Security Evaluation supported by Information Security Mechanisms

Jakub Breier*
Institute of Applied Informatics
Faculty of Informatics and Information Technologies
Slovak University of Technology in Bratislava
Ilkovičova 2, 842 16 Bratislava, Slovakia
breier@fiit.stuba.sk

Abstract

Information security plays a key role in protection of organization's assets. There exist a number of standards and guidelines providing huge lists of security controls that, if properly used, might be useful against cyber threats. However, these standards leave the process of controls selection to the organizations. Security manager has to carry out a decision on implementation of security controls. Deciding which controls should be encompassed and which bypassed could be tough and indeterminate, since different sources usually prefer another solutions. This work presents motivation for using metrics as an instrument for a risk analysis.

The main goal of this work is to define proper security evaluation model for an organization, based on the score of security mechanisms. We present a mathematical model of evaluation, which minimizes subjectivity in this process and it should lead to more automatized risk analysis and make the results of the analysis more comparable. Our work is based on the ISO/IEC 27002 standard on which is built our evaluation model.

Categories and Subject Descriptors

K.6.5 [**Management of Computing and Information Systems**]: Security and Protection; K.6.m [**Management of Computing and Information Systems**]: Miscellaneous—*Security*

Keywords

Information Systems, Information Security, Security Standards, Security Metrics, ISO 27002

1. Introduction

Information security risks pose a serious threat to organizations dependent on their information systems. Both known and unknown vulnerabilities can be exploited to compromise security attributes - confidentiality, integrity, and availability of information used by organization. There exist different layers of security including physical protection, protection by cryptography, ensuring authenticity or asset classification in order to minimize the effect of both internal or external threats. It is necessary that responsible leaders and managers understand their responsibilities and support the information security management so it could improve the protection of organization assets.

Operational cybersecurity is becoming more significant area of Computer Science. It is difficult to demonstrate a progress in this area, all the systems connected to the Internet are periodically under attack and the statistics about successful attacks still show the same ratio. In [5] authors analyze the progress in the automobile safety and compare it to the computer security. It is easier to eliminate known threats that do not change over time, as in the automobile industry the adversaries are natural laws that remain the same. In terms of computer security there are human adversaries that are evolving over time, therefore it is impossible to define static goals and to reach them.

The main process that is supposed to help in security decisions is a risk analysis. Outputs of a risk analysis are essential inputs for risk management [23, 27]. It provides a risk manager with a set of significant risks and with data to assist in treatment of these risks. We can divide risk analysis approaches into two major groups: quantitative and qualitative. Quantitative methods are usually preferred because, if following a proper methodology, they can provide us with more accurate results. Qualitative methods are influenced by subjective perception of a risk analyst that conducts this process, so they tend to be biased.

There are many documents describing risk assessment techniques, they usually propose theoretical approaches and provide generic guidances on choosing security controls. But they usually fall short on describing practical aspects and giving an objective discrete-scale evaluation. Risk managers and security professionals need formalized quantitative risk measures and metrics, so they can efficiently and correctly measure risks. The comprehensive risk management framework with risk metrics would improve the risk assessment by giving organizations and would enable easier decision making in information security management.

*Recommended by thesis supervisor: Assoc. Prof. Ladislav Hudec

Our goal is to bring the objectivity into the process of the risk assessment and evaluation and to express the security score in an organization in five basic security attributes. We used the security mechanisms implementation score to measure the quality of implemented security controls and the Analytic Hierarchy Process technique to express the importance of particular mechanisms. Security controls are originated from the ISO/IEC 27002:2005 [11] standard and we propose security mechanisms for each control objective from this standard.

The rest of the paper is structured as follows. The section 2 provides an overview of a related work in the field of the security evaluation and states problems associated within this field. The section 3 describes our approach for this problem and defines methods used in our work. Section 5 provides the discussion and the last section 6 concludes this document and provides a motivation for further work.

2. Related Work

There are many works in the field of information security measurements and information security evaluation. Some of them are important and necessary in making progress in this field.

Subsection 2.1 discusses most important works in the field of security quantification and subsection 2.2 outlines works dealing with the security mechanisms and their evaluation

2.1 Quantification of Security

There exist a number of recent papers describing the security evaluation supported by some sort of metrics or proposing an evaluation model based on quantitative criteria.

In [18] Sarmah et. al. constructed a formal model for organization security patterns. This paper uses Formal Concept Analysis (FCA)[16] method to generate the security pattern lattice that could be used as a hierarchy classification model for information security attributes and high-level security mechanisms. The work is based on Common Criteria for Information Technology Security Evaluation (CCITSE)[12], which serves as a database for trusted elements used in the model. However the proposed model does not concern security evaluation, it only discusses the way how the information security elements could be organized.

In [6] Ekelhart et. al. propose a security ontology for organizing knowledge on threats, safeguards, and assets. This work constructs classification for each of these groups and creates a method for quantitative risk analysis, using its own framework. The work does not use known standards or guidelines as an input for its evaluation model, so desired mechanisms and countermeasures have to be defined in the process of risk analysis.

Fenz, Ekelhart and Neubauer [7] went further with this approach, they provide information security risk management methodology with their own software solution - automated framework called AURUM. This complex framework, based on previously proposed security ontology, helps in automatizing following processes:

- define business-critical assets and calculate their value,
- determine threat probabilities based on the organization-specific threat environment,
- determine security control implementation gaps,
- provide multi-objective decision support methods to interactively select control implementation portfolios based on existing implementations.

