Program-Technical Aspects of Encryption Protection of Users' Data

Natalia Loginova, Elena Trofimenko, Olexander Zadereyko, Rashid Chanyshev

Abstract - **The effective protection of different storage devices is impossible without multifunctional encryption software. For this task solution it is suggested to use TrueCrypt, the crossplatform cryptographic software, allowing to carry out the on-the-fly encryption. There was conducted the analysis of TrueCrypt performance capabilities and efficiency. The algorithm of TrueCrypt practical application for storage device protection was worked out. It was shown that TrueCrypt implementation is the most effective measure which allows to prevent the losses of users' confidential information stored on PC as well as on removable storage devices.**

Keywords - **information security, TrueCrypt, cryptocontainer, information protection, data protection, removable storage device, on-the-fly encryption.**

I. Introduction

In practice the providing of information security for personal computer (PC) users is a set of problems, closely associated with the usage of program-technical facilities intended for different purposes.

The matter is that in different institutions the most widespread feature of the PC exploitation is the public-staff access not limited by the authorities. It inevitably results in situation when a single PC is accessible for out-of-control number of users. Such multiuser exploitation mode generates sooner or later the necessity of protection of the data stored as well as direct users' data.

The decision of this problem is argued by the objective reasons determinating the importance of providing the users' information security:

- rapid growth of PC quantity and information burst;
- PC extensive application in the different spheres of human activity;
- accumulation of information content on PC;
- expansion of user base;
- PC connection to the local or corporate network with its simultaneous Internet connection.

The partial solution of this problem can be realized due to the user's individual information storage, such as flash cards, removable hard disks etc.

However, in fact it does not solve the problem of an unauthorized access by another persons, malefactors or harmful software during connecting of the individual storage to the PC. Besides, it should be noticed that it is not unsafely to entrust the significant information to these devices. First of all, there is a risk of information loss (physical or mechanical) especially if there is some confidential information of great significance written on it, so the consequences of such loss can appear to be the most sorrowful.

In this connection, **a task of providing the reliable users' data protection is actual** as never before.

The most widespread methods of reliable information security for computer removable storage devices are:

1. Creation of the hidden partition;
2. Creation of the archive blocked by a password;
3. Access restriction to the files/folders.

It should be noticed that the methods of information protection mentioned above have some drawbacks. The presence of the hidden partitions is easily determined by comparing the actual and real capacity of storage device.

The creation of the archives blocked by a password inevitably increases:

- probability of PC software absence;
- time loss in creating-unzipping the archive;
- probability of input the wrong (casual) password for archive;
- probability of partial information loss in the process of archive creating, this probability especially increases when using the flash (because of exceeding the number of recording-reading cycles granted by a producer) [1].

An access restriction to the files/folders is carried out as a rule by means of additional software: Folder Crypto Password; Secure Folder; Hide Folder; Lock Folder etc. by means of built-in facilities of the operating system (OS). In this case, access to the protected information is limited by the administrative facilities of OS, that is unreliable of itself.

In connection with stated above, it should be concluded that for reliable users' information protection the only remaining choice is to use some cryptoprotection in real-time mode. It will allow to realize the continuous work of encryption/decryption traffic algorithm from PC to the removable storage device in the process of recording/reading [2].

II. Instruction for Authors

For a proper task solution to be made, the TrueCrypt – free, crossplatform cryptographic software with open source code for on-the-fly encryption – is the ideal option in practice.

On-the-fly encryption (OTFE) represents a method

Natalia Loginova, Elena Trofymenko, Oleksandr Zadereyko, Rashid Chanyshev - National University "Odessa Law Academy", Fontanska doroga Str., 23, Odesa, 65009, UKRAINE,
E-mail: loginova@onua.edu.ua; trofymenko@onua.edu.ua; zadereyko@onua.edu.ua; rashchan@onua.edu.ua

used by some disk encryption software and refers to the fact that data is automatically encrypted or decrypted as it is loaded or saved. The entire file system within the volume is encrypted including file names, folder names, file contents, and other meta-data [3].

