Security Risk Analysis and the Security Need in Citizen Oriented Applications

Dragos PALAGHITĂ, Bogdan VINTILĂ
Economic Informatics Department, ASE, Bucharest, Romania
mail@dragospalaghita.ro, vb@vintilabogdan.ro

The paper presents the concept of citizen-oriented informatics application. Types of citizen-oriented informatics application are considered. The ambient environment of risk is analyzed. A risk analysis model for citizen-oriented applications is developed. Based on the model risk assessment formulas are presented.
***Keywords**: security, risks, model, informatics application, citizen-orientated*

1 Introduction

The continuous development of the IT&C leads to the need of developing new informatics applications that use the new technologies. The old applications are developed to solve a certain problem, have limited functionality and high maintenance costs. In the knowledge economy a new category of informatics applications appears, which benefits from the advantages of using the new technologies and is based mainly on knowledge in the developing and maintenance processes. The new category is represented by the citizen oriented informatics applications.

Citizen oriented informatics applications aim at the maximization of the user's satisfaction [4]. The target group of the citizen oriented informatics applications is very big and it is represented by all the persons that must solve a certain problem. Considering the diversity of the target group, in order to maximize the user's satisfaction, the citizen oriented informatics applications must comply with certain quality characteristics that are not a necessity for the classic informatics applications. The citizen oriented informatics applications are characterized by:

- inexistent or very low using costs;
- available online, granting access to users disregarding the geographical location or hardware platform;
- auto configuring, allowing users to speed up their access to most used options of the applications;
- customizable;
- ensures the correctitude of the results;
- completeness assumes solving of all the problems that could appear while solving the problem the application was developed for;
- maintenance costs quantified by time and economic resources are very low assuring a long lifecycle;
- have intuitive user friendly interfaces so as the users need no previous training in using the informatics application;
- portability;
- precision represents the application's property of computing using a large number of decimals;

The higher these characteristics are complied with, the higher the user's satisfaction is. User satisfaction comes also from the security level insured by the informatics application. Security is a basic quality characteristic of every application either web based or distributed. Considering the fact that the evolution of the IT&C market is geared towards a fully interconnected market place this poses high security risks for both companies and users. Thus the breach a computer terminal in this type of network will jeopardize the whole network and cause damage that will have an impact on everybody that is relaying on it.

A key point in ensuring an application is safe is determining the risk that will affect the it during its life time. Risk is a complex measure which is not easily approximated as there are many factors that influence it.

2 Types of citizen oriented informatics applications

Considering the very large and diverse target group, the citizen oriented informatics applications are also very diverse in order to solve all the problems. These applications are categorized using many criteria as follows:

Interaction criterion is classifying the applications by the application's degree of interaction with the user. This leads to the following types:

- applications that the user doesn't supply data to;
- applications in which the user selects the input data from predefined lists;
- applications in which the user supply input data;

Content criterion classifies the informatics applications by the content modifications in time. The following types of applications are obtained:

- static content applications;
- applications which content modifies through appending data;
- applications which content is time dependable;
- dynamic content applications;

Complexity criterion takes into consideration the number of solved sub-problems, the flexibility of methods, selection criteria, diversity of resource allocation and payment methods. Following types are identified:

- specialized applications;
- medium complexity applications: e-store, virtual museum;
- high complexity applications: e-banking, stock exchange transactions;

Security criterion is considering the security to be the very important. As it is indeed a very important characteristic, the users always chose to use a secure application to an unsecure application's detriment even if the costs are higher [7]. By this criterion the application types are:

- secure applications;
- unsecure applications;

Cost criterion classifies the applications by the costs raised by their use. The identified types of applications are:

- free applications;
- session-pay applications;
- applications that are used with a subscription;
- applications for which the user pays a license of use;

Other criteria can be defined for classifying the citizen oriented informatics applications. The classifying criteria assure a division of the applications by criteria directly regarding the citizens. The clearer the application's classification on the criteria base, the quicker the citizen decides to use a certain application from the multitude of applications.

3 Risk analysis

According to [2] and [5] risk analysis plays an important role in ensuring an effective security policy in citizen-oriented applications.

