Designing Security System Using Aspect Model

Mario Sajko, Danijel Radošević
Faculty of Organization and Informatics, Pavlinska 2, 42000 Varaždin, Croatia
{mario.sajko;danijel.radosevic}@foi.hr
Tedo Vrbanec
The Faculty of Teacher Education, Ante Starčevića 55, 40000 Čakovec, Croatia
tedo.vrbanec@gmail.com

Abstract: *Complexity and high number of cause-effect relationships in information systems aggravates observing and managing information security issues. What is missing here is the method of conceptual modeling that will be used for describing and visualizing features and interdependence of security system elements. Up to now there have been some attempts to solve this problem, but the existing solution does not satisfy completely. What is suggested in this paper is a graphic technique of conceptual modeling based on the aspect model following the example of the application generator script model. Such modeling of a security system is used in solving the problem of multiple inheritances of security attributes and it makes the analysis of complex hierarchy among the security objects possible to be observed from different aspects. In this paper we have defined some basic graphic elements of aspect model used to show information resources and their relationships and attributes as well as protection measures, and the way of forming models is shown on the examples.*

Key words: security, aspect model, security model

1. Introduction

Information security issue (*infosec*) is an important part of business planning. The demands of government institutions as well as the demands of indirectly international integrations have a great influence on even more and more increasing trend of interest for *infosec*, besides more common security incidents. Information security is even less and less a means of differentiation among business subjects, but more a demand which is a component part of business.

Infosec managing process is marked by the use of different approaches and the use of formal and informal solving methods [9], [2]. There are numerous concepts for IS revision, methods and methodologies for security risk assessment, additional software tools maturity assessment models, tools for observing security systems performances, norms and security criteria. What is typical is that they have more similarities, sometimes they even have important differences, but generally speaking we can say that they mutually complete. So we can differ different approaches with typical group representatives [5]:

- Process oriented, (ISM3, CMMI, ISO9001:2000, ITIL/ITSM);
- Controls oriented (ISO27001:2005, BSI-ITBPM , ISO13335-4);
- Product oriented (Common Criteria / ISO15408);
- Risk analysis oriented (CORAS, CRAMM, Magerit, Mehari, Octave);
- Best practice oriented (ISO/IEC 17799:2000, Cobit, ISF-SGP).

Despite their big number and longer time period during which *infosec* is very important, there are also some determined unknowns and obscurities in security risk management. It is still unknown which approach is the most suitable one to a particular problem. The choice has been determined by bigger number of criteria that take into consideration all features of a business subject as well as security demands coming from different sources.

1.1. Experiences

Recently it has become obvious that security solutions should be integrated. The reason for that is the fact that business subjects have to implement security system according to more than one security concepts because of different security demands (law regulations, business partners, other countries standards, satisfying international norms). During forming and implementations of security systems CISO engineers more frequently connect different solutions into one integral system. That is the reason why in technical and scientific literature readers can find many similarity and difference analysis of particular approaches that through the so called “security direction mapping” are trying to establish overlapping and similarities.

Regardless of the chosen infosec problem solving approaches, in all approaches it can be observed the lack of techniques for modeling and graphic description of security systems. The previously mentioned approaches are concentrated on information assets and connect it with business processes. In that way they determine the way to keep business uninterrupted, or they give directions for development of the so called best practice [4]. In risk assessment regarded as a security promotion

instrument, information infrastructure is connected with potential threats.

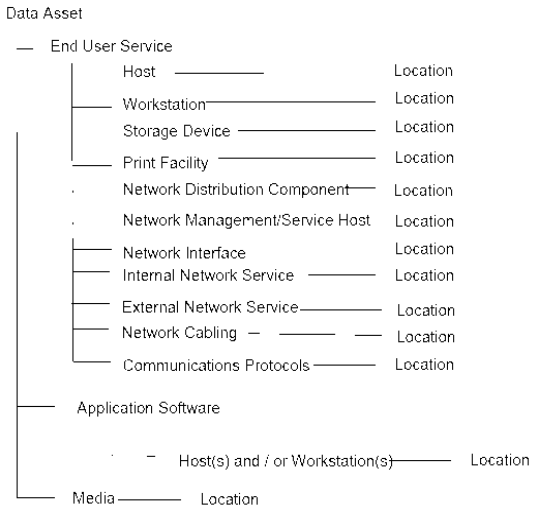
But all these approaches concentrate more on the questions “what” (should be done) while on the other hand they do not give the answers on the question “how” (to do it)”. That is the reason why formation of a security system can become a very tiring process. That happens because of an interdisciplinary area integrating organizational-technical-human security aspects and special features of information infrastructure existing in many forms (material and immaterial), and it can be very complex when we talk about information contents.

