DATA SECURITY MANAGEMENT ON STORAGE DEVICES IN REAL TIME

Marián Švída*, Jaroslav Majerník
Department of Medical Informatics, Faculty of Medicine, Pavol Jozef Šafárik University in Košice, Slovakia
** Corresponding author: marian.svida@upjs.sk*

ARTICLE HISTORY
Received 28 February 2014
Revised 28 March 2014
Accepted 16 April 2014
Available online 13 May 2014

KEYWORDS
data protection
data security
encryption
storage media

ABSTRACT — *The article deals with some basic approaches to the management of secured access to data on external storage devices in real time. Basic steps of effective, safe and easy-to-use handling of personal and/or confidential data are described. Further, a method to protect logins and passwords during their registration into the various applications is presented in the article. Main features of several most commonly used software products are also described considering data protection when used online and stored on various storage devices. The main reasons to apply data protection in the area of medicine and health care services are stated in this article as well.*

INTRODUCTION

Recent trends of data management have been subject to dynamic changes. Reason for this is particularly an immense growth in development of new technologies and their almost unlimited usage in personal and commercial areas. The need to have data always available rises together with this growth. Users want to have their documents, pictures, songs or movies wherever they are and available from any device connected to the Internet including Personal Computers (PCs), tablets, smartphones etc. In principle, it achievable quite easily thanks to features of today's technologies, which allow for data transmission, synchronization and storage. Various devices are available for these purposes, either traditional such as internal or external Hard Disk Drive (HDD), Compact Discs (CD), Digital Versatile Disc (DVD), Blue-ray disc (BD), flash memory, e-mail account, or the "modern" ones such as remote storage services, Network Attached Storage systems (NAS), cloud computing and many others.

Whatever is used to satisfy the needs of a particular user, it is necessary to secure all important data and protect it against any unauthorized manipulation. Unauthorized persons include not only accidental finders of physical storage devices, but also hackers, network administrators and others who may get in to the digital contact with data along the data flow path.

Even if the most of the data storage services guarantee that the data will not be offered to the third-party, there is always the chance the data can be stolen, manipulated or misused while transferred, stored or archived. Unfortunately, many users still work with their data without any hardware or software protection including both the local and the distributed data files. These unfavorable conditions are caused either by their poor computer literacy, absence of information about security tools or by the fact the work without encryption is mistakenly considered as easier and faster. Consequences arising from this non-acquaintance or indifference may be fatal, depending on the importance of randomly or intentionally misused data. The real hazard with confidential data is usually recognized in internet banking usage through free Wi-Fi networks, especially if these are weakly or not protected at all. It is also important to recognize whether the data are personal or belong to the company's database, although both of them may be of high importance.

Transfer and subsequent leak of data from commercial to private sphere and vice-versa is the main reason for increasing technical level of digital information reliability, especially in the case of confidential data (clients, business partners etc.). Very high importance of digital files protection is considered in the case of patients and their personal and health related data. Information systems designed for clinics

and hospitals solve the data security and protection at least at the level of authorized users, but the problem may arise if such kind of information is used outside the system, for example to be applied in educational or research activities. Therefore, the paper aims to increase the awareness in this area and to introduce the need of use data security and protection tools.

DATA MANAGEMENT IN REAL TIME

We do not consider the questions of safe data storage in the sense of guaranteed storage period or possibilities of physical destruction; our focus is mostly safe usage and direct work with data, including processes as distribution, storing as well as file protection with passwords. There are plenty of methods how to manage secured data and they can be available either as free or commercial. All have their pros and cons, but our primary requirement is a simple and effective handling in real time, where almost no delay should be registered by the users. Nevertheless, passwords usage is considered as a standard that is also essential while working with data on local computers. From this point of view, it is possible to use tools intended to manage passwords immediately when needed while ensuring protection against their tracing during systems' entering process (keylogger). Here, a freeware tool KeePass can be used quite efficiently as mentioned later. Activity of keylogger, if not revealed by antivirus program, can be partially eliminated using virtual onscreen keyboards with screen capture protection, no copy and paste features or randomly located keys. In such case the password (for example password to access Keepass) is entered using computer mouse and drag and drop method (Neo's SafeKeys). Characters on this on screen keyboard can be selected pressing the left mouse button or using "Hover mode" where no mouse clicks are needed to select particular character/symbol.

