https://lms.hse.ru/?apview&h_id=FE746748-1965-4346-81E6-52925EA9B121

Name:	Чудников Александр Александрович
Academic supervisor:	Нестеренко Алексей, профессор, доцент
Faculty:	Московский институт электроники и математики им. А.Н. Тихонова
Department/Group:	СКБ201
Level of education:	Специалитет
Degree programme:	Компьютерная безопасность
E-mail:	sasha.chudnikov@mail.ru
Contact phone number:	+7(909)953-57-67
Title (topic) in Russian:	Исследование реализации виртуальных криптографических сетевых интерфейсов в ядре OS Linux
Title (topic) in English:	Research on the Implementation of Virtual Cryptographic Network Interfaces in the Linux Kernel
Language:	Russian
Percent of borrowed content:	0
Publication date (time and date):	08-01-2026 20:42:57

Abstract:
Тема: Исследование реализации виртуальных криптографических сетевых интерфейсов в ядре ОС Linux.
Цель работы: Целью работы является исследование механизмов ядра семей ства операционной системы Linux с целью последующей реализации вир туальных сетевых интерфейсов на базе криптографических протоколов, опи санных в государственных стандартах (ГОСТ).
Поставленные задачи:
• исследование методов реализации виртуальных сетевых интерфейсов в ядре Linux;
• анализ криптографической подсистемы ядра «Crypto API» на возмож ность встраивания криптографических протоколов, описанных в ГОСТ;
• изучение существующих виртуальных сетевых интерфейсов;
• выбор оптимального набора криптографических протоколов;
• разработка и тестирование прототипа виртуального криптоинтерфейса.
Полученные результаты: В ходе выполнения работы было принято решение об использовании WireGuard в качестве основы для встраивания криптогра фических протоколов, описанных в ГОСТ. Был успешно разработан набор базовых криптографических примитивов в виде загружаемых модулей ядра (LKM) с использованием Crypto API. На базе архитектуры WireGuard разра ботан модуль WireGost, использующий отечественные криптографические алгоритмы.
Тестирование показало, что WireGost способен работать на скоростях вплоть до 900 Мбит/с. Это подтверждает преимущество реализации в ядре перед ре шениями в пространстве пользователя, тем не менее уступает оригинальному

WireGuard. Наиболее медленной частью системы стал блочный шифр «Куз нечик», который, по сравнению с «ChaCha20», используемым в оригинальном протоколе, является гораздо более дорогим с точки зрения вычислительной сложности.
Предложенные рекомендации: Для повышения производительности разра ботанного решения и приближения его показателей к скорости физическо го канала рекомендуется пересмотреть методы реализации блочного шиф ра «Кузнечик» в виде загружаемых модулей ядра, а также обеспечить более эффективную поддержку базовых математических операций используемых в ГОСТ.

Abstract (English):
Topic: Research on the implementation of virtual cryptographic network interfaces in the Linux OS kernel.
Purpose: The purpose of the work is to study the mechanisms of the Linux operat ing system family kernel with the aim of the subsequent implementation of virtual network interfaces based on cryptographic protocols described in state standards (GOST).
Tasks:
• research of methods for implementing virtual network interfaces in the Linux kernel;
• analysis of the kernel cryptographic subsystem "Crypto API" regarding the possibility of embedding cryptographic protocols described in GOST;
• study of existing virtual network interfaces;
• selection of an optimal set of cryptographic protocols;
• development and testing of a virtual cryptointerface prototype.
Results: While carrying out the research the author decided to use WireGuard as a basis for embedding cryptographic protocols described in GOST. A set of basic cryptographic primitives was successfully developed in the form of Loadable Kernel Modules (LKM) using the Crypto API. Based on the WireGuard architecture, the WireGost module was developed using domestic cryptographic algorithms.
Testing showed that WireGost is capable of operating at speeds up to 900 Mbps. This confirms the advantage of inkernel implementation over userspace solutions; nevertheless, it yields to the original WireGuard. The slowest part of the system proved to be the "Kuznyechik" block cipher, which, compared to "ChaCha20" used in the original protocol, is much more expensive in terms of computational com plexity.
Recommendations: To improve the performance of the developed solution and bring its metrics closer to the physical link speed, it is recommended to revise the implementation methods of the "Kuznyechik" block cipher in the form of loadable kernel modules, as well as to ensure more efficient support for basic mathematical operations used in GOST.

Hereby I declare that this Bachelor's/Master's thesis has been composed solely by myself, and it:

1. does not reproduce any of my own previous works without due reference thereto provided;
2. does not reproduce the work created by other authors without reference to the academic or research literature, articles, websites, completed assignments or notes of other students;
3. has not been previously submitted for a higher degree;
4. contains properly used quotations and references;
5. contains a complete bibliography of references and sources used for preparing this thesis.

I am aware that violation of quotation and referencing rules is considered cheating or misrepresentation attempt and is therefore qualified as a violation of HSE Internal Regulations.

I ~~hereby grant HSE~~ / refuse to grant HSE (select as applicable)

(specify the reason for refusing the publication right)

the publication right to my Bachelor's/Master's thesis in order to reproduce and publish it in full (make it universally available) free of charge, indicating my authorship, date of producing this work and information about my academic supervisor, on HSE corporate website (portal) - www.hse.ru, so that the full version of my thesis may be accessed by any user of this website, from any place, and at any desired time.

Date: 12-01-2026

Signature: