Exploring Information Security Issues in Public Sector Inter-organizational Collaboration

Anne Fleur van Veenstra and Marco Ramilli

Faculty of Technology, Policy and Management, Delft University of Technology,
Jaffalaan 5, 2628 BX Delft, The Netherlands
a.f.e.vanveenstra@tudelft.nl
Dipartimento di Elettronica Informatica e Sistemistica, University of Bologna,
Via Venezia, 52 – 47023 Cesena, Italy
marco.ramilli@unibo.it

Abstract. Joining up service delivery of multiple organizations often requires public organizations to exchange citizens' information. To ensure their privacy and realize information security, controlling data access is paramount. However, limited research was found on issues that emerge when realizing data access control in inter-organizational collaboration. Security is typically achieved by implementing security patterns, which are proven technical solutions. This paper explores data control issues for realizing information security by looking at the application of security patterns in practice. By investigating a case study of inter-organizational collaboration in the Netherlands we explore the use of two security patterns that control access to information: Extended Role-Based Access Control (ERBAC) and Single Access Point/Check Point. We investigated whether those patterns were implemented in the right way and whether they were sufficient for guaranteeing access control. We found issues related to access control to be crucial in realizing information security, which can only be realized by implementing organizational arrangements in addition to technical solutions. Therefore, we recommend development of a framework for information security in inter-organizational collaboration including technical and organizational aspects.

Keywords: Information Security, e-Government, Inter-Organizational Collaboration, Security Patterns.

1 Introduction

Public organizations aim to improve their service delivery to citizens and businesses by realizing integrated service delivery. From the perspective of a client, service delivery is integrated when multiple organizations collaborate and the client need not provide the same information to each of these organizations but, instead, just once to one organization [1]. Thus, for realizing integrated service delivery, multiple organizations need to share information about their clients. Furthermore, for their daily operations, public organizations increasingly rely on data gathered by other organizations as well as on information stored in vital registries, such as the citizens

M. Janssen et al. (Eds.): EGOV 2011, LNCS 6846, pp. 355–366, 2011.

registry, and the address and car registrations. Therefore, unique registries are set up to facilitate information sharing. Governments, thus, retain, process, and exchange citizens' data that are increasingly being re-used.

To ensure the privacy of citizens, information security is key to these e-government initiatives [2]. Information security is threatened by attacks on networks and data transactions and through unauthorized access by means of false or defective authentication [3]. Besides tightly securing information systems in the public domain, controlling access to citizens' information is the main challenge for realizing information security [4,5]. This paper investigates issues that emerge in relation to access control of citizens' information for realizing information security when multiple public organizations collaborate. We found that there is limited research on information security in the field of e-government as it is often primarily seen as a technical matter. Moreover, most of the studies on security in e-government are concerned with security in e-participation or e-voting (e.g. [6-9]) or of government websites (e.g. [10]). Carter and McBride [4], therefore, call for more research on information privacy in the field of e-government.

This paper aims to contribute to e-government security by identifying information access control issues. Looking at a large case study of inter-organizational collaboration in the Netherlands, we investigate how information security was realized. Security is often realized through the implementation of predefined security patterns. Security patterns are reusable solutions to security problems [11]. They are used to implement pre-specified and tested solutions. Studying e-government access control security applying the state of the art in methodology and designed patterns would reveal if the technology sphere could solve such issues or if there is a need for enhanced solutions. As these design patterns are central to achieving information security, we first examine existing security patterns for data access control. Then, we carry out the case study to find out how these security patterns are implemented in practice and whether any other security arrangements are used. The case study findings are followed by a discussion and by conclusions and recommendations.

2 Security Patterns for Information Access Control

A common way to ensure information security is through the application of security patterns [12-16]. Security patterns are based on the notion of design patterns. A *design pattern* is defined as a general reusable solution for a commonly occurring problem [14,17]. It is a high level description of 'what to do' or 'which steps to follow' in order to solve a recurring problem. Applying tested design patterns to solve a security issue saves time and effort, as they allow for the rapid design of a robust solution by using proven techniques. Besides providing commonly used solutions, design patterns provide a common vocabulary to designers, architects and developers to allow them to convey ideas without having to describe every detail of the intent of the design [13,15]. Many different types of patterns exist, such as structural design patterns that are essential to building complex systems, computational design patterns to identify the system's key computations, algorithm strategy patterns related to the high level strategies to exploit the system's characteristics, implementation patterns related to the realization of the source code, and security patterns to solve security related problems [18-21].