Other anti-keylogger tools with possibilities of randomly specified key layouts like "Oxynger KeyShield" or older but still powerful "Mouse Only Keyboard" are based on similar principles and allow for entering sensitive data protected against mouse logging in web browsers as well.

In general, the digital data management can be subdivided into three main phases. These are data file opening, data editing and data file closing. Another optional phase, called data backup, can be also considered because of its usefulness. Direct access to data files is convenient only in cases of public and open information. However, data related to scientific research, patients' health status, bank transfers etc., has to be hidden in order to be inaccessible and/or invisible for unauthorized persons.

Applications that accept passwords use hashing algorithms as an essential security consideration to protect passwords that are stored in application's database. Hashing algorithm applied to user's passwords before storing makes original passwords hard to be revealed by attackers. Hash functions can be characterized as follows:

- small change of input data will result in meaningful changes of output data,
- it is not possible to reveal original text from hash data,
- statistically, it is not likely to have identical hash data for two different texts.

In this point of view, the hashing processes should be based on "salt" method rather than on former MD5 or SHA1 because of modern computer equipment makes "brute force" attacks faster and trivial. A cryptographic salt can be imagined as additional data which makes hashes significantly more difficult to crack.

REQUIREMENTS OF SECURE DATA MANAGEMENT

Management of sensitive or personal data requires ensuring of several basic conditions to prevent their stealing, misuse or destruction. Such conditions include:

- data encryption using strong passwords,
- files stored on technically reliable memories,
- regular backup using various drives or storage places,
- periodic readability checking of all stored records,
- backup of applications used to encrypt and decrypt data files,
- save storage devices on physically different places,
- functional and reliable hardware to read and write data on storage media.

SECURITY SOFTWARE TOOLS

Software products intended for the secure data management can be classified into several categories.

Simple encryption

The most frequently used method represents traditional and direct password entering technique through ZIP or RAR file compression with encryption, but files access and management itself is usually uncomfortable and cumbersome. Weakness of the method is that the weak password used to protect compressed files can be unlocked using special hacking software. Moreover, the data files can be mistakenly stored/kept on memories of device on which such data files are managed. Simple encryption is provided by applications like 7-ZIP, WinRAR, WinZIP etc. These compression and encryption techniques are widely used, but offers only very basic password protection settings. Usually, they are not equipped by features to control strong

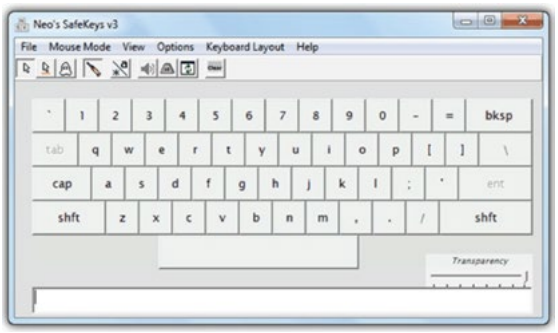

Figure 1: On screen keyboard Neo's SafeKeys defeats keyloggers very efficiently

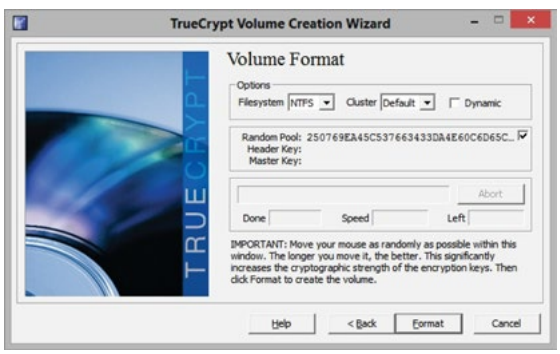

Figure 2: Volume creation wizard in TrueCrypt

password rules or to specify secure encryption algorithms. Then the data files protection can be broken using brute-force methods. In general, this category can be considered as outdated and inappropriate.

