On Identifying Proper Security Mechanisms

Jakub Breier, Ladislav Hudec

On Identifying Proper Security Mechanisms

Jakub Breier and Ladislav Hudec

Faculty of Informatics and Information Technologies,
Slovak University of Technology, Bratislava
{breier,lhudec}@fiit.stuba.sk

Abstract. Selection of proper security mechanisms that will protect the organization's assets against cyber threats is an important non-trivial problem. This paper introduces the approach based on statistical methods that will help to choose the proper controls with respect to actual security threats. First, we determine security mechanisms that support control objectives from ISO/IEC 27002 standard and assign them meaningful weights. Then we employ a factor analysis to reveal dependencies among control objectives. Then this knowledge can be reflected to security mechanisms, that inherit these dependencies from control objectives.

Keywords: Risk Evaluation, Information Security, Security Standards, Security Mechanisms, ISO/IEC 27002 standard

1 Introduction

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 [4] 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.

We have to define security mechanisms that will help us to face the actual threats. There are numbers of these mechanisms, some are very effective, others have greater costs, but provide necessary industry protection controls and a number of them becoming useless as the Internet and computer networks evolve.

According to Baker et. al. [2], organizations tend to think more about quantity than quality. They are not aware, which mechanisms are the best for their purposes, so they often deploy as many as possible. Wrong mechanisms can actually add deficiencies to the system instead of increasing the security state.

In this paper we will try to find a way of defining proper security mechanisms for the organization. We will inspect the control objectives from ISO 27002:2005 [8] standard and assign one or more security mechanisms to each of 131 control objectives. We will also inspect dependencies between these mechanisms in order to correctly determine an evaluation criteria.

The main motivation for using security mechanisms is the clarity of their measurement. We cannot effectively measure the quality of control objectives implementation in the organization, but it is much easier with security mechanisms. If we have to use for example a mechanism called 'Implementation of authentication and authorization mechanisms - passwords, tokens, biometrics,' it is easy to decide whether it is fulfilled or not.

The overall goal is to determine whether the organization has satisfiable security controls in accordance to the ISO 27002:2005 standard and therefore it is able to demonstrate compliance with the ISO 27001:2005 [7] standard.

The rest of this paper is structured as follows. Section 2 provides an overview of a related work dealing with the problem of security mechanisms selection. Section 3 proposes our approach and describes methods used for choosing proper security mechanisms and for identification of relationships between them. Section 4 concludes this paper and provides a motivation for further work.

2 Related Work

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.

Singh ans Lilja [11] use Plackett & Burman (PB) design for determining the critical security controls [10]. 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 [9] 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 [12], assign them weights with support of security experts and estimate their efficiency against security breaches.

There are security standards, like the ISO 27002:2005 [8] or NIST 800-30 [12] that provide a database of security controls. But they fall short on choosing proper controls for the organization and on evaluation of quality of these controls. They also do not take in consideration relationships and dependencies over the security controls.

In [3] and [5] the authors deal with the similar problem looking at a more technical aspect - they introduce a scalable firewalling architecture based on dynamic and adaptive policy management facilities which enable the automatic

generation of new rules and policies to ensure a timely response in detecting unusual traffic activity as well as identify unknown potential attacks.

3 Methods

This section provides an overview of methods for selection of security mechanisms. Our approach emanates from the ISO/IEC 27002:2005 standard. We identify security mechanisms for each control objective from this standard and consider the importance and implementation quality of these mechanisms.

This section is divided into three subsections, the first one, the 3.1, provides the overview of the proposed weighting methods, the second one, the 3.2, describes relationships between security mechanisms and the last one, the 3.3, explains how to select and evaluate them.

3.1 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 [12]. 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 [9] 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:

$$RawWeighting_i = wP_i.owP_i + wD_i.owD_i + wR_i.owR_i \tag{1}$$

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:

$$RelativeWeighting_i = \frac{RawWeighting_i}{\sum_{j=1}^{n} RawWeighting_j} \tag{2}$$

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:

$$RawWeighting_i = wI_i.owI_i + wM_i.owM_i + wP_i.owP_i \tag{3}$$

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 2.

Table 1 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 [9] 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.

3.2 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 [6]. 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.

Table 1: 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**

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.

Verizon publishes Data Breach Investigations Reports [1] every year. It contains statistical records of incidents collected from various companies, divided into categories, providing detailed information about the overall state of the cyber security in our society.

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 2 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

Table 2: Control objectives' protection against Top 10 security threats.

Sec. Clause / 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

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 negligable 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 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 2. Besides other important characteristics we get the Pearson's correlation matrix. In this matrix we can see dependencies between each two control objectives:

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

Table 3 shows us the unrotated component matrix, consisting of three main factors. This matrix represents the significance of elements within each factor.

