УДК 004.056

СОПОСТАВЛЕНИЕ ПОПУЛЯРНОГО СОФТА ДЛЯ ОРГАНИЗАЦИИ ЗАШИФРОВАННЫХ КРИПТОКОНТЕЙНЕРОВ

Калько А.И., аспирант

Барановичский государственный университет

г.Барановичи, Республика Беларусь

Бобов М.Н. – док. тех. наук, профессор

Аннотация. В данной статье рассмотрено сравнение криптоконтейнеров TrueCrypt и VeraCrypt. Требовались достаточно надежные, но при этом легкодоступные криптографические алгоритмы. Долгое время востребованная в большей степени в военной среде, теперь криптография широко используется в дипломатической, коммерческой, банковской, государственной и иных сферах.

Ключевые слова: криптоконтейнеры, TrueCrypt, VeraCrypt, шифрование

Введение. На сегодняшний день тема конфиденциальности и защиты данных является наиболее актуальной и широко обсуждаемой. Одним из способов хранения наиболее ценной информации является использование криптоконтейнеров (от английского Crypt — шифровать). Сейчас на информационном пространстве существует достаточно большое множество программного обеспечения на различные платформы для создания зашифрованных контейнеров. Наиболее известными среди них являются TrueCrypt, VeraCrypt и Bitlocker. Среди менее известных аналогов вышеперечисленных можно выделить AxCrypt, DiskCryptor, FreeOTFE, Cryptic Disk. В данной статье будет произведено объективное сравнение TrueCrypt и VeraCrypt, описаны преимущества и недостатки каждого программного обеспечения.

Основная часть. Прежде чем начать сравнение, познакомимся с довольно интересной и загадочной историей TrueCrypt.

Первая версия была выпущена в 2004 году, и в то время TruCrypt была единственной программой шифрования сценариев Quick Go с открытым исходным кодом. С 2004 по 2014 год TruCrypt регуля рно обновлялся. Некоторые функции были исключены. Например, была удалена поддержка гибких дисков и некоторых протоколов шифрования. Поэтому в последней и седьмой версиях TrueCrypt б ыли удалены криптографические протоколы, использующие 64-битный (Тройной DES, Blowfish, CAST5).

За десять лет проект TrueCrypt был разработан и преобразован в надежную систему защиты данн ых. Все это время имена разработчиков программы держались в секрете, что привело к появлению ряда слухов об участии частных сервисов в разработке приложения. Одни говорят, что программа была разработана ФБР, другие говорят, что если бы не ФБР, в программе обязательно были бы ф ичи и баги.

Популярность TrueCrypt росла до беспрецедентного события весной 2014 года. Проект TrueCrypt закрылся 28 мая 2014 года. Точные причины закрытия проекта пока не раскрываются. Сами разработчики заявили на официальном сайте, что использование TrueCrypt небезопасно, они рекомендуют перейти на BitLocker, над которым всегда высмеивают.

Есть 4 версии случившегося. Первая гласит, что разработчикам угрожали спецслужбы. Во-вторых, они были склонны работать на Microsoft, как объясняется в объявлении BitLocker. В-третьих, они устали продвигать l Поддерживать проект, который не приносит денег. В-четвертых, они обнаружили потенциальную уязвимость системы безопасности в продукте, которую не смогли устранить.

Интернет-сообщество вступило в дебаты по поводу безопасности TrueCrypt, и в начале апреля 2015 года был завершен независимый аудит TrueCrypt, на который было пожертвовано более 60 000 долларов США. Он не выявил никаких дыр в безопасности или серьезных недостатков в архитектуре приложения и продемонстрировал, что TrueCrypt - это хорошо разработанная программа шифрования.

В 2013 году французский разработчик Мунир Идрасси летом 2013 года представил миру проект IraCrypt - самый популярный форк TrueCrypt на сегодняшний день. Форк (от англ. Fork - форк, форк) или форк - использует кодовую базу программного проекта как начало другого проекта, при этом основной проект продолжает или прекращает свое существование [1]. Разветвленный или разветвленный проект может поддерживать контент и делиться с ним основным проектом, либо он может приобретать совершенно другие функции, не имея ничего общего с исходным проектом. Основная идея заключалась в создании более безопасного решения TrueCrypt.

Особенности TrackCrypt и отличия от TrueCrypt [2]:

1. TrueCrypt выполнил недостаточное количество итераций для PBKDF2 (стандарт генерации паролей для ключа шифрования), количество дубликатов системного раздела в VeraCrypt увеличилось с 1000 до 327 661, а для других разделов и держателей файлов с 2000 до 655 331, т. е. ключ сопротивления значительно увеличился.

