COMPUTERS & SECURITY 55 (2015) 100–112

Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

The information systems' security level assessment model based on an ontology and evidential reasoning approach

Kresimir Solic [a,c,*], *Hrvoje Ocevcic* [b,c], *Marin Golub* [d]

[a] *Faculty of Medicine, University of Osijek, Josipa Huttlera 4, HR-31000 Osijek, Croatia*
[b] *Hypo–Alpe-Adria-Bank d.d., Slavonska avenija 6, 10000 Zagreb, Croatia*
[c] *Faculty of Electrical Engineering, University of Osijek, Josipa Huttlera 4, HR-31000 Osijek, Croatia*
[d] *Faculty of Electrical Engineering and Computing, Zagreb University, Unska 3, HR-10000 Zagreb, Croatia*

ARTICLE INFO

Article history:
Received 12 December 2014
Received in revised form 26 June 2015
Accepted 31 August 2015
Available online 5 September 2015

Keywords:
Information security model
Information security
Risk assessment
Security control selection
Security management
OWL
Ontology
Evidential reasoning

ABSTRACT

In the area of information technology an amount of security issues persists through time. Ongoing activities on security solutions aim to integrate existing security guidelines, best practices, security standards and existing solutions, but they often lack a knowledge base or do not involve all security issues, particularly human influence.

In this paper, we presented a model that can be the basis for a novel information systems security evaluation solution. This solution should be able to cover a wide range of all possible information security issues. Our model is based on an OWL ontology for knowledge base, uses an enhanced Evidential Reasoning algorithm for mathematical calculations and possesses a simple reflex intelligent agent's algorithm as a decision supporting element.

Properties for this model supervene from properties of its constructing elements. Knowledge base being built on OWL ontology is a major element of the model. It can provide high flexibility and applicability to different information systems and business organizations; upgradeability to be up to date regarding current security issues and new threats; and high versatility, taking into evaluation all possible aspects regarding security issues, e.g., network security, software and hardware issues, human influence, security policies and disaster recovery plans. Enhanced Evidential Reasoning algorithm is based on the Dumpster–Shafer theory and is well suited for calculations with expert's subjective judgements combining qualitative with quantitative evaluation grades. We designed an algorithm for back coupling based on a simple reflex intelligent agent for results presentation and decision support.

In our work, we explained how to connect and use each of the model's constructive elements to obtain information security evaluation results. In addition, we conducted a case study with the proposed model on a small business organization. To test our model, we also used the standard qualitative risk assessment method on the same business organization in order to compare both qualitative results.

Preliminary testing results have shown that the presented model could achieve its goal if it would be developed into an integrated software tool with a well-defined and up-to-date ontological knowledge base.

* *Corresponding author.* Tel.: +385 917550631.
E-mail addresses: kresimir.solic@mefos.hr (K. Solic), hrvoje.ocevcic@hypo-alpe-adria.hr (H. Ocevcic), marin.golub@fer.hr (M. Golub).
http://dx.doi.org/10.1016/j.cose.2015.08.004
0167-4048/

1. Introduction

An amount of information security problem issues persist through time, even though there are different security guidelines and software tools for security evaluation and risk management that cover different approaches and solve different security issues. Additionally, business managers and security experts often use different terms for similar or the same security issues, so they hardly understand each other in joint efforts to solve security issues.

Several ongoing activities on security solutions aim to integrate existing guidelines, best practices, security standards and existing solutions. The main information resources are the ISO/IEC 27000 series of standards, ENISA agency, NIST agency, InfoSec institute, SANS institute, national CERT organizations, different national IT Security guidelines (BSI, 2007; CNiL, 2010) and others. They are used as the basis for several integrated solutions and knowledge bases, such as the ontology of security metrics (Sajko et al., 2010), Common Body of Knowledge (Schwittek et al., 2012) and Security Ontology (Fenz et al., 2011). Additionally, there are several risk management tools that exist, such as the AURUM software tool based on the NIST SP 800-30 risk management standard (Ekelhart et al., 2009), the GSTool based on the German IT Grundschutz Manual (BSI, 2013), the EBIOS methodology tool based on the French EBIOS standard (ANSSI, 2013), the risk analysis based CORAS method (Lund et al., 2011) that partly supports the ISO/IEC 27001 standard, the risk based DDP tool supported technique for quantitative risk analysis reasoning method (Cornford et al., 2006) or the MOPM method based on combining the Analytic Hierarchy Process (AHP) and Particles Swarm Optimization (PSO) (Awad et al., 2011).