Advantages of TrueCrypt [4]:

- possibility of the portable use (portable truecrypt);
- software works with Windows OS, starting with 2000/XP/7 (x32/x64), GNU/Linux (32- and 64-bit versions, core 2.6 or compatible) and Mac OS X (10.4 Tiger) and higher;
- use of stable encryption-decryption algorithms - AES - 256, Serpent and Twofish (with possibility of their mutual combination);
- real time encryption unnoticeable for the user;
- pre boot-up authentification on encrypting the HDD boot partitions;
- possibility of file-hosted containers creation including the containers dynamically expanding on NTFS disk;
- creation of cryptocontainers in cloud storage;
- a cryptocontainer can look as an ordinary file with any expansion, for example, txt, doc(x), mp3, img, iso, mpg, avi etc., or without expansion;
- complete encryption of hard disks, removable storage devices content;
- creation of the hidden volumes, including hidden OS;
- variations of plausible deniability, including impossibility to define the presence of TrueCrypt volumes – they are just a set of occasional data. Their identification is unlikely to be possible by means of TrueCrypt (not counting the method of termorectum cryptoanalysis).
- the most important features of TrueCrypt is providing of two levels of plausible deniability. Operating principle consists in the creation of encrypted disk with two passwords – the real password makes the real data accessible from a disk, and the second boots other data [5]. So, for instance, when encrypted storage device is withdrawn, the user can open the second password and all important data accessible with the real password will appear still hidden;
- change of passwords and key files for a TrueCrypt volume without the loss of encrypted data;
- creation of an encrypted virtual disk;
- possibility to use TrueCrypt on the PC with a real user's rights.

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. Unmount Disk into the encrypted partition.

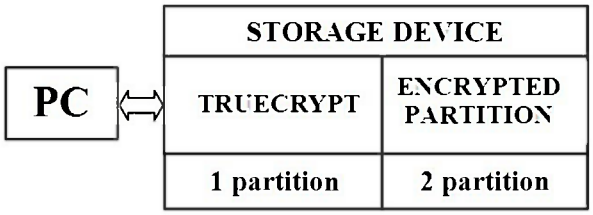

Fig.1. Structure of the encrypted storage device

Comparative analysis of the PC performance with TrueCrypt usage

The figures 2-4 represent the experimental research results of the problem formulated as follows: How does encryption with TrueCrypt impact the PC performance for both Desktop and Laptop (red – encrypted mode, blue – unencrypted mode) [6].

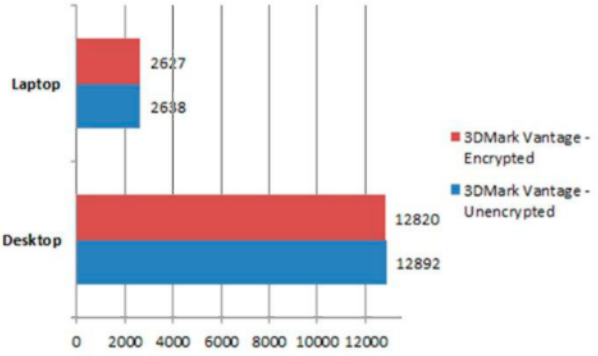

Fig.2. Comparative performance of PC video adapters.

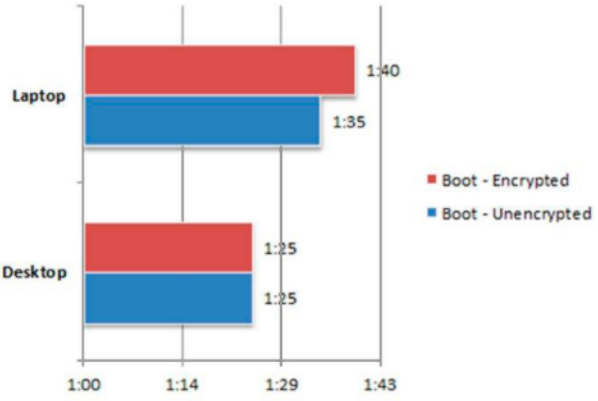

Fig.3. Analysis of OS boot timing with/without data encryption

As it can be observed from the diagrams presented on Fig. 2-3, the productivity of PC video adapter does not go down but at OS boot time it even increases for Laptop with the use of SDD.

