Network model of security system

Piotr Adamczyk[1], Grzegorz Kiryk[1], Jarosław Napiórkowski[1], Andrzej Walczak[1 a]

[1]*Faculty of Cybernetics, Military University of Technology (WAT), Gen. Sylwestra Kaliskiego 2 Str., 00-908 Warsaw, Poland*

Abstract. The article presents the concept of building a network security model and its application in the process of risk analysis. It indicates the possibility of a new definition of the role of the network models in the safety analysis. Special attention was paid to the development of the use of an algorithm describing the process of identifying the assets, vulnerability and threats in a given context. The aim of the article is to present how this algorithm reduced the complexity of the problem by eliminating from the base model these components that have no links with others component and as a result and it was possible to build a real network model corresponding to reality.

1 Are the network models suitable for risk assessment? The information based on the standards.

One of the regulations describing the risk assessment techniques is the international standard PN-EN 31010: 2010 [1] "Risk management - Risk assessment techniques." It describes the concept and process of risk assessment and provides guidelines for the selection and application of the systematic and methodical risk assessment techniques [2, 3]. The examples include "brainstorming", Delphi technique, preliminary analysis of threats, Failure Mode and Effects Analysis, FMEA, Fault Tree Analysis, FTA, methods based on Bayesian statistics and Bayesian networks. Risk assessment carried out in accordance with this standard supports other measures of risk management. It shows the use of certain techniques, referring to other international standards, which describe in more detail the concept and application of these techniques. This standard, Table A.1 (Applicability of tools used for risk assessment) contains special classification, proposal of the techniques that can be applied at each stage of risk assessment and their usefulness. The techniques are classified according to their use at different stages:

- risk identification;
- analysis of the consequences at the stage of risk analysis;
- qualitative, quantitative or semi-quantitative estimation of the probability at the stage of risk analysis;
- analysis of control effectiveness at the stage of risk analysis;
- evaluation of risk level at the stage of risk analysis;
- risk assessment;

At each stage of risk assessment, it is possible to use various tools and methods.

The standard indicates 31 tools that can be used at each of these stages. Apart from the tools of the groups of supporting methods (Delphi technique), Business Impact Analysis, BIA, or functional analysis, the standard also provide for some statistical methods, including:

- Markov analysis,
- Monte-Carlo simulation,
- Bayesian statistics and Bayes Nets.

Only one of these tools is based on the network approach.

Methods based on Bayesian statistics and Bayesian networks are classified as non-applicable to risk identification of qualitative, quantitative or semi-quantitative estimation of the probability at the stage of risk analysis or risk assessment at the stage of risk analysis. At the same time, the standard shows them as having application to the analysis of the consequences at the stage of risk analysis and risk assessment.

According to the standard, one of the strong points of this approach is the fact that only the Bayes rule and knowledge of a priori probabilities are required.

What is more, the language is easy to understand and the method provides a mechanism for using subjective beliefs.

At the same time, it has some limitations, such as:

- defining dependency on the Bayesian network may not be feasible due to the complexity and costs related thereto;
- the Bayesian approach requires knowledge of a number of conditional probabilities, which are generally determined on the basis of expert knowledge. The software based on the Bayesian network can provide answers only on the basis of such assumptions.

The first limitation indicates a problem that all links need to be defined with the use of complex systems. Furthermore, even a relatively simple system allows

[a] Corresponding author: andrzej.walczak@wat.edu.pl

direct application of the Bayesian networks. The second limitation is the necessity of knowledge of many conditional probabilities, which are usually delivered by experts.

Taking an inventory of resources and identifying the processes of vulnerability and risks, the scale effect should be taken into account [4]. The size of the network representing expertise knowledge can also be a problem. Obviously, it would translate into the complexity of the algorithms, in particular the Bayesian network algorithms.

