Improvement of Security Patterns strategy for Information Security Audit Applications

Lyazzat Atymtayeva[1] and Mahmoud Abdel-Aty[2]
[1]*Kazakh-British Technical University , Department of Information Systems Management, 050000, Tole bi str., 59, Almaty, Kazakhstan*
[2] *Zewail City of Science and technology, Giza, Egypt*
l.atymtayeva@gmail.com, amisaty@gmail.com

Keywords: Security patterns repository, application development, security ontology, fuzzy expert systems, information security audit.

Abstract: In the growing influence of information security level onto the business processes at the companies and organizations and their functioning by applying the software applications there is a necessity to develop systems with demanding level of security. Application developers are often confronted with difficulties in choosing or embedding security mechanisms that are necessary for building software secure applications, since this demands possessing expertise in security issues. This problem can be circumvented by involving security experts early in the development process. Usually it is accompanied with very high costs: experts in information security (IS) area are quite expensive specialists. An automation of some security implementation and evaluation tasks can reduce these costs and potentially increase the quality of IS strategies being developed and quality of IS audit processes. We believe that expert systems approach can be beneficial in achieving this automation. Though information security is a very broad field, encompassing many complex concepts, we are trying to develop a methodology of formalizing of IS knowledge to build a knowledge base for expert system that can serve as IS audit expert. With developing the special security patterns repository as a part of common framework for application development we can accumulate knowledge and expertise in the area of security, and help to software developers as well as IS audit stakeholders to have benefits from the processes of automation.

1 INTRODUCTION

Many current systems have serious security problems. We believe that a good way to have secure systems is to build applications and systems software in a systematic way, where security belongs to the part of the lifecycle.

The expert systems approach with developing of ontology can be beneficial in the building of framework for development of secure applications and for automation of processes of information security audit.

Building secure applications is a complex and demanding task developers often face. Meeting the specified security requirements, or embedding security mechanisms, however, is a process that involves expertise in the area of security, which most of the time software developers do not posses. Therefore, security experts often have to be involved during application development. This strategy entails high costs for software development; moreover the communication between developers and security experts is seldom smooth.

The same picture is observed in the processes of information security audit where attracting the security specialists often demands the high costs.

This paper suggests a different strategy for incorporating security in application development to solve the problems of secure software development and some processes of security audit.

It advocates the use of security patterns, by proposing a security patterns repository as a part of common framework for security applications development. The paper also addresses the issue of the limited usability of security patterns in software development, by customizing the patterns' structure so as to include security specific properties, such as threats and vulnerabilities, assets and controls. Thus, this paper aims to

Atymtayeva L. and Abdel-Aty M.
Improvement of Security Patterns strategy for Information Security Audit Applications.
DOI: 10.5220/0005887101990204
In *Proceedings of the Fifth International Symposium on Business Modeling and Software Design (BMSD 2015)*, pages 199-204
ISBN: 978-989-758-111-3

- describe the adapted framework for development of secure applications
- propose an enhanced structure for security patterns
- describe a repository for security patterns in information security applications

Section 2 describes the framework for development of secure applications and security ontology. Section 3 deals with the security patterns in the development process, describes the improvement in creating security patterns repository based on ontology. In conclusions we present the summarizing of research work and define the directions for future research.

2 DESCRIPTION OF FRAMEWORK FOR SECURE APPLICATIONS DEVELOPMENT

The proposed adapted framework is intended for the effective introduction of security attributes in the process of application development. The initial version was proposed by Balopoulos Th. , et.al., 2006. Within the research process, security ontologies were first employed in order to explore how they can help developers better understand the application context and communicate with security experts and with the further expanding how it can use for the automation of the processes of information security audit.