To access control information, security patterns were also designed. The access to citizens' personal information needs to be controlled and monitored in order to assure privacy and information security of entire population. The use of Access Control Mechanisms (ACMs) is a mandatory implementation step to assure that only authorized users can deal with personal citizen information [5]. Although many different types of ACMs exist [22-25], in this paper we focus on two of the most commonly used patterns: the Extended Role-Based Access Control (ERBAC), which is an extension of the standard Role-Based Access Control (RBAC) pattern, and the combination of Single Access Point and Check Point. Single Access Point/Check Point is the most commonly used design pattern able to provide identification and authorization of the final user [26].

2.1 Role-Based Access Control Pattern

One of the most commonly used security pattern to control access of information is Role-Based Access Control (RBAC). It controls access to information by associating users to roles that are allowed to access to specific information [24,25]. Although it was a theoretical pattern, it can be easily applied in practice using an implementation model [23]. Most organizations have a variety of job functions that require a different set of skills and responsibilities. Most of the time employees (and employers) can be classified according to their functions or tasks; common tasks require similar sets of rights. The RBAC pattern helps organizations to define precise access rights for its members according to the 'need-to-know' policy. As many other security policies this policy aims to make unauthorized access to information difficult. The 'need-to-know' policy also aims to discourage 'browsing' of sensitive material by limiting access to the smallest possible number of people.

The RBAC model is shown in Fig.1. The 'ProtectionObject' class represents the information that needs protection from unauthorized users. It has an ID and a name to distinguish between different protected information sources. Users (employees) are assigned to detailed roles and roles are given rights according to their functionalities. The association class called 'Right' defines the access type that the user, with his role, has regarding to the protected object. The user may be able to read the protected information, modify or delete it. Each user may have one or more roles, depending on how many tasks he or she performs. Each role may have the rights to use one or more protected objects depending on their functionality. The approach can be extended to a real life scenario using three new entities such as:

1. *Group*: users can be divided into groups depending on their working area;
2. *Session*: representing the way to use a role;
3. *Administrator*: the person who has the right to assign roles and rights to users and group of users.

An RBAC model including *Group*, *Session,* and *Administrator* entities is referred to as the *extended* RBAC (ERBAC). The entity called Group collects the users who belong to the same job category. *Roles* can be applied directly to a Group since the "common tasks require similar sets of rights, ergo roles". A single user can have a specific set of roles in addition to the group roles because he or she may have special

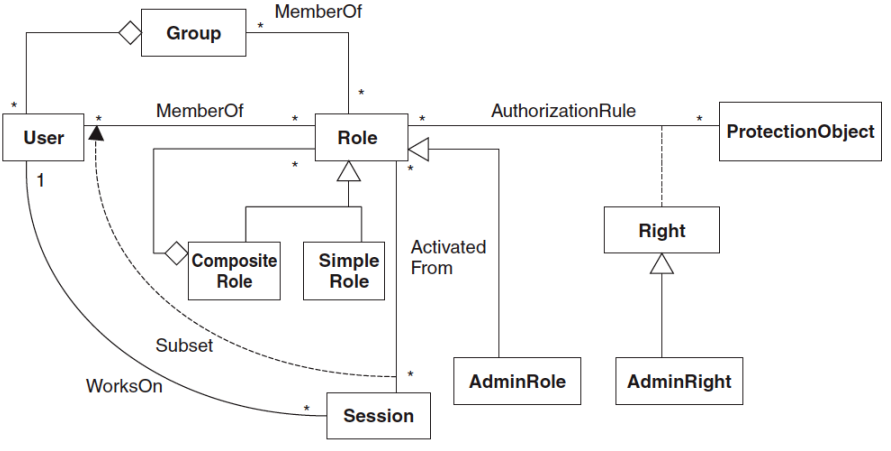

Fig. 1. Extended Role-Based Access Control with Group, Session and Administrator entities

or temporary permission in addition to the ones normally attributed to the group (for example, a medical director can be a doctor with more access rights).

