Information systems security management in virtual organizations

Kokolakis Spyros, Karyda Maria, Gritzalis Dimitris

Dept. of Informatics
Athens University of Economics and Business
76 Patission Str., Athens GR-10434, Greece
e-mail: {sak, mka, dgrit}@aueb.gr

Abstract

The virtual organization is a new form of organization possessing the characteristic of incorporating business units with a high degree of autonomy. This form of organization, which is expected to become the dominant organizational paradigm for the 21st century, strongly depends on the effectiveness of cooperation among the autonomous Information Systems (IS) of each business unit. Developing a security policy and installing security controls for each IS appears as a prerequisite for the survival of the virtual organization, but on the other hand it may severely hinder IS cooperation, as policies and controls often give rise to conflicts and interoperability problems. In this paper, we analyse the problem of managing IS security in multi-policy environments and introduce a Security Policies Management System (SPMS) that facilitates the management of IS security in virtual organizations and supports the resolution of conflicts between security policies.

Keywords: Cooperating Information Systems, Information Security Management, Information Security Policies, Virtual Organizations.

1. Introduction

The environment in which modern corporations operate and evolve is dynamic and prone to changes. These characteristics call for a high degree of and a great competence in rapidly adjusting and responding to change. To meet these requirements, a number of new corporations with no hierarchical structure appear themselves and evolve in great speed, while existing corporations restructure their organization in a radical way, applying a new type of organization, which is expected to become the dominant organizational paradigm world-wide in the near future [DaMa92].

The new organizational form has been given various names, such as Virtual Organization [Mows97a, Mows97b], Virtual Corporation [DaMa92], Cybercorp [Mart96], Federated Organization [WeSr99], and Networked Organization [PoSh91]. We have adopted the term *Virtual Organization*, which in our opinion depicts the essence of the new organizational form, that is the cooperation of several autonomous business units to form a flexible and effective organization.

Each unit is responsible for operating and managing its own IS. Moreover, each unit develops its own security policy and installs the corresponding security controls in order to protect the valuable IS infrastructure. However, as these security policies may be incompatible to each other or even conflicting, the cooperation among IS within a virtual organization may suffer severely from interoperability problems.

In this paper, we firstly analyse the issue of IS security management in virtual organizations and then introduce a Security Policies Management System (SPMS) that aims to support the management of security policies in this new organizational form.

2. Virtual organizations and IS cooperation

2.1 Main characteristics of the virtual organization

The concept of *virtual organization*, being a relatively new concept, is interpreted in many different ways and therefore a clarification of the defining characteristics that distinguish the virtual organization from traditionally structured organizations is required (see Table 1).

A virtual organization

- is the response to the need of providing a *virtual product* or *service* [DaMa92], that is a product, or service, which is produced instantaneously and is customized according to the customer's individual requirements;
- provides a high degree of administrative independence to the business units that comprise it;
- assigns part of its functionality to third parties, usually in the form of 'outsourcing';
- shares part of its assets (mainly knowledge, information and capital) with others, such as customers, suppliers or even competitors;
- takes advantage of the new information and communication technologies to transform itself to a human-electronic organism [Mart96], and
- cooperates closely with other organizations, corporations, groups or individuals (e.g. in the case of a joint venture).

Thus, the virtual organization is characterised by the interconnection of administratively independent units that may fall within or outside its perimeter. The main attribute that distinguishes the virtual organization from other organizational forms is the abolishment of hierarchical structure, which is substituted by a more flexible network structure. In a traditionally organized corporation the hierarchical structure serves the purpose of controlling complexity and is used:

- as a means of communicating information, from the employees to top management, through several intermediate management layers, and
- as a means of conveying instructions from the top management to the employees and exercising control.

In modern organizations, information systems have diminished the need for a hierarchical management structure. Computer networks convey information and instructions and thus form the nervous system of the organization [Mart96]. Furthermore, virtual organizations relax the internal control and foster trust relationships.

Concluding, we may say that the main feature that distinguishes a virtual organization is its organizational form and not the kind of technology it uses. It would be wrong, therefore, to confuse the virtual

organization with a company whose operational field is the Internet, or one that uses virtual reality based technologies, teleconferencing, electronic trading, etc.