Encrypted data package

Encrypted data packages provided by tools as BitLocker, FileVault, Pointsec or TrueCrypt offer more secure work with sensitive data on local as well as remote drives. These products are usually equipped by special key features including "on the fly" encryption, data protection in the case of unexpected power supply interruption, random number generator with enhanced mechanisms, standard and cascade encryption algorithms (AES, Serpent, Twofish, AES-Twofish, AES-Twofish-Serpent, Serpent-AES, Serpent-Twofish-AES, Twofish-Serpent), HASH-algoritmy (RIPEMD-160, SHA-512, Whirlpool) etc. Encrypting applications can usually encrypt files, folders or whole drives into the form of data package where the work with files and applications is realized in real time as it is in the case of data that are not encrypted. On the other hand, users should work with appropriate responsibility to keep computer up-to-date, protected in networks, and not opened to access encryption key.

Effective and very secure data management can be obtained using one of the above mentioned tools. We prefer to use application called TrueCrypt that offers easy-to-use features for the majority of common users, who can simply open a storage space (folder, disk drive, remote folders and drives etc.) and use it for direct work with data files. The only additional operation is entering the password to open the system by an authorized person. TrueCrypt offers both the user friendly graphical interface and the command prompt mode. Graphical mode allows specifying various settings using mouse control, selection of virtual drives as well as other parameters used to open data files under operating system. Command mode is intended for users who prefer to specify particular settings in the form of short scripts. Both modes initiate particular files and their virtual opening to be able to work with them as it is in traditional way. The difference is in data protection while used in open files. Traditional way, for example ZIP compression with encryption, uses open files stored directly on physical storage devices and thus unprotected and easily discoverable. Using tools like TrueCrypt, allows managing files where the open part of data file is stored only in RAM, which is always erased when the computers is turned off. The time of potential security risk is significantly reduced. Figure 2 shows the screen during encrypted volume creation process in free open source disk encryption software TrueCrypt.

Graphical user interface and availability of its features make TrueCrypt very popular and easy to use. Management of data files and applications is almost the same as their common usage. Therefore, it can be also considered as useful for non-technical users, to be used for everyday work with data including medicine.

To create TrueCrypt data storage place it is necessary to download this application. It is recommended to use the only developer's website (http://www.truecrypt.org) as prevention against downloading infected products equipped with various add-ins and/or so called backdoors. TrueCrypt can be used on Windows, but also Mac and Linux computers. Once installed, the user will create new volume using "Create Volume" button. Wizard will guide users through several simple steps where they confirm or specify creation of encrypted file container, standard TrueCrypt volume, file location, encryption algorithm, volume size, volume password and volume format. The volume will be created and ready to be used within few minutes. It is recommended to use some of the cleaning tools (for example DiskWipe, http://www.diskwipe.org) to clean former disk space and ensure irreversible deletion after copying of old unencrypted files into the new encrypted disk storage place created by TrueCrypt. Figure 3 shows a virtual encrypted drive created in TrueCrypt.

Password depositories

Passwords depositories offer advanced management of passwords used for various applications and