A special case is the Administrator, who has a different subset of roles as the *trusted point* of the model. The Administrator is the root, which initializes the access control mechanism by setting up roles, groups, rights and at least one user. In a company the administrator may be the delegate system that takes care of the process of defining roles, users, and groups. The Session is the entity that keeps track of 'who is doing what'. Furthermore, the Session records which user is working on a specific role. And finally, the Roles can be simple (by meaning of atomic ones) or composite (by meaning of an aggregation of two or more roles).

2.3 Single Access Point and Check Point Patterns

Single access point and check point patterns are often used together to protect the system from misuse or damage. The single access point defines a clear entry point to the system that can be assessed implementing the desired security policy. The check point pattern builds an easy access control mechanism on top of the single access point that is able to distinguish between authorized and unauthorized attempts to access the system [26]. A military check point is a good example for explaining how these patterns work in practice as they apply strict rules to entry. Every time somebody passes the check point that person need to be authorized to enter or leave the secured zone. At the same time, authorized people (clients) need to be able to go easily. Therefore, the difficulty is to distinguish between the two types of users (authorized and unauthorized) as every mistake could turn into a problem. Fig. 2 describes the proposed solution by applying the Check Point pattern on top of the Single Access Point pattern.

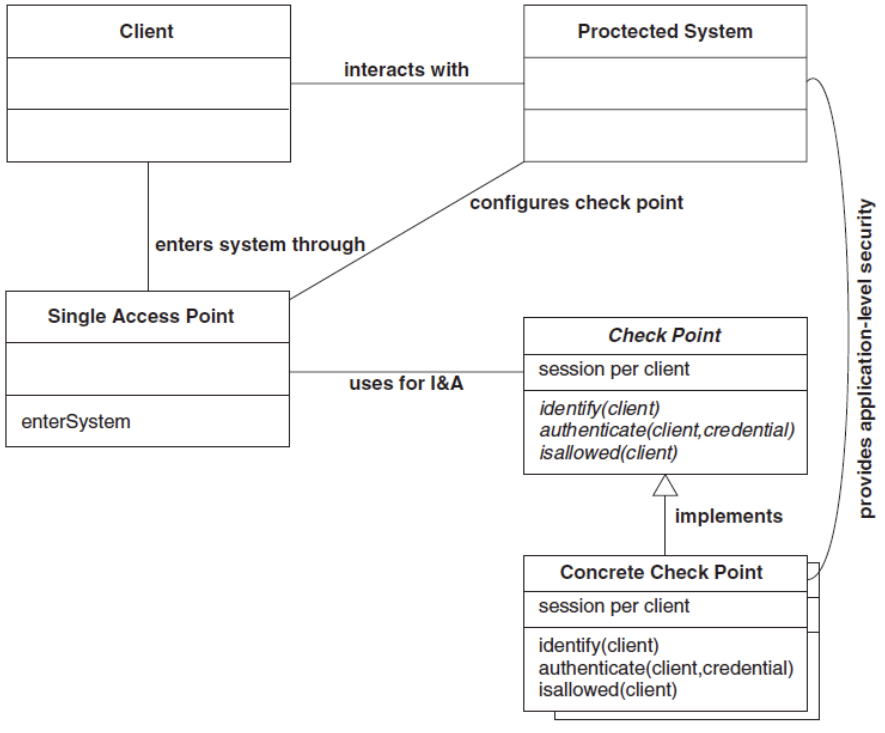

Fig. 2. The Single Access Point pattern and the Check point Pattern

In order to interact with the protected system, the client needs to enter into the environment through a Single Access Point employing a Check Point pattern for identifying and authenticating each client (Fig. 2). The Check Point pattern identifies and authenticates every access to the protected area by tagging each allowed client. This tag represents the security session. Everybody with the right to access in the protected area exhibits a tag certifying the right to be there. Through the security session the client is able to use the protected system. The goal of these two patterns fitted together is to regulate access to a system. They make it possible to deny access to the protected area when too much clients have accessed the area, to control access for statistics, to differentiate tasks and roles and to protect the access to unauthorized clients.