Traditional organization	Virtual organization
Explicit limits, closed organization	Vague limits, open communication
Rigid structure	Independently administrated entities, lose ties
Management role: making decisions and giving instructions	Management role: relationship management
Control and authority allocation structures	Trust relationships
Hierarchical structure	Flat/horizontal or networked structure
Well-defined and standardised tasks	Virtually organised tasks
Mass production	Virtual products and services

Table 1: Virtual organizations versus traditional organizations

2.2 The role of IS security in virtual organizations

Based on the above observations we may conclude that the IS infrastructure is of vital importance for the virtual organization [StLS98]. There is yet another important factor, however, that underlines the role of IS security for a virtual organization's functions, and that is *trust*. It is evident that all types of companies and organizations benefit when trust relationships are in place, since the presence of trust has a positive impact on a company's development and efficiency. The reason for this is that trust relationships contribute to transaction cost reduction and can be easier developed within an

organization, rather than among market players [Will93, MaDS95].

In the case of virtual organizations in particular, the development of trust relationships is of critical importance, as noted by the majority of researchers in the area of networked organization's studies [JaKL98, Fuku97, Holl98, JaSh98, IsMa99]. In a virtual organization trust can be viewed as a substitute for loose control and as a means of preserving its coherence.

Trust relationships are developed through communication and in the case of the virtual organization, communication is mostly realised through the underlying information infrastructure. When security problems emerge, communication is affected, with negative results on virtual relationships.

Furthermore, the amount of threats faced by virtual organizations is much heavier than the one faced by traditionally organized corporations, due to the fact that their functionality relies mainly on the exchange of information and knowledge and the cooperation with third parties. Therefore, one of the main objectives of the virtual organization should be the protection of the IS infrastructure. This involves the development of effective security policies and the installation of those security controls needed to apply the security policies. Since each of the business units that constitute the virtual organization is administratively independent, each unit shall develop its own security policy and decide on the security controls to be installed.

On the other hand, the effective cooperation of the units that constitute the virtual organization requires a high level of interoperability among the corresponding information systems. Thus, improving interoperability and reinforcing IS cooperation are equally important aims.

3. Multiple security policies and interoperability problems

As mentioned above (Table 1) a basic feature for a virtual organization is the cooperation among individually administrated entities (business units), each one operating and controlling independent information systems. The more independent the entities which form a virtual organization are, the more IS security related problems arise [Fran96]. Individual administration of each IS means that different policies are applied in all relevant sectors, including IS security. In this way, multiple independent security policies are developed for each participating entity. Therefore, we may refer to

this case as the case of a multiple security policy environment.

In the remaining part of this paper, we explore and present solutions to the problems that stem from the incompatibility in security policies in a multiple security policy environment. We consider these problems to be interoperability problems, where by interoperability we refer to 'the ability of two or more information systems to provide services to, and accept services from, other IS and to use the services so exchanged to enable them to cooperate effectively together.'

Interoperability of IS depends on their ability to provide each other with valid information and useful services at the right time. Security policies, however, and the corresponding protective measures that implement them, are often obstacles to this kind of exchange and consequently hinder the cooperation among different IS [LuSl99].

4. Security Policies Management System (SPMS)

Our analysis so far shows that interoperability problems emerge in the cooperation among independent IS, when their individual security policies are incompatible. To overcome this problem we propose the implementation of a Security Policies Management System (SPMS). The suggested structure of a SPMS, which is described in the following sections, was based:

- On the recognition of *metapolicies* as a means of resolving interoperability problems of this kind [Hosm92a, Hosm92b, Hosm96, Kuhn95, Kuhn99, HaKu99, KuKo95, Bryc97], and
- On a generic methodological framework for achieving interoperability in multiple security policies environments by means of developing metapolicies, previously described in [KoKi00].

4.1 What is a security policy?

The term security policy is interpreted in many different ways. Quite often the term security policy is used to describe a collection of "policy statements" expressed in natural language, e.g. "passwords should be sufficiently long so that they are difficult to guess or determine from the encrypted text". The same term is also used to refer to formal models [Koko96], such as the Chinese-Wall Security Policy, or the Bell-LaPadula Policy. Finally, in some cases the term is used to refer to the guidelines included in legal and regulatory documents.