2 Networks - basic definitions and advantages of the network models

Network is the collection of all ordered triples:

$$S = <G, \{\Phi i\}, \{\Psi\} \quad (1)$$

where:

$$G = (X, E, P) \quad (2)$$

is an arbitrary graph

$$\{\Phi_i\} = \{\Phi_1, \dots, \Phi_I\} \quad (3)$$

is a set of functions defined on set X of vertices of graph G

$$\Phi_i : X \rightarrow R,\ i = 1...\mathrm{I} \text{ and } \{\Psi_j\} = \{\Psi_1, \dots, \Psi_J\} \quad (4)$$

is a set of functions defined on set E on the edges of graph G

$$\{\Psi_J\} : \mathrm{E} \rightarrow R,\ i = 1...\mathrm{I} \quad (5)$$

The function Φ can describe the type of vertex of the graph, e.g. resource, resource vulnerability, threat. While the function Ψ is usually, in practice, a function that builds a network graph on the basis of the links between the nodes of the graph and is used to express the characteristics of the links between the described graph arcs.

The degree of vertex

$$k(x_i) = k + (x_i) + \mathrm{k} - (x_i) + \mathrm{k}^{\sim}(x_i) + \mathrm{k}^{\circ}(x_i) \quad (6)$$

where:
$k + (x_i)$– the number of arcs “going out" of vertex x_i
$k - (x_i)$ – the number of arcs “going in" to vertex x_i
$\mathrm{k}^{\sim}(x_i)$ – the number of edges incident to vertex x_i
$\mathrm{k}^{\circ}(x_i)$ – the number of loops incident to vertex x_i

The graf is a network in which:

$$\{\Phi i\} = \{\Psi_j\} = \emptyset \quad (7)$$

(we omit such trivial functions as functions numbering vertex and branches)

In the surrounding reality, networks are understood as a set of vertices and branches representing the interaction between these vertices together with the ubiquitous functions assigned to the graph.

In the safety analysis of the system, we are looking for nodes with specific characteristics of connections between nodes, threats and vulnerability nodes.

Apart from the obvious advantage of the network model, which is the ability to visualize the links between the effects of hazards, the network models are also built to determine which probability distributions should be applied in a given network. Furthermore, if the links described by the edges are clearly defined - which is relatively easy in the network - the introduction of priors for performing the Bayesian analysis on such network is feasible and bears the characteristics of objectivity, not of a subjective expertise. However, the most important thing is that the network models are typical tools for analysing the situation, in which there is no valid characterization of probability based on tests with a given repetition. The security systems do not provide such models of probability. Therefore, the network feature, which gives a possibility of statistical analysis, not based on the prevalence of an event, predestines the networks to examine the safety issues.

Developing methods for building the network security models may prove to be a truly cost-effective method of analysis of potential security despite the above-mentioned limitations.

3 Model office - example of analysis

The inspiration for the development of the network risk analysis model was to establish the security analysis information for the model of an office, which would be used in case of the documents containing classified information:

- safe storage of existing documents,
- secure document flow with the prerogative of full accountability for both the document and the user,
- safe environment for work with documents,
- safe environment for drawing up new documents,

A model office was developed for storing and viewing classified documents using the RFID technology to mark media information stored in the office. Due to the sensitivity of the information produced and processed in the office, the primary goal was to make it an area isolated from the rest of the office building. The separated area, which the office has become, has a single protected input/output zone, equipped with electronic access control systems and monitoring of items that are brought in. Upon entering the office, there is an area inaccessible to people unauthorized to use it, i.e. the zone for storing the documents. Only the employees of the office may have access to this zone. The last zone, available to persons authorized to use the office, is the zone of the reading room, where one can work on documents taken from the storage or to produce new documents. All office areas are equipped with the systems for monitoring the movement of objects or documents protected by RFID tags [5].

In developing the concept of the model office, the basic criteria of its organization, which had to be taken into account, resulted from the Polish applicable law.

4 Reference model of the security system

The security model used in the Office applies the general reference model shown below.

Figure 1. Network reference model. Source: own elaboration.

This model reflects the general approach to inventory, including its vulnerability and identification of threats that may, based on such vulnerability, have negative impact on the resources.

5 Overview of the methodology

The vast majority of the presently used methodologies for risk analysis are based solely on the expertise of the person conducting this analysis. Assuming only such guarantee of safety, the in-built system can lead to serious deficiencies resulting from intentional or unintentional omission or failure to notice a threat. Equally dangerous could be failure to see vulnerability of the resources to certain threats. Risk assessment of threat implementation by the resource completely depends on the expert knowledge of the issues.

All these defects of the risk analysis method may lead to impairment of the protection system, which in turn can lead to loss of confidentiality, integrity or availability of the protected information.

