МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Факультет прикладной математики и информатики
Кафедра математического моделирования и анализа данных

Аннотация к дипломной работе

АНАЛИЗ БЕЗОПАСНОСТИ СПЕЦИФИКАЦИИ LUKS

ЛАТЫШЁНОК АНТОН ОЛЕГОВИЧ

Научный руководитель:
Старший научный сотрудник НИЛ
математических методов защиты информации
Гайдук Антон Николаевич

МИНСК, 2022

РЕФЕРАТ

Дипломная работа: 31 страница, 2 главы, 1 рисунок, 7 таблиц, 1 приложение, 31 использованных источников.

Ключевые слова: ДИСКОВОЕ ШИФРОВАНИЕ, АНАЛИЗ БЕЗОПАСНОСТИ.

Объект исследования: дисковое шифрование.

Цель работы: исследование безопасности спецификации LUKS.

Методы исследования: а) теоретическое изучение источников, посвящённых управлению ключевой системы, программному обеспечению для шифрования дисков и анализу безопасности спецификации LUKS б) практическое определение параметров, влияющих на безопасность спецификации LUKS.

В результате работы получена оценка минимальной длины пароля в зависимости от мощности используемого алфавита для обеспечения стойкости спецификации LUKS к атаке полного перебора в течении одного календарного года.

Область применения: использование спецификации LUKS.

РЭФЕРАТ

Дыпломная праца: 31 старонкі, 2 раздзелы, 1 малюнак, 7 табліц, 1 дадатак, 31 выкарыстаных крыніцы.

Ключавыя словы: ДЫСКАВАЕ ШЫФРАВАННЕ, АНАЛІЗ БЯСПЕКІ.

Аб'ект даследавання: дыскавае шыфраванне.

Мэта працы: даследаванне бяспекі спецыфікацыі LUKS.

Метады даследавання: а) тэарэтычнае вывучэнне крыніц, прысвечаных кіраванню ключавой сістэмы, праграмнаму забеспячэнню для шыфравання дыскаў і аналізу бяспекі спецыфікацыі LUKS б) практычнае вызначэнне параметраў, якія ўплываюць на бяспеку спецыфікацыі LUKS.

У выніку работы атрыманы крытэрыі неабходныя для стойкасці пароля на працягу аднаго года.

Вобласць прымянення: выкарыстанне спецыфікацыі LUKS.

ABSTRACT

Diploma thesis: 31 pages, 2 chapters, 1 figure, 7 tables, 1 attachment, 31 sources.

Keywords: DISK ENCRYPTION, SECURITY ANALYSIS.

Object of study: disk encryption.

Purpose of work: to investigate the security of the LUKS specification.

Research methods: a) theoretical study of sources, devoted to key system management, software for disk encryption and analysis of LUKS specification security; b) practical determination of parameters, affecting LUKS specification security.

The result is the criteria required for password persistence for one year.

Field of Application: use of the LUKS specification.

Введение

Мобильные устройства, ноутбуки, USB-накопители используются повсеместно и хранят большое количество информации. Если такие устройства будут утеряны или украдены, то риск несанкционированного раскрытия на них информации является очень высоким.

Возможным решением упомянутой проблемы является шифрование всего жесткого диска (Full Disk Encryption, FDE), которое работает путем шифрования каждого бита данных “на лету” хранящихся на устройстве. FDE направлено на обеспечение конфиденциальности данных, даже в том случае, когда зашифрованное устройство утеряно. Без ключа шифрования, данные, хранящиеся на диске, остаются недоступными для атакующих.

Одной из основных проблем, стоящих перед FDE, является управление паролями. Ключ полного шифрования тома, используемый для шифрования всего диска, находится на самом диске. При получении атакующим носителя с защищенной информацией, сложность ее раскрытия не превышает сложность раскрытия пароля пользователя путем полного перебора.

Существуют различные программные реализации для шифрования дисков, которые предоставляют обширный набор функций безопасности. Одной из программных реализаций является программное обеспечение для шифрования диска LUKS (Linux Unified Key Setup).

В основе данной работы лежит задача анализа безопасности спецификации LUKS, которая широко используется в различных дистрибутивах семейства Unix.