In our perspective, a policy is "a set of authoritative statements that define the set of acceptable, or preferred, options in future selection

processes". That is, security policies are mandatory guidelines, which guide decision-makers in security related decisions. So, a policy may be formal as well as informal and the level of abstraction should be high enough to cover a wide range of instances of selection process and low enough to keep the number of acceptable options (decisions) in each selection process minimum.

A SPMS should be able to manage security policies expressed both in formal notation and natural language, the last being the most common case. This feature distinguishes the SPMS from previous attempts to address the problem of incompatible security policies [LuSl99, Kuhn95, Kuhn99, HaKu99, KuKo95, Bryc97].

Metapolicies are a means of resolving conflicts among incompatible security policies. Metapolicies are policies about policies consisting of a set of rules for coordinating the enforcement of multiple policies, specifying, for example, the order in which multiple policies are enforced, and which results have precedence if a conflict occurs.

4.2 Main objectives of the SPMS

The proposed SPMS aims:

- to represent and store security policies and security metapolicies in a manageable form;
- to support the task of managing security policies and security metapolicies, in a virtual organization; and
- to support the task of resolving problems, which are caused by incompatible or conflicting security policies.

4.3 Requirements and constraints

According to the objectives we have so far described, a SPMS, in order to be effective, should fulfil the following requirements. A SPMS should:

- Provide the ability to register security policies expressed in various languages (formal notation, or natural language) and in various levels of abstraction.
- Provide the ability to monitor the application of security policies.
- Provide the ability to compare different security policies, to locate problems caused by conflicts and incompatibility and support their resolution.

- Be applicable to a virtual organization, without interfering with, or affecting the organizational structure and their individual management style.
- Register all relevant facts, which concern the evolution and management of security policies.

The requirements described above cannot be viewed as a complete requirements specification list. This is an innovative system and there exist no users with experience in this kind of systems that could provide us with user requirements. For these reasons, based on the general requirements that stem from the analysis that has been presented in the previous sections, we have developed a prototype that implements the basic functionality of a SPMS.

5. SPMS architecture

The SPMS (Figure 1) proposed in this paper consists of the following six basic subsystems:

1. The Security Policies Repository
2. The Repository Interface
3. The Subsystem for the Coordination and Facilitation of Negotiations
4. The Security Policies Manager
5. The Conflicts and Incompatibilities Detection Subsystem
6. The Security Metapolicies Development Subsystem

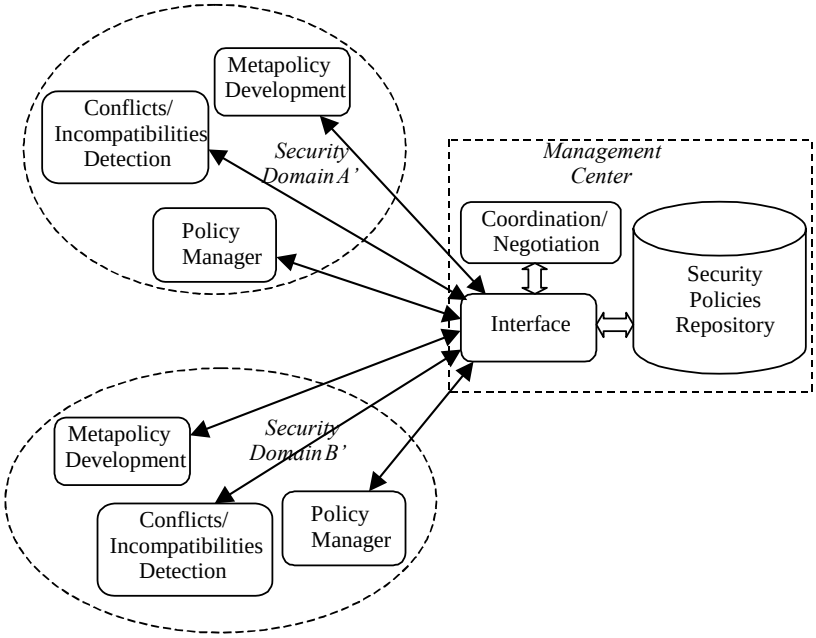

Figure 1: The Security Policies Management System (SPMS)

5.1 The Security Policies Repository

The Security Policies Repository stores the individual policies for each security domain, and the agreed-upon metapolicies. Security policies may be represented in a formal or informal (e.g. natural language) way and in various abstraction levels. The Security Policies Repository is located at the Management Center. The Management Center, as an administration unit, is not hierarchically related to other administration units. Its only purpose is to provide the infrastructure needed for the development and operation of the Security Policies Repository.