The first usage of the Analytic Hierarchy Process (AHP) for the information security purposes was proposed by Wang and Wulf in [22]. Their goal was to construct a framework for measuring system security. In the paper is described the first sketch of this framework. At the time of publication, in 1997, there was a serious lack of formal methods in information security. The authors wanted to solve following problems:

- define the term 'computer security'
- define a measure that is acceptable to the definition of computer security
- define a methodology to make useful if not rigorous estimates of the measures
- validate the measures.

They clearly defined problems associated with this area and they realized it is not possible to define fully automatized quantitative model, because some of the components are not easily measurable. Their model decomposed the system into small parts and used pair-wise comparisons to determine the relative importance among these parts. The work contains guidelines on simple measurements using questionnaires that could be transformed into metrics.

The work proposed by Cuihua et al. [4] uses the AHP and Grey Relational Analytic Process (GRAP) to combine qualitative evaluation with quantitative decision. First, it uses the AHP technique to get the security elements weights and then it analyzes the evaluation data with GRAP. The paper is also based on CCITSE, but it does not clarify the process of assigning weights to elements from this standard. They provide an abstraction of the AHP and GRAP mathematical model, so that it is not easy to use their methodology without usage of other sources. The main idea is interesting, but lacks a validation.

A similar method was used by Yameng et al. [25], but with a higher number of classes from the Common Criteria standard. They were evaluating a high-assurance architecture of secure sharing of different security-level information, called Multiple Independent Levels of Security and Safety (MILS). Their method is almost identical, with similar problems with mathematical model. Both papers do not mention that they do not use the plain GRAP, since it is not sufficient enough for this purpose. They combine this method with another multi-criteria decision method, Complex Proportional Assessment (COPRAS). This combination was proposed by Zavadskas et al. in [26].

There are further works that use AHP as a main technique for the security evaluation [8, 13, 24], these do not, however, follow some well-known standard in information

security and are very similar to previously described papers.

There is also a paper by Verendel [21] criticizing the quantitative security evaluation approach stating that there is a lack of validation and comparison between these methods against empirical data. The author analyzes significant works between 1981 and 2008 with respect to security perspective and discuss the validity of proposed methods. He argue that usually authors of such methods use common and well-known techniques to evaluate data, however these are not compared to other works in this field, so it is nearly impossible to determine their quality.

2.2 Security Mechanisms

In the field of security mechanisms and controls there are a few papers trying to propose an approach for their selection and implementation into the organization's information systems.

Barnard and von Solms [3] proposed security mechanisms selection and evaluation even before the beginning of electronic commerce era. They chose the British Standard 7799 (a predecessor of the ISO/IEC 27002) as a basis for their work and they propose four main security aspects that need to be evaluated - Functionality, Assurance of Correctness, Assurance of Effectiveness and Assurance of Operation.

Singh ans Lilja [19] use Plackett & Burman (PB) design for determining the critical security controls [15]. This design requires minimum number of experiments to determine the effect of individual controls. For N controls it requires N+1 experiments. Each control can be implemented either as a low quality component or as a high quality component. These controls are then arranged in a matrix in a following way. Each row represents one experiment with numbers in columns either +1 or -1, indicating the control quality. Using these values together with the cost of each experiment we can determine the effect of particular security controls.

Authors compare 17 technical security controls, such as firewall, log analyzer, browser settings, etc.. They set up an experiment and provide an example of their method to prove its benefit in measuring impact of security enhancements.

Llanso [14] introduces CIAM - an approach that provides an initial prioritization of security controls. His approach uses data related to security incidents, vulnerabilities, business impact, and security control costs. He selects security controls from NIST 800-30 [20], assign them weights with support of security experts and estimate their efficiency against security breaches. He examines security controls from in three attack-related areas - prevention, detection, and response with respect to their defense against top security breaches that are listed in 2011 Data Breach Investigations Report published by Verizon [1].

3. Methods

The methods described in this section are used for security evaluation based on security mechanisms. This evaluation is based on the ISO/IEC 27002:2005 standard [11].

This section is divided into two subsections. The section 3.1 provides an overview of the proposed model. The section 3.2 describes the Analytic Hierarchy Process (AHP) technique and its usage for our problem - assignment of weights in the levels of hierarchy provided by the standard. The section 3.3 provides a motivation of using I/M/P method for determining weights in the security mechanisms' level in hierarchy. The section 4 explains how to reveal correlation among control objectives by using the factor analysis method.

3.1 Overview

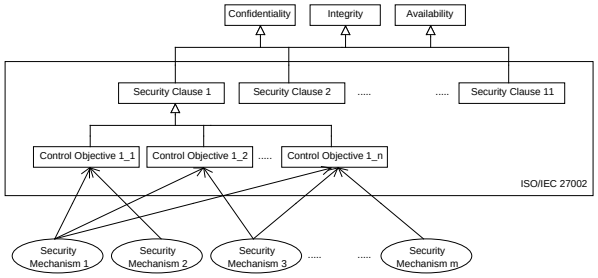

Figure 1: Security mechanisms implement security controls desired by control objectives in standard in order to improve the overall score of information security attributes, depicted at the bottom.

