TrueCrypt

Материал из Википедии — свободной энциклопедии

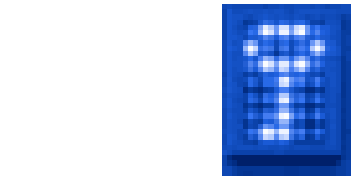
TrueCrypt — компьютерная программа для шифрования на «лету» для 32- и 64-разрядных операционных систем семейств Microsoft Windows NT 5 и новее (GUI-интерфейс), Linux и Mac OS X. Позволяет создавать зашифрованный логический (виртуальный) диск, хранящийся в виде файла. С помощью TrueCrypt также можно полностью шифровать раздел жёсткого диска или иного носителя информации, например, флоппи-диск или USB-флеш-накопитель. Все сохранённые данные в томе TrueCrypt полностью шифруются, включая имена файлов и каталогов. Смонтированный том TrueCrypt подобен обычному логическому диску, поэтому с ним можно работать с помощью обычных утилит проверки и дефрагментации файловой системы.

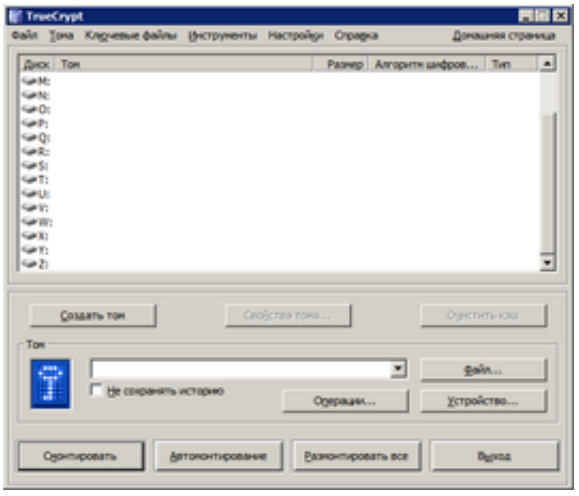
Лицензия программы считалась свободной, однако при её проверке для включения TrueCrypt в дистрибутив Fedora в октябре 2008 года были обнаружены опасные и делающие её несвободной неоднозначности[3][4]. К ноябрю в лицензию были внесены исправления[5].

28 мая 2014 года проект был закрыт, разработка свёрнута. Все старые версии удалены, репозиторий очищен. Обстоятельства закрытия проекта вызвали множество догадок и обсуждений в ИТ сообществе.

Содержание

TrueCrypt





TrueCrypt (Windows XP)

Тип	Криптография
Разработчик	TrueCrypt Foundation
Написана на	C, C++, Ассемблер[1]
Интерфейс	WxWidgets
Операционная система	Microsoft Windows NT 5+, Linux, Mac OS X
Языки интерфейса	30 языков [2] (хотя большинство из них неполные переводы)
Первый выпуск	2 февраля 2004
Последняя версия	7.2 (28 мая 2014)
Состояние	Сайт был закрыт
Лицензия	TrueCrypt License v 3.1, TrueCrypt Collective License
Сайт	www.truecrypt.org (http://www.truecrypt.org/) andryou.com/truecrypt_orig (http://a

ndryou.com/truecrypt_orig/) andryou.com/truecrypt (http://andryou.com/truecrypt/) truecrypt.ch (http://truecrypt.ch/)

Возможности TrueCrypt

TrueCrypt умеет создавать зашифрованный виртуальный диск:

1. в файле-контейнере, что позволяет легко работать с ним — переносить, копировать (в том числе на внешние устройства в виде файла), переименовывать или удалять;
2. в виде зашифрованного раздела диска, что делает работу более производительной и удобной, в версии 5.0 добавилась возможность шифровать системный раздел;
3. путём полного шифрования содержимого устройства, такого как USB флеш-память (устройства флоппи-диск не поддерживаются с версии 7.0).