5.2 The Repository Interface

The Security Policies Repository has to be in connection with the rest of the SPMS subsystems, which are distributed in different location areas. The Repository Interface serves this need for communication and handles operational issues, such as message translation and forwarding, and controls the communication of the repository with other subsystems.

5.3 The Subsystem for the Coordination and Facilitation of Negotiations

As described in [KoKi00], in order to agree on a set of security policies and metapolicies, the autonomous administration units that control the corresponding security domains, where different security policies are applied, must negotiate with each other. The process of this negotiation cannot be fully automated, due to the abstract nature of security policies. A SPMS, however, may facilitate this process, by providing coordination and communication services. The central "Subsystem for the Coordination and Facilitation of Negotiations" coordinates the negotiation process, which is performed through the "Metapolicies Development Subsystems" that are installed in each security domain.

5.4 The Security Policies Manager

Through the "Security Policies Manager", each information security manager (or security officer) in charge of a separate security domain can store in the Repository the security policies applied in her domain of control and retrieve from the Repository information concerning any security policy in the repository. Furthermore, through the Security Policies Manager, the security officer may monitor if a policy has been violated and detect the specific rules that have been violated.

5.5 The Conflicts and Incompatibilities Detection Subsystem

This subsystem's role is to detect possible conflicts and incompatibilities among different security policies. With regard to security policies that are represented in a formal notation, detection of conflicts can be automatically done by the SPMS. In all other cases, the Conflicts and Incompatibilities Detection Subsystem support security officers to detect, recognize and classify conflicts and incompatibilities. This service is provided on each security officer on an individual basis, by installing the "Conflicts and Incompatibilities Detection Subsystem" in every security domain.

5.6 The Security Metapolicies Development Subsystem

This subsystem supports the development of metapolicies that require the agreement of more than one administration units. It

provides the user interface for the development, representation and storage of metapolicies. While the "Security Metapolicies Development Subsystem" provides an interface to the user, the negotiation is actually managed by the specialised "Subsystem for the Coordination and Facilitation of the Negotiations", as it was mentioned above.

6. Development of a SPMS prototype system

In order to assess the possible effectiveness of the SPMS presented above, as well as to explore technologies and tools, which can be used for the implementation of the SPMS, a prototype system was developed. The prototype system consists of three of the aforementioned subsystems, namely the Security Policies Repository, the Repository Interface and the Security Policies Manager. The SPMS prototype that has been implemented:

- Is designed to meet the requirements described above, and
- Implements a basic functionality, which can be used to solicit further, more specific requirements.

The following limitations have also been taken into account:

- Current technology does not support the development of systems that permit the full automation of tasks, such as comparing informal security policies and providing solutions to possible conflicts and incompatibility cases.
- Organizations interested in implementing a SPMS might not have the ability to develop a specialized technical infrastructure for this purpose. Such organizations should, however, be able to take advantage of the existing infrastructure, like Internet and Intranet.

The implementation of three basic subsystems is presented in the following sections.

6.1 Implementation of the Security Policy Repository

The Security Policy Repository is based on ConceptBase, a tool described in [JGJ+95], and was installed in a Sun Ultra workstation, running Solaris 2.5.1. ConceptBase is a deductive object manager for meta-data management that supports a knowledge representation language, O-Telos [MBJK90, JJNS98].

The main difference of a knowledge representation language from

other types of languages, such as programming or design languages, is that knowledge representation languages besides representing facts they also perform automatic inferences. They are used to develop and operate knowledge bases, which not only store known facts given by its users, but also provide access to facts implicit in the knowledge base [MBJK90].