The question of security system modeling or visualization of its elements (information assets) and their associated features (risk, vulnerability, importance etc.) has not been adequately solved yet nor in literature nor in security practice. That is why some specific problems appear, and particularly those concerning security and cost planning, as well as observing connections and relations among the components of a security system

1.2. Related work and idea of this paper

CRAMM Expert software package, which is a part of the similar method [3] is mentioned as one possibility for visual modelling that we can mostly find in practice.

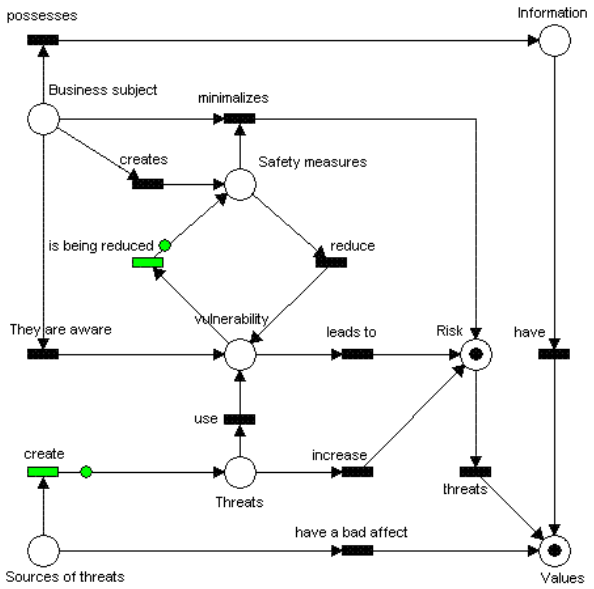
It can be used for describing mutual connection of data assets with physical assets, locations and software assets. In that each pair data asset/end-user service is created by separate models. A data asset is the type of assets the financial or quantitative value of which is very important for a business process. End User Services is CRAMM information assets concept which defines the way of keeping, analyzing and transferring data. The model is used for defining hierarchical relation of threats for particular information means and inheritance principle among the system elements (Picture 1).



Picture 1: Metamodel of relationships and connections among information assets [3]

Petri nets are the second option that we can find in practice [11][1].

Security system modeling is supported by tools as CPN and ReNew for coloured nets (colour petri nets). In that, resources (information assets) are marked with a circle and their relationship with a rectangle. Tokens (circles) represent the action initiator. The example of designing with the help of these tools is shown in the picture (down). Petri nets are more suitable to operatively-technical security segment and less to operative, human and organizational component. One example of Petri nets use in describing security system is shown in picture 2.



Picture 2: Example of graphic modelling of security risk factors by Petry nets

This is the reason why the purpose of this research is to expose presumptions for conceptual modelling of a security system based on aspect model.

Such way of planning security system elements will facilitate the installation of a security system as well as the managing of the already built system.

1.3. Outline

Aspect model of a security system or in other words its elements and the way of modelling are presented in the further part of the text. First of all, what is described is the graphic and verbal description technique of security system features. Point 2.1 describes the basic idea of such model. Point 2.2 describes the symbols and role of particular aspect model elements. Point 2.3 shows the example of using the model in case study. Point 3 tends to describe clearly the sequence of steps under which the model is being formed. Point 4 considers the possibilities for using the shown model in practice, and the final chapter 4 brings the conclusion.

2. Security aspect model

Aspect model is first of all a graphic model of a security system. So in the further part of the text it will be described through:

- Basic elements
- Way of formation.

Basic elements include all security factors of some information system as information resources or assets and their value, security threats and assets vulnerability. They are represented by adequate symbols and connections with other elements. Beside this here is also the size of risk for a particular resource, way of detecting and observing security, way of reporting and other features that make verbal description of a system.

2.1. Basic idea of aspect model

The idea about aspect security model was taken form generative programming as a discipline of automatic programming. In that, aspects were representing features that are not tied to particular organization programme units as functions or classes, but can appear in different parts of applications [7]. That was defined with the adequate model, so called *Join points* model [6], similarly to the meta-scripts diagram [8] in generator scripting model[8].