Some results of these efforts have already been published in the works (Buschmann, F., et al., 1996 , Taylor, R.N., et.al., 2010). Following this, the research indicates that security patterns would be an appropriate tool for capturing security expertise, and that this can be formalized by employing security ontologies. Thus, based on the ontologies developed, we can explore the use of security patterns in the specific application contexts: we can design an appropriate structure for security patterns and a security patterns repository (Fernandez, E.B., 2006). This paper presents the adapted holistic framework employed, which can provide a useful solution for developers, especially those involved in the development of security critical applications as well as for the processes of the expert systems development in the area of information security.

This framework is depicted in Figure 1. It serves for incorporating security characteristics and accommodating security requirements in application development.

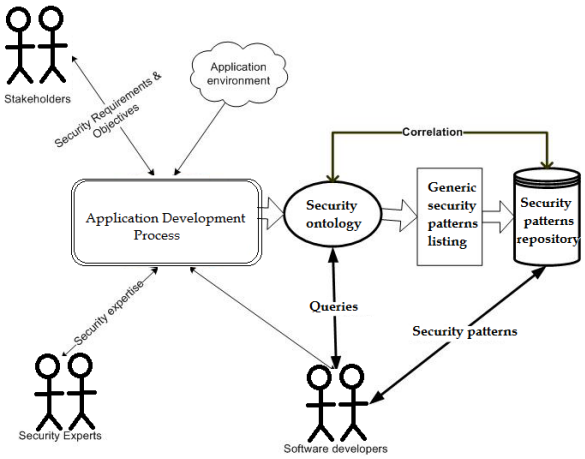

Figure 1: The adapted framework for secure application development.

By following the methodology of secure application development proposed by Balopoulos Th., 2006, we can create the adapted framework that is based on the principles of security ontology and automation of the processes of information security audit. This framework contains the security ontology which generates security patterns stored in repository, the part of application development process which can be presented as a reflection of the processing of a knowledge base for the best understanding of the specific security domain by software developers and stakeholders.

The adapted framework proposed in this paper constitutes an integrated approach that is addressed to developers for their applying the specialized knowledge and for supporting them in making use of recorded solutions to known security issues.

Key actors in this framework include

(a) the system stakeholders, i.e. the application users, the administrators and the management,

(b) security experts whose knowledge and expertise is needed to enhance the application development process by successfully introducing security features in applications, and

(c) the software developers. The latter are the ones that can use this framework for accommodating all different requirements and objectives with regard to security.

Information system stakeholders along with security experts and the software developers set the business and security objectives for the specific application. Existing security expertise is used along with the knowledge of the environment in which the specific application is going to be deployed in order to introduce environment specific security requirements. The development of corresponding ontology makes it possible to achieve the set goals

by capturing and articulating the application context that can be used by developers. The principles of the processing of Knowledge Base in security area allow to create a security patterns and automate the process of the development of secure applications.

2.1 Different Approaches to Use Security Related Issues in Development

Regarding the use of security related issues in software development there are a lot of research and publications. The most of them study elaboration of different software design tools and methodologies like UMLsec (Mouratidis H., and Giorgini, P., 2004, Braz, F., et.al., 2008, Fernandez, E.B. and X.Yuan, 2010), Model-Driven Architecture (MDA) (Basin, D.A., et.al., 2006) , XML based models (Nagaratnam, N., et.al., 2005), industrial approaches like Microsoft solutions (Lipner, S. and Howard, M., 2005).

It is interesting to mention about the other types of security domain applications based on quantum information security. Classical computationally secure cryptosystems may be susceptible to quantum attacks, which means that attacks by adversaries able to process some levels of security via quantum information (Shor P.W., 1994, Biham E., at al 2000). These researches show that unitary bases can be central to both encryption of quantum information, at the same time the generation of states can be used in generalized quantum key distribution.

There are a lot of researches based on the ontological approach (Raskin et al, Dritsas,S.,et.al., 2005, Akerman, A. and Tyree, J., 2006, Voroviev, A. and Bekmamedova, N., 2010), and directions related to security patterns (Mouratidis H., and Giorgini, P., 2004).

We are going to focus on the approaches related to the use of security ontology of knowledge base.

