БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Факультет прикладной математики и информатики

Кафедра компьютерных технологий и систем

Аннотация к дипломной работе

«Разработка модуля ядра с криптографической функцией и реализация интерфейса взаимодействия с модулем в операционной системе Linux»

Кульгавый Иван Сергеевич

Научный руководитель – доцент
кафедры компьютерных технологий и систем ФПМИ
Василевский К. В.

Минск, 2025

АННОТАЦИЯ

Дипломная работа, 56 страниц, 1 приложение, 15 источников

Ключевые слова: ОПЕРАЦИОННАЯ СИСТЕМА, LINUX, МОДУЛЬ ЯДРА, КРИПТОГРАФИЧЕСКАЯ ФУНКЦИЯ, ВСТРАИВАНИЕ В ЯДРО, ШИФРОВАНИЕ.

Объект исследования – процесс статического встраивания модулей в ядро LINUX.

Предмет исследования – исходный код ядра Linux, связанный с загрузкой и инициализацией статических модулей, а также механизмы работы криптографических функций в пространстве ядра.

Цель исследования – разработка и оптимизация статического модуля ядра Linux, реализующего криптографическую функцию шифрования, с оценкой его производительности в сравнении с пользовательскими аналогами.

Методы исследования – анализ исходного кода ядра Linux, разработка и компиляция статических модулей, тестирование на различных конфигурациях ядра.

Полученные результаты и их новизна: успешно реализован модуль ядра Linux, содержащий криптографическую функцию шифрования, проведён сравнительный анализ скорости работы одинаковых реализация алгоритма шифрования в пользовательском пространстве и в ядре, доказана повышенная эффективность алгоритма, работающего в пространстве ядра.

Достоверность материалов и результатов дипломной работы: достоверность материалов и результатов дипломной работы: использованные материалы и результаты дипломной работы являются достоверными. Работа выполнена самостоятельно.

Область возможного практического применения – защита данных в операционных системах, повышение производительности криптографических операций, использование в системах информационной безопасности и встраиваемых решениях на базе Linux.

АНАТАЦЫЯ

Дыпломная праца, 56 старонак, 1 дадатак, 15 крыніц

Ключавыя словы: АПЕРАЦЫЙНАЯ СІСТЭМА, LINUX, МОДУЛЬ ЯДРА, КРЫПТАГРАФІЧНАЯ ФУНКЦЫЯ, УСТАЎКА Ў ЯДРО, ШЫФРАВАННЕ.

Аб'ект даследавання – працэс статычнай устаўкі модуляў у ядро LINUX.

Прадмет даследавання – зыходны код ядра Linux, звязаны з загрузкай і ініцыялізацыяй статычных модуляў, а таксама механізмы працы крыптаграфічных функцый у прасторы ядра.

Мэта даследавання – распрацоўка і аптымізацыя статычнага модуля ядра Linux, які рэалізуе крыптаграфічную функцыю шыфравання, з ацэнкай яго прадукцыйнасці ў параўнанні з карыстацкімі аналагамі.

Метады даследавання – аналіз зыходнага кода ядра Linux, распрацоўка і кампіляцыя статычных модуляў, тэставанне на розных канфігурацыях ядра.

Атрыманыя вынікі і іх навізна: паспяхова рэалізаваны модуль ядра Linux з крыптаграфічнай функцыяй шыфравання, праведзены параўнальны аналіз хуткасці работы алгарытма ў карыстальніцкай прасторы і ў ядры, даказана павышаная эфектыўнасць алгарытма, які працуе ў прасторы ядра.

Дакладнасць матэрыялаў і вынікаў дыпломнай працы: дакладнасць матэрыялаў і вынікаў дыпломнай работы: выкарыстаныя матэрыялы і вынікі дыпломнай работы з'яўляюцца дакладнымі. Праца выканана самастойна.

Вобласць магчымага практычнага прымянення – абарона дадзеных у аперацыйных сістэмах, павышэнне прадукцыйнасці крыптаграфічных аперацый, выкарыстанне ў сістэмах інфармацыйнай бяспекі і ўбудавальных рашэннях на базе Linux.

ANNOTATION

Diploma work, 56 pages, 1 appendix, 15 references

Keywords: OPERATING SYSTEM, LINUX, KERNEL MODULE, CRYPTOGRAPHIC FUNCTION, KERNEL INTEGRATION, ENCRYPTION.

The object of the research – the process of statically embedding modules into the Linux kernel.

The subject of the research – Linux kernel source code related to loading and initializing static modules, as well as mechanisms for operating cryptographic functions in kernel space.

The aim of the research – analysis of Linux kernel source code, development and compilation of static modules, testing on various kernel configurations.

Research methods – analysis of the Linux kernel source code, development and compilation of static kernel modules, testing on various kernel configurations.

The results of the work and their novelty: successful implementation of a Linux kernel module containing an encryption function, comparative analysis of encryption algorithm performance in user space vs. kernel space, demonstrated higher efficiency of the kernel-space implementation.

Authenticity of the materials and results of the diploma work: reliability of materials and results of the thesis: the materials used and the results of the thesis are reliable. The work was done independently.

Recommendations on the usage – data protection in operating systems, increasing the performance of cryptographic operations, use in information security systems and embedded solutions based on Linux.