In picture 1 we can see the main idea of our model. We select appropriate security mechanisms for each control objective from the standard. One security mechanism can contribute to one or more control objectives and one control objective can be supported by one or more security mechanisms. These relations are weighted, so we can adjust the influence of each assignment. We can express this part of a model with the weighted sum:

$$CO_x = \sum_{1}^{n} M_i \times W(M_i), \tag{1}$$

where M_i is the score of the security mechanism i and $W(M_i)$ is its weight. As we can see in the table 1, variable M_i can take six values in accordance to correctness of implementation and variable $W(M_i)$ can take values from interval [0;1]. For example, Cobit [10] defines similar classification in its Maturity model for internal control, however there is no quantitative parameter - the status of internal control implementation is expressed in a verbal way.

Total sum of incoming weights to one control objective is 1. Following this proposal, each control objective is evaluated by one value from interval [0;1], which can tell us, how the organization successes in its implementation.

The other part of the picture depicts the relationship between control objectives and security clause. The standard does not tell us anything about the importance of particular control objectives for the security clause, however the importance cannot be distributed equally considering just particular security attribute. We will use the weighted sum to get the evaluation of security clauses:

$$SC_x = \sum_{1}^{n} CO_i \times W(CO_i), \tag{2}$$

Table 1: Overall score of security mechanisms implementation.

Level	Score	Description
0	0.0	Not implemented
1	0.2	Implemented with serious limitations
2	0.4	Implemented with minor unknown limitations
3	0.6	Implemented with known limitations
4	0.8	Implemented well, not tested in a real environment
5	1.0	Implemented well, tested and verified in a real environment

where variable CO_i is the evaluation of the control objective i and variable $W(CO_i)$ is its weight.

The last part of the picture is about relationship between security clauses and security attributes. We have chosen the way of expressing the overall security score in an organization with standard security attributes, confidentiality, integrity and availability in order to maximize simplicity of the result. It improves readability of the final security report also for people who are not familiar with the ISO/IEC 27002 standard. The security clauses are listed below together with the abbreviations used later in the text:

- Security policy (SP)
- Organization of information security (OIS)
- Asset management (AM)
- Human resources security (HRS)
- Physical and environmental security (PES)
- Communications and operations management (COM)
- Access control (AC)
- Information systems acquisition, development and maintenance (ISADM)
- Information security incident management (ISIM)
- Business continuity management (BCM)
- Compliance (CMP)

Each security clause affects each security attribute in some way. We have to add the weight of each relation to express how significantly does the security clause contribute to particular security attribute. We will use the following expression to evaluate the chosen security attribute:

$$SA_x = \sum_{1}^{n} SC_i \times W(SC_i), \tag{3}$$

where variable SC_i is the evaluation of the security clause i and variable $W(SC_i)$ is its weight.

3.2 Analytic Hierarchy Process

Analytic Hierarchy Process (AHP) [17] is a technique of organizing and analyzing complex decisions. Decision factors are arranged in a hierarchic structure, splitted into overall goal, criteria, subcriteria and alternatives in successive levels. We make the judgements upon the lowest level elements of the hierarchy in the form of paired comparisons. Following the hierarchical structure, we compare them on a single property, without concern about the other properties, which makes it easier to decide which one has an advantage over the other one. The comparison is based on verbal judgements (equal, moderately more, strongly more, very strongly more, extremely more), expressed in odd values from 1 to 9.

This technique was previously used in several papers concerning risk assessment and security evaluation in information systems [8, 4, 13, 24]. It can be used to analyze security decisions and to provide recommendations on investing into the right security controls.

In our work we use the AHP to determine weights of particular security mechanisms, so we can find out how do they contribute to security attributes. Our model is depicted in Figure 2. The model is splitted into the levels following the AHP technique. First, we define five overall goals - security attributes. Then we assign meaningful weights to security clauses (SC) and corresponding control objectives (CO) within each attribute. And finally, we assign weights to security mechanisms (M) chosen for every control objective. AHP will give us the overall score of each security mechanism in the context of a security attribute, which will be further used as a parameter for security evaluation.

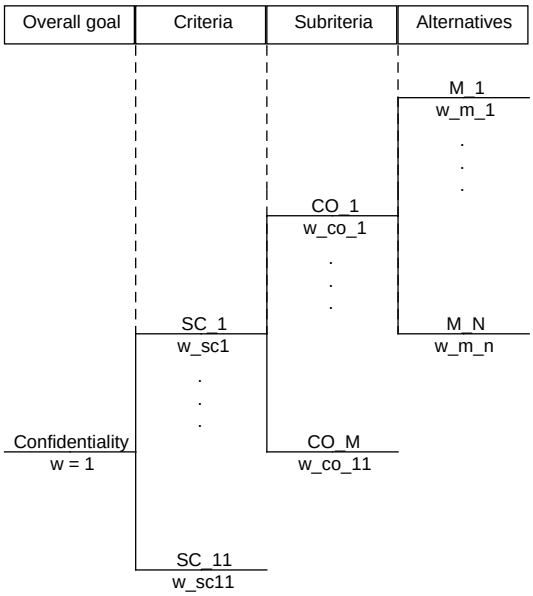

Figure 2: Splitting and weight selection process following the AHP technique.

