2010 IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology

A Security Framework for Audit and Manage Information System Security

Teresa Susana Mendes Pereira
Informatics Department
Superior School of Business Studies
Polytechnic Institute of Viana do Castelo
Valença, Portugal
Email: tpereira@esce.ipvc.pt

Henrique Santos
Information System Department
School of Engineering
University of Minho
Guimarães, Portugal
Email: hsantos@dsi.uminho.pt

***Abstract*—Auditing Information Systems Security is difficult and becomes crucial to ensure the daily operational activities of organizations as well as to promote competition and to create new business opportunities. A conceptual security framework to manage and audit Information System Security is proposed and discussed. The proposed framework is based on a conceptual model approach, based on the `ISO/IEC_JCT1` standards, to assist organizations to better manage their Information Systems Security.**

***Keywords*-Security audit management, information system security, ontology and conceptual model.**

I. Introduction

Speed and accessibility operations promoted by information and communication technologies, particularly the Internet and the new Internet-enabled services, leads the organizations to become heavily dependent on the performance of their information systems. On the other hand the evolution of wireless communication and the rapid growth and availability of new services to facilitate accessibility, such as, for example, the new cloud computing services, have been gaining popularity not just by the organizations, but by generic users as well. Although these new solutions offer a better service with a promising technological initiatives at low operating cost, they also brings a set of new and unexpected risks [5]. Consequently new forms of security protection become crucial and existing security procedures may need to be reviewed. One strategy is to perform regular information system security audits, to evaluate the performance of the security information management and analyze if the existing security practices need to be reviewed. A security audit of an information system is conducted to assess the effectiveness of an organization's ability to protect its valued or critical assets [5]. This paper intends to present an investigated approach to improve security management through a conceptual framework developed to assist organizations to classify attacks, identify assets and mitigate their vulnerabilities and threats. The proposed framework is based on a conceptual model with capability to represent the semantic concepts and their relationships in the information security domain, defined accordingly to the established security standard `ISO/IEC_JTCI1`[1] [4].

The paper is structured as follows: in the section II it will be presented an overview of security management concepts; section III presents the proposed conceptual model, which contains the semantic concepts specified in the information security domain, and their relationships, hierarchical structured in an ontology; section IV presents the proposed framework to manage and audit information systems security, based on the ontology structure; conclusions and future work are presented in section V.

II. Security Management

Managing information system security is increasingly concerning organizations, due to the continuous growing dependence of organizations on technology to conduct theirs businesses, to create a competitive advantage and achieving higher ROI. Organizations rely significantly on technology, such as Internet, for businesses operations and secure business transactions [6]. However organizations must consider how they are going to succeed to the continuous changing risk environment, since the technical controls alone are no longer guaranteed, but mainly dependent on other security requirements such as legislation, culture or the environment [6]. Currently security is a fundamental principle for organizations businesses performance. As a result, organizations need to evolve security management strategies in response to the evolving information security requirements. A properly security strategy demands for a rigorous process, similar to any other business process, where every agent interacting with critical resources need to be aware and participate in security management, both adopting secure behaviors and continuous evaluating security control's performance [1].

The regular audit of information system security is one approach to evaluate the organizations information systems practices and operations. An auditing process will enable to obtain evidences of organizations information systems security policies efficiency to maintain the assets integrity, confidentiality and availability, the typical organizations security

[1] International Organization for Standardization (ISO)/ International Electrotechnical Commission (IEC), Joint Technical Committee (JTC 1)

978-0-7695-4191-4/10 $26.00 © 2010 IEEE
DOI 10.1109/WI-IAT.2010.244

objectives. There are a few models or frameworks to support the security audit, most of the time based on more or less liberal interpretations of the security fundamental concepts [5]. It is important to underlie that guidelines for security auditing exist and are provided by recognized authorities. The most relevant examples is the authority of Information Security Audit and Control Association (ISACA[2]) that provides guidelines for security auditing and best security practices for information, systems and process auditing. They stipulate computer systems audits and controls guidelines such as the control objectives for information and related technology (CoBIT[3]) developed by IT Governance Institute. Alternatively there are the *Guidelines for information security management systems auditing*, released in 2007 by `ISO/IEC` and the ISO 17799 Checklist [2] developed by SANS [4] (System Administration, Networking and Security). These standards precisely define the main procedures, but are limited concerning the strict relations or process flows necessary to undertake a security task, such as an audit. To address this lack, it is presented a framework to support the security audit of information systems security, based on a conceptual model.