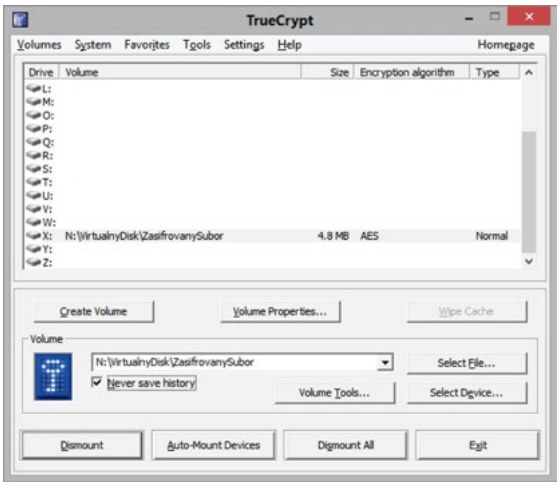

Figure 3: Virtual encrypted drive in TrueCrypt

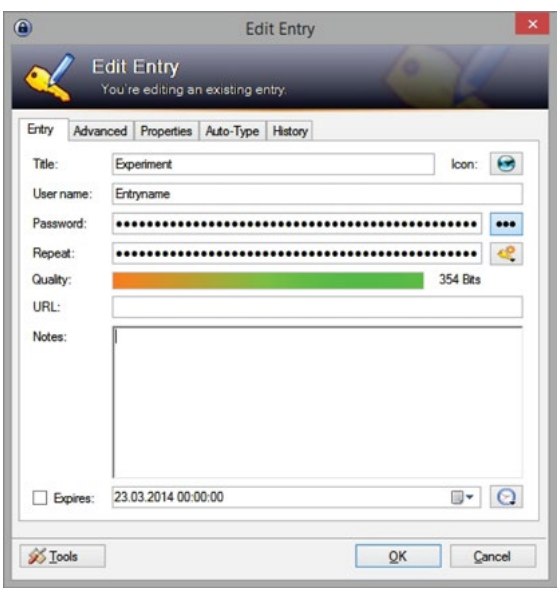

Figure 4: Password edited in KeePass

systems. Users usually consider passwords as core elements in most of the data security processes. Their decisions often fight between strong passwords and passwords that can be efficiently memorized. Here, the application KeePass is considered as very useful and secure. It belongs to the password managers where all users' passwords are protected by one so called master password. Using such applications it is not possible to reveal sequence of characters entered on the keyboard. Users usually prefer portable versions that can be used everywhere and with no risks to keep digital tracks in the system. Passwords are stored in a separate encrypted file as in depository, and their management is clear as a multilevel tree structure. Using password for a certain application is based on copy or drag and drop methods. Very useful security feature is the possibility to set time after which the copied sequence of characters will be automatically deleted from the cash memory. Password generator is also a common feature included in such types of password security tools.

KeePass should be downloaded from http://keepass.info to ensure the original version is obtained. This free open source tool can be operated under Windows, Mac OS X, Linux and also other OS. Both the installed and portable versions are available. The user has to create a new password database at first. The master password should be specified here. In order to increase security level a key file and/or windows user account can be combined to open this database. Once the password database is created and opened the user can easily manage his/her passwords for different systems. New entry (access data) allows specifying title of the system, username, password, URL, and additionally adds the files, change colors, enable autotype feature etc. An integrated password generator (Figure 5) can be used to generate strong passwords according user's preferences. Saved access data can be used in particular application using recommended drag and drop method. If the users prefer to use copy and paste method than the clipboard, the auto-clear function can be used to delete access data automatically. The predefined time is set to 12 seconds, but it can be changed according to user's needs.

Data protection on web pages

Data protection on web pages should be a matter of high importance as well. In real practice, it is very often required to store data files in public accessible storage places as domain portals. These data files even if encrypted are then accessible for particular groups of users using their logins and passwords. Owners of such domains should use some of the security forms to allow access from public network. Here, the server application Apache with security files .htaccess, .htpasswd and other commands is the way how to protect misuse of data files. This can be used to allow or deny access for various groups of users based on their login data or even IP address. In this case it is necessary to remark that the data files are not well protected inside the networks, where for example the authorized personnel can access the data.

Real-time dataflow security in public networks

"Real-time dataflow security in public networks" especially, but not only in wireless networks can be ensured using Virtual Private Networks. VPN offers high security level and high reliability applicable in personal as well as commercial areas while communicating in the public networks. Various VPN tools (i.e., OpenVPN) protect data using encrypted connection based on the standard security protocols.

SLA, QoS and other features can be applied in such real-time communication. Co-workers can be interconnected all around the world and use company services with permissions and restrictions as it is in company's LAN network. VPN connection has features of private cloud computing for local networks and computerized systems.

Cloud computing

"Cloud computing" represents a specific way to handle computerized programs and digital data. Considering economic and organizational aspects, it can be used for unevenly distributed activities during year and companies with a lack of skilled specialists. Industrial and big administrative working environments should plane its usage very carefully, especially when having own infrastructure and professionals at their disposal, and the data to be processed are confidential or secret. The main advantages of clouds are high flexibility of data access and reliable administration of data storage infrastructure. Many users prefer to use clouds because of relatively simple data sharing with friends or co-workers. Economic advantages of cloud computing include financial, personal, material and office facilities. To mention disadvantages, the confidentiality of administrator or data transfer risks are the most resonant ones.

