

# MISSM GRADUATE ABSTRACTS (LISTED ALPHABETICALLY)

## Contents

|  |   |
|--|---|
| <b>CHOL, EMMANUEL</b> .....  | 2 |
| STUDY OF THE ENTERPRISE SECURITY MANAGER / SECURITY INCIDENT MANAGER (ESM / SIM)<br>COMMERCIAL AND OPEN SOURCE SOLUTIONS ..... | 2 |
| <b>DARI, BASHAR</b> .....  | 2 |
| EXPANDING OCTAVE TO FACILITATE SYSTRUST .....  | 2 |
| <b>DEFORGES, BENOIT</b> .....  | 2 |
| LOW ASSURANCE PROTECTION PROFILE FOR NETWORK ACCESS CONTROL .....  | 2 |
| <b>DIOP, MAME</b> .....  | 2 |
| INFORMATION SECURITY MANAGEMENT IN FRANCE: PERCEPTIONS AND INFLUENCE OF CULTURE,<br>REGULATIONS .....                          | 2 |
| <b>FIOGBE, JOSE</b> .....  | 3 |
| MODELING INFORMATION SECURITY GOVERNANCE IN THE ECOWAS ZONE: THE MATURITY MODEL<br>REVISITED .....                             | 3 |
| <b>GICHOHI, FRANCIS</b> .....  | 3 |
| INFORMATION SECURITY IMPLICATION OF E-LEARNING IMPLEMENTATION IN KENYA .....   | 3 |
| <b>GILBERT, VINCENT</b> .....  | 3 |
| MEASURING PERFORMANCE OF TWO APPLICATION SERVERS FOR JAVA DEVELOPED WEB SERVICES UNDER<br>HEAVY LOADS .....                    | 3 |
| <b>IDDRISU, FUAD</b> .....   | 3 |
| INFORMATION SECURITY AWARENESS -- ISSUES AND PROPOSED SOLUTIONS .....  | 3 |
| <b>JANOT, ETIENNE</b> .....  | 4 |
| SQLDOM4J: PREVENTING SQL INJECTIONS IN OBJECT-ORIENTED APPLICATIONS - A JAVA SOLUTION BASED<br>ON THE SQL DOM .....            | 4 |
| <b>LINDSKOG, DALE</b> .....  | 4 |
| A NOVEL STRATEGY FOR INTERNETWORK SEGMENTATION AND ZONING .....  | 4 |
| <b>MA, BILLY</b> .....   | 4 |
| ISSUES AND PROPOSED SOLUTIONS BASED ON ROLE-BASED ACCESS CONTROL METHODOLOGY .....   | 4 |
| <b>MAMOS, JAKUB</b> .....  | 4 |
| SCADA INFORMATION SECURITY MANAGEMENT GUIDE .....  | 5 |
| <b>MURRAY, BRIAN</b> .....   | 5 |
| REVERSE DISCOVERY OF PACKET FLOODING HOSTS WITH DEFENSE MECHANISMS .....   | 5 |
| <b>NJI, LIONEL</b> .....   | 5 |
| STATISTICAL ANALYSIS OF SOFTWARE DESIGN ERROR VULNERABILITY DATA .....   | 5 |
| <b>PERHR, TRISH</b> .....  | 5 |
| SCOPING ITGC'S FOR SOX 404 AUDITS .....  | 5 |
| <b>PASULA, JOHN</b> .....  | 5 |
| ELEMENTS OF A NEW COMPREHENSIVE RISK METHODOLOGY .....   | 5 |

|  |   |
|--|---|
| SACHEDINA, NISHA .....   | 5 |
| SYSTEMATIC METHOD OF ACHIEVING SARBANES-OXLEY (SOX) COMPLIANCE BY HARMONIZING COBIT, ITIL AND ISO 27002/17799..... | 6 |
| VIEGAS, EDWINA .....   | 6 |
| PRIVACY CLASSIFICATION OF HEALTH INFORMATION IN ALBERTA – ISSUES, PROPOSED SOLUTION AND BENEFITS .....             | 6 |

## Chol, Emmanuel

### ***Study of the Enterprise Security Manager / Security Incident Manager (ESM / SIM) commercial and open source solutions***

The research paper provides in depth analysis of commercial and open source Enterprise Security Manager/Security Incident Manager solutions.

## Dari, Bashar

### ***Expanding OCTAVE to facilitate SysTrust***

In the research paper, two main components of OCTAVE-S are mapped against SysTrust criteria and controls. These two components are: security practices questionnaires and threat profiles. Mapping OCTAVE-S security practices statement to SysTrust controls allow organization to better understand its readiness for a SysTrust certification audit by identifying which SysTrust controls are in place, which are missing, and which can be compensated by other controls. Developed threat profiles for application, ORACLE database, and UNIX server provides a template or start point for organizations who need to conduct a TRA for IT assets with similar types. These threat profiles that are mapped to SysTrust controls can help organizations in identifying controls needed to mitigate unacceptable risks. They can also help prioritizing OCTAVE-S action items and mitigation plans based on their alignment with SysTrust.