III. Proposed Conceptual Model

The proposed framework is based on conceptual ontology, which models the fundamental concepts of attacks, threats and vulnerabilities, and their relationships to other security concepts. The defined conceptual model comprises 8 concepts and 16 relationships, based on the security standards `ISO/IEC_JCT1,`as illustrated in the figure 1. These concepts are described as following:

Incident – A single or series of unwanted or unexpected events that might have significant probability to compromise the information system security.

(Security) Event – An identified occurrence of a particular set of circumstances that changed the status of the information system security.

Asset – Any resource that has value and importance to the organization, which includes information, programs, network and communications infrastructures, software, operating systems, data and people.

CIA – The information properties to be ensured, namely: confidentiality, integrity and availability; besides these main security properties, and depending on the context, other security properties may need to the addressed, such as: authenticity, accountability and reliability.

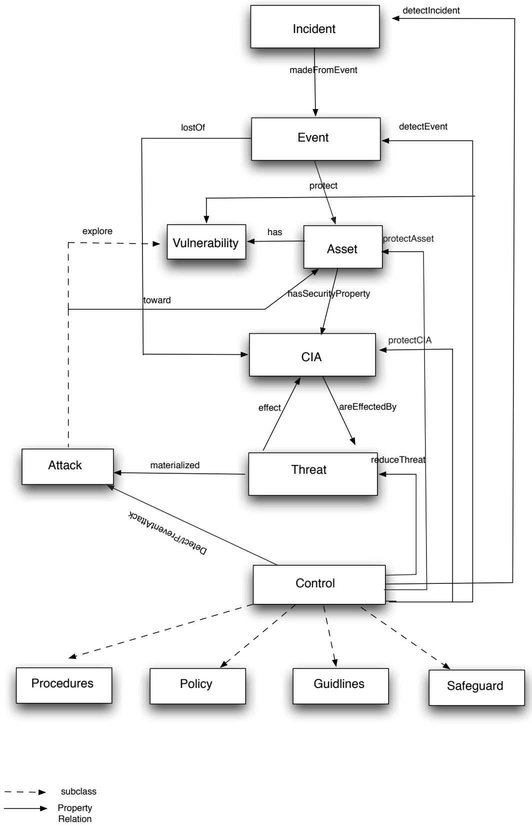


Figure 1. Concepts and relationships defined in the conceptual framework, adapted from [9]

Threat – Represents the types of dangers against a given set of properties (security properties). The attributes defined in this concept follow the Pfleeger approach (Pfleeger 2007), which include an attacker actions or position to perform an interception, fabrication, modification and interruption, over a resource.

Attack – A sequence of actions executed by some agent (automatic or manual) that explore any vulnerability and produce one or more security events.

Control – A mechanisms used to detect an incident or an event, to protect an asset and their security properties, to reduce a threat and to detect or prevent the effects of an attack.

Vulnerability – Represents any weakness of the system.

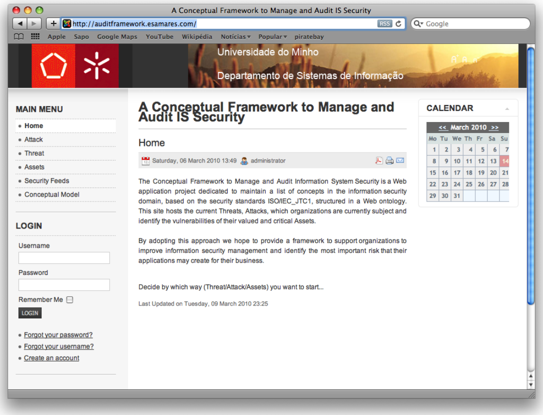
In short, the rational behind the ontology is structured as following: an incident is made from – *madeFromEvent* – events; the occurrence of an event can lead to a lost of – *lostOf* – a set of security properties (CIA); an asset has security properties – *hasSecurityProperties* – and each one