- Our choice of a knowledge representation language is based on the following observations. A security policy includes both explicit and implicit facts that should be taken into consideration in all decisions based on the policy. In addition, security policies rarely specify in detail how information and resources should be handled. Usually, their purpose is to guide the regular decision processes concerning the protection of information and resources. In this perspective knowledge representation languages seem to be more appropriate for security policy representation than formal specification languages. O-Telos was chosen among several knowledge representation languages, mainly because:
- It is simple, flexible and object-oriented and has been used in the successful development of applications in IS analysis and design, software engineering, business process modelling, multiple data bases and data mining [DaBP95, NJJ+96, Robi96, StKR97, RoPa99].
- It offers the ability to register in the same repository not only the security policy, but also models of the IS and the organization itself.
- It provides full conceptual structuring mechanisms, such as generalization and classification, which make possible the management of security policies that are in different levels of abstraction. This feature is especially useful in multiple security policy environments.
- It supports the processing of temporal knowledge, thus enabling the control and monitoring of security policies evolution.

6.2 Implementation of the Security Policies Manager

The Security Policies Manager was developed using MS/Visual C++ and operates under MS/Windows (Figure 2). The Security Policy Manager supports the following tasks:

- Define a new security policy.
- Query about existing security policies.
- Check for policy violations.
- Define assets, agents, activities, security domains, formal rules and informal policy statements.

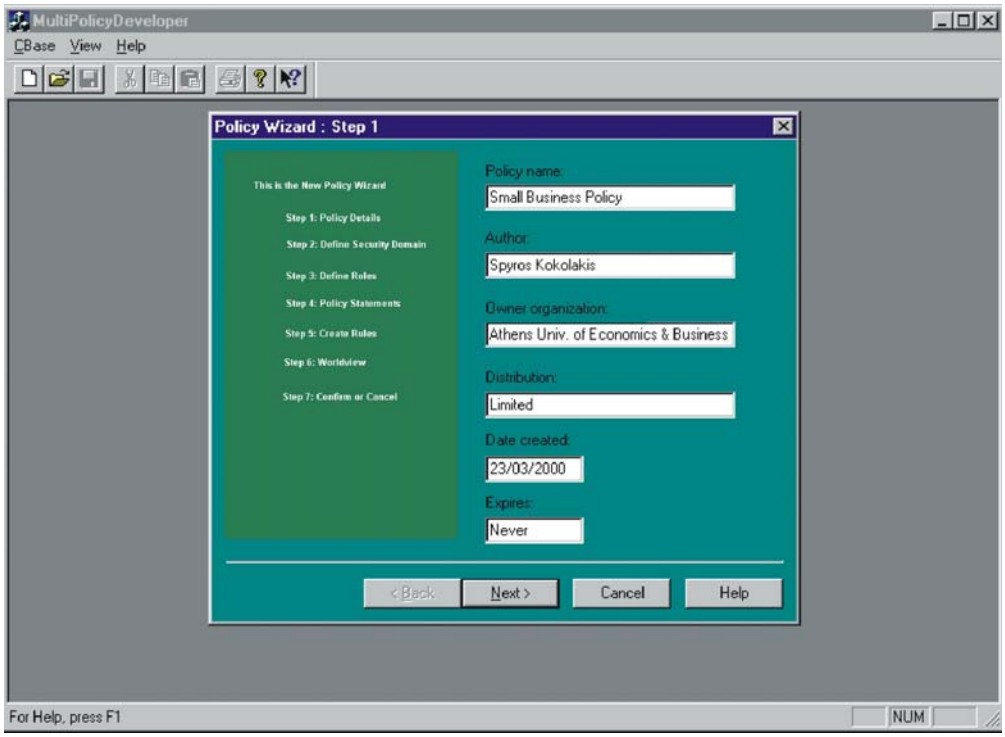

Figure 2: The Security Policies Manager (Define New Policy Wizard)

The Security Policies Manager communicates with the Security Policies Repository through the Repository Interface, as shown in Figure 3. The Repository Interface communicates with the Security Policies Repository via Internet Process Calls (IPCs).