The proposed method is explained on a concrete example, which can provide an overview, how the evaluation model works. To save the space, we have chosen security attribute availability only to illustrate the evaluation.

$$
\begin{array}{lcccccccccccc}
\text{Availability} & & SP & OIS & AM & HRS & PES & COM & AC & ISADM & ISIM & BCM & CMP \\
SP & \Big(& 1/1 & 2/1 & 1/5 & 9/1 & 1/5 & 1/3 & 5/1 & 5/1 & 7/1 & 1/7 & 3/1 \\
OIS & & 1/2 & 1/1 & 1/7 & 9/1 & 1/7 & 1/6 & 2/1 & 3/1 & 7/1 & 1/7 & 2/1 \\
AM & & 5/1 & 7/1 & 1/1 & 9/1 & 3/1 & 2/1 & 7/1 & 7/1 & 9/1 & 2/1 & 5/1 \\
HRS & & 1/9 & 1/9 & 1/9 & 1/1 & 1/9 & 1/7 & 1/3 & 1/2 & 1/2 & 1/9 & 1/7 \\
PES & & 5/1 & 7/1 & 1/3 & 9/1 & 1/1 & 2/1 & 5/1 & 5/1 & 9/1 & 2/1 & 5/1 \\
COM & & 3/1 & 6/1 & 1/2 & 7/1 & 1/2 & 1/1 & 5/1 & 5/1 & 7/1 & 1/2 & 5/1 \\
AC & & 1/5 & 1/2 & 1/7 & 3/1 & 1/5 & 1/5 & 1/1 & 1/3 & 2/1 & 1/8 & 2/1 \\
ISADM & & 1/5 & 1/3 & 1/7 & 2/1 & 1/5 & 1/5 & 3/1 & 1/1 & 7/1 & 1/6 & 4/1 \\
ISIM & & 1/7 & 1/7 & 1/9 & 2/1 & 1/9 & 1/7 & 1/2 & 1/7 & 1/1 & 1/8 & 1/3 \\
BCM & & 7/1 & 7/1 & 1/2 & 9/1 & 1/2 & 2/1 & 8/1 & 6/1 & 8/1 & 1/1 & 8/1 \\
CMP & \Big) & 1/3 & 1/2 & 1/5 & 7/1 & 1/5 & 1/5 & 1/2 & 1/4 & 3/1 & 1/8 & 1/1
\end{array} \tag{4}
$$

$$
W_{ava}^{T} = \begin{array}{c} \begin{array}{ccccccccccc} SP & OIS & AM & HRS & PES & COM & AC & ISADM & ISIM & BCM & CMP \end{array} \\ \big(\begin{array}{ccccccccccc} 0.077 & 0.052 & 0.236 & 0.012 & 0.185 & 0.128 & 0.026 & 0.043 & 0.020 & 0.192 & 0.029 \end{array} \big) \end{array} \tag{5}
$$

The first parameter of the model - the availability matrix - contains the paired comparisons of security clauses. It denotes how do they contribute in ensuring availability of assets in an organization. For example, if the comparison between Asset management (AM) and Physical and environmental security (PES) is 3/1, it means that AM is three times more important than PES from the availability point of view. Numbers in the matrix are estimated from the detailed descriptions of the clauses from the ISO/IEC 27002 standard. We can see this matrix in Equation 4.

After three consistency improvals (squaring the matrix by itself) we get the final normalized weight vector for security clauses (numbers are rounded to three decimal places) in Equation 5. We can see that the most important clauses from the availability point of view are Asset management, Physical and environmental security, Business continuity management and Communications and operations management.

3.3 IMP Model and Security Mechanism Weighting

Since there are many security mechanisms, an organization has to decide, which of them are useful and which are ineffective in contribution to its security goals.

There are eleven security clauses in the standard and each one is dealing with the different part of security, we have to use different types of security mechanisms. A NIST classification of security mechanisms constitutes three categories [20]. From our point of view, mechanisms used in our model also fits to one of these categories, therefore it is not necessary to use a new classification. Every security mechanism can be assign to one of the following groups: *Management, Operational or Technical.* It is much easier to measure the quality of the technical mechanisms, like firewall or intrusion prevention system, but it is impossible to quantify the quality of management or operational mechanisms, like information security policy. Because of character of ISO/IEC 27002 security clauses, that are mostly policy-based, we cannot measure all the mechanisms incorporated in the evaluation process automatically. But we can significantly improve the objectivity and simplicity of the evaluation.

We have to inspect them in two ways: how do they prevent against security breaches and how do they contribute to control objective fulfillment. Llanso [14] introduces an approach for selecting and prioritizing security controls (in the terminology of this paper, we use the term 'security mechanism' instead of the 'security control' because the latter term could indicate the usage of NIST 800-30 security controls). First, he computes weights of these controls, using three component weights - *Prevention, Detection and Response (P/D/R)* against an attack. The weight of a control i is computed by following equation:

$$RawWeighting_i = wP_i.owP_i + wD_i.owD_i + wR_i.owR_i \tag{6}$$

where overall weightings have values $owP_i = 0.5, owD_i = 0.25, owR_i = 0.25$, because prevention is more valuable than the other two. Control's contribution to these three actions (wP_i, wD_i, wR_i) are scores. These are determined by subject matter experts (SMEs) and each of them holds a value in interval $< 0, 1 >$.

After this step, he computes relative weighting as a ratio between one security control and all the other controls:

$$RelativeWeighting_i = \frac{RawWeighting_i}{\sum_{j=1}^{n} RawWeighting_j} \tag{7}$$

Then he is able to compute the priority, using relative weightings, scores, attack step frequencies, CVSS impacts and costs.

Since we do not have the cost dimension in our model, we will not use the whole prioritization approach. We will adopt the relative weighting process and adjust it in a meaning of contribution of security mechanisms to control objectives. We are not weighting these mechanisms with respect to possible attacks, but we are looking at how well do they assure the control objective function. So instead of *P/D/R* components we will use *Implementation, Maintenance and Policy (I/M/P)* components. The equation remains the same, just with another components and with another overall weightings:

$$RawWeighting_i = wI_i.owI_i + wM_i.owM_i + wP_i.owP_i \tag{8}$$

where overall weightings have values $owI_i = 0.6, owM_i = 0.20, owP_i = 0.20$. The implementation is the most important component, whithout them the maintenance components does not have a meaning, so we have to take

them into consideration. That is why it has the highest value. The maintenance ensures the correct function of the control objective and the policy component specifies, whether the security mechanism supports also a formal policy. The relative weighting formula remains the same as in Equation 7.