[2] http://www.isaca.org/
[3] http://www.itgi.org/
[4] http://www.sans.org

can be *affected* by a threat; on the other hand, a threat can *affect* one or more security properties; and finally, an asset *has* vulnerabilities. A threat is *materialized* by an attack, while the attacks *exploit* one or more vulnerabilities; an attack is also triggered *toward* an asset. Further, the implementation of control mechanisms help to *reduce* threats, to *detect* and *prevent* an attack, to *protect* security properties, to *protect* assets and vulnerabilities, as well to *detect* events, in order to *protect* assets [7] . The description of those concepts and their relationships, presented in the ontology, was formalized through the use of the W3C standard language for modeling ontologies Web Ontology Language (OWL). This web language has been developed by the Web Ontology Working Group as a part of the W3C Semantic Web Activity [11]. In spite of OWL has not been designed to specifically express security issues, it was selected because it is a W3C recommendation since February of 2004 and due to its expressiveness with superior machine interpretability. The OWL is build upon Resource Description Framework (RDF) and Resource Description Framework Schema (RDFS). In fact the OWL vocabulary is an extension of RDF and uses RDF/XML syntax. The formalization of this ontology in OWL will be a step forward to promote its interoperability among different information security systems. In the next section, it will be presented the framework under proposal, which follows the hierarchical structure of the semantic concepts represented in the defined ontology, and try to provide an easy way to understand user interface so all users in an organization can participate in security auditing like tasks.

IV. Proposed Security Framework to Manage and Audit Information System Security

The establishment of `ISO/IEC_JTC1` standards promoted the standardization of the semantic concepts defined in the information security domain. The correct understanding and identification of those concepts are the primarily requirement to be considered in the execution of a proper evaluation of the information system security effectiveness, and further to identify and characterize an occurred security incident, as well as to estimate its impacts. The proposed conceptual framework intends to assists the organization, firstly to precisely determine what should be protected (the assets) and their weaknesses (vulnerabilities) involved in their daily activity. Secondly to assess what vulnerabilities can be exploited by an attack, as well the threats that might be materialized in an attack. Finally, evaluate the efficiency and the effectiveness of the policy and controls implemented, in order to evaluate if they are being correctly implemented or if they need any adjustment [7]. Figure 2 illustrates the conceptual framework proposed, presenting these three nuclear concepts: attack, threat and assets. The auditor can select the concept from which he/she intends to start the auditing process, and proceed to the directed related concepts. Each concept contains a list of elements that are linked to the other concepts, conforming to the hierarchical structure of the semantic concepts, defined in the ontology. These three concepts were included in the front-end of the framework, rather the others, due to the nature of the audit operation, which the auditor intends to perform. Traditionally, a security audit is conducted once an incident has occurred (reactive followed by a corrective audit), that is when an asset has been compromised. In this case, an audit is requested in order to determine the source of the attack and how the incident happened, proceeding with the adequate corrective mechanisms. However a security audit is not only about investigating security break-ins, but rather to mitigate recognized threats, in order to ensure: (1) the security compliance; (2) the security of critical assets; (3) the right controls are in the right place. In this last view a security audit is performed in the context of the security risk management process, and aims to produce or evaluate a security policy. Being conducted by the main concepts and their relationships defined by an ontology, the proposed framework intends to assist organizations to understand, prepare and perform security audits, by themselves. This framework does not focus exclusively on technical controls involved with information security, but enforces procedures and practices to assist organizations to maintain consistently high levels of useful and good quality information concerning their information security systems. Within the ontology, each concept is mapped to real subjects. For example a malicious code attack is connected/linked to the affected assets, the vulnerability it explores, and the security properties that have been compromised. Despite the large amount of information available to complete a basic ontology, we accept that each organization will develop its one view of security awareness. The framework is modular concerning this aspect, allowing evolving the ontology by adding the relevant subjects. This way, the auditor may proceed through



A Conceptual Framework to Manage and Audit IS Security

Home

Saturday, 06 March 2010 13:49 administrator

The Conceptual Framework to Manage and Audit Information System Security is a Web application project dedicated to maintain a list of concepts in the information security domain, based on the security standards ISO/IEC_JTC1, structured in a Web ontology. This site hosts the current Threats, Attacks, which organizations are currently subject and identify the vulnerabilities of their valued and critical Assets.

By adopting this approach we hope to provide a framework to support organizations to improve information security management and identify the most important risk that their applications may create for their business.

Decide by which way (Threat/Attack/Assets) you want to start...

Last Updated on Tuesday, 09 March 2010 23:25

<< March 2010 >>

Mo	Tu	We	Th	Fr	Sa	Su
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

Figure 2. Developed framework

the examination of the relevant vulnerabilities in the assets that can compromise the security of the information system, within the organization; or the auditor may go along with the analyses of new threats that might be materialized in an attack.