2.2 The Security Ontology

An ontology is a description of the entities and their relationships and rules within a certain domain (Lazaros Gymnopoulos1, et.al. , 2006). Ontologies have been widely used within the fields of artificial intelligence, expert systems and the semantic web, mainly for knowledge representation and sharing. Computer programs can use ontologies for a variety of purposes including inductive reasoning, classification, a variety of problem solving techniques, as well as to facilitate communication and sharing of information between different systems. Ontologies are a great tool for defining and communicating the different ways in which people perceive a specific domain.

Ontology for the expert system is assigned to represent domain specific knowledge in the form which can be used by a computer to effectively operate on this knowledge.

Security ontologies are ontologies covering the domain of security .

In order to consider the combination of ontologies that related to the development of expert system in information security domain we can use proposed framework and all relations (Fenz S. and Ekelhart A. 2009, Maljuk A.A. 2010).

The Security Ontology shown in Figure 1 aims at covering and recording available knowledge regarding business and security objectives of a specific application development environment.

During the development of Expert systems for Information Security area (Atymtayeva L., et.al., 2014) we used adopted security ontology (Fenz S. and Ekelhart A. 2009, Maljuk A.A. 2010) that consists from four main entities and relationships between them(see Figure 2) .

The ontology is divided into two parts: the concepts representing information security domain knowledge (which actually are core concepts of the domain) and the concepts representing concrete information about considered organization, which are essential in measurement of its security level. These concepts are:

-Threat is a potential cause of an unwanted incident, which may result in harm to a system or organization [ISO].

-Vulnerability is a physical, technical or administrative weakness which could be exploited by threats.

-Control concept is used to mitigate vulnerabilities by implementing either organizational or physical measures.

-Asset is anything that has value to the organization [ISO]. Also assets are used to implement controls.

The most important relations between these concepts are:

-Threat threatens asset.

-Vulnerability is exploited by threat Severity.

-Vulnerability is mitigated by control.

-Control is implemented by asset Effectiveness.

-Asset has vulnerability.

The process followed for developing the security ontology, based on the method proposed by Akerman, A. and Tyree, J., 2006, is iterative and includes four phases: determining competency questions, enumerating important terms, defining classes and the class hierarchy, and finally, the instantiation of the hierarchy.

The competency questions which guided the security development process are loosely structured security oriented questions that the developed security ontology should be able to answer. These questions are taken from typical situations developers face when confronted with security requirements. Next, the most important terms with regard to security were enumerated; the most important of them formed ontology classes; others formed properties of classes and some were not used at all.

The main relations between ontology components and questionnaire process are depicted on the figure 2.

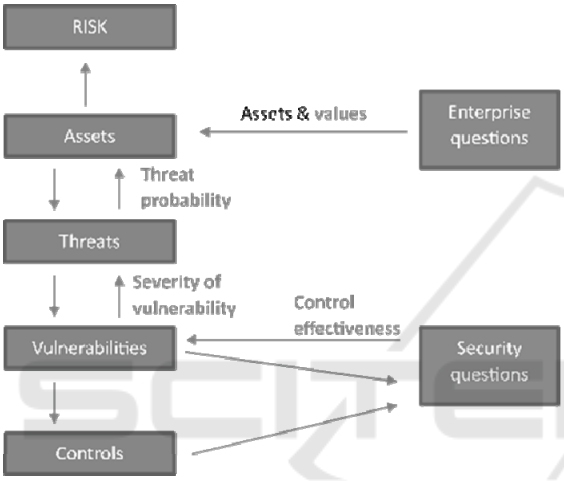

Figure 2: Security Domain Expert System Ontology.

For more precise definition of significance of questions and their ranking as well as the impact of the answers we use the special weight coefficients (Atymtayeva L., et.al., 2012). These coefficients allow make it easy the classification of questions during the process of their selection. This approach is very useful for developing of fuzzy expert system.

