



DELHI TECHNOLOGICAL UNIVERSITY

DECLARATION

I hereby declare that the Report of the Major project-2 Work entitled “Role Based Access Control with SELinux” which is being submitted to the Delhi Technological University, in partial fulfillment of the requirements for the Sixth semester MAJOR PROJECT-2 course of the Master of Technology Degree in Software Technology in the Department of Computer Engineering, is a bonafide report of the study carried out by me. The material contained in this report has not been submitted to any University or Institution for the award of any degree.

Harpreet Singh

Department of Computer Engineering

Place: Delhi Technological University, Delhi.

Date:



DELHI TECHNOLOGICAL UNIVERSITY

CERTIFICATE

This is to certify that the project report entitled “Role Based Access Control with SELinux” is a bona fide record of work carried out by **Harpreet Singh (2K11/SWT/07)** under my guidance and supervision, during the academic session 2013-2014 in partial fulfillment of the requirement for the degree of Master of Technology in Software Technology from Delhi Technological University, Delhi.

To the best of my knowledge, the matter embodied in the thesis has not been submitted to any other University/Institute for the award of any Degree or Diploma.

Dr. (prof) Daya Gupta

Professor

Department of Computer Engineering

Delhi Technological University

Delhi

Ms. Divyashikha Sethia

Assistant Professor

Department of Computer Engineering

Delhi Technological University

Delhi



DELHI TECHNOLOGICAL UNIVERSITY

ACKNOWLEDGEMENT

With due regards, I hereby take this opportunity to acknowledge a lot of people who have supported me with their words and deeds in completion of my research work as part of this course of Master of Technology in Computer Science Engineering.

To start with I would like to thank the almighty for being with me in each and every step of my life. Next, I thank my parents and family for their encouragement and persistent support.

I would like to express my deepest sense of gratitude and indebtedness to my guides and motivators, **Dr. (Prof.) Daya Gupta**, Department of Computer Engineering Department, Delhi Technological University and **Ms. Divyashikha Sethia**, Associate Professor, Department of Computer Engineering, Delhi Technological University for their valuable guidance and support in all the phases from conceptualization to final completion of the project.

Last but not the least, I would like to thank all the people directly and indirectly involved in successfully completion of this project.

Harpreet Singh

Roll No. 2K11/SWT/07

Master of Technology (Software Technology)

Delhi Technological University

Bawana road, Delhi - 110042

TABLE OF CONTENTS

Declaration.....	i
Certificate.....	ii
Acknowledgement	iii
Table of Contents.....	iv - vii
List of Figures.....	viii
List of ScreenShots	viii
List of Tables	ix
Abstract.....	x
Chapter 1: Introduction.....	1
1.1: Context and Motivation	1
1.2: Role based access control in Healthcare information system.....	2
1.3: Report Outline.....	2
Chapter 2: Background	3
2.1 Introduction	3
2.2 Access Control	4
2.2.1 Authentication and Authorization	4
2.2.2 Access Control Models	5
2.2.2.1 Discretionary Access Control	6
2.2.2.2 Mandatory Access Control	7
2.3 Access Control Lists	8
2.4 Reference Monitor	10
2.5 Mandatory Access Control Models	11
2.5.1 Bell-LaPadula Model	11
2.5.2 Biba Model.....	13
2.5.3 Role-Based Access Control Model	14
2.5.4 Domain and Type Enforcement Model.....	16
2.6 Layers of Security	16

Role Based Access Control with SELinux

2.7 Operating System Mandatory Access Control	17
2.7.1 Security Enhanced Linux	18
2.8 Summary	20
Chapter 3: Introduction	21
3.1: Introduction.....	21
3.2: RBAC Concept of Role and Permission.....	22
3.3: Principles of RBAC	23
3.4: Applications	24
3.5: RBAC Standards.....	24
3.5.1 Core RBAC.....	25
3.5.2: Hierarchical RBAC.....	28
3.5.3: Static Separation of Duty Relations	31
3.5.4: Dynamic Separation of Duty Relations	32
3.6: Methodology to create an RBAC Package	33
Chapter 4: SELinux to Enforce Mandatory Access Control in Health Information Systems.....	34
4.1 Introduction	34
4.2 SELinux Architecture	35
4.2.1 Linux Security Module Framework	35
4.2.2 Flask Architecture	35
4.2.2.1 Terminology	39
4.2.2.2 Identity	39
4.2.2.3 Domains	41
4.2.2.4 Types	41
4.2.2.5 Roles	41
4.2.2.6 Security Context	41
4.2.2.7 Transition: Labeling	42
4.2.2.8 Policies	43
4.2.2.9 SELinux Policy Rules	43
4.2.2.10 Type and Role Declarations	43
4.2.2.11 File Contexts	44
4.2.2.12 User Roles	45

