УДК 004.056.5

Informatics and Mathematical Methods in Simulation
Vol. 5 (2015), No. 4, pp. 347-352

PROGRAM AND TECHNICAL ASPECTS OF CRYPTOGRAPHIC DEFENCE OF DATA STORAGE

A.V. Zadereyko, A.V. Troyanskiy

Odessa National Polytechnic University,
1, Shevchenko Ave., Odessa, 65044, Ukraine; email: alexander.zadereyko@opu.ua,
alexander.zadereyko@gmail.com

Data storage defense is an aggregate of problems, interlinked with the use of cryptographic program facilities of the different setting. For the decision of this task - using free of charge cross platform cryptographic TrueCrypt software with the opened source code, allows to make coding of information «on the fly». The analysis of TrueCrypt software possibilities is executed. The algorithm for defense of data storage with practical application TrueCrypt software is developed. The productivity comparative analysis of the personal computer with/out cryptographic TrueCrypt software is resulted. Actual absence of the productivity decline is showed. Independent audit considered cryptographic TrueCrypt software did not expose the greatest threats his vulnerability. Personal author's 10-years experience in exploitation TrueCrypt software for defense of data storage allows to assert a blamelessness, reliability and stability of it work.

It's shown that cryptographic TrueCrypt software and its subsequent modifications, is the most effective measure, which allows preventing the losses of confidential information of users, placed on the personal computer and external data storage.

Keywords: cryptographic defense, cryptographic software, TrueCrypt, cryptocontainer, defense of carriers of data, coding of information «on the fly.

The essence of a problem

Ensuring the protection of the users of personal computers (PCs) in practice is a set of problems closely related with using software and hardware for various purposes. [1]

The most common feature of the operation PC users in different organizations is practically nobody does not restrict access to them. This inevitably leads to the fact that a "unit" PCs have access uncontrolled number of users. Such a "multi-user" mode of operation eventually gives rise to the need to protect data as stored on a PC, so data users themselves.

The solution of this problem is argued by objective reasons, determining the importance of ensuring the protection of user information:

- rapid growth of the number of PCs;
- widespread use of PCs in various spheres of human activity;
- accumulation of large amounts of data on PC;
- expansion of the users range who have access to PC;
- availability PC connecting to LAN or corporate network with Internet access.

A partial solution to this problem can be realized by using their individual user information data storage - flash cards, portable hard disks, etc.

However, it did not really solve the problem of protecting information from unauthorized access, "third parties" by hackers or malicious software (software) when connecting individual carriers to the PC. Furthermore, it should also be noted that these devices trust important information is unsafe. First of all because there is the risk of data loss (physical or mechanical), especially if recorded on the data storage any confidential information of high importance, the consequences of such a loss can appear to be the most sorrowful.

In this regard, the task of ensuring reliable protection of user data is current as ever.

Latest research and publications analysis have taken the initiative towards solving the problem.

The most common methods of protecting information on connected data storage in a customer environment include:

1. Create a hidden partition [2];
2. Create an archive, locked password [3];
3. Restrict access to files / folders. [4]

These methods of information protection have a number of drawbacks. The presence of hidden partitions easily installed by comparing the actual and the real capacity of the storage medium.

Creating archives locked password, inevitably increases:

- the probability of a lack of software on the PC;
- long time of creating and extracting;
- the probability of an incorrect input (random) password when creating an archive;
- The probability of a partial data loss in the process of creating an archive especially grows when using flash cards (due to exceeding the number of read-write cycles guaranteed by the manufacturer) [5].

Restrict access to files/folders is performed, usually with the help of additional software: Folder Crypto Password; Secure Folder; Hide Folder; Lock Folder, etc. or built-in operating system (OS). In this case, access to the protected data is limited to OS administrative means, which in itself is unreliable.

Conclusions and prospects for further research in this direction

In connection with the above, it can be concluded that a reliable protection for user data only option is to use any encryption in real time. This allows to realize continuous operation of the encryption/decryption algorithm of traffic from the PC to the data storage medium during recording/reading [6].

The purpose of the article

Consider the feasibility of cryptographic protection data storage users.

The basic material of the presentation

To solve this problem almost perfect free, cross-platform cryptographic TrueCrypt software open source encryption of data "on the fly» (On-the-fly encryption). Under the encrypted "on the fly" is to be understood that all data is encrypted and decrypted before the direct appeal to them (read, execute, or save). The data is encrypted in its entirety, including the file headers, the contents, metadata, etc. [7].

Considered software allows to create a file cryptocontainers, encrypt partitions themselves HDD, including OS, as well as removable storage devices: USB-drives and external HDD.