Table 2 presents the "Controls against malicious code" control objective from "Communications and operations management" security clause. We assigned five security mechanisms to this control objective and used the same approach for determining weights as Llanso [14] did. We constituted a group of security professionals for this purpose, so they could discuss if the security mechanisms are properly assigned and what values can they achieve in each of three components. The last column represents a relative weighting of particular security mechanisms. Each component weight has a value on a discrete scale from 1 to 10, 1 means minimal importance, 10 is the most significant importance.

Table 2: Controls against malicious code.

Security Mechanism	wI	wM	wP	RW
Implementing operating system policies prohibiting the use of unauthorized software, downloading unsigned executable files and working with other than data files on workstations without privileges.	9	5	7	**0.244**
Implementing strong account policies with separated privileges and clear accountability and non-repudiability.	7	3	9	**0.206**
Deployment of antivirus software on each system with the real-time check of unwanted code and periodical update of this software.	9	9	2	**0.238**
Ensuring that installed programs are up to date.	3	9	7	**0.156**
Providing business continuity plan - backuping and version management.	3	7	9	**0.156**

4. Correlation of Security Mechanisms

There is another dimension in the security mechanisms selection problem - a correlation between individual mechanisms. We cannot look on particular mechanisms as on the independent attributes, each one can affect the implementation of another one. It is usually better to have implemented for example three of them at an average implementation quality level than just one individual mechanism at a comprehensive level [9]. The cost is also a dimension that plays significant role in the above statement - the maximal quality of the implementation demands usually excessive resources. Commonly, it is more efficient to choose the way of implementing reasonable amount of mechanisms at a reasonable quality.

Since there are 131 control objectives and around 3-5 security mechanisms assigned to each of them at average, it would take a huge amount of time to determine correlation among each pair. We decided to choose a higher level of abstraction and to inspect a correlation between control objectives. We integrate this part of the model with the protection against security breaches, stated in the beginning of this section.

Statistical data will bring real world into our model. Verizon publishes Data Breach Investigations Reports [1] every year. This report contains comprehensive statistics that can be used to improve the judgement of particular elements in the AHP model. The report contains a sample of 761 security breaches organized into the matrix and splitted into categories. Each security breach is then identified with four properties:

- Agent - who performs an attack (internal, external, partner).
- Action - attack type (malware, hacking, social, misuse, error, physical, environmental).
- Asset - which asset was affected (servers, networks, user devices, offline data, people).
- Attribute - which security attributes were compromised (confidentiality, possession, integrity, authentication, availability, utility).

We will use the Top 10 threat action types by number of breaches from this record and inspect, how particular control objectives provide prevention against these breaches. Ideal for this purpose is the Factor Analysis (FA) method, which describes variability among observed correlated variables. In this method, the measured variables depend on a smaller number of latent factors. Each factor can affect several variables in common, so they are known as *common factors*. Particular variables can be then represented as a linear combination of the common factors. The coefficients in this combination are known as *loadings*. FA can be used to reduce the redundant information contained in several correlated variables. However we will use it to reveal these correlations and to insert these dependencies in our measurement model.

To save the space, we will not use the whole set of control objectives, but we will pick one sample objective from each security clause. These are listed in Table 3 among columns in the following order: Information security policy document (CO_1), Confidentiality agreements (CO_2), Inventory of assets (CO_3), Information security awareness, education, and training (CO_4), Physical entry controls (CO_5), Disposal of media (CO_6), User password management (CO_7), Input data validation (CO_8), Reporting information security events (CO_9), Business continuity and risk assessment (CO_{10}), Protection of organizational records (CO_{11}). The evaluation is based on a discrete scale from 1 to 10, 1 means no protection and 10 means maximal protection. We can see that there are control objectives which are important in the view of these breaches, like Information security policy document, Information security awareness, education, and training, or User password management. On the other hand, there are objectives that have negligible importance, like Inventory of assets or Business continuity and risk assessment. The purpose of this evaluation is not to determine the control objectives' significance, but to reveal possible hidden

Table 3: Control objectives' protection against Top 10 security threats.

Con. Obj. / Breach	CO_1	CO_2	CO_3	CO_4	CO_5	CO_6	CO_7	CO_8	CO_9	CO_{10}	CO_{11}
Keylogger/Form-grabber/Spyware	7	1	1	7	3	1	5	5	5	1	3
Exploitation of default or guessable credentials	7	3	1	8	3	1	9	1	4	1	3
Use of stolen login credentials	3	1	1	5	7	3	7	1	5	1	5
Send data to external site/entity	5	1	1	7	3	3	5	1	3	1	5
Brute force and dictionary attacks	7	1	3	9	5	3	9	1	5	1	5
Backdoor	5	3	1	7	5	1	5	5	5	1	3
Exploitation of backdoor or command and control channel	5	1	1	5	3	1	5	3	5	1	7
Disable or interfere with security controls	7	3	1	7	8	1	5	2	5	1	5
Tampering	8	3	1	8	3	1	1	1	5	1	3
Exploitation of insufficient authentication	7	3	1	8	7	1	5	1	3	1	5

Table 4: Unrotated component matrix.