2. IraCrypt исправил ошибки, улучшил загрузчик и позволил использовать алгоритм SHA-256 в качестве хэш-функции при шифровании системного раздела жесткого диска, в то время как TrueCrypt использовал менее надежный алгоритм RIPEMD-160.

3. Драйверы VeraCrypt имеют цифровую подпись Microsoft, которая необходима для правильной установки в Windows 10.

4. Версии 1.18 и более ранние позволяют переводить компьютеры с Windows с использованием UEFI вместо BIOS и устранять риски, связанные с отображением скрытых разделов.

5. Начиная с версии 1.0f, IraCrypt поддерживает множество разделов и контейнеров, включенных в TrueCrypt, а также возможность конвертировать скрытые индексы TrueCrypt и недисковые разделы в форматы IraCrypt.

6. Исправлено множество программных ошибок: утечка памяти, перегрузка из-за ошибок и загрузка dll.

7. Был проведен полный анализ и рефакторинг кода.

8. Доступны версии для MACOS и Linux.

Сравнение VeraCrypt и TrueCrypt:

Скорость шифрования и дешифрования криптоконтейнеров. Тесты проводились на ноутбуке с процессором Intel Core i3-8600(2.0GHz, 3MB L3 Cache), 16GB Ram и 128GB SSD с операционной системой Windows 10 Профессиональная Service Pack 3. На рисунках 1 и 2 представлены результаты тестов скорости алгоритмов шифрования.

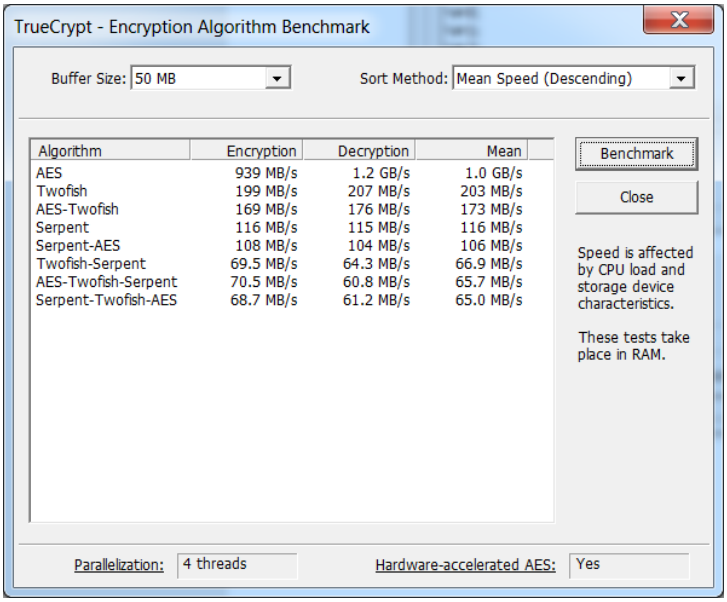

Рисунок 1 – Тест скорости алгоритмов шифрования TrueCrypt

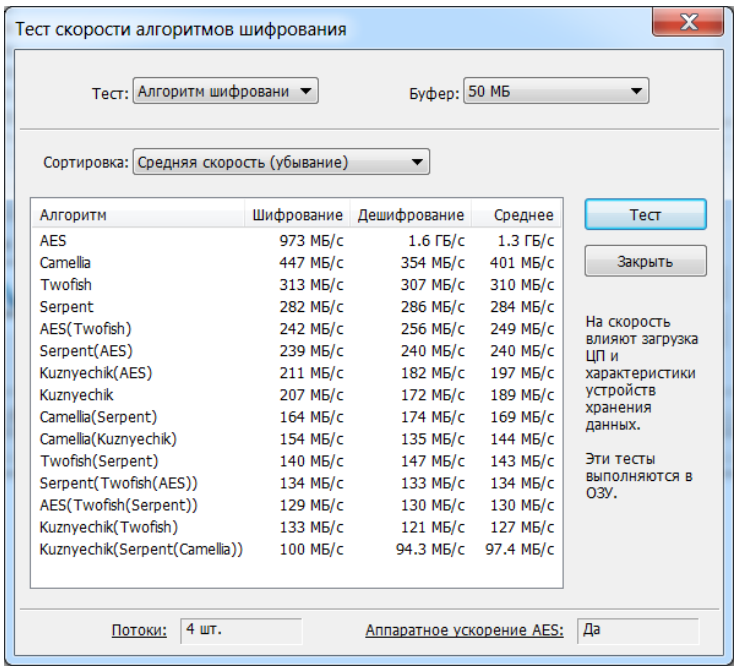

Рисунок 2 – Тест скорости алгоритмов шифрования VeraCrypt

Как можно видеть из результатов тестов, большинство алгоритмов работают быстрее в VeraCrypt. Также можно отметить и более широкий набор алгоритмов в VeraCrypt, чем в TrueCrypt.