3 Case Study

To study the use of the security patterns for ensuring information security in cross-organizational collaboration we use a case study from the Netherlands. In the Netherlands, several inter-organizational collaborative networks can be identified that share citizens' data. The network under study is a service chain in which multiple organizations collaborate to deliver services to the unemployed, such as helping to

find a job (re-integration) and issuing social security allowances. We carried out the case study by doing semi-structured interviews with people from the business side as well as from the IT-department. We asked questions about current as well as future security issues. Furthermore, we asked them how their current policies for data and system security are set up and what the major challenges were. Finally, we asked them how these policies and arrangements are followed in practice and whether they had to be adjusted over time. Eight people from different organizations were interviewed between October 2010 and February 2011.

The case study is a collaboration between two large executive organizations, one focusing on the social security for pensioners and the other on social security for the unemployed, and the municipal social security offices. This reflects the implementation of social security policies on two levels: on the national level by the large executive organizations and on the local level by the municipalities. The main objectives of this inter-organizational collaboration is to help people get a job when they have become unemployed, and determine the height and length of the social security allowance. To support this process, a number of different systems have been developed. The main systems used for collaboration are an online environment, including an electronic intake and filing system that allows sharing information between the supporting agencies and the unemployed, and a system that the different organizations use to look at and re-use each other's citizens information. These two systems will be taken a closer look at to determine how information security is implemented.

At the front end the executive agency for social security collaborates with the municipalities in 'work centers' where 'work coaches' from both the local and the national level help their clients to find a job. In these work centers citizens' data will only be looked at by the client and by the work coach helping the client. The information that is shared is rich information on the specific working situation of clients. At the back end of the processes, much of the data is processed automatically. For example, the organization taking care of pensioners allowance processes the information mostly at night, with as little human interference as possible. Only in case of a complaint filing, case workers look into citizens' data. The information that is shared at the back end includes age, address, marital status as well as income data and information on the possession of property and vehicles. To estimate the social benefits for the unemployed individual case workers make individual requests of citizens information such as income data from the inland revenue service, car ownership data from the executive organization registering motorized vehicles, and address and marital status from the local level. The case workers from the organization determining the social security allowance for pensioners also have the right to view this information if necessary but the degree of usage is much lower.

The employees that make use of these systems are allowed to use certain applications and access and change certain data based on their role within the organization. However, usage and authorization of usages differs among the different applications. For some shared applications, authorization is based on the role that is given to persons by human relations management (HRM) applications of the social security executive organization. However, as many of the employees at the local governments are not included in the HRM system of the social security executive organization, they cannot be assigned a role to use the system, even though their

function requires them to access information. Therefore, from time to time at the front end of the system, user's credentials are shared between employees, which is not allowed.

To test whether the system is sufficiently secured from attacks from the outside, the system is routinely hacked by professionals. But although the level of security from outside attacks is considered sufficient, the main problem threat to information security is from the inside. Employees from the executive organizations look, sometimes, for citizens' information that they do not need to see as part of their work. For example, information on people often appearing on television is much more often retrieved that that of others. A shortlist of names and addresses is, therefore, blacklisted and cannot be accessed by the employees of the executive organizations. Furthermore, the retrieval of citizen's information outside the normal case load, is reported to the manager of the person retrieving the information and also published in the organization's in-house magazine.

Another measure to secure the personal information of citizens is an agreement between all the parties involved in sharing citizens' information on the norms of information sharing. Still, employees of the pensions executive organization found that while they applied very strict rules to information management, this is not the case in all municipalities. While sometimes evading rules on security may be useful for individual citizens when employees try to help them with their re-integration process, this can result in security breaches with severe consequences. And finally, also a general law on information security is in place. In the Netherlands, both the provider and the user of personal information at the government level are subject to legislation protecting personal data by having to be goal bound and proportionate in their information sharing. This means that both can be held accountable in case of the misuse of personal data.

