Towards Ontological Approach to Security Risk Analysis of Information System:
Model and Architecture

Oluwasefunmi Tale Arogundade, Laboratory of Management Decision and Information Systems, Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing, China & Department of Computer Science, Federal University of Agriculture, Abeokuta, Nigeria
Olusola Adeniran, Department of Mathematics, Federal University of Agriculture, Abeokuta, Nigeria
Zhi Jin, School of Electronics Engineering and Computer Science, Peking University, Beijing, China
Yang Xiaoguang, Laboratory of Management Decision and Information Systems, Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing, China

ABSTRACT

Resource allocation decisions can be enhanced by performing risk assessment during the early development phase. In order to improve and maintain the security of the Information System (IS, hereafter), there is need to build risk analysis model that can dynamically analyze threat data collected during the operational lifetime of the IS. In this paper the authors propose an ontological approach to accomplishing this goal. They present analyzer model and architecture, an agent-based risk analysis system (ARAS) which gathers identified threats events, probe them and correlates those using ontologies. It explores both quantitative and qualitative risk analysis techniques using real events data for probability predictions of threats based on an existing designed security ontology. To validate the feasibility of the approach a case study on e-banking system has been conducted. Simulated IDS output serves as input into the risk analysis system. The authors used JADE to implement the agents, protégé OWL to create the ontology and ORACLE 11g SQL developer for the database. Optimistic results were obtained.

KEYWORDS
Agent, Countermeasures, Intrusion Detection System, Ontology, Risk, Security, Threats

1. INTRODUCTION

Resource allocation decisions can be enhanced by performing risk assessment during early development phase of information system. In order to improve and maintain the security of the Information system (IS, hereafter), there is need to build risk analysis model that use real time data collected during the operational lifetime of the IS. This model will help to identify the high risk threats based on the post analysis of threats profile so that remedial actions may be taken. This will help to control and optimize the security quality of the IS in the future. This paper proposes an ontological approach to accomplishing this objective.

There has been increase in the impact of information system security (ISS) abuses because of the high level of dependency of organizations on the IS. This has made ISS to attract much attention both from the academics and the practitioner.

DOI: 10.4018/IJSSE.2016070101

Copyright © 2016, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.
The openness of service oriented information system to both hackers and legal users alike has made a threat to data security to become a major concern to both users and organizations that own those applications. Establishing and maintaining trust between organizations and stakeholders entails maximum protection of information if the organizations are to preserve their reputation. In addition to handling the current threats adequately, risk analysis must also be considered. Risk analysis forms the core part of security information management system. The ability to counter these threats in a cost effective way is a vital component to a diligent and trustful IS. When evaluating threats to IS, it is important to recognize the viability of the threats and to evaluate the impact that an event would have on the continuity of the IS operations (McCumber, 2004). Attacks could come in various ways depending on the following: environment, in which the systems were deployed, the data they process and the context within which the system is being used. Everyday attack can include non-authorized access to data, theft of passwords, password guessing etc. Each attack has different levels of risk and impacts on the systems. Some attacks could be very dangerous and can affect the whole organization, while some are limited to few resources. Detecting and preventing attacks are costly in terms of time and money considering the limited resources of the organization.

A threat assessment methodology is a vital component of IS security information management because the threats to IS are real and very unpredictable therefore the ability to recognize and plan for them directly will influence the impact of a potential attack. The likelihood and impact of a security failure will determine the cost in terms of money and time that stakeholders will be willing to dedicate in order to satisfy a security control measure.

Proper security measures and means to effectively calculate risk assessment of information system after deployment has been an ultimate challenge to many organizations. There is no way to completely overcome the threats that an organization is exposed to but the risk of the threats can be minimized. The need for secure systems that are capable of performing post analysis of security risk and predicting the risks has become more essential especially in security critical organizations like banking system, health management system. The description of threats can be highly reusable, risks must normally be determined from time to time and from application to application. Risk management must be done consistently and completely to be useful. Risk management is not a one-time occurrence it must be done continuously. The reason is that risk management involves taking a snapshot in time and using it to anticipate what might happen in the future. Environmental conditions do change extremely and dynamically. This may challenge the validity of assumptions incorporated when managing risk. Hence, it is wise to revalidate risk management continuously throughout the life cycle of a business process project (Kliem, 2000).

For instance, two ATM machines in different locations may face the threat of spoofing; the associated risks may be quite different. Usually the security administrators are not that much aware of security risk processes with technical skills. As a result, there is a gap between organizations assets security and the software security. Closing this gap is one of the purposes of our approach. In our earlier work we have proposed a framework for modeling safety and security requirements of information system during the development process (Arogundade et al., 2011). The model was later enhanced and developed into use-misuse case security ontology (Arogundade et al. 2012).

In practice, the ISS risk assessment is quite complex and full of uncertainty. (Winkler, 1996). The uncertainty that exists in the process of risk assessment has been the primary factor that influences the objectivity and effectiveness of the ISS risk assessment (Ekelhart, A. et al 2007). In order to address the highlighted issues of concern, we are proposing an ontology based IS risk analysis system. In this study, the system provides an approach to automatically assess the IS security risk taking a snapshot of time. We explore real time data and used probability as a long term frequency approach to assess the risk value.

The rest of this paper is organized as follows. Section 2 reviews related works. While in section 3 we presented the proposed approach. Then we discuss the process of achieving ISS risk assessment in detail in section 4. The system architecture is implemented and validated in section 5 via a case study. Finally, we gave our contributions and presented our on-going and future research in section 6.
Related Content

Applicability of Lehman Laws on Open Source Evolution
www.igi-global.com/chapter/applicability-of-lehman-laws-on-open-source-evolution/135229?camid=4v1a
Some Key Topics to be Considered in Software Process Improvement
Gonzalo Cuevas, Jose A. Calvo-Manzano and Iván García (2014). *Agile Estimation Techniques and Innovative Approaches to Software Process Improvement* (pp. 119-142).
[www.igi-global.com/chapter/some-key-topics-to-be-considered-in-software-process-improvement/100275?camid=4v1a](www.igi-global.com/chapter/some-key-topics-to-be-considered-in-software-process-improvement/100275?camid=4v1a)

Supporting Customizable Business Process Models Using Graph Transformation Rules
[www.igi-global.com/article/supporting-customizable-business-process-models-using-graph-transformation-rules/170519?camid=4v1a](www.igi-global.com/article/supporting-customizable-business-process-models-using-graph-transformation-rules/170519?camid=4v1a)

A Novel Software System Protection Scheme Based on Behavior and Context Monitoring
[www.igi-global.com/article/a-novel-software-system-protection-scheme-based-on-behavior-and-context-monitoring/245808?camid=4v1a](www.igi-global.com/article/a-novel-software-system-protection-scheme-based-on-behavior-and-context-monitoring/245808?camid=4v1a)