	F_1	F_2	F_3
CO_1	0.858	0.313	0.048
CO_2	0.690	-0.145	-0.434
CO_3	-0.128	0.851	0.436
CO_4	0.693	0.720	-0.023
CO_5	-0.195	0.040	-0.303
CO_6	-0.727	0.540	-0.027
CO_7	-0.317	0.432	0.082
CO_8	0.176	-0.573	0.671
CO_9	-0.081	-0.188	0.413
CO_{10}	-0.720	-0.121	-0.218
CO_{11}	-0.506	0.059	-0.073

relationships between them. Then we can reflect these findings in the security evaluation.

Now we can use the factor analysis on the matrix obtained from Table 3. Besides other important characteristics we get the Pearson's correlation matrix. In this matrix we can see dependencies between each two control objectives (Equation 9).

Table 4 shows us the unrotated component matrix, consisting of three main factors. This matrix represents the significance of elements within each factor. By inspecting factor 1, we can see that it depends on the following control objectives: Information security policy document, Confidentiality agreements, Information security awareness, education, and training. It means that these control objectives are somehow bounded together from the view of security breaches. Factor 2 has higher loadings for control objectives Inventory of assets, Information security awareness, education, and training, and Disposal of media. The last factor has higher loading only for Input data validation, so we can say there will be no dependence emanating from this factor.

Obviously, the dependence cannot be determined only by mathematical methods because of the character of particular control objectives. For example, if we have an objective that supports implementation of antivirus software and the other objective, implementing periodical software updates, these are clearly highly correlated. However, we can say that the second one supports the first one highly, but it does not work in the opposite way. Software updates are not affected by implementation of antivirus software, so there is only one-way dependence. We have to use a group of security professionals to determine the character of dependencies.

We can explicate the results in the following way. Information security policy document is clearly an important control objective, Confidentiality agreements and Information security awareness, education, and training objectives depend on it. The latter two do not contribute to the first one, so there will be only one way correlation. Similarly, they do not have cross-dependency. Disposal of media and Inventory of assets are dependent on Information security awareness, education, and training. Disposal of media is also dependent on Inventory of assets. So we have five relationships in total, each of them is only one way dependence. Now we can use the correlation values to affect the evaluation of security mechanisms.

In Equation 10 we can see the evaluation of control objective i. S_{CO_i} is the score of control objective i, obtained by the evaluation, RW_{CO_i} is its weight, S_{CO_j} is the score of control objective j, that is correlated with i and COR_{ij} is the correlation between them. It is easy to see that the fraction can gain values from interval $< 0, 0.5 >$ and can significantly improve the value of the final score, if both the correlation and the correlated control objective's score are high.

$$FinalScore_{CO_i} = RW_{CO_i} * \prod_{j=1}^{n} \left(S_{CO_i} + \frac{S_{CO_j} * COR_{ij}}{1 + COR_{ij}} \right) \quad (10)$$

The score of S_{CO_i} depends on evaluation of security mech-

$$
\begin{array}{c}
 \\
CO_1 \\
CO_2 \\
CO_3 \\
CO_4 \\
CO_5 \\
CO_6 \\
CO_7 \\
CO_8 \\
CO_9 \\
CO_{10} \\
CO_{11}
\end{array}
\begin{array}{c}
\begin{array}{ccccccccccc}
CO_1 & CO_2 & CO_3 & CO_4 & CO_5 & CO_6 & CO_7 & CO_8 & CO_9 & CO_{10} & CO_{11}
\end{array} \\
\left(\begin{array}{ccccccccccc}
1 & 0.484 & 0.208 & 0.788 & -0.171 & -0.498 & -0.208 & -0.092 & -0.043 & -0.715 & -0.400 \\
0.484 & 1 & -0.333 & 0.410 & 0.263 & -0.655 & -0.273 & -0.063 & -0.124 & -0.333 & -0.469 \\
0.208 & -0.333 & 1 & 0.519 & 0.053 & 0.509 & 0.515 & -0.232 & 0.207 & -0.111 & 0.156 \\
0.788 & 0.410 & 0.519 & 1 & -0.073 & -0.054 & 0.127 & -0.265 & -0.254 & -0.573 & -0.473 \\
-0.171 & 0.263 & 0.053 & -0.073 & 1 & 0.103 & 0.139 & -0.190 & 0.033 & 0.404 & 0.255 \\
-0.498 & -0.655 & 0.509 & -0.054 & 0.103 & 1 & 0.417 & -0.456 & -0.135 & 0.509 & 0.307 \\
-0.208 & -0.273 & 0.515 & 0.127 & 0.139 & 0.417 & 1 & -0.190 & -0.056 & 0.212 & 0.128 \\
-0.092 & -0.063 & -0.232 & -0.265 & -0.190 & -0.456 & -0.190 & 1 & 0.432 & -0.232 & -0.267 \\
-0.043 & -0.124 & 0.207 & -0.254 & 0.033 & -0.135 & -0.056 & 0.432 & 1 & 0.207 & -0.097 \\
-0.715 & -0.333 & -0.111 & -0.573 & 0.404 & 0.509 & 0.212 & -0.232 & 0.207 & 1 & 0.156 \\
-0.400 & -0.469 & 0.156 & -0.473 & 0.255 & 0.307 & 0.128 & -0.267 & -0.097 & 0.156 & 1
\end{array}\right)
\end{array}
\tag{9}
$$

anisms associated to the control objective i and it is the product of the security mechanism's weighting and its score. The calculation of S_{CO_i} is stated in Equation 11. The score of the security mechanism's implementation ($S_(M_j)$) is determined by security analyst and can have a value in interval $< 0, 1 >$, 0 means no implementation and 1 means that it is implemented well, tested and verified in a real environment.

$$S_{CO_i} = \sum_{j}^{n} S_{M_j} * RW_{M_j} \tag{11}$$

The evaluation of control objective's weight (RW_{CO_i}) is not in the scope of this paper, since we do not propose the complete evaluation model, we only designate a selection method for security mechanisms and identify their relationships and dependencies.

