AFRL-IF-RS-TR-2003-22
Final Technical Report
February 2003

SECURITY MANAGEMENT FOR SE LINUX

George Washington University

Sponsored by
Defense Advanced Research Projects Agency
DARPA Order No. N624/00

AIR FORCE RESEARCH LABORATORY
INFORMATION DIRECTORATE
ROME RESEARCH SITE
ROME, NEW YORK

This report has been reviewed by the Air Force Research Laboratory, Information Directorate, Public Affairs Office (IFOIPA) and is releasable to the National Technical Information Service (NTIS). At NTIS it will be releasable to the general public, including foreign nations.

AFRL-IF-RS-TR-2003-22 has been reviewed and is approved for publication.

APPROVED:

JERRY F. LIPA
Project Engineer

FOR THE DIRECTOR:

JAMES W. CUSACK, Chief
Information Systems Division
Information Directorate

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	FEBRUARY 2003	Final May 02 – Dec 02

4. TITLE AND SUBTITLE
SECURITY MANAGEMENT FOR SE LINUX

5. FUNDING NUMBERS
C - F30602-02-1-0113
PE - 62301E
PR - N624
TA - 00
WU - 01

6. AUTHOR(S)
Sead Muftic

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
George Washington University
2121 I Street NW
Washington DC 20052

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Defense Advanced Research Projects Agency
3701 North Fairfax Drive
Arlington Virginia

AFRL/IFSA
525 Brooks Road
Rome New York 13441-4505

10. SPONSORING / MONITORING AGENCY REPORT NUMBER
AFRL-IF-RS-TR-2003-22

11. SUPPLEMENTARY NOTES

AFRL Project Engineer: Jerry F. Lipa/IFSA/(315) 330-4494/ Jerry.Lipa@rl.af.mil

12a. DISTRIBUTION / AVAILABILITY STATEMENT
APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

12b. DISTRIBUTION CODE

13. ABSTRACT ***(Maximum 200 Words)***
This effort designed, specified, and implemented a security management system for SE Linux that included an automatic, user-friendly installation, customization of default installation parameters, and adjustment of default access control parameters.

14. SUBJECT TERMS
Linux, Security Management

15. NUMBER OF PAGES
7

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UL

TABLE OF CONTENTS

Security Management for SE Linux

(Final Project Report)

1 Project Schedule

Project "Security Management for SE Linux" was scheduled to start on May 1st, 2002 and finish on August 31st, 2002. The project was completed fully within its schedule, i.e. it started on May 1st, 2002, technical R&D activities were completed by July 31st, 2002 and documentation and the final project report were delivered before August 31st, 2002. In addition, since the budget was not completely exhausted, the project received a no cost extension until Dec 31st, 2002

This document represents the final project report and was created on November 7th, 2002.

2 Tasks and Deliverables

Detail plan of activities, tasks, and deliverables in the project included the following:

Task 1: Compilation of SE Linux and its integration with the current Linux kernel;
Task 2: Analysis, design and creation of kernel options and modules for different target platforms;
Task 3: Design and implementation of SE Linux Installer;
Task 4: Design and implementation of policy administration tool using GUI;
Task 5: Testing of the overall system on several target platforms;
Task 6: SE Linux security administration manual;
Task 7: Cooperation with other developers and potential users.

3 Final Project Report

All activities and deliverables in the project have been completed. The results are as follows:

3.1 Task 1: Compilation of SE Linux and its integration with the current Linux kernel

After downloading the SE Linux package, the team encountered minor inconsistencies and compilation problems. They were all corrected and SE Linux has been successfully compiled. Deliverable from this task is ZIP–ed version of SE Linux source files which loads and executes without any errors.