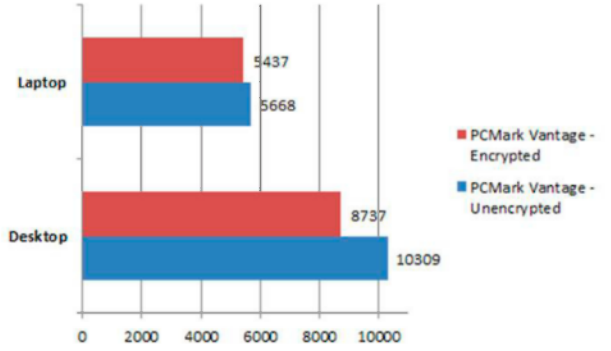

Fig.4. Comparative analysis of the computing performance for encrypted and unencrypted PCMark

The observation of the diagram (Fig. 4) shows decrease in performance of Laptop of SSD version (-15%). At the same time the initial velocity of solid-state drive is so high, that they anyway win from the PC with HDD, which lose only 4% in performance.

The comparative testing conducted on PC of the next configurations: (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 PC - Intel Core2 Quad CPU Q9000 @ 2.00 GHz, 6 GB of RAM DDR2, ATI Mobility Radeon HD 4650, Seagate Momentus XT 500GB HDD.

Presently the TrueCrypt has got the further development in separate trends – CipherShed [7] and VeraCrypt [8], which are fully noteworthy. Started in June, 2013 this software is successfully developing and supported. Moreover, some errors of its predecessor are eliminated in it [9].

The TrueCrypt original codebase is taken as above mentioned software basis. It should be also noted that the formats of VeraCrypt cryptocontainers are incompatible with TrueCrypt. On the contrary, CipherShed cryptocontainers are compatible with TrueCrypt.

TrueCrypt independent audit conducted by *iSEC Partners* company showed in total 11 threats to users' information security in its code. 4 of which have a middle level of threat, other 4 – a low level, the others are difficult to classify in principle through their insignificance. More detailed results of audit were published in a document, placed on the internet resource *www.opencryptoaudit.org* [10, 11].

III. Conclusion

In summary, the application of cryptographic software discussed above is the most effective decision, which allows to prevent the leak of users' confidential data placed on PC and external storage devices. The personal 10-year experience in TrueCrypt exploitation allows this article authors to confirm blamelessness, reliability and stability in operation of the software presented.

References

[1].Fakty: skolko tsiklov zapisi u fleshki? [Electronic resource]. – URL: http://hi-news.ru/periferiya/fakty-skolko-ciklov-zapisi-u-fleshki.html.

[2].Zaschischaem informatsiyu na s'yomnyih diskah. [Electronic resource]. – URL: http://wd-x.ru/protect-info-on-removable-drives/.

[3].Osobennosti natsionalnoy konspiratsii: shifruem diski s pomoschyu Luks/dm-crypt, Truecrypt i Encfs. [Electronic resource]. – URL: https://xakep.ru/2011/03/14/54794/.

[4].«TrueCrypt» — programma dlya shifrovaniya. [Electronic resource]. – URL: https://te-st.ru/tools/truecrypt/.

[5].Otritsaemoe_shifrovanie. [Electronic resource]. – URL: https://en.wikipedia.org/wiki/Deniable_encryption.

[6].What is the performance impact of system encryption with TrueCrypt. [Electronic resource]. – URL: http://www.digitalcitizen.life/what-performance-impact-system-encryption-truecrypt.

[7].CipherShed. [Electronic resource]. – URL: https://ciphershed.org.

[8].Veracrypt: uluchshennaja versija Truecrypt. [Electronic resource]. – URL: https://xakep.ru/2014/10/14/veracrypt/.

[9].VeraCrypt. [Electronic resource]. – URL: https://veracrypt.codeplex.com.

[10]. Audit ishodnogo koda TrueCrypt: sereznyih ugroz ne vyiyavleno. [Electronic resource]. – URL: http://www.3dnews.ru/818668/print.

[11]. Vtoraya faza audita TrueCrypt zavershena: vyiyavleno chetyire uyazvimosti. [Electronic resource]. – URL: http://webware.biz/?p=3370