In adapted framework to examine the rigor of the Security Ontology developed we use queries (or specially constructed logic) expressed in the Fuzzy Relational Inference Language (FRIL). This language uses micro-logic, logic programming associates and support fuzzy logic, meta-programming and can be helpful for constructing the logic of queries (Protsenko N., Atymtayeva L., at all, 2012).

3 SECURITY PATTERNS IN SYSTEM DEVELOPMENT

In 1993 Gamma introduced patterns and since then their application in software development has continuously grown. This section is devoted to description of software and security patterns, and ways of designing the security repository.

3.1 Software and Security Patterns

Software patterns predefine a solution of recurring software development problems by specific way.

By using existing, well-proven experience in software development they can help promoting effective software design practices.

Each pattern may relate to the specific, repeating problem in software design and can be used to build applications with definite properties. So, "a pattern for software architecture describes a particular recurring design problem that arises in specific design contexts, and presents a well-proven generic scheme for its solution" (Buschmann et al. 1996). The solution scheme is defined by describing its constituent components, the existing relationships, and the ways in which they collaborate.

Patterns can provide a systematic and effective development of high-quality applications with defined functional and non-functional requirements. There are a lot of advantages of using patterns in software engineering (Buschmann et al. 1996).

A pattern system is defined as a collection of patterns for software architecture, including guidelines for their implementation, combination and practical use in software development. The main aspect for security patterns to be effectively used is its concise categorization within each pattern system.

The evolution of software patterns leaded to the modification of the concept of security patterns that was introduced in order to incorporate security techniques and best practices into the software development process.

A security pattern can be defined as a particular recurring security problem that arises in a specific security aspect, and presents a well-proven generic scheme for its solution (Schumacher 2003).

Application of security patterns can help bridge the gap between security professionals and system developers. Security patterns can assist developers implement effective security solutions and use them "in a right way". Security patterns are described by using a set of predefined elements, which compose the structure of the pattern, and their values (Balopoulos Th. , et.al., 2006).

The fundamental structure for describing and developing security patterns consists from the following six main elements (as was proposed by Schumacher 2003 and Kienzle et al. 2005):

Name of Element \ Security Context (a.k.a. Motivation) \ Security Problem \ Security Solution \ Forces \ Related Patterns (a.k.a. Security Pattern Relations)

The complementary elements of security pattern may include information about examples, resulting context, rationale, known uses, and etc.

3.2 Design of Security Patterns Repository

The problems in using security patterns based on the mostly ad hoc way accompanied by failed communication between security experts and the software developers generates the necessity in creating a security patterns repository.

In order to design the repository of security patterns, we first had to decide on their structure. In order to develop a security patterns' structure that would accommodate the security related requirements of using patterns, it was developed a security ontology, based on the one presented in (Dritsas et al. 2005). An ontology is a logical theory accounting for the intended meaning of a formal vocabulary. The intended models of a logical language using such a vocabulary are constrained by its logical commitment. An ontology indirect reflects this commitment (and the underlying conceptualization) by approximating these intended models (Mekhilef 2003). Thus, an ontology is the attempt to express an exhaustive conceptual scheme within a given domain, typically a hierarchical data structure containing all the relevant entities, their relations and the rules within that domain.

Based on the fundamental structure of security pattern by using the comprehensive information about security elements and relations between them together with their impact of each other we can construct the detailed security ontology depicted on figure 3 (Atymtayeva L., et al. 2014).

This ontology besides the main elements described before includes the additional elements (by adaption of the security ontology of Dritsas et al, 2005) such as Stakeholder\ Objective and Attacker \Attacks and their relations to the main model. All other elements has the relations of each other caused by the sources and reasons for their appearance in the model.

The ontology depicted in Figure 3, aimed to

(a) capture and express the most important security concepts for application development,

(b) describe the relations among these concepts,

(c) provide a common understanding and vocabulary of security issues among application developers,

and (d) facilitate the development of secure applications.