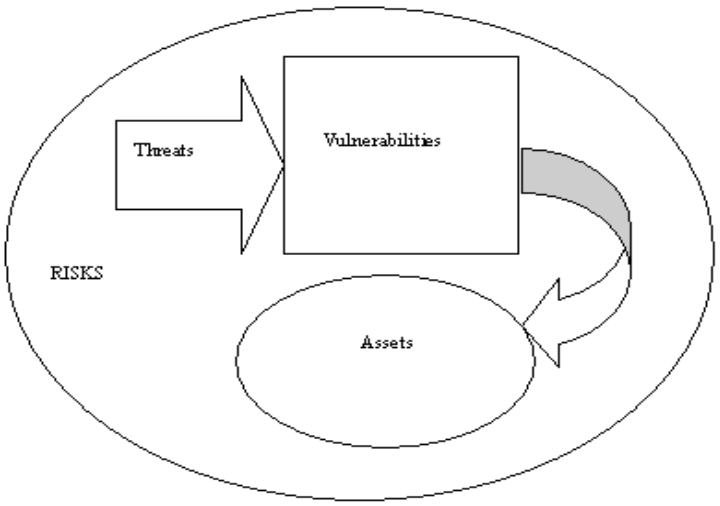

Fig. 1. Ambient environment of risk

The risk analysis has the following advantages:

- development of secure applications;
- minimizes development costs;
- identify application vulnerabilities;
- simplify the work of programming, providing programmers clear specifications about combating risks;
- plays an important role in decisions regarding the security architecture of the application [1]
- better monitoring of assets and protection [1];

The risk is measured according to [1] by vulnerabilities, threats and assets. To better estimate the risks a model for efficient risk analysis is needed. Model risk analysis is developed in [3] based on three elements that form the ambient environment of risk:

- the vulnerabilities model;
- the threat model;
- the goods model.

Figure 1 illustrates the ambient environment elements of risk as described above.

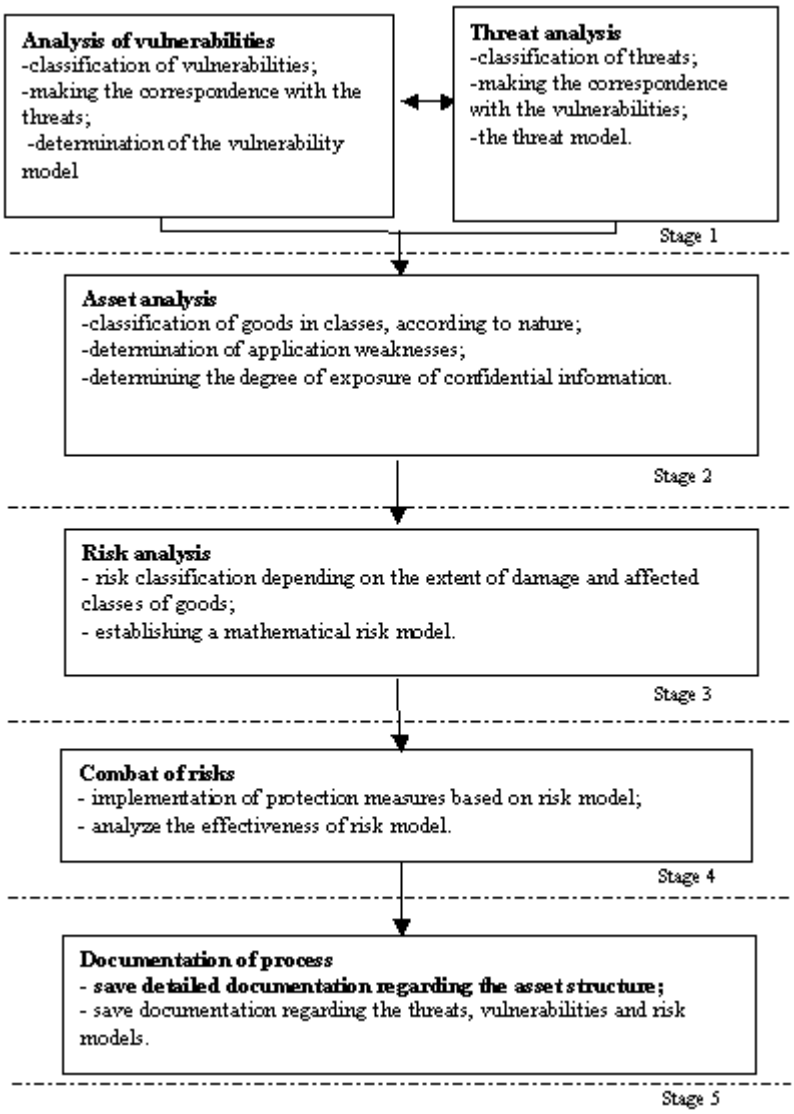

Fig. 2. Risk analysis model

A risk analysis model needs to be developed in order to easily identify each component and its contribution as a risk factor.