The process of risk analysis requires, at every stage, the verification of the results by other experts. Interactivity and complexity of this process means that it takes a long time to be implemented (so it is costly) and there is no guarantee of its accuracy and completeness.

Expert analysis of any problem, including identification of the resources, their vulnerability and existing threats lead to extensive and complex semantic description of the problem.

Typically, all components listed in the diagram in Figure 1 are introduced by way of a description, with no strict rules of its creation. In addition, all components must be independent and the resulting links between them must be generated in accordance with the definition of the links in the form of all possible subsets of the Cartesian product of sets of threats, vulnerabilities and assets.

The complexity of this description makes the analysis of the impact of a particular threat on the whole system time-consuming and feasible only by an expert, who developed this description. This is due to the lack of consistent methodology formalizing the rules of impact of the threat description on the resources. As a result, any security consequences and risk analysis constitute a document of considerable volume, which is prepared only because such are the normative and legal requirements. On the other hand, the technique for creating this documentation may contain and usually contains infringement arising from subjective expert knowledge.

The work carried out for the constructed model of the secret office relied on the expert's:

- identification of assets,
- identification of risks,
- identification of vulnerability,

These works resulted in the identification of:

- 213 assets,
- 61 risks,
- 211 susceptibility threats.

Attempts have been made to automate the construction of risk analysis, which showed the complexity of the problem and indicated the key role of an expert. Additionally, a broader view of the obtained results allowed to note the following rule:

- assets described as nouns,
- threats described as nouns,
- vulnerability is described as adjectives or (in Polish) adjective participle or adjective phrase.

With regard to the reference model of the network we obtain the following context (in the sense of grammar) of the network model:

Figure 2. Context model of the network. Source: own elaboration.

The diagram shown in Figure 2 is an indication of the element of the methodology of the network security model.

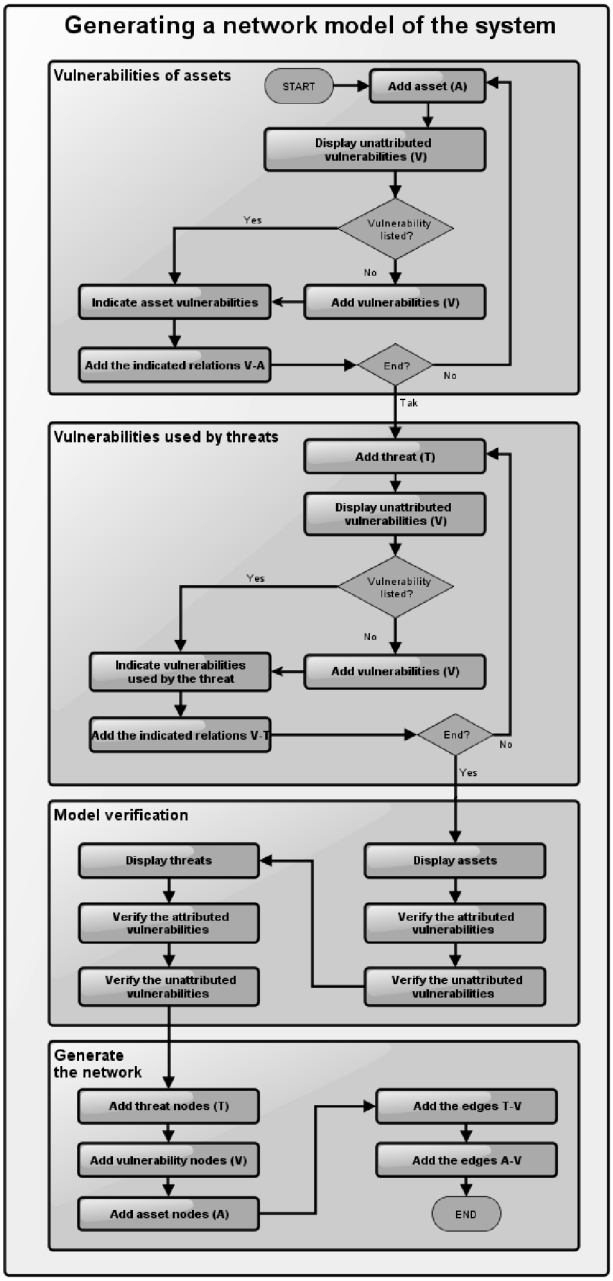

Figure 3. Generation diagram of the network model. Source: own elaboration.