## Deforges, Benoit

### ***Low Assurance Protection Profile for Network Access Control***

This research paper first provides a comprehensive analysis of the important concepts surrounding Network Access Control (NAC), and a description of how NAC products work. Based on the analysis, a new Common Criteria Protection Profile for NAC is proposed. A description of the rationale for the developed Protection Profile is given. The compliance of current NAC products with the proposed Protection Profile is also discussed in the paper.

## Diop, Mame

### ***Information Security Management in France: Perceptions and Influence of culture, regulations***

This study attempts to reveal some of the impact of culture, regulations on security approach; and also why a security certification is not well adopted in French companies in opposition to other countries like Japan or US. The central objective is also to give an answer to what many security professionals agree (or not) that culture and local rules/regulations are something we have to deal with in order to preserve security.

This study attempts to reveal some of the impact of culture, regulations on security approach; and also why a security certification is not well adopted in French companies in opposition to other countries like Japan or US. The central objective is also to give an answer to what many security professionals agree (or not) that culture and local rules/regulations are something we have to deal with in order to preserve security.

## **Fiogbe, Jose**

### ***Modeling Information Security Governance in the ECOWAS Zone: The Maturity Model Revisited***

This paper examines information security governance in the Economic Community of West African States (Ecowas). It uses the ITU Digital Opportunity Index and e-government ratings to estimate a country security governance index. The index is then used to rank countries by their current maturity level of information security governance. It proceeds to offer a causal analysis and pinpoint factors that could improve that maturity. In the paper, we extend the initial security governance maturity model. Our innovation is to do what nobody have done before us, that is to evaluate information security governance in underprivileged West African countries, using an extension to the information security governance maturity model. Although not perfect, this work should be seen as a trailblazer. Our pioneering research helps to open up a new line of research in the promising field of information security governance.

## **Gichohi, Francis**

### ***Information Security Implication of E-learning Implementation in Kenya***

In the paper we explore, analyze, and discuss the information security implications of e-learning implementation in Kenya using information security framework.

## **Gilbert, Vincent**

### ***Measuring performance of two Application Servers for Java developed Web Services under heavy loads***

Businesses are increasingly migrating legacy web applications towards Web Services however; there is a limited choice available for platforms which can support this technology. Furthermore, these same legacy applications are increasingly the prey of Denial of Service attacks in order to deprive businesses of their ability to operate normally. Many security mechanisms exist to protect the confidentiality and the integrity of web services but there is little emphasis on availability. During this research, I will develop a secure java Web Service which I will then deploy on two separate platforms, the Oracle Business Process Execution Language Process Manager as well as the Sun Java System Application Server 9.1 under a Windows operating system. The performance of these afore mentioned configurations is tested by exposing them to heavy concurrent load situations with varying types of requests and results of the test are analyzed in the research paper.

## **Iddrisu, Fuad**

### ***Information Security Awareness -- Issues and Proposed Solutions***

This research paper investigates what private and public organizations in Edmonton are doing to promote Information Security awareness, how organizations in Edmonton measure the level of awareness and the consistency of the awareness program. This paper determines the applicability of the Security Awareness Index metrics. A qualitative approach using survey method of data collection supplemented by interviews with Information Security managers was used to answer the research questions. Secondary data in the form of reports served as additional evidence.

## **Janot, Etienne**

### ***SQLDOM4J: Preventing SQL Injections in Object-Oriented Applications - a Java solution based on the SQL DOM***

Most of today's online applications rely on databases (DBs) to store data persistently. The SQL language used to communicate with the database management systems does not have separate data and control channels thus rendering these newly exposed systems vulnerable to code injection attacks. SQL Injection Attacks (SQLIA's) make up nearly a fourth of web application vulnerabilities and threaten their confidentiality, integrity and availability. This paper develops the fundamentals of an API solution for Java applications, which prevents SQLIA's by leveraging both the strongly-typed nature of OO applications and JDBC's pre-compiled type binded statement interface, PreparedStatement. This paper shows that the use of the SQLDOM4J API, which is based on McClure's SQL DOM, to build and execute database queries, effectively protects applications against SQLIA's. Moreover, it will be argued that from a programmer's perspective, the SQLDOM4J solution brings the DB structure to the development environment (IDE) and thus facilitates DB applications development. The solution's performance is also evaluated and possible future improvements are identified in the paper.