Table 3: 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

For better visualisation, the results are stated in Figure 1. 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 4 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

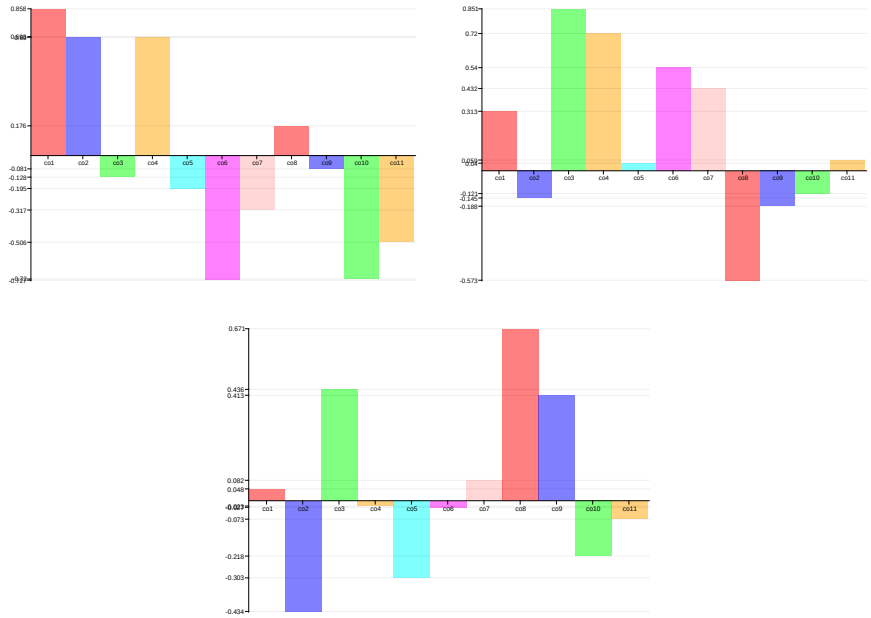

Fig. 1: Components and control objectives.

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.

$$FinalScore_{CO_i} = RW_{CO_i} * \left(S_{CO_i} + \frac{S_{CO_j} * COR_{ij}}{1 + COR_{ij}} \right) \tag{4}$$

The score of S_{CO_i} depends on evaluation of security mechanisms 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 5. 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.

$$S_{CO_i} = \sum_{j}^{n} S_{M_j} * RW_{M_j} \tag{5}$$

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.

3.3 Security Mechanism - Selection Process and Evaluation

To summarize the previous sections, the assignment of security mechanisms to control objectives consists of following steps:

1. Assignment of the security mechanisms with respect to control objective's description. Usually there are three to five mechanisms supporting one control objective.
2. Definition of the weight of each mechanism - this parameter shows us, how important is this mechanism for the contol objective fulfillment. We use the I/M/P model with three weight components for this purpose. The sum of relative weights of mechanisms is 1.
3. Determination of weights of control objectives - these weights have to reflect the organization's security goals, for example necessary requirements for confidentiality, integrity or availability of organization's assets.
4. Estimation of dependencies with the factor analysis method, adjusted by the security analyst's judgement.

4 Conclusions

In this paper we proposed a way of choosing proper security mechanisms that will protect the organization's assets. We defined a method for the determination of importance of these mechanisms by assigning weights. These weights express, how well the particular mechanism contributes to the implementation, maintenance or policy fulfillment of the control objective, to which it was allocated. The whole model consists of about four hundred security mechanisms, that were allocated for each of 131 control objectives from the ISO/IEC 27002:2005 standard.

We also proposed the approach for determining relationships between security mechanisms. For this purpose we choosed the factor analysis, a statistical method that can reveal hidden correlation among observed variables. We explore these correlations on the control objectives layer, because inspecting every security mechanism would be exceedingly comprehensive and space consuming. The factor analysis gave us meaningful results that need to be further adjusted by security professionals to express the dependencies correctly.

Verendel [13] claims that quantitative security evaluation is still very unclear and it is almost impossible to validate the methods against empirical data. We would like to confute this claim by building a quantitative evaluation method that will be based on a number of smaller components, that work together and could be verified standalone. In this paper we presented the component dealing with the security mechanisms problem.

In the future, we would like to use the results of this work to construct a security evaluation system, that will measure the real security state in an organization by evaluating the quality of implemented security mechanisms.

Acknowledgment. The paper was prepared with partial support of research grant VEGA 1/0722/12 entitled "Security in distributed computer systems and mobile computer networks".

References

1. W. Baker, A. Hutton, D. Hylender, J. Pamula, Ch. Porter, and M. Spitler. 2012 Data Breach Investigations Report. Technical report, Verizon, 2012.
2. W. Baker and L. Wallace. Is information security under control?: Investigating quality in information security management. *IEEE Security and Privacy*, 5(1):36–44, January 2007.
3. A. Castiglione, A. De Santis, U. Fiore, and F. Palmieri. An enhanced firewall scheme for dynamic and adaptive containment of emerging security threats. In *Broadband, Wireless Computing, Communication and Applications (BWCCA), 2010 International Conference on*, pages 475 –481, nov. 2010.
4. G. Cybenko and C. E. Landwehr. Security analytics and measurements. *IEEE Security & Privacy*, 10:5–8, 2012.
5. A. De Santis, A. Castiglione, U. Fiore, and F. Palmieri. An intelligent security architecture for distributed firewalling environments. *Journal of Ambient Intelligence and Humanized Computing*, pages 1–12, 2011.
6. L. A. Gordon and M. P. Loeb. The economics of information security investment. *ACM Trans. Inf. Syst. Secur.*, 5(4):438–457, November 2002.
7. ISO. *ISO/IEC Std. ISO 27001:2005, Information Technology - Security Techniques - Information security management systems - Requirements*. ISO, 2005.
8. ISO. *ISO/IEC Std. ISO 27002:2005, Information Technology - Security Techniques - Code of Practice for Information Security Management*. ISO, 2005.
9. 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.
10. R. L. Plackett and J. P. Burman. The design of optimum multifactorial experiments. *Biometrika*, 33(4):305–325, 1946.
11. 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.
12. G. Stoneburner, A. Goguen, and A. Feringa. *NIST Special Publication 800-30: Risk Management Guide for Information Technology Systems*. NIST, 2002.
13. 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.