In the framework of security model on one hand we are talking about security threats or dangers for normal functioning of a system. And on the other hand we are talking about security measures by which we want to decrease the exposure of a system and its components to security threats. The idea brought in the further part of this paper is to present the security system by aspect model, following the example of the already mentioned generator scripting model.

In the case of security system modeling, protection measures would have the role of aspects similarly to specification elements in generator model. The assumption is that a particular protection measure can be applied in different parts of the system that is being protected. In this case we can state such protection measure within specification and join it to different resources responding to meta-programs from script model. Such joining is done through responding connections that in this case are threats (protection measures are joined to threats).

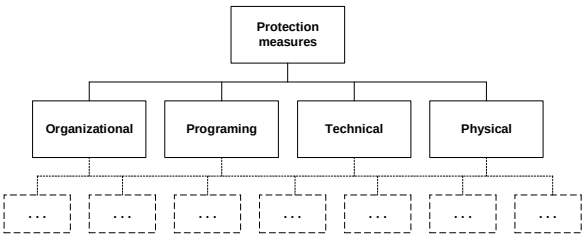
It is expected that security model is made for a particular kind of protection (e.g. data protection or physical protection) and that it consists of two diagrams:

- *Specification diagram*
- *RTP diagram (Resource-Threads-Protection).*

The *specification diagram* defines the used protection measures, and the *RTP diagram* defines their joining to resources inside a security system.

2.2. Aspect model diagrams and specifications

Specification of security measures is defined by the specification diagram, in which the starting point is basic division of protection measures (according to [10]) that divides them in organizational, programming, technical and physical. *The Specification diagram* is a hierarchical diagram used for defining types of the applied security measures in the system (picture 3).



Picture 3: The specification diagram

Specification consists of attribute-value pairs, where attributes are defined inside the specification diagram, as in the following case:

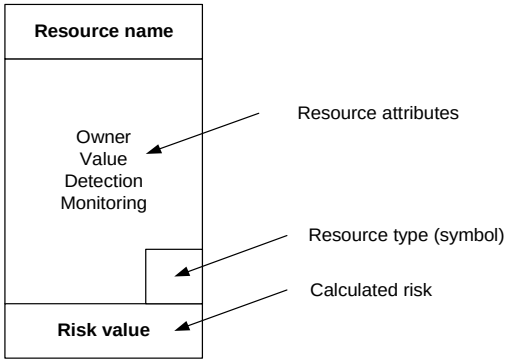
Security measures
Organizational
<attribute> : <value>
. . .
Programming
<attribute> : <value>
. . .
Technical
<attribute> : <value>
. . .
Phisycal
<attribute> : <value>
. . .

The Resources-Threads-Protection (RTP) diagram is defined by three basic elements:

- Resources
- Security threats
- Protection measures.

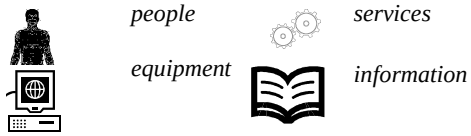
Resources present all that could be exposed to security risk, and must be protected. We use a rectangle for marking resources, inside which we inscribe values of the responding (picture 4) as well as the other attributes.

- Resource owner (responsible person)
- Threat detection instruments
- Way of observing resource performances
- Risk size as a product of value intensity, threat and protection.



Picture 4: Resource

The Resource diagram presents a resource hierarchy of the protected system with joined threats and protection measures. It is expected that threats and protection measures are inherited from superior to inferior resources. In that, within each of this group, it is possible to define the produced number of subgroups. Resources are divided in four groups, what is defined with the right symbol (picture 5).

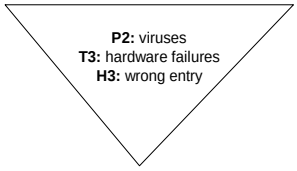


Picture 5: Used symbols for resources

Threats are classified in 5 categories what is subsequently marked with the responding letter. Intensity 1-5 or 1-3 depending on the chosen classification is joined to each threat.

Threats are marked with the sign of a triangle in which types of threats (initial letter) and intensity (number 1-5 or 1-3) are inscribed (Picture 6).