The model is an adaptation of [1] made up of five stages, each describing particular models. The model is presented in figure 2.

Stage 5 is crucial for future risk analysis processes as it forms the basis of statistical

analysis categorizing the risk countermeasures according to the results they provide. The statistical results will provide an increase in value of the model because using the available knowledge base there will be significant cost reductions when choosing the right strategy to handle a risk.
The presented model is designed to be used in a preliminary risk assessment in order to identify the core components of risk.

3.1 Quantitative risk analysis

In **stage 1** there are two models:
A. The vulnerability model, formed from the set of vulnerabilities $SV = \{V_1, V_2, \ldots, V_n\}$ which has associated the set of probabilities $PSV = \{PV_1, PV_2, \ldots, PV_n\}$. Where V_i represents the vulnerability i, and PV_i is probability that the vulnerability was being exploited. The result of the vulnerabilities model is the vulnerability matrix, presented in Table 1.

Table 1. Vulnerability matrix [1]

Vulnerability	Exploit probability
V_1	PV_1
V_2	PV_2
…	…
V_n	PV_n

B. The threat model is composed of a set of threats $SA = \{A_1, A_2, ..., A_m\}$, with has associated a set of probabilities= $\{PA_1, PA_2, \ldots, PA_m\}$. Where A_i is the threat i, and PA_i represents the probability of the threat to quantify. The result of the threat model is the threat matrix presented in Table 2

Table 2. Threat matrix [1]

Threat	Appearance probability
A_1	PA_1
A_2	PA_2
…	…
A_m	PA_m

Stage 2 has been materialized in the development of the goods model which is represented by all the goods used by the application $SB = \{B_1, B_2, \ldots, B_k\}$.
Stage 3 represents the analysis of risks occurrence probability. It is considered that a threat exploits a set of vulnerabilities, each vulnerability of the set has an exploit probability PV_i, thus a matrix of perceived risk is developed by adapting the model described by [1] adding the consideration of threats at the vulnerability collectivity level, the matrix is presented in table 3.

Table 3. Exposure to risk model through the sets of vulnerabilities.

Threat	Appearance probability		Vulnerability set	B_1	B_2	B_3	...
A_1	PA_1	→	SV_1	PSV_1EB_1	PSV_1EB_2	PSV_1EB_3	...
A_2	PA_2	→	SV_2	PSV_2EB_1	PSV_2EB_2	PSV_2EB_3	...
A_3	PA_3	→	SV_3	PSV_3EB_1	PSV_3EB_2	PSV_3EB_3	...
…	…	→	…	…			…

where:
SV_i – no. i vulnerability set
PSV_iEB_j – the exploit probability of one or more vulnerabilities from set i in order to get access to asset j; PSV_iEB_j is computed as:

$$PSV_i EB_j = \prod_{k=1}^{v} PV_{ik} * EB_j \text{ , where}$$

PV_{ik} is the exploit probability of vulnerability k from vulnerability set i by a threat A_l.

Step 4, combating the risk, consists in the use of countermeasures to minimize the threat. Thus each threat A_i from the set SA, is associated with a set of reduction factors $SFD = \{FD_1, FD_2, \ldots, FD_k\}$.

The probability of risk quantification through a set of vulnerabilities is determined using the formula below:

$$R = \sum_{i=1}^{m} \left[PA_i * \frac{\left(\sum_{j=1}^{k} \mathrm{PSV_i EB_j} \right)}{k} * FD_i \right] * \frac{1}{m}$$

Using the above formula a clearer picture is given over the quantitative aspects of risk. In Figure 1 the risk model analysis model is presented.