CONCLUSION

Recent trends in the development of new technologies equipped with many on-line applications and services lead to following a few main ICT perspectives, including dynamic network services, team cooperation, mobile business, data protection and security, green IT for sustainable development with low energy consumption demands. The data security plays the most significant role in all of these areas. Unfortunately, many users and organizations still depreciate it. The reasons may originate in weak computer erudition or low information level of the data security tools. In this point of view it will be necessary to instruct users about the ways and possibilities to prevent misuse of their data. Organizations should improve internal rules and specify personal liability according to the legislation given by the national authorities.

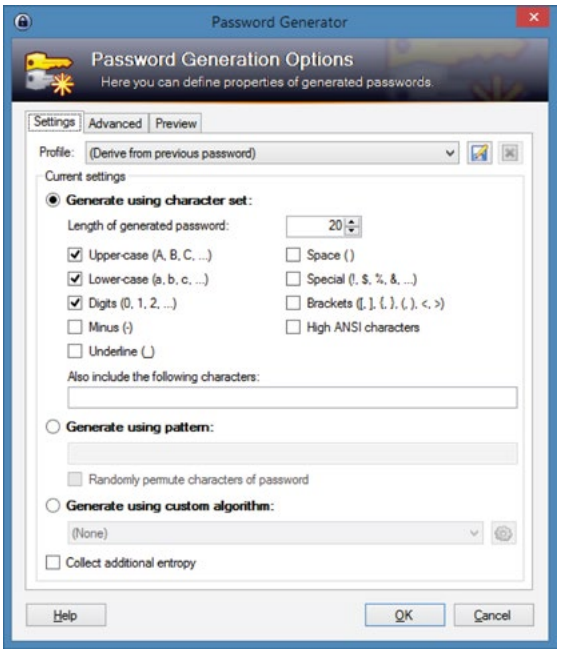

Figure 5: Password generator options available in KeePass

Ing. Marián Švída

ACKNOWLEDGEMENTS

This paper was elaborated within the framework of the project KEGA 005UPJS-4/2012 (50%) and within the framework of the project "Support research and development in the Moravian-Silesian Region 2013 DT 1 – International research teams" (RRC/05/2013), financed from the budget of the Moravian-Silesian Region (50%).

REFERENCES

[1] Útoky na operační paměť. [On-line] Available at WWW: <http://www.pepak.net/bezpecnost/utoky-na-operacni--pamet/#more-1823>
[2] Seďa J. Zabezpečená L2 síť. [On-line] Available at WWW: <https://dip.felk.cvut.cz/browse/pdfcache/sedaj2_2009bach.pdf>
[3] Hallová M. Cloud computing – definícia, výhody a nevýhody. [On-line] Available at WWW: <http://www.fem.uniag.sk/konferencie_a_seminare/zborniky/ki2013/zbornik/Hallova.pdf>
[4] Cloud computing. [On-line] Available at WWW: <http://skola.elibos.sk/?page_id=413>
[5] Rezek, J.: Pět klíčových trendů pro budoucnost ICT. [On-line] Available at WWW: <http://computerworld.cz/technologie/pet-klicovych-trendu-pro-budoucnost-ict-44055>
[6] Penhaker M, Kasik V, Snasel V. Biomedical distributed signal processing and analysis. Lecture Notes in Computer Science 2013; 8104: 88–95.
[7] Šimšík D, Siman D, Galajdová A, Krajňák S. Mainstreaming on ambient inteligence and the role of eaccessibility networking. Assistive Technology Research Series 2013; 33: 391–396.
[8] Program KeePass. [On-line] Available at WWW: <http://keepass.info>
[9] Program TrueCrypt. [On-line] Available at WWW: <http://www.truecrypt.org>
[10] Hašovací funkce. [On-line] Available at WWW: <http://cs.wikipedia.org/wiki/Ha%C5%A1ovac%C3%AD_funkce>