Thus, the developed ontology comprises a rich source of information regarding the security requirements of the specific application environment and, more importantly, is also a source of

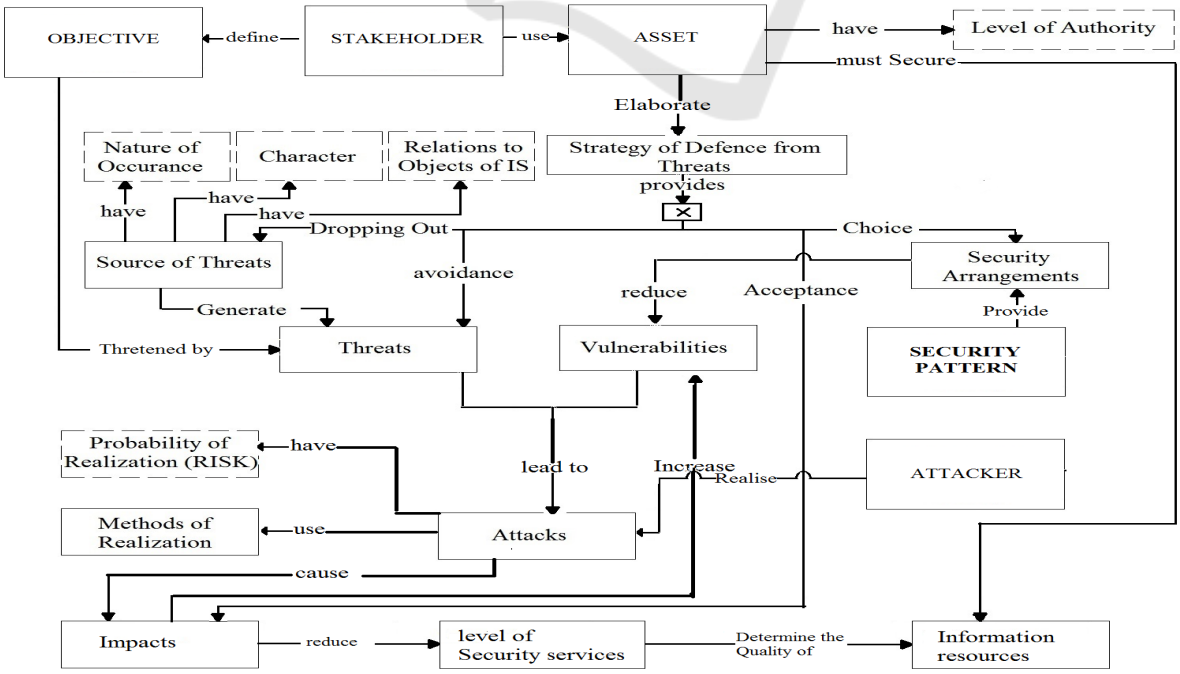

Figure 3: Detailed security ontology.

information regarding the way several key actors in the software development process view and judge those requirements.

4 CONCLUSION

This paper introduces some elements in improvement of representation security components with integration of software components by using security patterns and creating the security patterns repository. It was shown that this approach may be used to development of expert systems in security domain.

It was shown the improved security ontology with taking into account the elements of fuzzy expert system.

The security patterns repository and security patterns approach provides opportunity to software engineers, who are not security experts, to make the appropriate choices regarding security mechanisms and solutions, thus facilitating the development of secure applications. As a next step, this repository will be employed in the development of a security domain application, such as development of expert systems for information security active audit.

REFERENCES

Akerman, A. and Tyree, J. 2006. Using ontology to support development of software architectures. *IBM Sys. Journal, vol. 45, N0 4,* pp. 813-825.