Step 5 is needed for future risk analysis as this will speed up the process in the future. Keeping clear and well documented records regarding past threats and vulnerabilities will provide the development team valuable statistical information regarding the evolution of the vulnerabilities and threats models effects on the asset model thus helping to develop better countermeasures to handle the risk.

3.2 Qualitative risk analysis

In **stage 1** the threat and vulnerability models are associated with five degree scale consisting of a set of scale factors *SF = {Very Low, Low, Medium, High, Very High}* In table 4 the Qualitative vulnerability matrix is presented, it lists the vulnerability and the appropriate associated scale factor

Table 4. Qualitative vulnerability matrix

Vulnerability	Exploit factor
V_1	SF_1
V_2	SF_2
…	…
V_n	SF_n

Table 5 presents the qualitative threat matrix, which lists the threats and their associated occurrence probability scale factors.

Table 5. Qualitative threat matrix

Threat	Probability of occurrence
A_1	SF_1
A_2	SF_2
…	…
A_m	SF_m

Stage 2 is composed of the goods model same as in the quantitative risk analysis. Table 6 describes the scale factors associated with the set of goods $SB = \{B_1, B_2, \ldots, B_k\}$. Here the scale factors describe the impact to the system if a particular asset is compromised.

Table 6. Qualitative asset matrix

Asset	Impact if compromised
B_1	SF_1
B_2	SF_2
…	…
B_m	SF_m

Stage 3 is based on the elaboration of the risk model presented in table 7. The risk model combines the threats, vulnerabilities and goods models in order to give a better view of the qualitative aspects of risk.

Table 7. Qualitative exposure to risk model through the sets of vulnerabilities

Threat	Appearance factor		Vulnerability set	B_1	B_2	B_3	...
A_1	SF_1	→	SV_1	SFV_1EB_1	SFV_1EB_2	SFV_1EB_3	...
A_2	SF_2	→	SV_2	SFV_2EB_1	SFV_2EB_2	SFV_2EB_3	...
A_3	SF_3	→	SV_3	SFV_3EB_1	SFV_3EB_2	SFV_3EB_3	...
…	…	→	…	…			…

where :

SV_i – no. *i* vulnerability set

SFV_iEB_j – the exploit scale factor of one or more vulnerabilities from set *i* in order to get access to asset *j*; it is determined based on the exploit factor of the vulnerability within the set, the probability of occurrence of the threat and the impact if the asset is compromised as an aggregated risk measure.

Stage 4 consists of applying a set of countermeasures $SFD = \{FD_1, FD_2, \ldots, FD_k\}$. to decrease the exposure to risk. Such that each risk has associated a countermeasure with a scale factor to match its effectiveness.

Stage 5 consists of recording all the scale factors given to each model in order to have a statistical background in future examinations.

3.3 Quantitative vs. qualitative

In [6] qualitative analysis is regarded as an efficient method to finding the key areas of the system that present high risks but lacks the advantages given by the quantitative analysis to output numbers that give a better foundation for the cost benefit analysis. One main disadvantage of the qualitative analysis is that the outputted figures are difficult to transpose to a qualitative scale thus being easy to compute the global impact but hard to build a quality scale based on it.

In order to develop an efficient risk analysis both qualitative and quantitative methods must be correlated for maximum efficiency. Figure 3 presents an adaptation of [6] connections between the two in the context of risk management.