The benefits of encryption software TrueCrypt [8]:

- the ability to use a portable (portable version);

- software works with Microsoft Windows, starting with 2000 / XP / 7 (x32 / x64), GNU / Linux (32- and 64-bit versions of the kernel 2.6 or compatible) and Mac OS X (10.4 Tiger and above);
- use strong encryption algorithm - AES-256, Serpent, and Twofish with the possibility of a mutual combination);
- real-time encryption, and it is not noticeable to the user;
- pre-boot authentication to encrypt the system partition HDD;
- the possibility of creating separate file of cryptocontainers, including dynamically expanding in the data storage with NTFS file system;
- creation cryptocontainers in the "cloud storage";
- cryptocontainers may look like an ordinary file with any extension, for example, txt, doc (x), mp3, img, iso, mpg, avi, etc., with or without enlargement;
- full encryption of the contents of devices – HDD and removable data storage;
- creation of hidden volumes, including and the hidden OS;
- the OS cannot determine the presence of TrueCrypt volumes - they are just a set of random data and identify them with TrueCrypt software does not seem possible (not counting method termorectum cryptoanalysis);
- ensure that the two levels of plausible deniability of the encrypted data is one of the most important features of the software TrueCrypt. Their operating principle is the ability to create an encrypted carrier with two passwords - password of the available real data, and the second - the other data [9]. Thus, in a situation where the encrypted user's data storage formally withdrawn, the user can open the second password, wherein all important data that are available at present the password will remain hidden.
- change passwords and key files for the TrueCrypt software volume without loss of encrypted data;
- create an encrypted virtual drive;
- ability to use TrueCrypt software on PC as a normal user.

TrueCrypt practical use for storage devices protection (see Fig. 1):

1. Removable storage device (external HDD or flash card) is to be divided into two partition [2]. The size of the first partition is determined by TrueCrypt size and makes 2-5 Mb.
2. Copy a TrueCrypt portable variant into the first partition.
3. Start TrueCrypt and implement the encryption of the second partition.
4. Mount the encrypted partition onto a Disk.
5. Perform the information transfer onto a Disk.
6. Umount Disk into the encrypted partition.

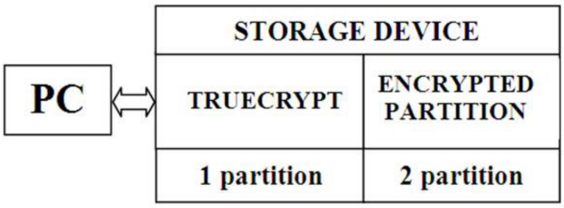

Fig.1. Structure of the encrypted storage device

Comparative analysis of the PC performance with using the TrueCrypt software

Pictures 1-3 show the results of an experimental study of the effect on PC performance when running encryption TrueCrypt software using PC stationary and its mobile version (Laptop) [10].

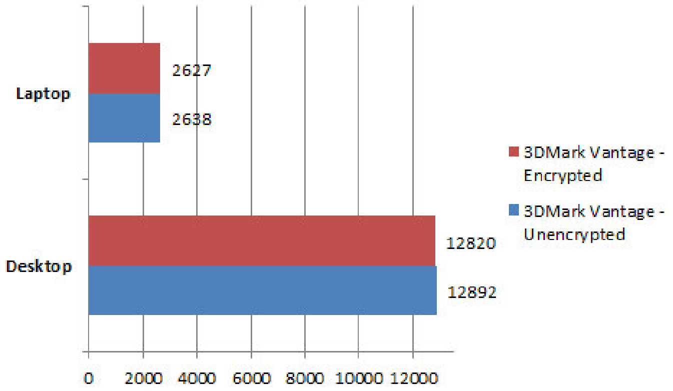

Fig. 1. Comparative performance PC video adapters.

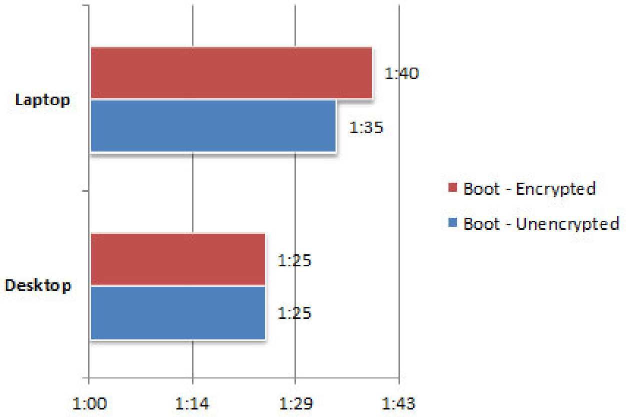

Fig. 2. Load time OS analysis with/out using Truecrypt software data encryption.