3.2 Task 2: Analysis, design and creation of kernel options and modules for different target platforms

Within this task the project team analyzed criteria for classification of target platforms significant for inclusion or exclusion of different modules in the Linux kernel. The type of processor architecture and support for SCSI devices were selected. Based on these, eight kernel options have been created by alternative compilation steps with the following characteristics:

Options	Type of Processor	SCSI Support
Option 1	i386	No
Option 2	i486	No
Option 3	Pentium 3	No
Option 4	Pentium 4	No
Option 5	i386	Yes
Option 6	i486	Yes
Option 7	Pentium 3	Yes
Option 8	Pentium 4	Yes

All options are created for Linux kernel version 2.4.18, and are named SILK.2.4.18.1, SILK.2.4.18.2, etc. ("SILK" is the code name for the SELinux created by the CSPRI – **S**ecurity **I**ntegrated with **L**inux **K**ernel). Eight kernel options are included in the distribution CD.

3.3 Task 3: Design and implementation of SELinux Installer

Once the eight kernel options were created and SELinux was compiled, the next step was to create the automated `SILK Installer`. This program:

- loads from the distribution CD,
- examines the target machine for characteristics of the installation options given above,
- copies SELinux and the corresponding kernel option from the CD, and
- installs the kernel and SELinux on the target machine.

During installation the original Linux modules, which are replaced the security–extended modules of SELinux, are archived so that they can be later un–installed by SILK Uninstaller, which was also implemented as part of this effort.

3.4 Task 4: Design and implementation of policy administration tool using GUI

This task designed and implemented a simple GUI–based policy administration tool. After installation, SELinux must be configured, referred to in the original (www.nsa.gov/selinux) version as command–line editing of several policy configuration files. In addition, the administrator must also edit the Linux configuration files. This is not a simple task, especially for a large number of users, resources, and processes and, if not performed correctly, may introduce inconsistencies in the SELinux operations. The goal of this task was to design and implement a simple, fully functional, integrated and easy–to–use policy administration tool, which will assist security administrators to specify individual users, resources and their permissions by a simple click of a button.

This task has been completed, all modules have been tested and are fully functional. The use of the policy GUI is described in detail in the SILK Manual. Through this interface it is also possible to create new security policy, to examine the policy creation log and SELinux system operation log.

3.5 Task 5: Testing of the overall system on several target platforms

When Task 4 was completed and the policy administration tool was created, the project team tested the overall SELinux system. Various default features of the security policy were examined, especially those denying access to certain resources. Some results are included in the "*SILK Administration Manual*", but this area requires further investigation, which is beyond the scope of this project.

3.6 Task 6: SE Linux security administration manual

This task has produced the complete and fully professional "SILK Administration" manual which explains in detail the installation, customization, and administration of SELinux. The manual also includes various examples of policies and SELinux actions.

3.7 Task 7: Cooperation with other developers and potential users

Throughout the lifetime of the project, in addition to R&D activities, the project team has established many contacts and cooperative activities with other developers and potential users of SELinux.

In the area of *development*, the team had contacts with NAI Labs, Mark Westerman and the Finish company SOT.

In the area of *potential developers*, the team met with several local companies interested in using SE Linux: Adaptech Systems (Rama Kant and David Niemi), Free Standards Group (Scott McNeil), Secure Software Solutions (John Viega), Intel, etc.

The team had several meeting and made presentations to many *potential users* (DOD/DISA, Office of the CIO/Navy, The World Bank, etc.).

4 Conclusions, Results and Benefits

In conclusion, all planned activities and deliveries have been completed. The project has created and delivered all planned results. The team has also created an initiative for further R&D cooperation with Universities, industry and Government.

The final result is a simple, easy–to–install and easy–to–use version of SELinux, with its full functionality and benefits, and with the full documentation for its installation, administration and use.

The research team has already created a proposal for the next short–term follow up project and a strategic, three–year plan for design and implementation of a comprehensive network security system based on SE Linux.

5 Project Team

5.1 *Dr. Sead Muftic*, CPI/GWU, PI
5.2 *Tony Stanco*, CPI/GWU, Senior Policy Analyst
5.3 *Martin Dean*, SAIC, GWU doctoral student
5.4 *Emre Saglam*, The World Bank, network administration
5.5 *Michael Ngumba*, CPI/GWU, research assistant
5.6 *Frankiln Hum*, CPI/GWU, research scientist
5.7 *Donald Tomczak,* CS/GWU, doctoral student
5.8 *Juan Bocanegra,* CPI/GWU, research assistant