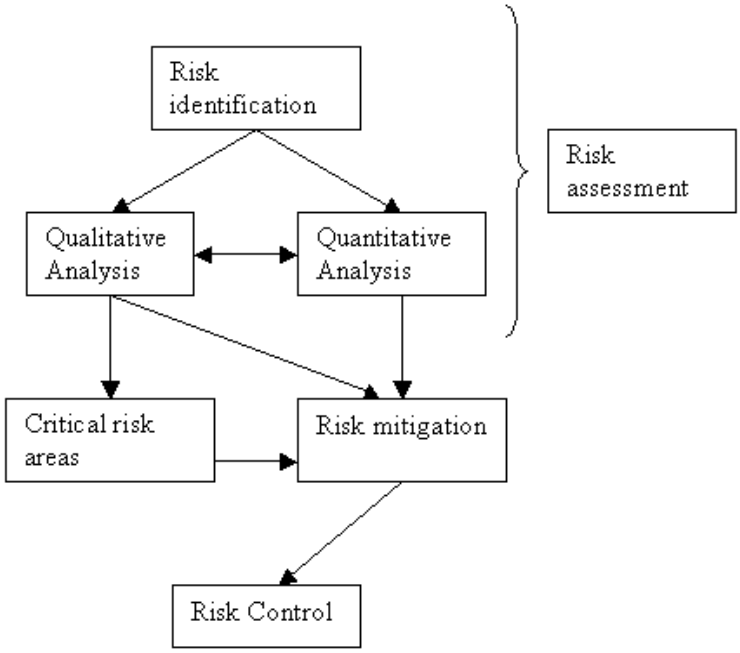

Fig. 3. Risk management

The two analysis methods make are used to fundament decisions in the risk mitigation stage of the risk management process thus using the result from both must be imperative in efficient risk assessment.

4 Conclusions

The knowledge based society requires a new type of applications to solve problems for citizens. Citizen-oriented applications are made to solve the problems of citizens and have as their central element the citizen itself. Citizen-oriented applications are targeted to meet new quality characteristics that traditional applications do not have or only partially meet.

In citizen-oriented applications security risk analysis plays an important role because it creates the preconditions for the development of security policies to ensure effective maximum safety for ongoing transactions.

Using both quantitative and qualitative approaches in the risk assessment stage provides an in depth view of the risk environment the security system is facing in a real world scenario.

The proposed model of risk analysis allows the development of more secure, cheaper and more efficient computer applications due to methodology of discovery and handling of threats and vulnerabilities.

The target group of this model is formed by government organizations or companies deploying citizen oriented applications that must insure a low level of risk while maintaining costs to a minimum

Further research implies integrating the risk assessment in a reengineered risk mitigation model in order to put the foundations of developing a customizable risk management process.

Acknowledgements

This article is a result of the project „Doctoral Program and PhD Students in the education research and innovation triangle". This project is co funded by European Social Fund through The Sectorial Operational Programme for Human Resources Development 2007-2013, coordinated by The Bucharest Academy of Economic Studies.

References

[1] H. P. In, Y. G. Kim, T. Lee, C. J. Moon, Y. Jung and I. Kim, *A Security Risk Analysis Model for Information Systems*, D.-K. Baik (Ed.): AsiaSim, LNAI 3398, pp. 505-513, Springer-Verlag, Berlin, Heidelberg, 2005.

[2] A. Jones, *A framework for the management of information security risks*, BT Technology 30 Journal, Vol. 25, No. 1, January 2007.

[3] R. A. Caralli, J. F. Stevens, L. R. Young and W. R. Wilson, *Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process*, May 2007, Available at: http://www.cert.org/octave.

[4] I. Ivan, L. Săcuiu and D. Milodin, "The development of computer science oriented towards the citizen," *The Proceedings of Journal ISOM*, Vol. 2, No. 2, December 2008.

[5] I. Ivan and M. Doinea, "Vulnerability optimization in distributed applications," *Economic Growth and E.U. extension process, International Conference*, ASE, Bucharest, 2008.

[6] http://csrc.nist.gov/publications/ nistpubs/ 800-30/sp800-30.pdf

[7] I. Ivan and C. Ciurea, "Entry data validation in citizen oriented applications," *4th International Conference on Applied Statistics*, Nov. 20-22, 2008, NIS Publishing House, Bucharest, Romania.

Dragos PALAGHITA graduated from the Academy of Economic Studies of Bucharest, Cybernetics Statistics and Economic Informatics faculty, Economic Informatics section in 2008. He is programming in C++ and C# and his main areas of interest are Informatics Security, Software Quality Management, large data set analysis and graphical representation enchancements. Currently he is undergoing PhD studies at the Academy of Economic Studies of Bucharest, Cybernetics Statistics and Economic Informatics. He published 14 articles in JAQM, Informatica Journal, Economie Teoretica si Aplicata journal, Revista Romana de Automatica si Informatica.

Bogdan VINTILĂ graduated the Bucharest University of Economics, the Faculty of Cybernetics, Statistics and Economic Informatics. He is currently a PhD candidate in the field of Economic Informatics at University of Economics. He is interested in citizen oriented informatics applications, developing applications with large number of users and large data volumes, e-government, e-business, project management, applications' security and applications' quality characteristics.