В список поддерживаемых TrueCrypt 6.2 алгоритмов шифрования входят AES, Serpent и Twofish. Предыдущие версии программы также поддерживали алгоритмы с размером блока 64 бита (Triple DES, Blowfish, CAST5) (включая версии 5.x, которые могли открывать, но не создавать разделы, защищённые этими алгоритмами). Кроме того, возможно использование каскадного шифрования различными шифрами, к примеру: AES+Twofish+Serpent.

Все алгоритмы шифрования используют режим XTS, который более безопасен, нежели режимы CBC и LRW для шифрования «на лету», применяющиеся в предыдущих версиях (работа с уже созданными шифроконтейнерами в этих форматах также возможна).

Программа позволяет выбрать одну из трёх хеш-функций: HMAC-RIPEMD-160, HMAC-Whirlpool, HMAC-SHA-512 для генерации ключей шифрования, соли и ключа заголовка.

Для доступа к зашифрованным данным можно применять пароль (ключевую фразу), ключевые файлы (один или несколько) или их комбинации. В качестве ключевых файлов можно использовать любые доступные файлы на локальных, сетевых, съёмных дисках (при этом используются первые 1 048 576 байт) и генерировать свои собственные ключевые файлы.

Одна из примечательных возможностей TrueCrypt — обеспечение двух уровней правдоподобного отрицания наличия зашифрованных данных, необходимого в случае вынужденного открытия пароля пользователем:

1. Создание скрытого тома, что позволяет задать второй пароль (и набор ключевых файлов) к обычному тому для доступа к данным, к которым невозможно получить доступ с основным паролем, при этом скрытый том может иметь любую файловую систему и располагается в неиспользованном пространстве основного тома.
2. Ни один том TrueCrypt не может быть идентифицирован (тома TrueCrypt невозможно отличить от набора случайных данных, то есть файл нельзя связать с TrueCrypt как с программой, его создавшей, ни в какой форме и рамках).

Другие возможности TrueCrypt:

- Переносимость, что позволяет запускать TrueCrypt без установки в операционной системе (необходимы права группы администраторов в NT).
- Поддержка создания зашифрованного динамического файла на дисках NTFS. Такие тома TrueCrypt увеличиваются в размере по мере накопления новых данных вплоть до указанного максимального размера. Однако использование подобной возможности несколько уменьшает производительность и безопасность системы.
- Шифрование системного физического либо логического диска для Microsoft Windows-систем с дозагрузочной аутентификацией. (TrueCrypt не способен выполнять шифрование GPT дисков, которые установлены на большинстве современных компьютеров, поэтому

перед шифрованием их необходимо преобразовать в MBR (master boot record)). (Такая же функциональность встроена в Windows Vista (не всех редакций), Windows 7 (Корпоративная и Максимальная), Windows Server 2008, Windows 8.1 под именем BitLocker. Однако, BitLocker не предлагает функционала правдоподобного отрицания и имеет закрытый исходный код, что делает невозможной проверку на наличие уязвимостей или встроенных лазеек для обхода защиты. Своя система шифрования встроена в Mac OS X, она называется FileVault, и начиная с версии 2.0 может зашифровать весь диск. Как и BitLocker, FileVault не предлагает функционала правдоподобного отрицания и имеет закрытый исходный код, что делает невозможной проверку на наличие уязвимостей или встроенных лазеек для обхода защиты).
- Изменение паролей и ключевых файлов для тома без потери зашифрованных данных.
- Возможность резервного сохранения и восстановления заголовков томов (1024 байт).
  - Это может быть использовано для восстановления заголовка повреждённого файла, чтобы монтировать том после ошибки на аппаратном уровне, в результате которой повредился заголовок.
  - Восстановление старого заголовка также сбрасывает пароль тома на тот, который действовал для прежнего заголовка.
- Возможность назначать комбинации клавиш для монтирования/размонтирования разделов (в том числе и быстрого размонтирования со стиранием ключа в памяти, закрытием окна и очисткой истории), отображения и сокрытия окна (и значка) TrueCrypt.
- Возможность использовать TrueCrypt на компьютере с правами обычного пользователя (в том числе создавать и работать с контейнерами в файлах), правда, первоначальную установку программы должен сделать администратор.