Atymtayeva L., Kozhakhmet K., Bortsova G., Inoue A. 2012. Expert System for Security Audit Using Fuzzy Logic. *Proc of MAICS, April 21-22, 2012, Cincinnati, USA,* pp. 146-151

Atymtayeva L., K. Kozhakhmet, G. Bortsova, 2014, Building a Knowledge Base for Expert System in Information Security. *Soft Computing in Artificial Intelligence Advances in Intelligent Systems and Computing Volume 270*, pp 57-76

Balopoulos Th. , et.al., 2006. A Framework for Exploiting Security Expertise in Application Development. *In Lecture Notes in Computer Science,* Volume 4083, pp 62-70

Basin, D.A., Doser, J., and Lodderstedt, T. 2006. Model driven security: From UML models to access control infrastructures. *ACM Trans. on Software Engineering and Methodology, vol. 15, No 1*,pp. 39-49

Biham, E. Boyer M., Boykin P. O., Mor T., and Roychowdhury V. 2000. A Proof of the Security of Quantum Key Distribution. *Procs of the 32'nd Ann. ACM Symposium STOC'00, ACM Press*, pp. 715-724.

Braz, F., Fernandez, E.B.,and VanHilst, M. 2008. Eliciting security requirements through misuse activities. Procs. of the 2nd Int. Workshop SPattern'07, Turin, Italy, September 1-5, 2008, pp.328-333.

Buschmann, F., et al. 1996. *Pattern- oriented software architecture*, Wiley.

Dritsas,S., Gymnopoulos, L., Karyda, M., Balopoulos, T., Kokolakis, S., Lambridounakis, C., and Gritzalis, S. 2005. Employing ontologies for the development of security critical applications. *Procs, of the IFIP I3E Conf., Oct. 2005,* pp.187-201.

Fenz S. and Ekelhart A. 2009. Formalizing information security knowledge, *ASIACCS '09, ACM.*

Fernandez, E.B., Larrondo-Petrie, M.M., Sorgente, T., and VanHilst, M., 2006. A methodology to develop secure systems using patterns, Chapter 5 in "*Integrating security and software engineering: Advances and future vision*", H. Mouratidis and P. Giorgini (Eds.), IDEA Press, pp. 107-126.

Fernandez, E.B. and X.Yuan. 2010. Semantic analysis patterns and secure semantic analysis patterns", in revision for the *IJICS, Inderscience Publishers*.

Gamma E., 2001. Design patterns ten years later. *In Broy, M., Denert, E., eds.: Software Pioneers: Contributions to Software Engineering, Springer-Verlag*. pp. 689–699.

Lazaros Gymnopoulos1, et.al., 2006 Developing a Security Patterns Repository for Secure Applications Design

Lipner, S. and Howard, M. 2005. The Trustworthy Computing Security Development Lifecycle, *MSDN Library*

Maljuk A.A. 2010. Information Security: Contemporary Issues*, Security Information technology; № 1,* pp.5-9.

Mouratidis H., and Giorgini, P. 2004 Analysing security in information systems. Procs. of the 2nd Int. Workshop ICEIS 2004, Porto, Portugal.

Nagaratnam, N., Nadalin, A., Hondo, M., McIntosh, M., and Austel, P. 2005. Business-driven application security: from modeling to managing secure applications. *IBM Systems Journal, vol. 44, No 4,* pp.847-867

Protsenko N., Atymtayeva L., Kozhakhmet K. 2012. Using FRIL in Development of Expert System Applications, *Proc. ICITM 2012, Riga, Latvia*, p. 98.

Shor P. W. 1994 Algorithms for quantum computation: Discrete logarithms and factoring. *In Procs of the 35nd Annual Symposium on FCS IEEE CSP*. pp. 124–134.

Schumacher M., Fernandez E.B., et.al., 2006. *Security Patterns: Integrating Security And Systems Engineering*, John Wiley&Sons Inc.

Taylor, R.N., Medvidovic, N., and Dashofy, N. 2010. *Software architecture: Foundation, theory, and practice*, Wiley.

Voroviev, A. and Bekmamedova, N. 2010. An ontology-driven approach applied to information security. *J. of Research and Practice in Information Tech., vol. 42, No 1,* pp.61-76.