formal Security Model Based on an Object-Oriented Data Model, Department of Computer Science, University of Zurich, Technical Report, no. 93.41.

Leymann F., Altenhuber W. (1994): "Managing business processes as an information resource", IBM Systems Journal, vol. 33, no. 2, pp. 326-348.

Martin M., Dobson J. (1990): "Enterprise Modeling and Security Policies", in: Jajodia S., Landwehr C. E. (Eds.): IFIP WG11.3 Workshop on Database Security, Halifax, U.K., Elsevier Science Publishers B.V., pp. 117-149.

Medina-Mora R., Winograd T., Flores R., Flores F. (1992): "The Action Workflow Approach to Workflow Management Technology", in: Turner J., Kraut R. (Eds.): Proceeding of the ACM Conference on Computer Supported Cooperative Work, Toronto, ACM, New York, pp. 281-288.

Neumann P. (1992): "Trusted Systems", in: Jackson K. M., Hruska J., Parker D. B. (Eds.): Computer Security Reference Book, Butterworth-Heinemann Ltd, Oxford, pp. 837-862.

Picot A. (1994): "Restrukturierung von Unternehmen und Beschäftigungsperspektiven", Office Management, vol. 1994, no. 11, pp. 10-14.

Pohl H., Weck G. (1993): "Stand und Zukunft der Informationssicherheit", Datenschutz und Datensicherung, vol. 17, no. 1; 2, pp. 18-22; 78-86.

Pottas D., Solms S. H. (1992): "MAPS - Model for Automated Profile Specification", in: Gable G. G., Caelli W. J. (Eds.): IFIP TC 11 Eighth International Conference on Information Security, IFIP/SEC'92, Singapore, Elsevier Science Publishers B.V., pp. 113-126.

Scherr A. L. (1993): "A New Approach To Business Processes", IBM Systems Journal, vol. 32, no. 1, pp. 80-98.

Steinke G., Jarke M. (1992): "Support for Security Modeling in Information Systems Design", in: Thuraisingham B. M., Landwehr C. E. (Eds.): IFIP WG 11.3 Sixth Working Conference on Database Security, Vancouver, Canada, Elsevier Science Publishers B.V., pp. 125-141.

Ting T. C., Demurjian S. A., Hu M.-Y. (1992): "A Specification Methodolgy for User-Role Based Security in an Object-Oriented Design Model", in: Thuraisingham B. M., Landwehr C. E. (Eds.): IFIP WG 11.3 Sixth Working Conference on Database Security, Simon Fraser University Burnaby, Vancouver, British Columbia, Elsevier Science Publishers B.V., pp. 351-378.

Winograd T. (1988): "A Language/Action Perspective on the Design of Cooperative Work", in: Greif R. (Eds.): Computer Supported Cooperative Work: A Book of Readings, Morgan Kaufmann Publishers, pp. 623-653.

Winograd T., Flores F. (1986): Understanding Computers and Cognition, Ablex Publishing Corp., Norwood, New Jersey.

Woo C. C., Lochovsky F. H., Lee A. (1985): "Document Management Systems", in: Tsichritzis D. (Eds.): Office Automation, Springer, Berlin, pp. 21-40.