История TrueCrypt

TrueCrypt основан на программе Encryption for the Masses (E4M). E4M была популярной программой с открытым исходным кодом для шифрования «на лету», первая версия которой выпущена в 1997 году. Однако в 2000 году работа над программой была прекращена, так как её автор, фр. *Paul Le Roux*, переключился на коммерческие разработки.

Первая версия TrueCrypt увидела свет 2 февраля 2004 года. На тот момент TrueCrypt был единственной программой с открытым исходным кодом для шифрования «на лету» с полной поддержкой Windows XP и обеспечивающей высокую отказоустойчивость.

TrueCrypt версии 1.0 поддерживал Windows 98/ME и Windows 2000/XP. Последующая ревизия 1.0a уже не поддерживала Windows 98/ME, так как автор драйвера под Windows 9x для E4M заявил, что он не давал разрешения на использование его кода в иных проектах, кроме E4M. Замечание: Авторы Scramdisk и E4M обменивались своими кодами (автор Scramdisk обеспечивал разработку драйвера под Windows 9x, а автор E4M отвечал за разработку драйвера под Windows NT, который позволил появиться на свет Scramdisk NT как Shareware продукту).

7 июня 2004 года была выпущена версия TrueCrypt 2.0. Вероятно, потому, что над программой работали уже разные группы (авторы), подпись создателей была изменена на *TrueCrypt Foundation*. Предыдущие версии подписывались создателями как *TrueCrypt Team*. Версия была выпущена под лицензией GNU General Public License. Несколько недель спустя вышла версия TrueCrypt 2.1, но на этот раз под оригинальной лицензией E4M «*во избежание потенциальных проблем, связанных с лицензией GPL*».

1 октября 2004 года вышла версия TrueCrypt 2.1a на ресурсе SourceForge.net, и truecrypt.sourceforge.net (http://truecrypt.sourceforge.net) стал официальным сайтом TrueCrypt. Где-то с начала мая 2005 года официальным сайтом TrueCrypt становится снова www.truecrypt.org (htt

p://www.truecrypt.org), а сайт на SourceForge.net уже перенаправляет на официальный.

TrueCrypt версии 4.0 был выпущен 1 ноября 2005 года. Была добавлена поддержка Linux, x86-64, Big Endian machines, ключевых файлов (двух-факторная аутентификация), хеш-алгоритм Whirlpool, языковые модули и многое другое.

TrueCrypt версии 4.1 увидел свет 26 ноября 2005 года. Был добавлен режим LRW, обеспечивавший более безопасный режим шифрования «на лету», нежели режим CBC.

TrueCrypt версии 4.2 вышел 17 апреля 2006 года. В этой версии были добавлены различные возможности для работы под Linux, возможность создавать тома, изменять пароли и ключевые файлы, генерировать ключевые файлы и резервировать/восстанавливать заголовки томов. В версии для Windows NT появилась поддержка динамических томов.

TrueCrypt версии 4.3 вышел 19 марта 2007 года. В этой версии появилась поддержка 32- и 64-разрядных версий Windows Vista и некоторые другие улучшения (например, горячая клавиша для затирания кэша), а также были исправлены ошибки. В данной версии исключена возможность создания зашифрованных разделов с алгоритмами, имеющими размер блока 64 бита (3DES, CAST5, Blowfish), однако осталась возможность работы с уже созданными разделами (в версии 5 такой возможности может не быть).

TrueCrypt — 4.3a вышла 3 мая 2007 года.

TrueCrypt версии 5.0 вышел 5 февраля 2008 года. Наиболее важные новшества:

- возможность шифрования всей системы под Microsoft Windows;
- графический интерфейс для Linux.

TrueCrypt версии 5.0a вышел 12 февраля 2008 года, данная версия в основном содержит исправление ошибок.

В версии TrueCrypt 5.1 от 10 марта 2008 года включена поддержка спящего режима при шифровании системного диска под Microsoft Windows. Также используется реализация алгоритма AES на языке Ассемблер, что обеспечивает большее быстродействие по сравнению с реализацией на C.