4.2.2.13 Access Vector Rules: allow	45
4.2.2.14 Role Allow Rules	46
4.2.2.15 Transition and Vector Rule Macros	46
4.2.2.16 SELinux Policy Configuration Files	47
4.2.2.17 Compiling SELinux Modules	47
4.2.2.18 Interface Files	47
4.2.2.19 Types Files	48
4.2.2.20 Module Files	48
4.2.2.21 Security Context Files	48
4.2.2.22 User Configuration: Roles	49
4.2.2.23 Policy Module Tools	50
4.2.2.24 Sample Files.....	50
4.3 Conclusion	54
Chapter 5: Hierarchal Role-Based Access Control and Type Enforcement for Health Information Systems	55
5.1 Introduction.....	55
5.2 SELinux Profiling	56
5.3 Healthcare Scenario	59
5.3.1 The HIS Applications.....	60
5.3.2 Working with Roles	61
5.3.3 Role Based Access Control and Type Enforcement.....	63
5.3.4 Creating and Implementing the Policy Module.....	70
5.3.5 Creating Users and Assigning Roles	73
5.3.6 A closer look at SELinux Profiles.....	74
5.4 Healthcare Attack Scenario	77
5.4.1 RBAC Context	77
5.5 Conclusion	83
Chapter 6: Conclusions	85
6.1 Research Findings.....	85
6.2 Future Work.....	90

References.....	91
Appendix A.....	I
Appendix B.....	XVII

LIST OF FIGURES

Figure 1. Traditional Access and RBAC	22
Figure 2. Relationship Flow	23
Figure 3. Core RBAC	25
Figure 4. Hierarchical RBAC.	29
Figure 5. Hierarchy in a Hospital.....	29
Figure 6. Hierarchy in a Corporate	30
Figure 7. General Role Hierarchy	30
Figure 8. Limited Role Hierarchy	31
Figure 9. Static Separation of Duty.....	32
Figure 10. Dynamic Separation of Duty Relations	33
Figure 11. Methodology to Create RBAC Package.....	33
Figure 12. SELinux LSM Module and the Flask Architecture.....	38
Figure 13. SELinux Profiles Assigning Process	57
Figure 14. Loadable Policy Modules Management Process	59
Figure 15. Role Hierarchy in HIS	63
Figure 16. SELinux Profiles hospital_sys and appointment applications for Pathologists	76

LIST OF SCREENSHOTS

Screenshot 1. Doctor checking patient medication records.....	81
Screenshot 2. Nurse trying to access application with Doctor role	82
Screenshot 3. AVC message logs showing denied access	83

LIST OF TABLES

Table 1. Access Control List.....	8
Table 2. Roles in ACLs.....	9
Table 3. Role-Permission assignment in ACLs.	9
Table 4. User-role Matrix	27
Table 5 Permission-role Matrix	27
Table 6 Access Control Table.....	28
Table 7. HIS Roles.....	62
Table 8. HIS Application Types	64
Table 9. HIS Application Roles, Domains and Types	68
Table 10. Linux Shell Types.....	70
Table 11. Security Attributes for the HIS Application Executable File.	78
Table 12. SELinux Profiles for doctors and pathologists.	80

ABSTRACT

In a typical healthcare information system, multiple users access data stored in different files related to patients. Healthcare organizations have to adhere to security regulations while storing sensitive data of patients and also providing access control to various users of the system, like doctor, administrators, nurses, pharmacists, pathologists etc.

To provide secure access control, application layer security is already provided in the system to restrict access control for various users to classified information in Hospital Information System (HIS). Discretionary Access Control (DAC) is the most commonly implemented access control model to restrict access to resources at the OS layer. But these measures, application layer security and DAC, becomes insufficient in case of virus/malware attacks.

This thesis investigates about providing Hierarchical Role based access control (RBAC) using SELinux to provide security using checks provided by SELinux at OS layer. SELinux provides Mandatory Access Control (MAC) mechanisms at the OS layer which can contain attack from compromised application and restrict access according to security policy implemented.

The main contribution of this research is to provide a RBAC using SELinux to a typical Hospital Information System (HIS). The roles and the hierarchy have been defined for users in a typical HIS and security policy has been developed around this hierarchy to provide security to classified information in HIS to different roles.

The feasibility of using SELinux profiles in HIS has been demonstrated through the creation of a prototype application, which was submitted to various attack scenarios. The prototype has also been subjected to testing during emergency scenarios, where changes to the security policies had to be made on the spot. Attack scenarios are based on vulnerabilities common at the application layer.

SELinux demonstrates that it can effectively contain attacks at the application layer and provide adequate flexibility during emergency situations.

Access control is decided on the role played by different users in the organization. It is similar to concept of groups in linux. It categorizes the groups of users and group of permissions as compared to user groups which define user sets