Master's Project Proposal Plan

Evaluation of System Security using Security Patterns

Loy Abaine Kakuri Muhwezi

January 2007

1 Project Description

1.1 Overview

Security of information systems is increasingly becoming crucial in the twenty-first century as computing systems and network technologies evolve with new threats and risks. An information system in this project will mean a system whether automated or manual, that comprises people, machines, and/or methods organized to collect, process, transmit, and disseminate data that represent user information as defined by ATIS [1]. Both developed and developing countries are equally affected, as globalization becomes the order of the day. Stealing and modifying information, interruption of services, unauthorized access to systems and many other threats are increasing. Adequate security for sensitive information and information systems is becoming an important topic yet few systems are designed with comprehensive security in mind. Embedding security strategies in design and development phase is the only way businesses and organizations can avoid loosing information and incurring financial loses.

Given the size of current businesses and organizations, with many branches all over the place, they do not only employ many people of different levels but also interact with many other businesses and organizations in different locations. This result in more interaction with more open networks, which worsens the situation, and security threats, become a global concern. Safe guarding systems of any kind during design and development stage by use of security patterns [[2], [3], and [5]], have been proposed and are already being implemented by some system developers and implementers.

Security patterns were first proposed by Yonder and Barcalow [2] for the software community to address recurring security problems. Since then a lot has been published on security patterns and many of them have been written. A security pattern describes a recurring security problem that arises in specific contexts, and presents a well-proven generic solution for it [3]. The essence is to help system developers understand security and plan for it in the infancy of system development other than considering it as an after thought.

However, in developing countries connectivity to rural areas by use of Internet is still hard, but businesses and organizations operate their branches in such areas. This is because broadband availability is still limited, and global connectivity is only possible in few urban centres. All the same security issues need to be addressed in whichever network is being used.

In today's businesses and organizations both physical and logical access controls are required to restrict entrance or usage of not only the property of the organization but also its network. Access is the ability to use a system or its component (resource). Access control is the ability to allow or deny use of system resources by an individual or a process. It includes authentication, authorization and audit. Organizations currently have many employees both at their head and branch offices, who must interact with the organization's information system. More interaction causes more security problems to the system. Unless it is made clear who access what and how, security problems do increase.

With computer-based access controls, who or what accesses a specific system and by what means is specified. Techniques like Discretionary Access Control (DAC), Mandatory Access Control (MAC) and the most recent one Role Based Access Control (RBAC) have been prescribed to handle access control. Role based access control (RBAC) formalised by Ferraiolo *et al* [4], is based on the roles that individual users have as part of an organization. It was later described in form of a security pattern by Yonder [2] in 1997.

In this project we intend to evaluate security using security patterns, specifically RBAC pattern which is still a missing aspect in research. Our major problem is how does RBAC pattern provide security to a system? What are the benefits and limitations? Can one investigate the possibility of handling the limitations?

1.2 Scope of Work

Phase one of the project will involve two parts. First it will involve literature research on existing security patterns and specifically study RBAC. Secondly, a specific case study (the Management Information System (MIS) department of Bank of Uganda (BoU)) chosen from a developing country (Uganda) will be used. Physical observation, questionnaires and interviews with key people will be among the methods used to gather relevant information on infrastructure and organization of the department.

In phase Two, the data gathered will be analysed and a methodology to evaluate security using security patterns and RBAC in particular will be worked on. Other related case studies (from literature reviewed) in connection with the implementation of RBAC will also be used. Results of phase one and analyzed information will give us a basis of evaluating RBAC. If this requires use of models, then more literature will be studied as need arises. It is anticipated that this phase will see some chapters of thesis drafted.

The final phase (phase three) will involve presenting the findings and a proposed solution to MIS (BoU), Uganda. It will also involve writing the final version of the thesis report and presentation in The Netherlands.

All this is a tentative plan but changes might occur as the research goes on. However this will always be discussed and agreed on with the supervisor(s) depending on the information gathered in initial research at MIS of BoU.

1.3 Intended Results

- Thesis report describing the problem in detail, the methods used to solve it and the solution
- Description of possible approaches of implementing RBAC security mechanisms within MIS.
- Results of the whole evaluation

1.4 Anticipated benefits to MIS

It is anticipated that when RBAC security pattern is well implemented, high levels of security can be maintained as changing security policies and updating user profiles is done in an efficient manner. In addition through creation of roles and distributing administration to delegated administrators, RBAC can reduce the complexity of access control, which may exist in a large complex setup. Above all RBAC can reduce the cost of security administration in large networks.

Having given the background information, the rest of the sections are arranged as follows:

Section 2 gives the problem definition, Section 3 highlights the literature so far identified for use Section 4 describes the approaches and methods, and Section 5 gives tentative work plan.

2 Problem Statement

It is clear that security is a concern to every one. Organisations and businesses need to be interconnected but at the same time to have secure systems. Mechanisms in form of security patterns are put in place to safeguard information and information systems, but often such systems are not very secure and information is lost, manipulated or accessed illegally.

This research is focused around problem definition formulated as below:

How can security patterns be used to evaluate security in a system that uses private networks?

But to be able to define the problem properly; the research will further focus on a specific question:

How does Role Based Access Control (RBAC) pattern provide security to a system?

1. What is Access Control and what is RBAC?
2. How does RBAC differ from older approaches (Mandatory Access Control & Discretionary Access Control) and Access Control Lists?
3. How is RBAC implemented?
4. How does RBAC work?
5. What are the benefits and limitations of using RBAC?

