GENERIC SELINUX RULES & POLICIES FOR SECURE EXECUTION OF NETWORK SERVICES IN LINUX

Mario Roshane Ishara Fernando

158214U

Dissertation submitted in partial fulfillment of the requirement for the degree Master of Science in Computer Science

Department of Computer Science & Engineering

University of Moratuwa

November 2018

DECLARATION

I declare that this is my own work and this dissertation does not incorporate without acknowledgement any material previously submitted for degree or Diploma in any other University or institute of higher learning and to the best of my knowledge and belief it does not contain any material previously published or written by another person except where the acknowledgement is made in the text.

Also, I hereby grant to University of Moratuwa the non - exclusive right to reproduce and distribute my dissertation, in whole or in part in print, electronic or other medium. I retain the right to use this content in whole or part in future works.

Signature: .... Date: 16/11/2018

Name: M.R.I. Fernando

I certify that the declaration above by the candidate is true to the best of my knowledge and that this report is acceptable for evaluation for the Masters of Dissertation.

Signature of the Supervisor: .... Date: 16/11/2018

Name: Dr. Shantha Fernando

Signature of the Co-Supervisor: .... Date: ....

Name: Dr. Chandana Gamage

ABSTRACT

Usage of Network services and network stack-based applications on Linux systems are increasing rapidly, hackers around the world exploit security flaws there by executing sophisticated attacks on these services and compromising the entire system. Applying SELinux policies to a system which serves multiple network services has been a challenge due to policy conflicts. These policy conflicts are overridden by the security administrator there by applying SELinux rules to make the network services operational, however this might result in loop holes thereby information leakage from one or multiple services to another. This results in compromisal of not only the network service being attacked but other running services in the system which might lead to the entire trusted computing base being compromised. Deployment of SELinux Multi Level Security mandatory access control is an appropriate model to be applied over a system where we can segregate information flow from various security levels into the level of even categorized compartments. However, when running multiple network services over a single SELinux MLS enabled system, it is required to determine the security levels to be labelled over the subjects and the objects of the respective network services to overcome the ambiguity of the security levels in the information flow of a security lattice. Preserving both confidentiality and integrity of a system is a challenge and it is required to find the most secure way of information flow in a security lattice while achieving it using the existing SELinux MLS framework. This research focuses on a number of access control models, security models, lattice-based access control models and a wide range of SELinux security policy implementations. The goal of this research is to determine the security labels and security levels of the network services intended to run on a SELinux MLS enabled system while allowing information flow through the security lattice only if required.

Keywords: Security Enhanced Linux, Multi-Level Security, Bell Lapadula Model, Mandatory Access Control, Security Lattice, Type Enforcement, Sensitivities, Categories, Security Contexts

ACKNOWLEDGEMENT

I would like to express my special thanks of gratitude to my project supervisors, Dr. Shantha Fernando and Dr. Chandana Gamage for their patient guidance, enthusiastic encouragement and useful critique of my research work. Their willingness to give their time so generously have been very much appreciated. Especially mentioning the moral support and the continuous guidance by providing important feedback enabled me to complete my work successfully.

Also, I would like to thank Dr. Stephen Smalley from National Security Agency, USA and Mr. Dan Walsh from RedHat Incoperation, USA who supported me to carry out this research by providing valuable resources regarding the SELinux Multilevel Security domain. Finally, I would like to thank my spouse who supported and encouraged me throughout this project.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

BLP	Bell-Lapadula Model
DAC	Discretionary Access Control
GNU/GPL	GNU's NOT UNIX / General Public License
LSM	Linux Security Module
MAC	Mandatory Access Control
MLS	Multi Level Security
NSA	National Security Agency
RBAC	Role Based Access Control
SELinux	Security Enhanced Linux
TCB	Trusted Computing Base
TE	Type Enforcement