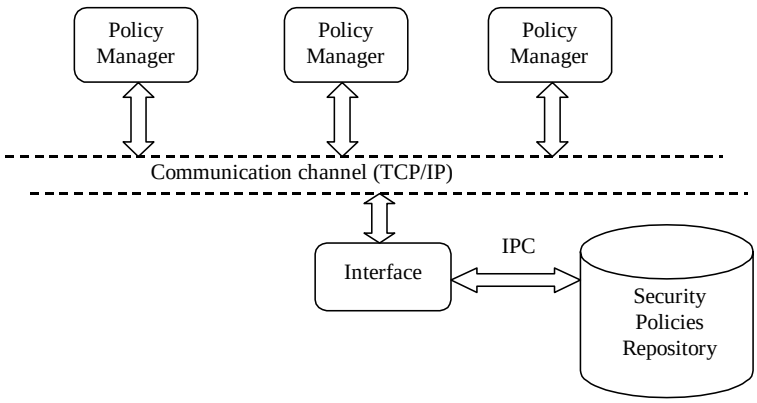

Figure 3: **The prototype system**

7. Conclusions and further research

Based on the prototype system that has been developed, we may conclude the following:

- The use of a knowledge base having an inference mechanism requires the use of workstations having significant processing power.
- Automatic monitoring of the enforcement of a security policy is only possible for the formally defined policy rules.
- The use of the SPMS requires trained personnel.

On the other hand, the SPMS

- may store and manage security policies expressed in both a formal notation and natural language and in various levels of abstraction, this being a characteristic that distinguishes SPMS from previous attempts to address the problem of incompatible security policies,
- may be used effectively by a virtual organization without interfering with, or affecting the organizational structure and their individual management style,
- may exploit the power of knowledge representation languages, such as the O-Telos language, and
- can also be used to represent and store the business process models of the organization.

Further research may focus on the development of a fully functional SPMS and the actual operation of the SPMS in a virtual organization.

8. References

[Bryc97] Bryce, C. and Kuhnhauser, W.: An approach to security for worldwide applications. In Katsikas, S. (Ed.), *Communications and multimedia security III*, Chapman & Hall, London, 1997.

[DaBP95] Dang, Q.C., Baylis, T., Patel, D.: Modeling a business through soft systems methodology in end-user development: a claim and an approach. In Mehandijiev, N., Bottaci, L. (Eds.), in Proc. of CAiSE*95 Workshop on supporting end-user development with visual programming and object-orientation, Finland, 1995.

[DaMa92] Davidow, W. and Malone, M.: *The virtual corporation: Structuring and revitalizing the corporation for the 21st century*. HarperBusiness, New York, 1992.

[Fran96] Frank, R.L.: Security issues in the virtual corporation. *Computers and security*, 15(6): 471-476, 1996.

[Fuku97] Fukuyama, F.: Trust still counts in a virtual world. *Forbes*, 1997.

[HaKu99] Halfmann, U., Kuhnhauser, W.: Embedding security policies into a distributed computing environment. *ACM Operating Systems Review*, 33(2), 1999.

[Holl98] Holland, C.P.: The importance of trust and business relationships in the formation of virtual organizations. In Sieber, P., Griese J. (Eds.), *Organizational virtualness: Proc. of the VoNet Workshop*, Simowa Verlag, Switzerland, 1998.

[Hosm92a] Hosmer, H.: The multipolicy paradigm for trusted systems. In *Proc. of the 1992 New Security Paradigms Workshop*, USA, IEEE Press, 1992.

[Hosm92b] Hosmer, H.: Metapolicies II. In *Proc. of the 15th National Computer Security Conference*, USA, 1992.

[Hosm96] Hosmer, H.: New security paradigms: orthodoxy and heresy. In S.K. Katsikas, D. Gritzalis (Eds.), *Information systems security: Facing the information society of the 21st century*. Chapman & Hall, London, 1996.

[IsMa99] Ishaya, T. and Macaulay, L.: The role of trust in virtual teams. In Sieber, P. and Griese J. (Eds), *Organizational virtualness and electronic commerce: Proc. of the 2nd international VoNet workshop*, Simowa Verlag, Switzerland, 1999.

[JGJ+95] Jarke, M., Gallersdorfer, R., Jeusfeld, M., Staudt, M. and Eherer, S.: ConceptBase: a deductive object base for meta data management. *Journal of intelligent information systems*, 4(2): 167-192, 1995.