Protection measures in a security model are joined to resources. Protection measures are presented by a rounded rectangle in which types of protection (initial letter) and intensity (number 1-5 or 1-3) are inscribed, and descriptively (picture 7).

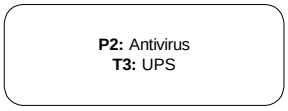


Picture 6: Security thread

A group in which threats and protection measures are joined to resource is defined for each particular resource exposed to security threat. The classification of protection measures consists of 4 categories what is the same as with threats marked with initial letter:

- Organizational (O)
- Programming (S - software)
- Technical (T)
- Physical (P).

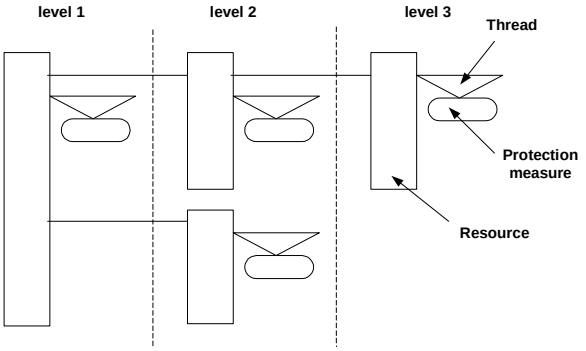
The assessment of protection measure intensity is indirectly used to establish resource vulnerability (or resistance) on threats activities.



Picture 7: Protection measure

2.3. Schedule of elements on the RTP diagram

The RTP (*Resources-Threads-Protection*) diagram is a multi-level diagram, or we can differ resources of higher and lower level in the framework of a security system. Resources of lower level inherit threats and protection measures from resources of higher level, and are as well exposed to their own threats and have their own protection measures (picture 8).



Picture 8: Formation of elements on RTP diagram

Inside the RTP diagram, previously described attributes (threat intensity, protection intensity, owner, detection instrument, value etc.) are joined to resources. These attributes are marked with numbers (1-the highest intensity, 5-the lowest) or descriptively (high, medium, low), and some other classifications are also possible.

Table I: Intensities of threads, vulnerability and value of the assets

descriptively 1-5	descriptively 1-3	number 1-5
Very Low	High	1
Low	Medium	2
Medium	Low	3
High		4
Very High		5

3. Forming model on the example

To show in which way the presented model is formed in case study, we are describing a few forming steps that can be divided in following:

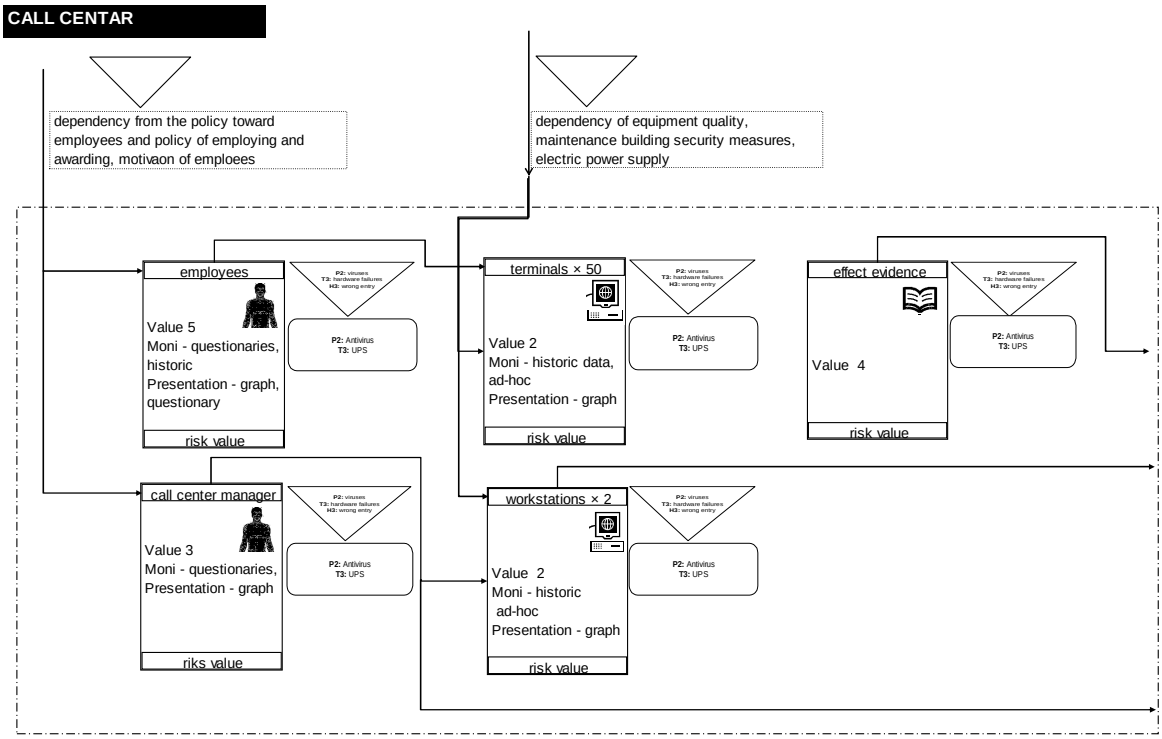
- Resource specification
  - Information assets list according to type, and relation according to other elements of the system
  - Other assets attributes entering
- establishing connections as "inherit from"
- drawing the RTP diagram respecting hierarchical order of system elements entering (from left to right)
  - Level 1: human resources
  - Level 2: equipment
  - Level 3: services
  - Level 4: information
- threats specification and security measures
- risk size entering