4 Findings

The main differences between the case study and the discussed security patterns are summarized in Table 1. The left-most column represents the desired high level elements, or blocks, that need to be present to ensure information security by following the security patterns. The correct implementation of these blocks assures the correct use of information providing control, identification and authorization to the protected resource. The next two columns describe how each designed pattern implements these high level blocks. Finally the right-most column describes how the case study implements (or not implements) the high level blocks.

The blocks one the left side, such as Groups, Roles, and Type of Users, represent the technical properties that need to be in place to implement the security patterns presented in section 2. As shown in Table 1, a number of these basic blocks that are part of the implementation of the security patterns are properly implemented in the case study, such as the assignment of groups with different access rights and the single entry point by implementing a log in mechanism. Other blocks, however, are not properly implemented, leading to security threats. The main threats that we identified are the sharing of username/password combinations among employees of different organizations that need to collaborate and access the same applications and

Table 1. Implementation of the security patterns in the case study

Blocks	**E-RBAC**	**Single Check Point**	**Case study**
Groups	Groups managed with different roles	NA	Different groups are distinguished
Types of users	Different types of users with different roles	NA	The different groups have different roles to information access
Roles	Implements roles, simple roles, composite roles and administrator roles	NA	Simple roles implementation
Rights	3 Way rights implemented (Read, Write, Execute)	NA	Multiple way rights
Protected Objects	Implemented	NA	Implemented by ACM
Sessions	Session to link roles to users, and users to rights and user to protected information	NA	Session controls are implemented
Entry Point	NA	Single access point from externals able to identify and to authenticate clients	Implemented by using a username/password combination for log in
Check Point	NA	Single access point from externals able to identify and to authenticate clients	Insufficiently implemented, as it is possible to use someone else's credentials to access the systems

the unauthorized access of information by authorized users. Although sharing the user credentials can be seen as a poor implementation of the technical solution as it is apparently possible to log on to the system without proper identification (such as by using biometric scans), it can be considered predominantly a non-technical problem of users not adhering to the rules of their organization. Therefore, we found that additional organizational arrangements are necessary to ensure information security in this case. Examples include training of employees working with citizen's information, and punishing unauthorized access of information.

The main issues for realizing information security identified from the case study are related to data access control. While measures taken to prevent the system from outside attacks were considered sufficient by the interviewees, unauthorized data access by employees was observed regularly. These issues are on the one hand the result of unauthorized access of information by employees, such as accessing personal information of celebrities, and on the other hand they are the result of organizations not collaborating properly. In the case study, the administrator role was not sufficiently fulfilled to the requirements of all the organizations making use of the applications, leading to insufficient support of the users' needs, and, thereby, to the

sharing of usernames/password combinations. Furthermore, as norms and interests differ across different organizations, security threats also emerge as a result of these differences, while individual employees are not seen to behave in an unauthorized manner. In order to improve data access control and realize information security, all three sources of security breaches need to be mitigated.

5 Discussion

Ensuring data access control for realizing information security is a recurring problem. In recent years, the need for measures to realize information security has arisen more strongly in the field of e-government. More collaboration between public agencies in networks in order to realize integrated service delivery and the increased sharing of citizens' information requires increased attention to information security. Information security in cross-organizational collaboration mainly focuses on the control of information access to be sure that only authorized people are able to read and modify information. As discussed in section 2, different security patterns exist that have been designed for data access control. We concluded, however, that these security patterns are currently only partly implemented in the case study. Furthermore, we found that additional organizational arrangements are necessary to ensure information security. And, finally, we also found that the inter-organizational nature of the collaboration requires these security patterns to be extended to cover threats that emerge as a result of the collaboration between different organizations. Therefore, in this section we discuss some recommendations for increasing information security in cross-organizational collaboration.