5. Discussion

We showed in the previous sections that the AHP technique can provide us meaningful results if we define proper relations between security elements. We also proposed and described the approach of selection of security mechanisms. Factor analysis can significantly help in a process of dependencies identification. This approach can be inherited in a complex security evaluation system in order to maximize the automation and to increase the objectivity.

The pair-wise comparison in the AHP is a reasonable approach for deciding weights of a complex system, such as the security evaluation system. The only problem could be the granularity. The question is if the 9-step judgement is precise enough. Xuhua et. al. [4] state this problem in their work, however they do not come to any results - following their opinion, some people consider it as reasonable, the others indicate that the precision of this approach is not sufficient. Xinlan et. al. [24] suggest to combine this approach with the fuzzy theory, that can bring in the continuousness. Because of that we decided to use more detailed evaluation on the lowest level - when measuring weights and scores of security mechanisms. We adjusted a method proposed by Lanso [14] for our purposes and used three component weights, implementation, maintenance and policy.

Our approach can serve as a basis for the automatized evaluation system. After successful determination of all weights in the model we will try to determine the metrics that measure the quality of implemented security mechanisms. Most of these metrics should be easy to gather, ideally in an automatic way, so after the completion of this system it could assess the security state in an organization periodically with the minimal amount of human input.

If we compare our methodology with published works in sections 2.1 and 2.2, we consider following parts of our work the most important from the view of contribution in the field of security evaluation:

- Construction of the whole evaluation model, not only one fraction of the model. In various works [18, 4, 25, 26, 8, 13, 24, 19] were published only partial model results, so that it cannot be verified if it works properly when employed as evaluation technique in some more complex model.
- Enhancement of objectivity by employing quantitative evaluation techniques. We used factor analysis by using security statistics from Verizon's Data Breach Investigations Report [2] and weight determination by subject matter experts in order to minimize subjective inputs that are brought into the model by collecting security mechanisms evaluation data.
- Unification of requirements when inspecting compliance with the ISO/IEC 27001 standard. Scores of security mechanisms are computed in a same way in every organization and results are expressed from the security clauses or security attributes point of view. We introduced formal measurements methods that are auxiliary to the standard and help in determining its fulfillment.

6. Conclusions

In this document we proposed a way to evaluate the security in an organization using the implementation level of the security mechanisms. We used the ISO/IEC 27002:2005 standard as a database for security controls and we assigned security mechanisms to each control objective from this standard. The Analytic Hierarchy Process technique helped us to determine proper weights of particular security elements from the standard and the I/M/P component weighting model was used to adjust weights of security mechanisms. These weights serve as parameters of security evaluation model which uses mechanisms' scores as input values and produces results in three main security attributes - confidentiality, integrity and availability.

There is also an option to view on the evaluation results from the security clauses' perspective, if we want to examine compliance with the standard.

For the evaluation based on our model we constructed a software tool that computes the security state in an organization. Security analyst will determine the score of security mechanisms and the model will give us meaningful values in security attributes.

The ISO/IEC 27001 risk analysis do not deliberate the quality of implemented security mechanisms, it only investigates whether these mechanisms are present at the organization's security processes. The purpose of the whole work is to extract the useful information from the selected metrics, evaluate it, and to show the results on a concrete scale which will show us the whole picture about security in the organization.

In the future, we would like to automatize also the mechanisms' scores gathering. The model could be enhanced by extracting the useful information from the selected security metrics and use it to determine the value of the mechanisms' scores. We would like to test the relevance of our settings in a real environment, by comparing our results with the known security state after the completion of the security software tool based on our model.

References

[1] W. Baker, A. Hutton, D. Hylender, J. Pamula, C. Porter, and M. Spitler. 2011 Data Breach Investigations Report. Technical report, Verizon, 2011.

[2] W. Baker, A. Hutton, D. Hylender, J. Pamula, C. Porter, and M. Spitler. 2012 Data Breach Investigations Report. Technical report, Verizon, 2012.

[3] L. Barnard and R. Von Solms. A formalized approach to the effective selection and evaluation of information security controls. *Computers & Security*, 19(2):185 – 194, 2000.

[4] X. Cuihua and L. Jiajun. An Information System Security Evaluation Model Based on AHP and GRAP. *2009 International Conference on Web Information Systems and Mining*, pages 493–496, Nov. 2009.

[5] G. Cybenko and C. E. Landwehr. Security analytics and measurements. *IEEE Security & Privacy*, 10:5–8, 2012.

[6] A. Ekelhart, S. Fenz, M. Klemen, and E. Weippl. Security ontologies: Improving quantitative risk analysis. In *System Sciences, 2007. HICSS 2007. 40th Annual Hawaii International Conference on*, pages 156a–156a, 2007.

[7] S. Fenz, A. Ekelhart, and T. Neubauer. Information security risk management: In which security solutions is it worth investing? *Communications of the Association for Information Systems*, 28(1):329–356, 5 2011.