The use of this model has led to the development of an algorithm that describes the process of identifying resources, vulnerability and threats in the context. This algorithm reduced the complexity of the problem by eliminating from the full Cartesian product these components that have no links. Therefore, it made it possible to build a real network model corresponding to reality.

Approval of the expert model is the foundation for building the network model, in which the nodes are the resources, risks and vulnerability. The key for the construction of the network model is the result of creating three pairs: resource - vulnerability and threat-vulnerability through links and connections leaving the nodes, showing the vulnerability, as in the diagram in Figure 2.

6 The use of the network model in the context under consideration

The adopted context model makes it finally possible to maintain an acceptable level of complexity and establish links in a controlled manner subject to the rule shown in Figure 2.

Only a fragment of the expert study was used for the purpose of clear imaging of the results. For this purpose, the following elements have been selected from different areas:

Threats:

- water supply system failure,
- AC system failure,
- heating system failure,
- back-up power system failure,
- emergency power supply system failure,
- external power supply system failure,
- device failure,
- IT system administrator failure.

Vulnerability:

- uncontrolled access of third party users,
- unauthorized access to telecommunications cabinets,
- insufficient physical protection of objects or their elements.

It seems that in the context of a full risk analysis, threats, the occurrence of which is possible rather incidentally, and vulnerability, which may also have to be marginalized, were identified. Therefore, an expert would define them. It turned out that by using the proposed model (risk - susceptibility - resource), the implementation of any of the eight selected threats, using any of the three identified vulnerability risks, may have impact on at least one resource of the 187 items identified in the model of the office.

During the construction of the network model, the fact that every threat affects the resource only based on the vulnerability that exists in this resource was considered. This means that a threat may affect an asset only in the context of specific vulnerability.

The data in Table 1 summarizes some threats and some vulnerability risks, which in the context of these threats will be able to interact with specific resources.

Table 1. Summary of threats and possibly contextually related vulnerability present in the constructed model office.

Threat (T)	Vulnerability (V)
T 0. Water supply system failure	V 70. Uncontrolled remote access of third party users
	V 74. Unauthorized access to telecommunications cabinets
	V 78. Insufficient physical protection of objects or their elements

T 1. AC system failure	V 70. Uncontrolled remote access of third party users
	V 74. Unauthorized access to telecommunications cabinets
	V 78. Insufficient physical protection of objects or their elements
T 2. Heating system failure	V 74. Unauthorized access to telecommunications cabinets
	V 78. Insufficient physical protection of objects or their elements
T 3. Back-up power system failure	V 70. Uncontrolled remote access of third party users
	V 78. Insufficient physical protection of objects or their elements
T 4. Emergency power supply system failure,	V 70. Uncontrolled remote access of third party users
	V 78. Insufficient physical protection of objects or their elements
T 5. External power supply system failure,	V 70. Uncontrolled remote access of third party users
	V 78. Insufficient physical protection of objects or their elements
T 6. Failure of equipment	V 70. Uncontrolled remote access of third party users
T 8. IT system administrator failure	V 70. Uncontrolled remote access of third party users

Table 2 shows a small portion of the statement concerning the vulnerability that can expose certain resources to threats. In such an uncomplicated model, the selected susceptibility exposes to risk almost all of the identified resources, which results in a considerable size of the table.

Table 2. Summary of the selected vulnerability and resources, in which such vulnerability exists, in the constructed model office.

Vulnerability (V)	**Asset (A)**
V 78. Insufficient physical protection of objects or their elements	A 181. Laptop
	A 182. Telephone line
	A 190. CCTV wiring
	A 192. LAN wiring (copper cable)
	A 193. LAN wiring (optical fibre cable)
	A 194. Intruder Alarm System (IAS) wiring
	A 195. Access control system wiring
V 70. Uncontrolled remote access of third party users	A 134. Firewall
	A 163. AC
	A 179. Back-up copies
	A 181. Laptop
	A 202. Cabinet software
	A 227. Router
	A 239. Alarm system
	A 242. Metal and electronic devices detection system (gate)
V 74. Unauthorized access to telecommunications cabinets	A 227. Router
	A 229. Surrounding
	A 245. Back-up power supply surveillance system
	A 295. Power supply