Уязвимости. 13 марта 2015 года на сайте Open Crypto Audit Project был опубликован финальный отчет о проведении аудита TrueCrypt. Результаты отображены на рисунке 3.

Application Summary	
Application Name	TrueCrypt
Application Version	7.1a
Application Type	Disk encryption software
Platform	Windows, C / C++

Engagement Summary	
Engineers Engaged	Three (3)
Engagement Type	Cryptographic Review
Testing Methodology	Source Code Review

Vulnerability Summary	
Total High severity issues	2
Total Medium severity issues	0
Total Low severity issues	1
Total Undetermined severity issues	1
Total vulnerabilities identified:	4

See section 3.1 on page 10 for descriptions of these classifications.

Category Breakdown:	
Access Controls	0
Auditing and Logging	0
Authentication	0
Configuration	0
Cryptography	4
Data Exposure	0
Data Validation	0
Denial of Service	0
Error Reporting	0
Patching	0
Session Management	0
Timing	0

Рисунок 3 – Результаты аудита TrueCrypt

В результате было выявлено 4 уязвимости, связаных с математической защитой данных: 2 уязвимости тяжелой сложности, 1 уязвимость средней сложности и 1 незначительная уязвимость.

В сентябре 2016 года команда Quarkslab провела аудит VeraCrypt, в ходе которого было выявлено 36 весовых коэффициентов, из которых 8 были оценены как критические, 3 - как посредники и 15 - как малые веса. Большинство проблем затрагивает сторонние библиотеки сжатия с загрузчиком VeraCrypt UEFI [3]. Наиболее важным фактором риска является загрузчик UEFI, который позволяет восстановить содержимое загрузочного пароля. Разработчики VeraCrypt адаптировали большинство проблем, выявленных при проверке в VeraCrypt 1.19.

Из вышеперечисленных результатов следует, что уровень команды разработчиков TrueCrypt намного выше, нежели VeraCrypt.

Устойчивость к брутфорсу. Благодаря передовому методу генерации ключей VeraCrypt в 10–300 раз более устойчив к атакам с применением насилия.

Быстрая установка контейнеров шифрования. Когда пользователь указывает правильный пароль в TrueCrypt, время ожидания перед доступом к зашифрованным данным на современном компьютере составляет одну десятую секунды. С iracrypt вам придется подождать еще немного [4].

Поддержка разработчиков. TrueCript больше не поддерживается разработчиками, используемые решения устаревают каждый день, а потенциальные уязвимости безопасности не исправляются. Это определенно плюс для VeraCript, который активно поддерживается и развивается.

Заключение. Проанализировав оба инструмента для создания криптоконтейнеров, можно отметить, что каждый имеет как свои преимущеста, так и свои недостатки. Однозначно определить победителя затруднительно. По этой причине некоторые специалисты по информационной

безопасности рекомендуют использовать оба инструмента. К примеру, создание криптоконтейнера TrueCrypt, в него положить криптоконтейнер VeraCrypt, а уже в нем размещать данные. Такая связка в разы надежнее каждой из программ в отдельности.

Список использованных источников:

1. The VeraCrypt Audit Results. URL: https://ostif.org/the-veracrypt-audit-results/ (дата обращения: 13.03.2022)
2. Balducci, A. Open Crypto Audit Project TrueCrypt: Cryptographic Review. NCC Group, Inc, 2015. – 20 с.
3. Сандруцкий Д. И., Колдушко С. Д., Калько А. И. Применение криптографических систем при создании мессенджера //Студенческий. – 2017. – №. 16. – С. 14-16.
4. Сандруцкий, Д. И. Криптографические сервисы Java / Д. И. Сандруцкий, С. Д. Колдушко, А. И. Калько // Содружество наук. Барановичи-2017 : материалы XIII Междунар. науч.-практ. конф. молодых исследователей, Барановичи, 18 мая 2017 г. : в 3 ч. / М-во образования Респ. Беларусь, Барановичский гос. ун-т ; редкол.: В. В. Климук (гл. ред.) [и др.]. – Барановичи : БарГУ, 2017. – Ч. 2. – С. 130–133.

UDC 004.056

MAPPING OF POPULAR SOFTWARE FOR ORGANIZATION OF ENCRYPTED CRYPTOCONTAINERS

A.I. Kalko, PhD student

Baranavichy State University

Baranovichi, Republic of Belarus

M.N. Bobov - doc. those. sciences, professor

Annotation. This article discusses the comparison of TrueCrypt and VeraCrypt crypto containers. Rather reliable, but easily accessible cryptographic algorithms were required. For a long time in demand more in the military environment, now cryptography is widely used in diplomatic, commercial, banking, state and other spheres.

Keywords: cryptocontainers, TrueCrypt, VeraCrypt, encryption