3 Literature Review

List of literature and how is intended to be used

Security patterns: [2], [3], [5]

Role Based Access Control: [4], [6], [7], [8]

Others as need arises

4 Approaches and Methods

4.1 Objective and Priorities

The project should be done and completed in time with relevant results.

The final report should give details of the problem and various methods to its solution.

4.2 Method of work

The research is an individual work, which I intend to do alone and where others make contributions it will be mentioned in my thesis. Reviewing necessary literature and answering questions 1 and 2 of the problem definition, could be done anywhere, but in order to settle at once part of it will be done concurrently with other parts of research at the specified location of the case study in Section 1. Question 2 will involve studying existing models and to come up with a framework to compare the techniques.

In order to answer questions 3, 4, and 5, it is necessary to do a case study in a developing country. To get vital information and a clear overview of infrastructure and organization at BoU, it will necessitate being at the organization for my initial research. The gathered information from the case study will then be a basis of RBAC evaluation.

Acquiring basic knowledge of how security mechanism can improve system security is beneficial but using the acquired knowledge and existing case studies will be fitting to evaluate security in a less developed country with network settings which are rare in a developed world.

4.3 Quality and Risk Control

The following steps will guide in achieving quality work, good performance and timely delivery of the thesis:

- Frequent communication with Supervisor
- Weekly reviews to ensure consistent progress
- Systematic documentation of methods and approaches

4.4 Contacts

Tentatively the people involved (Student, Supervisor Radboud University, and Supervisor BoU) in this project can be contacted at:

Loy Abaine Kakuri Muhwezi	muhwezi_loy@yahoo.com loy.muhwezi@gmail.com
Dr. M.D (Martijn) Oostdijk	martijno@cs.ru.nl
Mr. Alfred Rutta	arutta@bou.or.ug

5 Tentative Work Plan

5.1 Fixed Plan

Start date: 2-1-2007

Finish date (Latest): 30-8-2007

As part of the research period it is intended that a paper will also be developed and written together with the supervisor (Dr. M.D (Martijn) Oostdijk) to be presented at 3rd Annual International Conference on Computing and ICT Research – SREC07, August 5-8, 2007, Makerere University, Kampala, Uganda.

5.2 Variable Plan (Tentative Schedule)

The actual time of the periods may change due to unavoidable circumstances but the research project at BoU will not exceed 6 months and the overall thesis project will not go beyond 30-08-2007.

Task	**Activity**	**Time Period (Place)**
Project Proposal and Plan	Problem to be researched and solved and what approaches to be taken	Up to 21-12-2006 (NL)
Abstract	Extended abstract for SREC07 written	To 02-01-2007 (NL)
Final Project Plan	Actual approaches established at BoU	to 15-01-2007 (UG)
Literature review and	Literature on security	to 15-02-2007

information gathering	patterns, MAC, DAC, and RBAC studied and familiarization at BoU.	(UG)
Information gathering and data collection at MIS of BoU	Questionnaires and other methods described used to collect data at BoU's MIS department.	to 31-03-2007 (UG)
Holiday (Supervisor)	Dr. M.D (Martijn) Oostdijk on holiday	15 to 30-04-2007
Final SREC07 Paper	Submitting final paper	30-05-2007 (UG)
Data analysis and developing solution	Analyzing data collected and writing some chapters	to 08-06-2007 (UG)
Initial report to MIS	Reporting findings and proposed solution to MIS of BoU	Date to be determined but not later than 08-06-2007 (UG)
Final thesis report	Writing last parts of the master's thesis	16-06-2007 to 15-07-2007 (NL)
Preparing Presentation	Final presentation will be held at Radboud University Nijmegen	Date to be determined (NL)
SREC07 Paper	Paper presentation	5 to 8-08-2007 (UG)

NL = Netherlands

UG = Uganda

6 References

[1] http://www.atis.org/tg2k/_information_system.html

[2] J. Yoder and J. Barcalow: Architectural Patterns for Enabling Application Security. The 4th Pattern Languages of Programming Conference. Washington University Technical Report 97-34, 1997.

[3] M. Schumacher, E. F. Buglioni, F. Buschmann & P. Sommerland: Security

Patterns. Integrating security and system engineering. John Wiley & Sons Ltd, England. 2005.

[4] D.F.Ferraiolo and D.R.Kuhn: Role Based Access Control. 15th National Computer Security Conference. 1992.

[5] C. Steel, R. Nagappan, & R. Lai: Core Security Patterns. Best Practices and Strategies for J2EE, Web Services, and Identity Management. Pearson Education, Inc. September 2005.

[6] D.F.Ferraiolo, J.F. Barkley and D.R.Kuhn: A Role-Based Access Control Model and Reference Implementation within a Corporate Intranet. ACM Transactions on Information and System Security, Vol.2, No.1, February 1999, pg 34-64.

[7] R. Sandhu, D. F.Ferraiolo, and D.R.Kuhn: The NIST Model for Role-Based Access Control: Towards a Unified Standard. RBAC 2000, Berlin, Germany.

[8] M.P.Gallaher, Ph.D., A.C.O'Connor, B.A., and B. Kropp, Ph.D.: The Economic Impact of Role-Based Access Control. Final Report submitted to G. Tassey, Ph.D. NIST, Acquisition and Assistance Division. RTI Project Number 07007.012, March 2002.