[JaKL98] Jarvenpaa, S.L., Knoll, K., Leidner, D.E.: Is anybody out there? Antecedents of trust in global virtual teams. *Journal of management information systems*, 14(4): 29-64, 1998.

[JaSh98] Jarvenpaa, S.L. and Shaw, T.R.: Global virtual teams: integrating models of trust. In Sieber, P., Griese J. (Eds.), *Organizational virtualness: Proc. of the VoNet workshop*, Simowa Verlag, Switzerland, 1998.

[JJNS98] Jeusfeld, M.A., Jarke, M., Nissen, H.W., Staudt, M.: ConceptBase: Managing conceptual models about information systems. In Bernus, P., Mertins, K., Schmidt, G. (Eds.), *Handbook of architectures of information systems,* Springer-Verlag, 1998.

[Koko96] Kokolakis, S.A.: Is there a need for new information security models? In Horster, P. (ed.), *Communications and Multimedia Security II*, Chapman & Hall, 1996.

[KoKi00] Kokolakis, S., Kiountouzis E.: Achieving interoperability in a multiple-security-policies environment, *Computers and Security*, 19(3):267-281, 2000.

[KuKo95] Kuhnhauser, W.E., von Kopp Ostrowski, M.: A framework to support multiple security policies. In

Proc. of the 7th annual Canadian computer security symposium, Canada, 1995.

[Kuhn99] Kuhnhauser, W.E.: Policy groups. *Computers and Security*, 18(4): 351-363, 1999.

[Kuhn95] Kuhnhauser, W.E.: On paradigms for security policies in multipolicy environments. In J. Ellof and S.von Solms (Eds.) *Information security – the next decade*, Chapman & Hall, London, 1995.

[LuSl99] Lupu, E. and Sloman, M.: Conflicts in policy-based distributed systems management. *IEEE Transactions on software engineering*, 25(6), 1999.

[Mart96] Martin, J.: *Cybercorp: the new business revolution*. Amacom, New York, 1996.

[MaDS95] Mayer, R.C., Davis, J.H., Schoorman, F.D.: An integrative model of organizational trust. *Academy of management review*, 20(3): 709-734, 1995.

[Mows97a] Mowshowitz, A: Virtual organization. *Communications of the ACM*, 40(9): 30-37, 1997.

[Mows97b] Mowshowitz, A.: On the theory of virtual organization. *Systems research and behavioral science*, 14(6): 373-384, 1997.

[MBJK90] Mylopoulos, J., Borgida, A., Jarke, M., Koubarakis, M.: Telos: representing knowledge about information systems. *ACM Transactions on information systems*, 8(4): 325-362, 1990.

[NJJ+96] Nissen, H., Jeusfeld, M.A., Jarke, M., Zemanek, G.V. and Huber, H.: Requirements analysis from multiple perspectives: experiences with conceptual modeling technology. In *Proc. of the 2nd IEEE Conference on Requirements Engineering*, USA., 1996.

[PoSh91] Pockart, J.F., Short, J.E.: The networked organization and the management of interdependence. In Scott Morton, M.S. (Ed.), *The corporation of the 1990s: information technology and organizational transformation*, Oxford University Press, New York, 1991.

[Robi96] Robinson, W.N.: Automated assistance for conflict resolution in multiple perspective system analysis and operation. In *Proc. of the ACM Symposium on Foundations of Software Engineering*, USA, 1996.

[RoPa99] Robinson, W.N., Pawlowski, S.: Managing requirements inconsistency with development goal monitors. *IEEE Transactions on software engineering*, 25(6), 1999.

[StKR97] Staudt, M., Kietz, J.U., Reimer, U.: ADLER - An environment for mining insurance data. In *Proc. of the 4th Workshop on knowledge representation and databases* (KRDB '97), Athens, 1997.

[StLS98] Strader, T., Lin, F., Shaw, M.: Information infrastructure for electronic virtual organization management. *Decision Support Systems*, 23:75-94, 1998.

[WeSr99] Wexelblat, R.L., Srinivasan, N.: Planning for information technology in a federated organization, *Information and management*, 35: 265-282, 1999.

[Will93] Williamson, O.E.: Calculativeness, trust, and economic organization. *Journal of Law and Economics*, 36:453-486, 1993.