## **Lindskog, Dale**

### ***A novel strategy for internetwork segmentation and zoning***

In this research paper, a new systematic approach to segmenting nodes in an internetwork is proposed. The research paper shows advantages of screening traffic between clients and the servers with which they communicate. The proposed strategy is intended to supplement, but not displace, other approaches to network security zoning. Unlike many other firewall architecture strategies, the new strategy is not intended as a network solution to deficiencies in host security. Rather, this strategy is intended primarily to (1) mitigate the consequences of host compromise, and (2) to facilitate network security monitoring.

## **Ma, Billy**

### ***Issues and Proposed Solutions Based On Role-Based Access Control Methodology***

The research paper attempts to show the advantages and disadvantages of using RBAC as a security method to control access to information systems through its projected implementation to a bona fide government organization. Five comparative factors are used to demonstrate this point: (1) Simplified Systems Administration, (2) Enhanced Organizational Productivity, (3) Reduction of Employee Downtime, (4) Enhanced Systems Security and Integrity, and (5) Simplified Regulatory Compliance.

## **Mamos, Jakub**

## ***SCADA Information Security Management Guide***

This research paper attempts to show that employing information security management practice standard ISO/IEC17799:2005 and supplementing it with SCADA-specific existing research, to provide insight into specific requirements and limitations of process control systems, can provide a meaningful framework for the SCADA systems security management.

### **Murray, Brian**

#### ***Reverse Discovery of Packet Flooding Hosts with Defense Mechanisms***

The aim of this research is to devise a new method of discovering compromised hosts that are part of a botnet, and remove their effectiveness, in an automated and rapid way. A prototype protection mechanism against Denial of Service attacks is proposed in the research paper. The proposed system is composed of routers using specialized software that can discover compromised hosts, as well as defend against them, without the need for a complete deployment on all routers.

### **Nji, Lionel**

#### ***Statistical Analysis of Software Design Error Vulnerability Data***

The research is focused on the analysis of trends of software design error vulnerabilities. Statistical analysis methods were used in the research to analyze software design error vulnerability data that were collected after January 1988 and before January 2007. The research paper provides new and unique insight into the software designed error vulnerabilities during the above specified period.

### **Perhr, Trish**

#### ***Scoping ITGC's for SOx 404 Audits***

In the research, we demonstrate how to apply and combine several frameworks and methodologies that are now available to form a generalized recommendation on a scoping for ITGC's. The research paper demonstrates the benefits of the application of the combinations of the general controls frameworks on the size and the types of the organizations.

### **Pasula, John**

#### ***Elements of a New Comprehensive Risk Methodology***

Organizations may have multiple forms of risk management used within different organizational units. This paper presents the benefits of a comprehensive risk management framework which can be used to tie the different levels of risk management together into one comprehensive framework. These key elements may be used to develop a comprehensive risk management framework, which will bridge any gaps left by the individual risk management areas. This research paper starts with a brief introduction to risk management which clarifies the terminology used within the paper. From there, the concept of different levels of risk management is introduced and explained and then issues with current risk management frameworks are identified with case studies on some common frameworks. Next in the paper are the key elements of a new risk management framework, followed by the benefits of a new risk management framework. The paper concludes with examples of how the suggestions can be used and criticisms of the suggestions.

### **Sachedina, Nisha**

## ***Systematic method of achieving Sarbanes-Oxley (SOX) compliance by harmonizing Cobit, ITIL and ISO 27002/17799***

The Sarbanes-Oxley Act of 2002 (SOX) was passed in the United States in response to a number of major corporate and accounting scandals. The privacy act was enacted in many countries to protect the individual's right to privacy. Information has become a key asset in most organizations and the management is held accountable by law, to protect the information asset. The need to meet regulatory requirements in the areas of privacy and financial reporting has created a call for better corporate governance. This research paper investigates the co-existence of the frameworks, Control Objective for Information and Related Technology (COBIT) and Information Technology Infrastructure Library (ITIL), as an enabler for achieving SOX compliance requirements and how ISO 17799 standard can be used to identify and close security gaps.

## **Viegas, Edwina**

### ***Privacy Classification of Health Information in Alberta – Issues, Proposed Solution and Benefits***

The research demonstrates that by revising the existing privacy classification of health information in Alberta, marrying it with security classification of health information, and applying the corresponding security safeguards, privacy protection can be enhanced, and re-identification risks may be minimized. After a look at privacy classifications of health information in Canada, the United States of America, and the European Union, the paper recommends that a more granular classification of privacy could make Alberta's Health Information Act easier to administer. It goes on to propose a solution to issues with the current privacy classification of health information in Alberta. It recommends than an alignment with security classification, and corresponding safeguards, could have a positive impact on the bottom line.