Firstly, the security patterns need to be implemented properly. For example, in the case study only simple roles are defined. Secondly, we found that additional organizational arrangements need to be in place besides the proper implementation of the security patterns. Security patterns are merely technical implementations that are not able to mitigate these threats to information security and legal arrangements are often only useful in case harm has already been done, although it can be argued that some level of prevention goes out from having laws against misuse of information in place. Examples of organizational arrangements include the training of employees in information security, and punishing unauthorized use by informing the managers of these employees, publishing unauthorized use in the in-house magazine of the organization, or even firing the employees in case of gross misuse. Further research should look into which arrangements – as well as combinations of technical and organizational solutions – are effective in specific circumstances.

Thirdly, security patterns may need to be extended to cover multiple organizations. Implementing security patterns across multiple organizations presents a challenge for the role of administrator. In the case study the administrator role is linked to one organization, as it is now possible to only assign employees of one organization to applications, or to add employees of different organizations to its HRM systems, which may be undesirable. Furthermore, the division of groups needs to be done according to the differentiation of tasks. In the case study, the employees of the different organizations that collaborate need to use the same information in different ways. The organization having the task to calculate the allowances for those in the

Netherlands that are retiring, do only need to have full information on individual citizens in case someone files a complaint, while the employees having the task of re-integration of the unemployed need to access the information on individuals real-time to be able to help them get a new job. This may lead to different requirements for security of the same application, which may require additional or extended security patterns to be in place.

We recommend that further research should be done to identify which elements are necessary for data access control for realizing information security in cross-organizational collaboration by using arrangements from both spheres. For example, a combination of technical solutions implemented through the use of security patterns and organizational arrangements such as training. Furthermore, to enhance research into information security in inter-organizational collaboration, developing a comprehensive framework comprising both technical and non-technical arrangements is likely to spur new insights. Currently, no frameworks exists for guiding the research analysis process in such a way that it is able to assert whether the analyzed system is sufficiently secure. Such a framework, comprising designed patterns, investigation methodologies, recovery procedures, legal requirements, behavior analysis and interview patterns, can be a next step in achieving a standardized information security level in cross-organizational collaboration.

6 Conclusion

In order to join up their services, government organizations need to exchange citizens' information. To ensure their privacy, data access control is central to realizing information security. Many pre-defined security patterns exist that represent specific solutions to realize security. This paper explores issues related to data access control in cross-organizational collaboration through the application of two of such security patterns: E-RBAC, and Single Access Point/Check Point. To explore their use in practice, we applied these patterns to a case study of public sector inter-organizational collaboration in the Netherlands. We compared the implementation of measures to ensure data access control for realizing information security from the case study with the two security patterns from literature.

We found data access control to be a main issue in realizing information security in the case study, and we also found that additional organizational measures are necessary to mitigate security threats, such as providing training, implementing shared data access norms and punishing unauthorized access of information. Furthermore, the inter-organizational nature of the collaboration requires extending existing security patterns. For example, it requires the role of the administrator to be filled in such a way that is able to fulfill this role for multiple organizations, instead of only one organization. Therefore, we recommend to look further into how organizational arrangements need to be combined with technical and legal arrangements in order to achieve information security. Finally, a related recommendation from this study is the development of a comprehensive designed framework for realizing security in inter-organization collaboration.