As seen from the diagrams shown in Picture 1 and Picture 2, the performance of your PC video card is not reduced, and the boot time is increased by Laptop versions using SDD.

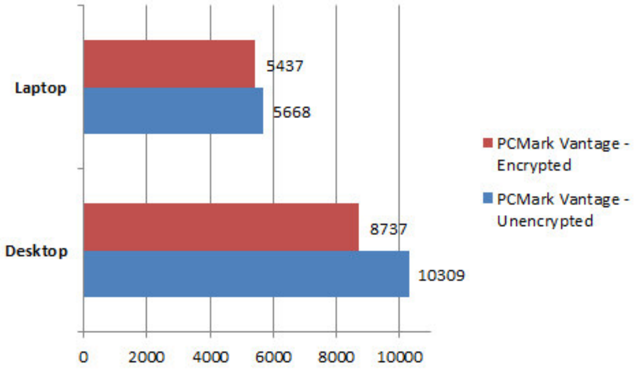

Fig. 3. Comparative analysis of the PC performance with using PCMark.

As seen from the diagrams shown in Picture 3, there is a drop in performance version of Laptop PCs with SSD (-15%). At the same time, the initial speed of SSDs is so high that they still out perform PC HDD, lost in the PCMark only 4%.

Comparative tests were carried out on the PC the following configurations: PC laptop performance (Laptop) - AMD Phenom II X4 905 (2.5 GHz), 6GB DDR3 1600 MHz, Radeon HD6870 OC 1GB DDR5, 120GB RunCore Pro V 2.5 "SATA III SSD; Stationary PCs - Intel Core2 Quad CPU Q9000 @ 2.00 GHz, 6 GB of RAM DDR2, ATI Mobility Radeon HD 4650, Seagate Momentus XT 500GB HDD.

Conclusions and prospects for further research in this direction

Currently, the development of encryption TrueCrypt software was further developed in the form of individual cryptographic software: CipherShed [11] and VeraCrypt [12]. The basis for the collection of the original code base TrueCrypt software. This cryptographic software successfully developed and supported. Moreover, they fixed some bugs encryption TrueCrypt software [13].

It should also be noted that the formats of cryptocontainers VeraCrypt software become incompatible with TrueCrypt software. For comparison, cryptocontainers CipherShed software compatible with TrueCrypt software.

Independent audit considered encryption TrueCrypt software, conducted by iSEC Partners showed that its code was found in a total of 11 members of security threats. 4 of them have an average level of danger, another 4 - low, remaining in principle, difficult to classify due to their insignificance. More detailed results of the audit were published in a document posted on site - opencryptoaudit.org [14, 15].

10-year author’s experience in the encryption operation with TrueCrypt software to protect the data storage suggests perfection, reliability and stability of the examination on. Thus, the use of encryption TrueCrypt software considered and its modifications, is the most effective measure that prevents leakage of confidential user information placed on your PC and external data storage.

References

1. Methods and tools for the protection of information in computer systems: Proc. benefits for students. Executive. Proc. institutions / Pavel Borisovich Horev. - M .: Publishing center "Academy", 2005. – 360 с.
2. Hidden partition. [Electronic resource]. // Access: http://cyberhound.ru/windows/zaschita/skrytye-razdely-zhestkogo-diska.html. - Title from the screen.
3. Creation of encrypted archives. [Electronic resource] // Access: https://the-bosha.ru/2010/06/19/zashifrovannie-archivi-v-linux/. - Title from the screen.
4. How to prevent access to the folder or file. [Electronic resource] // Access: http://www.vashmirpc.ru/publ/sistema/kak_zapretit_dostup_k_papke_ili_fajlu/2-1-0-75. - Title from the screen.
5. The facts: how many write cycles at the stick? [Electronic resource] // Access: http://hi-news.ru/periferiya/fakty-skolko-ciklov-zapisi-u-fleshki.html. - Title from the screen.
6. Protecting information on removable disks. [Electronic resource] // Access: http://wd-x.ru/protect-info-on-removable-drives/. - Title from the screen.
7. Features of national conspiracy: encrypt drives using Luks / dm-crypt, Truecrypt and Encfs. [Electronic resource] // Access: https://xakep.ru/2011/03/14/54794/. - Title from the screen.
8. «TrueCrypt» - program for encryption. [Electronic resource] // Access: https://te-st.ru/tools/truecrypt/. - Title from the screen.
9. Deniable encryption. [Electronic resource] // Access: https://ru.wikipedia.org/wiki/Отрицаемое_шифрование. - Title from the screen.
10. What is the Performance Impact of System Encryption With TrueCrypt. [Electronic resource]. // Access: http://www.digitalcitizen.life/what-performance-impact-system-encryption-truecrypt. - Title from the screen.
11. CipherShed. [Electronic resource] // Access: https://ciphershed.org. - Title from the screen.