Comprehensive visualization of the network model is shown in the figure below (Fig. 4):

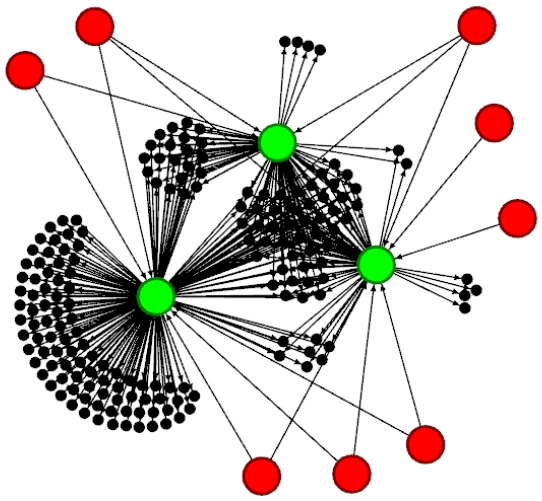

Figure 4. Network graph [6,7] for security model described in the office - selected portion of the assets. (black - asset node, green - vulnerability node, red - threat node). Source: own elaboration, Gephi ver. 0.9.1

A specially developed algorithm based on lexical system was used to create relevant data for the purpose of building a network graph out of the three contextual network models.

The research network algorithms frequently use the method for generating random graphs proposed by Barabasi and Albert [8]. Their model shows two causes - depending on the power series in the distribution of the number of edges coming out of the node. These causes constitute a gradual growth of the network and preferential attachment of the nodes.

Let us denote the network graph node as one vulnerability (V) of the object called asset (A). Let - in the selected V - the number of such recognized threats (T) be equal to m. If they are diagnostically equal (have equally significant impact on the likelihood of a threat), then m of such nodes modelling the risks will be attached to a node of vulnerability.

Figure 5. Result of PageRank algorithm. Algorithm: Sergey Brin, Lawrence Page, The Anatomy of a Large-Scale Hypertextual Web Search Engine, in Proceedings of the seventh International Conference on the World Wide Web (WWW1998):107-117, Source: own elaboration, Gephi ver. 0.9.1

Special training is prepared for the purpose of the work (Table 1). On the basis of the information contained in the database, a subnet considering the link with context three is built. In the study A.-L. Barabasi [9], the power distribution of Web was confirmed and the data analysis algorithm was used for indexing web pages developed by the founders of the company Google, Larry Page and Sergey Brin. The research shows that the network security model system shares some common properties with B-A networks.

During the work carried out in the Gephi environment, it turned out that the graph of the network was characterized by the power distribution of the degrees of vertices. As it can be observed, even the subnet shown in Figure 4 is characterized by the power distribution of the degrees of vertices shown in Figure 5. Apparently, this feature also describes the technical systems [10].

The power distribution, in contrast to, for example, the Gaussian, Poisson or exponential distribution, is a natural off-the-scale range. This means that talking about the average values of the degrees of vertices in such networks is ineffective, and, in many cases, the use of the concept of the medium degree leads to serious errors. In the network with the power distribution of the degrees of vertices, many nodes have only one edge, but it is possible to also find the nodes with a huge number of edges, the so-called hubs. This disproportion in an unusual way translates into properties of the off-the-scale networks and makes them very interesting objects of research (Figure 4). We can also observe the small-world phenomenon.

The network analysis can visualize the nodes that pose threats to the resources. It also allows to relatively easily identify a priori probabilities on finite and small set of nodes, which describe the threat.

7 Examples of security incidents - on the network (tripping hazard)

The data presented in Table 3 show the selected vulnerability (V 70. Uncontrolled remote third party user access) and seven threats that - in the context of this vulnerability - may affect the specific, identified assets.

Table 3. Threats and the associated contextual vulnerability present in the constructed model office.

Vulnerability (V)	Threat name (T)
V 70. Uncontrolled remote access of third party users	T 0. Water supply system failure
	T 1. AC system failure
	T 3. Back-up power system failure
	T 4. Emergency power supply system failure,
	T 5. External power supply system failure,
	T 6. Failure of equipment
	T 8. IT system administrator failure

The model of the network of the three, threat - vulnerability - asset was displayed in a way that radically changed its assessment and made it clear that the impact of the threat on the entire system was possible.