References

1. Van Veenstra, A.F., Janssen, M.: Architectural Principles for Orchestration of Cross-Organizational Service Delivery: Case Studies from the Netherlands. In: Assar, S., Boughzala, I., Boydens, I. (eds.) Practical Studies in E-Government: Best Practices from Around the World, pp. 167–185. Springer, New York (2011)
2. Dunkerley, K., Tejay, G.: Theorizing information security success: Towards secure e-Government. International Journal of Electronic Government Research 6(3), 31–41 (2010)
3. Belanger, F., Hiller, J.S., Smith, W.J.: Trustworthiness in electronic commerce: the role of privacy, security, and site attributes. Journal of Strategic Information Systems 11, 245–270 (2002)
4. Carter, L., McBride, A.: Information privacy concerns and e-government: a research agenda. Transforming Government: People, Process and Policy 4(1), 10–13 (2010)
5. Rezgui, A., Wen, Z., Bouguettaya, A.: Enforcing Privacy in Interoperable E-Government Applications. In: Proceedings of the 2002 Annual Conference on Digital Government Research (dg.o) (2002)
6. Bryl, V., Dalpiaz, F., Ferrario, R., Mattioli, A., Villafiorita, A.: Evaluating procedural alternatives: A case study in e-voting. Electronic Government 6(2), 213–231 (2009)
7. Moynihan, D.P.: Building Secure Elections: E-Voting, Security and Systems Theory. Public Administration Review 64(5), 515–528 (2004)
8. Ramilli, M.: Designing A New Electronic Voting System: Towards electronic voting systems. Lambert, Saarbrücken, Germany (2010)
9. Smith, A.D.: Securing e-voting as a legitimate option for e-governance. Electronic Government 4(3), 269–289 (2007)
10. Zhao, J.J., Zhao, S.Y.: Opportunities and threats: A security assessment of state e-government websites. Government Information Quarterly 27, 49–56 (2010)
11. Heyman, T., Yskout, K., Scandariato, R., Joosen, W.: An Analysis of the Security Patterns Landscape. In: Proceedings of the Third International Workshop on Software Engineering for Secure Systems (SESS 2007). IEEE Computer Society, Washington, DC (2007)
12. Araujo, I., Weiss, M.: Linking patterns and non-functional requirements. In: Proceedings of the ninth Conference on Pattern Language of Programs, PLoP (2003)
13. Fernandez, E.B., Wu, J., Fernandez, M.H.: User group structures in object-oriented database authorization. In: Proceedings of the IFIP WG11.3 Working Conference on Database Security VII, pp. 57–76. North-Holland Publishing Co., Amsterdam (1994)
14. Lehtonen, J.P.: A pattern language for key management. In: Proceedings of the eight Conference on Pattern Language of Programs, PLoP (2002)
15. Schmidt, D., Stal, M., Rohnert, H., Buschmann, F.: Pattern-Oriented Software Architecture, Patterns for Concurrent and Networked, vol. 2. Wiley, Hoboken (2000)
16. Schumacher, M.: Security Engineering with Patterns: Origins, Theoretical Models, and New Applications. Springer, New York (2003)
17. Flanders, E.B.F.: Data lter architecture pattern. In: Proceedings of the fifth Conference on Pattern Language of Programs, PLoP (1999)
18. Yoder, J., Barcalow, J.: Architectural patterns for enabling application security, Monticello, Illinois, USA (1997)
19. Braga, A., Rubira, C., Dahab, R.: Tropyc: A pattern language for cryptographic object-oriented software. In: Harrison, N., Foote, B., Rohnert, H. (eds.) Pattern Languages of Program Design, ch.16, vol. 4 (1998)
20. Fern, E.B., Pan, R.: A pattern language for security models. In: Proceedings of the seventh Conference on Pattern Languages of Programs, PloP (2001)

21. Heyman, T., Yskout, K., Scandariato, R., Joosen, W.: An analysis of the security patterns landscape. In: Proceedings of the Third International Workshop on Software Engineering for Secure Systems (SESS 2007), IEEE Computer Society, Washington, DC, USA (2007)
22. Pernul, E.W.G., Tjoa, A.M.: Access controls by object-oriented concepts. In: Proceedings of the IFIP TC11WG11.3, Eleventh International Conference on Database Security XI: Status and Prospects, pp. 325–340. Chapman & Hall, Ltd, London (1998)
23. Fern, E.B., Sinibaldi, J.C.: More patterns for operating systems access control. In: Proceedings of the Eight European Conference on Patterns Language of Programming, EuroPLoP (2003)
24. Kodituwakku, S.R., Bertok, P., Zhao, L.: Aplrac: A pattern language for designing and implementing role-based access control. In: Proceedings of the Sixth European Conference on Pattern Languages of Programs, EuroPLoP (2001)
25. Giuri, L.: Role-based access control on the web using java. In: Proceedings of the Fourth ACM Workshop on Role-based Access Control, RBAC 1999. ACM, New York (1999)
26. Schumacher, M., Fernandez-Buglioni, E., Hybertson, D., Buschmann, F., Sommerland, P.: Security Patterns: Integrating Security and Systems Engineering. John Wiley & Sons, Hoboken (2006)