В версии TrueCrypt 5.1a была исправлена критическая уязвимость, найденная в TrueCrypt 5.1[6].

Версия TrueCrypt 6.0 вышла 4 июля 2008 года. Появилась поддержка параллельного шифрования/дешифрования, что повышает производительность при запуске на многоядерных и многопроцессорных системах, возможность создавать скрытые разделы при работе в ОС на основе Linux и Mac OS, а также создавать и работать со скрытыми операционными системами, существование которых невозможно доказать.

Версия TrueCrypt 6.1a вышла 1 декабря 2008 года. Изменения: исправлены мелкие ошибки, незначительные улучшения безопасности.

Версия TrueCrypt 6.2 вышла 11 мая 2009 года. Изменения: добавлена буферизация упреждающего чтения, которая улучшает скорость чтения, особенно при использовании SSD-дисков, обычно на 30-50 %. (Windows)

Версия 6.2a вышла 15 июня 2009 года. Версия исправляет обнаруженные ошибки.

Версия 6.3 вышла 11 октября 2009 года. Полная поддержка Windows 7 и Mac OS X 10.6 Snow Leopard.

Версия 6.3a вышла 23 ноября 2009 года. Версия исправляет обнаруженные ошибки.

Версия 7.0 вышла 19 июля 2010 года. Изменения: ускорение алгоритма AES на некоторых процессорах, возможность автоматического монтирования томов на присоединённых устройствах, поддержка томов с размером сектора 1024, 2048 или 4096 байт, органайзер томов, использование API Microsoft для шифрования файлов подкачки.

Версия 7.0a вышла 6 сентября 2010 года.

Версия 7.1 вышла 1 сентября 2011 года. Изменения: полная совместимость с 32-битной и 64-битной Mac OS X 10.7 Lion.

Версия 7.1a вышла 7 февраля 2012 года.

Версия 7.2 вышла 28 мая 2014 года. Финальный релиз, возможно только дешифрование, возможность шифрования данных была удалена. Сайт и программа настоятельно рекомендуют переходить на BitLocker. Вероятные причины — взлом или воздействие на разработчиков. Предыдущие версии являются рабочими и не скомпрометированными. Переход на BitLocker считается бесполезным ввиду его закрытого исходного кода. Кроме того, BitLocker существует только в «старших» SKU операционной системы Windows — Enterprise/Ultimate, что означает невозможность его использования на большинстве ноутбуков с инсталляцией Windows Professional от производителя. Поскольку авторы TrueCrypt всегда высмеивали безопасность Bitlocker, то такой совет многие восприняли как свидетельство канарейки, то есть намёк на неискренность собственных слов и попытку сказать нечто важное через молчание.

Более точную информацию см. на официальной странице истории версий[7] TrueCrypt.

Аудит

В 2013 году начался сбор средств[8] для проведения независимого аудита TrueCrypt, толчком к которому послужила в том числе полученная от бывшего сотрудника АНБ Сноудена информация о намеренном ослаблении спецслужбами средств шифрования. Планировалось, что в ходе проверки будет проведён анализ совместимости лицензии TrueCrypt с другими открытыми лицензиями, будет произведён криптографический анализ и будет разработана технология, позволяющая делать компиляцию исходного кода программы с одинаковым результатом на разных компьютерах[9][10].

На аудит было собрано свыше 60 000 долларов. 14 апреля 2014 года завершился первый этап проверки, критических ошибок обнаружено не было[11][12].

К началу апреля 2015 года аудит был завершён. Он не выявил никаких уязвимостей или серьёзных недостатков в архитектуре приложения и показал, что TrueCrypt является хорошо спроектированной криптографической программой, хоть и не идеальной[13][14][15].

После прекращения разработки TrueCrypt на основе его исходных кодов появилось несколько форков, среди которых стоит отметить проект VeraCrypt, созданный ещё до закрытия TrueCrypt с целью усиления методов защиты ключей шифрования (заменой алгоритма RIPEMD-160 на SHA-512 и SHA-256) и CipherShed (в котором авторы попытались учесть замечания, выявленные в процессе аудита TrueCrypt)[16].