The graphic illustration in the system threat (T) - vulnerability (V) - asset (A) is much clearer than the presentation of the same problem in a tabular format. This forms additional grounds for usability of the network model.

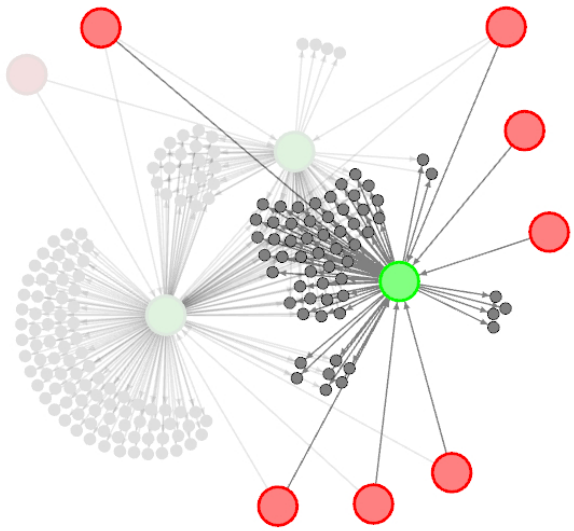

Figure 6. Assets that may be affected by the occurrence of one of the six above-mentioned threats in the context of vulnerability "Uncontrolled remote access of third party users." Source: own elaboration, Gephi ver. 0.9.1

In the above figure (Figure 6), it is easy to notice a group of resources that have one, two or three analysed vulnerability risks. There are also visible threats that can use only one, indicated susceptibility. In further stages of the safety analysis, it is possible to use this information to establish protection systems. They will be aimed at precisely selected vulnerability risks. The stage of establishing security must precede the full risk analysis.

8 Summary

On the example of the model office, including the documents of different classification levels [11], the construction of the network security model has been shown. For this purpose, the methodology procedure was developed, bearing the features of the new solution.

An analysis of the occurrence of a security incident and its impact on certain resources using the network model [12] is much more readable than the traditional tabular description. Additionally, it becomes apparent that the use of the Bayesian networks can be limited not to the full network configuration, but to its subgraph so as to include the selected hazards in the analysis. Basically, it will change the possibility of using the Bayesian networks in the safety analysis and determining priors.

While the grounds for restrictions in the normative documents concerning the use of the network could justify considerable complexity of the calculations (when we consider the full shape of the network with a number of elements that is determined by the Cartesian product A × V × T) and difficulty of assignment of probabilities by the Bayesian models, in drawings 5 and 7, the reduction of these restrictions to an acceptable level is clearly visible. Therefore, it was possible to develop a systematic methodology for the construction of networks. This indicates the possibility of a new definition of the role of the network models in the safety analysis.

References

1. *PN-EN 31010:2010 Risk management - Risk assessment techniques*
2. *PN ISO/IEC 27005 Information technology. Security techniques. Information security risk management*
3. *PKN–ISO GUIDE 73 Risk management - Terminology*
4. K. Liderman, *Risk Analysis and protection of information in computer systems* (2008)
5. M. Kiedrowicz (Editor), *Managing sensitive information* (2015)
6. A. Fronczak, P. Fronczak, *Świat sieci złożonych. Od fizyki do Internetu*, (Wydawnictwo Naukowe PWN, 2009)
7. R. Sinatra, P. Deville, M. Szell, D. Wang, A-L Barabási, *A century of physics*, Nature Physics, **11**, 791–796 (2015)
8. A.-L. Barabási, R. Albert, *Emergence of scaling in random networks*, Science, **286**, 509−512 (1999)
9. A.-L. Barabási, R. Albert, H. Jeong, G. Bianconi,, Science, **287**, 2115 (2000)
10. I. Eusgeld, C. Nan, S. Dietz , "*System-of-systems*" *approach for interdependent critical infrastructures*, Reliability Engineering and System Safety, **96,** 679-686 (2011)
11. J. Stanik J., M. Kiedrowicz, *Selected aspects of risk management in respect of security of the document lifecycle management system with multiple levels of sensitivity*, Information Management in Practice, 231-251, (2015)
12. Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners, NASA/SP-2011-3421, Sec.Ed (2011)