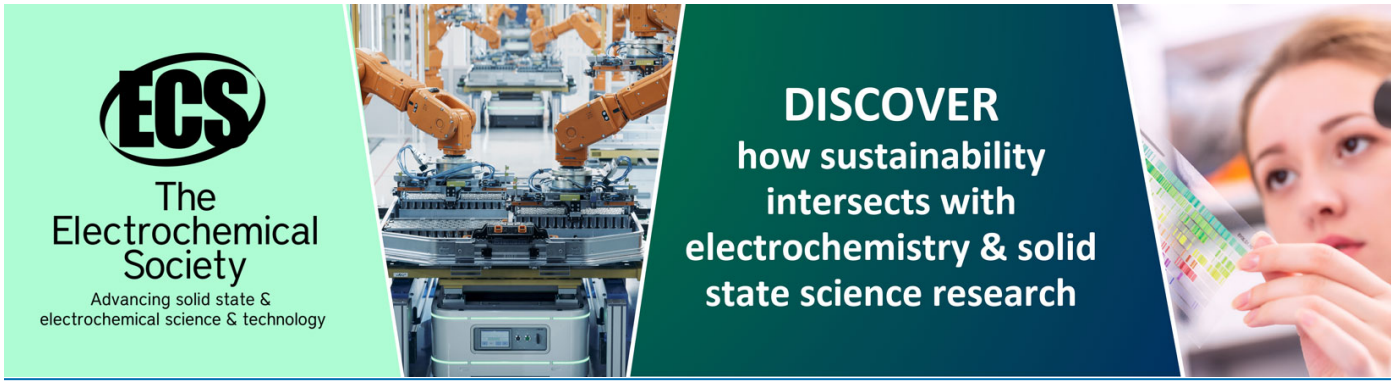
Problems of personal data and information protection in corporate computer networks



Problems of personal data and information protection in corporate computer networks

A L Zolkin[1], E M Abdulmukminova[2], V N Malikov[3] and A N Lepshokova [4]

[1] Computer and Information Sciences Department, Povolzhskiy State University of Telecommunications and Informatics, L.Tolstogo Street 23, Samara 443010, Russia
[2] Faculty of computer technology, computer engineering and power engineering, Dagestan State Technical University, I. Shamyl Street 70, Makhachkala 367000, Russia
[3] Department of General and Experimental Physics, Altai State University, Lenina Street 61, Barnaul, 656057, Russia
[4] Economics and Applied Informatics Department, Karachay-Circassian State University, Ordzhonikidze Street 2, app 12, Karachaevsk, 369200, Russia

E-mail: alzolkin@list.ru, povtias_dgtu@mail.ru, mirotnas@gmail.com, Alanida@mail.ru

Abstract. The article discusses the problems of personal data and information protection from intruders as well as methods of authentication and identification in corporate networks. Various methods of authentication and identification in computer networks are presented. Their comparative analysis is carried out, the features and disadvantages in various areas of use are highlighted, risks and possible damage from violation of data confidentiality are analyzed. The magnitude of violations of confidentiality, availability and integrity of information is growing every year, at the same time, the caused damage is growing. This situation makes it necessary for information security specialists to analyze all the risks of illegal access to information more and more thoroughly, and then resort to the introduction of modern means authentication, use new encryption methods, increasingly generate new passwords to access the system. Today, there are many ways and methods of authentication, but the specific of their application depends on the location of the information storage and its value. Meanwhile, authentication methods are not perfect protection methods, they are also vulnerable and here the situation is mostly depends on the skills of the attackers. In addition, the article discusses the problems of information security threats to flash drives, analyzes the FAT32 and NTFS file systems of flash drives as well as their vulnerabilities to malicious programs. The features of the algorithm of virus action on flash drives are highlighted. Today, there are many ways and methods of flash drives protection, but the specifics of their use depends on the location of the information storage and its value.

1. Rationale

Information security is the state of protection of information and supporting infrastructure from accidental or intentional influences of an artificial or inartificial nature (informational threats, threats to information security), which can cause unacceptable damage to the subjects of information relations.