Additionally, the proposed framework includes the typical functions of similar tools, enabling a set of functionalities, like the possibility of the auditor to generate a report with all steps performed, as well as the registration date of the audit. According to the results of the auditor' examinations, he can also schedule the next audit. Moreover, if the auditor during his examination detects a new incident, i.e. an attack that is not presented on the list of attacks, the auditor should report this new attack with its features, which will be validated by the administrator of the framework and, after that, the administrator will index the attack to the list of attacks. This procedure is the same if the auditor decides to conduct the audit through the examination of the assets or threats and during the process identifies a new vulnerability in an asset or a new threat.

V. Conclusion and Future Work

Regular security audits should be performed not only as a reactive response to an occurred incident, but also as a proactive audits to assess if security controls and procedures adopted by an organization are proper to protect their valued and critical assets. The need for permanent study of attacks, threats and the assets vulnerabilities in an information system is essential due it to their continue evolvement and the significantly impacts on an organization. Managing those concepts requires both a detailed understanding of security concepts and their relationships. Such understanding can assist organizations in implementing the right combination of protection controls to mitigate security risks related with the assets' vulnerabilities. The paper discusses the implementation of a conceptual model, to support the auditor to understand the business requirements in managing security of an organization, namely to: (1) properly identify the valued or critical assets; (2) properly identify the vulnerabilities of assets; (3) identify and mitigate potential threats; (4) evaluate the risks; (5) evaluate the efficiency and effectiveness of the security policies and safeguards defined and therefore analyze and implement the necessary adjustments to security policy adopted.

This solution introduces a new perspective to model information, in the security domain, since it is based on a conceptual model with capabilities to richly describe multiple security resources within an organization. Furthermore, it enables an organization evolving its own instantiation of the security ontology, obeying to standard concepts, but embedding its on view and assumed risk of exposition. Additionally the formalization of this ontology in OWL will be an important resource to promote its interoperability among different information security systems, as well its integration in other knowledge representation system in the security domain.

As future work we intend to assess the application of the proposed framework and analyze, if the system fulfills the evolution of information system security attacks.

References

[1] Da Veiga, A. and Eloff, J.H.P, An information security governance framework. *Information Systems Management 24*, 361-372, 2007.

[2] Information Security Management, Part2: Specification for Information security management systems AS/NZS 7799.2:2003 BS 7799.2:2002 (2003), [on-line], SANS, http://www.sans.org/score/checklists/ISO_17799_checklist.pdf.

[3] ISO/IEC FDIS 27000 Information technology – Security techniques – Information security management systems Overview and vocabulary, ISO copyright office. Geneva, Switzerland (2009).

[4] ISO/IEC FDIS 27001 Information technology – Security techniques – Information security management systems – Requirements, ISO copyright office. Geneva, Switzerland (2005).

[5] Onwubiko, C., 2009. A Security Audit Framework for Security Management in the Enterprise. In Global Security, Safety, and Sustainability. In *5th International Conference, ICGS3 2009, London, UK, September 1-2, 2009*.

[6] Onwubiko, C., Lenaghan, A. P., Challenges and complexities of managing information security. *Int. J. Electronic Security and Digital Forensic, Vol. 2, No. 3*, pp.306-321.

[7] Pereira, Teresa, Santos, Henrique, 2009. An Ontology Based Approach To Information Security. *Communication in computer and Information Science*, Sartori, Fabio; Sicilia, Miguel-Angel; Manouselis, Nikos, Eds. 2009, XIII, 330 p., Softcover. *3rd International Conference, Metadata and Semantics Research (MTSR 2009). ISBN: 978-3-642-04589-9*, pp. 183-193. Springer 2009, Milan, Italy. Sep-tember 30th - October 2009.

[8] Pfleeger, Charles, P., Pfleeger, Shari, L. (2007). Security in Computing, 4th ed., Prentice Hall PTR.

[9] Santos, H. D., ISO/IEC 27001 A norma das normas em Segurança da Informação, Publicação da Associação Portuguesa para a Qualidade, pp 11-19, Ano XXXV, N 1, ISSN 0870-6743, Primavera de 2006.

[10] Walker, David M., Jones, Ronald L. (2001). Management Planning Guide for Information Systems Security Auditing, special publication of the National State Auditors Association and the U.S. General Accounting Office, December 10, 2001, [on-line]. Available from: http://www.gao.gov/special.pubs/mgmtpln.pdf.

[11] Smith, Michael K., Welty, Chris, McGuinness, Deborah L.: OWL Web Ontology Language Guide, [on-line], W3C Recommendation 10 February 2004. Technical report, W3C (2004). Available from: http://www.w3.org/TR/owl-guide/.