[8] S. Fu and H. Zhou. The Information Security Risk Assessment based on AHP and Fuzzy Comprehensive Evaluation Sha Fu. *Finance and Economics*, pages 2–6, 2011.

[9] L. A. Gordon and M. P. Loeb. The economics of information security investment. *ACM Trans. Inf. Syst. Secur.*, 5(4):438–457, Nov. 2002.

[10] I. G. Institute. *Cobit 5*. ISACA, 2012.

[11] ISO. *ISO/IEC Std. ISO 27002:2005, Information Technology - Security Techniques - Code of Practice for Information Security Management*. ISO, 2005.

[12] ISO. *ISO/IEC Std. ISO 15408-1:2009, Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model*. ISO, 2009.

[13] X. Ji and C. Pattinson. AHP Implemented Security Assessment and Security Weight Verification. *2010 IEEE Second International Conference on Social Computing*, pages 1026–1031, Aug. 2010.

[14] T. Llanso. CIAM: A data-driven approach for selecting and prioritizing security controls. In *Systems Conference (SysCon), 2012 IEEE International*, pages 1 –8, march 2012.

[15] R. L. Plackett and J. P. Burman. The design of optimum multifactorial experiments. *Biometrika*, 33(4):305–325, 1946.

[16] U. Priss. Formal concept analysis in information science. *Annual Review of Information Science and Technology*, 40:521–543, 1996.

[17] T. L. Saaty. How to make a decision: The analytic hierarchy process. *European Journal of Operational Research*, 48(1):9–26, September 1990.

[18] A. Sarmah, S. M. Hazarika, and S. K. Sinha. Security pattern lattice: A formal model to organize security patterns. In *Proceedings of the 2008 19th International Conference on Database and Expert Systems Application*, pages 292–296, Washington, DC, USA, 2008. IEEE Computer Society.

[19] A. Singh and D. Lilja. Improving risk assessment methodology: a statistical design of experiments approach. In *Proceedings of the 2nd international conference on Security of information and networks*, SIN '09, pages 21–29, New York, NY, USA, 2009. ACM.

[20] G. Stoneburner, A. Goguen, and A. Feringa. *NIST Special Publication 800-30: Risk Management Guide for Information Technology Systems*. NIST, 2002.

[21] V. Verendel. Quantified security is a weak hypothesis: a critical survey of results and assumptions. In *Proceedings of the 2009 workshop on New security paradigms workshop*, NSPW '09, pages 37–50, New York, NY, USA, 2009. ACM.

[22] C. Wang and W. A. Wulf. Towards a framework for security measurement. In *Proceedings of the Twentieth National Information Systems Security Conference, Baltimore, MD*, pages 522–533, Oct. 1997.

[23] R. Williams, G. Pandelios, and S. Behrens. *Software Risk Evaluation (SRE) method description (version 2.0)*. Software Engineering Institute, 1999.

[24] Z. Xinlan, H. Zhifang, W. Guangfu, and Z. Xin. Information Security Risk Assessment Methodology Research: Group Decision Making and Analytic Hierarchy Process. *2010 Second World Congress on Software Engineering*, (2):157–160, Dec. 2010.

[25] C. Yameng, S. Yulong, J. Ma, C. Xining, and L. Yahui. Ahp-grap based security evaluation method for mils system within cc framework. In *Computational Intelligence and Security (CIS), 2011 Seventh International Conference on*, pages 635–639, 2011.

[26] E. K. Zavadskas, A. Kaklauskas, Z. Turskis, and J. Tamošaitienė. Multi-attribute decision-making model by applying grey numbers. *Informatica*, 20(2):305–320, Apr. 2009.

[27] P. Zhou and H. Leung. An integrated risk analysis method using spatial interpolation. In *Software Engineering Conference (APSEC), 2012 19th Asia-Pacific*, volume 1, pages 452–461, 2012.

Selected Papers by the Author

J. Breier and L. Hudec. On selecting critical security controls. In *Proceedings of the The Eighth International Conference on Availability, Reliability and Security, ARES 2013 (In Print)*, pages 1–7. IEEE, 2013.

J. Breier and L. Hudec. On identifying proper security mechanisms. In Khabib Mustofa, ErichJ. Neuhold, AMin Tjoa, Edgar Weippl, and Ilsun You, editors, *Information and Communicatiaon Technology*, volume 7804 of *Lecture Notes in Computer Science*, pages 285–294. Springer Berlin Heidelberg, 2013.

J. Breier and L. Hudec. New approach in information system security evaluation. In *Satellite Telecommunications (ESTEL), 2012 IEEE First AESS European Conference on*, pages 1–6, 2012.

J. Breier and L. Hudec. Towards a security evaluation model based on security metrics. In *Proceedings of the 13th International Conference on Computer Systems and Technologies*, CompSysTech '12, pages 87–94, New York, NY, USA, 2012. ACM.

J. Breier and L. Hudec. Information system security assessment method based on security mechanisms. In *Student Research*

Conference 2012. Vol. 2 : 8th Student Research Conference in Informatics and Information Technologies, pages 347–354. STU Press, 2012.

J. Breier and L. Hudec. Security mechanisms role in information security evaluation. *Information Technology Applications*, (1):5–15, 2012.

J. Breier and L. Hudec. Risk analysis supported by information security metrics. In *Proceedings of the 12th International Conference on Computer Systems and Technologies*, CompSysTech '11, pages 393–398, New York, NY, USA, 2011. ACM.