As an example we are showing a model of a real security system consisting of elements specified in table II.

Table II: Elements of guarded system

Name	Asset
50 PC computer	material
Workstation	material
Business report	information
Manager	human
50 employees	human

The example in picture 9 shows the way of forming the system composed of the stated resources. The system inherits the threats defined inside the resource of the observed subsystem and some other threats with the responding protection measures.



Picture 9: RTP diagram of real system

4. Conclusion

The conceptual security system model is suggested in this paper. This model is based on graphic diagrams.

It is called aspect model, as some protection measures can be joined to different resources, independently on organizational units where these resources are located. In other words they present security aspects. The purpose was to make security system easier to survey, thanks to visual presentation of its elements, which should later lead to easier security risk assessment. With such security system

modeling the following direct advantages are achieved:

- Model can be used in different security systems and security problems
- Visual, simple and well laid out way of showing security features of a particular information resource, threats, protection measures and connection with a superior object are shown
- Hierarchical specification of security measures, specified security measures are joined to responding resources
- The model is suitable for implementation on the computer.

The biggest benefits are expected in security risk assessment, as inside the protection measure model they are directly opposed to security threats together with their intensity

5. Bibliographic references

[1] H.Arafat Ali, A new model for monitoring intrusion based on Petri nets, Information Management & Computer Security 9/4 2001 175-182, MCB University Press

[2] Baća M., Sajko M., Rabuzin K.: Pregled najčešćih cjelovitih metoda procjene rizika sigurnosti informacijskog sustava, Policija i sigurnost, MUP RH, Zagreb, 2004

[3] CRAMM Expert, CRAMM Expert Home Page, http://www.cramm.com/, June 2007

[4] Gerber M., Solms V. Rossouw: From Risk Analysis to Security Requirements, Computer & Security, No. 20, <http://www.sciencedirect. com> November 2002

[5] ISM3: Information Security Management Maturity Model, -http://www.ism3.com/, 2007

[6] Kandé, M.M., Kienzle,J., Strohmeier, A.: From AOP to UML - A Bottom-Up Approach, 1st International Conference on Aspect-Oriented Software Development, 2002, Enschede, The Netherlands, http://lglwww.epfl.ch/workshops/ aosd-uml/Allsubs/kande.pdf, June 2004

[7] Lee, K.W.K.:An Introduction to Aspect-Oriented Programming, COMP610E: Course of Software Development of E-Business Applications (Spring 2002), Hong Kong University of Science and Technology, 2002

[8] Radošević, D.; Integration of Generative programming and Scripting Languages, doctoral thesis, Faculty of Organition and Informatics, Varaždin, Croatia, 2005

[9] Sajko M.: Analiza temeljnih pristupa unapređenju sigurnosti IS-a, Zbornik radova, MIPRO 2005, Opatija, 2005

[10] Sajko M.: Metrics for description of specific and general characteristics of security system, MIPRO 2006, page 176-180

[11] Yuan H., Frincke D., Tobin, D., Planning, Petri Nets, and Intrusion Detection
Center for Secure and Dependable Software, Department of Computer Science, University of Idaho