12. Veracrypt: improved version of Truecrypt. [Electronic resource] // Access: https://xakep.ru/2014/10/14/veracrypt/. - Title from the screen.
13. VeraCrypt. [Electronic resource] // Access: - https://veracrypt.codeplex.com. - Title from the screen.
14. The audit source TrueCrypt: serious threats have been identified. [Electronic resource] // Access: http://www.3dnews.ru/818668/print. - Title from the screen.
15. The second phase of the audit is completed TrueCrypt: four vulnerabilities identified. [Electronic resource] // Access: http://webware.biz/?p=3370. - Title from the screen.

ПРОГРАМНО-ТЕХНІЧНІ АСПЕКТИ КРИПТОГРАФІЧНОГО ЗАХИСТУ НОСІЇВ ІНФОРМАЦІЇ

О.В. Задерейко, О.В. Троянський

Одеський національний політехнічний університет,
просп. Шевченка, 1, Одеса, 65044, Україна; e-mail**:** alexander.zadereyko@gmail.com

Захист носіїв інформації є сукупністю проблем, тісно зв'язаних з використанням криптографічних програмних засобів різного призначення. Для вирішення цього завдання застосовується безкоштовне, кросплатформене криптографічне програмне забезпечення (ПО) TrueCrypt з відкритим кодом, що дозволяє здійснювати шифрування даних «на льоту». Виконаний аналіз можливостей ПО TrueCrypt. Розроблений алгоритм практичного вживання ПО TrueCrypt для захисту носіїв інформації. Приведено порівняльний аналіз продуктивності персонального комп’ютера з/без використанням ПО TrueCrypt, який показав фактичну відсутність зниження продуктивності. Незалежний аудит розглянутого криптографічного ПО TrueCrypt не виявив найвищих погроз його уразливості. Особистий 10-ти річний досвід авторів з експлуатації ПО TrueCrypt для захисту носіїв інформації дозволяє затверджувати бездоганність, надійність і стійкість його роботи.

Показано, що вживання криптографічного ПО TrueCrypt і його подальших модифікацій, є найбільш ефективною мірою, яка дозволяє запобігти витоку конфіденційної інформації користувачів, розміщеної на персональних комп‘ютерах та зовнішніх носіях.

Ключові слова: криптографічний захист, криптографічне програмне забезпечення, TrueCrypt, кріптоконтейнер, захист носіїв інформації, шифрування даних «на льоту».

ПРОГРАММНО-ТЕХНИЧЕСКИЕ АСПЕКТЫ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ НОСИТЕЛЕЙ ИНФОРМАЦИИ

А.В .Задерейко, А.В. Троянский

Одесский национальный политехнический университет,
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail: alexander.zadereyko@gmail.com

Защита носителей информации представляет собой совокупность проблем, тесно связанных с использованием криптографических программных средств различного назначения. Для решения этой задачи применяется бесплатное, кроссплатформенное криптографическое программное обеспечение (ПО) TrueCrypt с открытым исходным кодом, позволяющее осуществлять шифрование данных «на лету». Выполнен анализ возможностей ПО TrueCrypt. Разработан алгоритм практического применения ПО TrueCrypt для защиты носителей информации. Приведен сравнительный анализ производительности персонального компьютера с/без применением ПО TrueCrypt, который показал фактическое отсутствие снижения производительности. Независимый аудит рассмотренного криптографического ПО TrueCrypt не выявил наивысших угроз его уязвимости. Личный 10-ти летний опыт авторов в эксплуатации ПО TrueCrypt для защиты носителей информации позволяет утверждать безупречность, надежность и устойчивость его работы.

Показано, что применение криптографического ПО TrueCrypt и его последующих модификаций, является наиболее эффективной мерой, которая позволяет предотвратить утечки конфиденциальной информации пользователей, размещенной на персональных компьютерах и внешних носителях.

Ключевые слова: криптографическая защита, криптографическое программное обеспечение, TrueCrypt, криптоконтейнер, защита носителей информации, шифрование данных «на лету».