These solutions are often developed either for business and security managers or for security experts and technicians, and they mostly do not take into account human influence. Moreover, there is no overall, generally applicable solution to prove their productivity and quality, e.g., even some criticism towards ISO/IEC is highlighted (Beckers et al., 2012).

In this paper, we present an information security model based on an OWL ontology, an enhanced Evidential Reasoning algorithm and a simple reflex intelligent agent's algorithm. Knowledge base security ontology gives a logical basis for this model by defining descriptive formal knowledge on security issues (Gruber, 1995), while the enhanced ER algorithm is the mathematical evaluation algorithm of this model (Yang and Xu, 2002). The simple reflex intelligent agent's algorithm, as the decision supporting element for automated back coupling, should search through the ontology to find security critical elements or low security level subsystems (Russell and Norvig, 2010).

The main properties of this solution are aimed at: high flexibility and applicability to both different information solutions and different business organizations; upgradeability to be up to date in real time regarding security issues and new threats; and high versatility, taking into evaluation all possible aspects of security, e.g., network security, software and hardware issues, human factor, security policies and disaster recovery protocols.

Information security evaluation results gained with this model are as follows: overall grade on information system's security level; identification of low security level subsystems; and security critical elements of the evaluated information system. After determining the overall security level and identifying security critical elements of the evaluated system, it is left to business and security management to decide on necessary actions. Decisions on which security solution is the best for an evaluated business organization regarding ROI and business needs are left to the management.

We made three assumptions to build the proposed model. The first assumption was the consideration of the user as the constitutive part of the information system that will be evaluated. Because the user can significantly affect the overall systems security level (Solic et al., 2011), its behaviour or awareness regarding security issues has to be taken into evaluation. The second assumption was that the enhanced ER algorithm, which is developed for static and dynamic technical systems' state evaluations, can be used to evaluate users' behaviour (Solic et al., 2013). The third assumption was that, currently, looking from the information security perspective, data as written information is the universal currency and main asset in every business process (Haley, 2012). The third assumption makes the proposed model generally applicable.

Possible problems can be found in the quality of security ontology and subjective expert's assessment methodology. The first problem can be solved with ongoing work on building a common body of knowledge on security issues organized as ontology (Schwittek et al., 2012). The solution of the second problem is covered by using all properties of the enhanced ER algorithm, which is based on the Dempster–Shafer theory that mathematically addresses uncertainty and subjectivity (Yang and Xu, 2002).

Instead of focusing on known security threats and the identification of possible security breaches, the presented model searches for opened back doors and the smallest security critical elements of the examined information system and, by grading the overall security status and comparing it to referent values, gives a basis for decision on whether the security level should be improved. It also takes human impact into consideration, as humans are still the weakest link of an information security system (Sasse et al., 2001).

The proposed solution is applicable to differently sized business organizations as well as to small, standalone information systems, such as smart mobile phones. It can cover all possible aspects of security issues and can be highly up to date as long as the security ontology is well defined. This solution should be usable by both security experts and business managers because it tries to include both risk management and a technical approach towards security issues.

We applied the proposed model on a small business organization's information system. For testing purposes, we also used the standard qualitative risk assessment method on the same organization and compared the results.

The presented model aims to become the basis for a novel information systems security evaluation solution that should cover all possible information security issues.

In the next section, we discuss some related work, and, in Section 3, we present a detailed description of the proposed model design. In Section 4, we present usage of the proposed model and compare it with the qualitative risk assessment method. The conclusion and plans for further development are given at the end of this paper.