Примечания

1. ↑ TrueCrypt Free Open Source Encryption Software — C and C++ Programming Resources (http://www.mycplus.com/featured-articles/truecrypt-free-open-source-encryption-software/)
2. ↑ Invalid URL (http://www.truecrypt.org/localizations.php). Truecrypt.org. Проверено 1 июня 2014. (недоступная ссылка)
3. ↑ Forbidden items — FedoraProject (http://fedoraproject.org/wiki/ForbiddenItems#TrueCrypt)
4. ↑ TrueCrypt licensing concern (http://www.mail-archive.com/distributions@lists.freedesktop.org/msg00270.html)
5. ↑ Gentoo Bug 241650 — truecrypt has a dangerous license (http://bugs.gentoo.org/show_bug.cgi?id=241650)
6. ↑ openPGP в России / Новости / 2008 / Критическая уязвимость в TrueCrypt 5.1 (https://www.pgpru.com/novosti/2008/kriticheskajaujazvimostjvtruecrypt51)
7. ↑ TrueCrypt — Free Open-Source Disk Encryption — Documentation — Version History (http://archive.is/2KSqQ)
8. ↑ Open Crypto Audit Project (http://opencryptoaudit.org/).
9. ↑ IsTrueCryptAuditedYet? In part! (http://istruecryptauditedyet.com/).
10. ↑ Интрига TrueCrypt: выдержит ли легендарный криптоинструмент проверку? (http://www.computerra.ru/86038/truecrypt/), Комьютерра.
11. ↑ Закончился первый этап аудита безопасности TrueCrypt — критических багов не обнаружено (http://habrahabr.ru/post/219489/), Хабрахабр.
12. ↑ Open Crypto Audit Project TrueCrypt Security Assessment (https://opencryptoaudit.org/reports/iSec_Final_Open_Crypto_Audit_Project_TrueCrypt_Security_Assessment.pdf) (англ.).
13. ↑ *Matthew Green.* Truecrypt report (http://blog.cryptographyengineering.com/2015/04/truecrypt-report.html). *A Few Thoughts on Cryptographic Engineering* (2 апреля 2015).
14. ↑ Завершен аудит кода TrueCrypt / Хабрахабр (http://habrahabr.ru/post/254777/)
15. ↑ Завершен аудит TrueCrypt: Бэкдоров и ошибок архитектуры не обнаружено (http://www.securitylab.ru/news/472366.php)
16. ↑ Выпуск VeraCrypt 1.0f-2, форка TrueCrypt (http://www.opennet.ru/opennews/art.shtml?num=41996), OpenNET (8 апреля 2015). Проверено 14 июля 2015.

Ссылки

- Официальный сайт (http://www.truecrypt.org/) (англ.)
- Почти полная копия прежнего сайта (http://andryou.com/truecrypt_orig/) (англ.)
- Неофициальная копия сайта (http://andryou.com/truecrypt/) (англ.)
- Сайт проекта TCNext (http://truecrypt.ch/) (англ.) — который планирует продолжить дело TrueCrypt!
- Страница на Gibson Research Corporation (https://www.grc.com/misc/truecrypt/truecrypt.htm/) (англ.) — Первоисточник информации по случившемуся инциденту, ответ Дэвида и т. д. И, конечно же, ссылки на все сборки и исходники последней актуальной версии TrueCrypt.
- Репозиторий на GitHub (https://github.com/DrWhax/truecrypt-archive/) (англ.) — с полным архивом всех версий TrueCrypt, начиная с самой первой (даже когда программа ещё называлась Scramdisk).
- Open Crypto Audit Project (https://opencryptoaudit.org/) — Проект по независимому аудиту и криптографическому анализу TrueCrypt 7.1a
- Кто создал TrueCrypt? (http://news.softodrom.ru/ap/b19702.shtml/)

Источник — «https://ru.wikipedia.org/w/index.php?title=TrueCrypt&oldid=78812483»

Foundation, Inc.