The subjects of information relations are understood as both owners and users of information. The main goal of information security is to balance the protection of confidentiality, integrity and availability

of data, taking into account the appropriateness of the applicability and without any damage to the performance of the organization. This is achieved basically through a multi-step risk management process that identifies fixed assets and intangible assets, sources of threats, vulnerabilities, potential exposure and risk management capabilities. This process is accompanied by an assessment of the effectiveness of the risk management plan.

2. Analysis of methods and means of authentication and identification in the network

Identification and authentication procedures are inextricably linked with each other. They must be done every time you log on or resume work without logging out.

Identification is the assignment of individual names or numbers.

Authentication is a confirmation of the authenticity of the identification of the system subject.

Authorization is a procedure for granting certain access rights to system resources after they pass the authentication procedure. For each subject in the system, a set of rights that he can use during accessing its resources is determined [1].

In this case, a subject is any security participant, such as a user account created in AD DS.

In order to provide management and control over these procedures, administration and audit processes are additionally used.

Administration is the process of managing of access to system resources. This process includes:

- creation of an identifier (creation of a user account) in the system;
- management of user data used for his authentication (password change, certificate issuance, etc.);
- management of system resources access rights.

Audit is the process of system resources access control, which includes logging of actions when accessing system resources to ensure that unauthorized actions are detected.

To confirm the identity, user must provide some secret information. There are various types of such information, which can be denoted by one term "authentication factor".

Authentication factor is a certain type of information provided by the subject to the system during its authentication. This procedure can be implemented using one or more authentication factors. For example, a user may be prompted for a password, or a fingerprint may be required.

Single-factor authentication is a process that uses only one type of authentication factors.

Multi-factor authentication is a process that uses several factors. For example, during registration, the user must use a smart card and password [2,3].

The most common use has a combination of two types of authentication factors. A typical example is working with an ATM. We need to use the magnetic stripe card and PIN code at the same time.

Many business leaders do not pay enough attention to protecting their devices and the information that is stored on them. Such negligence often leads to financial losses as a result of information leakage.

Currently, there are three main methods of single-factor authentication: password authentication; biometric authentication; authentication using tokens (smart cards).

Combinations of the above authentication methods are also used. It is called two-factor authentication.

Password authentication is not the most secure way to authenticate the user. Typically, people use passwords that are easy to remember. If the password is strong enough and consists of a large number of characters, then users often write such passwords on stickers and stick them to the monitor, table, or inside of the keyboard. It is not difficult to obtain such a password.

The information security policy suggests changing the eight-digit password at least once a month. Memorizing a randomly generated password so often is quite difficult. If the user forgets the required sequence of characters than he contacts the administrator who sends the password. This procedure is also insecure, because the password can be intercepted in the network. To prevent this, the message with the password must be encrypted or transmitted over a secure channel. All these methods leads to additional costs. In many companies, a call to the administrator is not enough to obtain a password. Sometimes it is required

to execute a request or administrator shall visit the user personally. These steps in their turn also lead to wasted time and financial costs. It can be concluded that the password authentication method is ineffective due to the "human factor" [4].

Recently, so-called tokens, USB keys or smart cards have become widespread. This authentication method can be implemented using: generation of single-time passwords, storage of passwords, encryption keys, digital certificates in the device's memory. In addition to the password, the user must use the device. Depending on the needs, the appearance of the hardware can be different; a smart card with an embedded RFID tag is used to control access to personal computers or premises.

The most effective in terms of security will be the use of smart cards and USB keys, such an identifier is harder to steal, and its loss will be discovered faster than stealing a password. In addition, such devices use two-factor authentication, which significantly increases the reliability of the system, but you should also take into account the possibility of replacing the authentication server [5].

In corporate computer networks, biometric systems have begun to be used relatively recently. These systems are quite expensive, so few organizations can purchase and administer them.

Biometric authentication is a reliable method of authentication, but situations are not excluded in which this identifier can be stolen or corrupted. ID carrier fingerprints can be stolen, for example, from a glass, door handle, etc.

3. Algorithm of biometric authentication

The biometric authentication algorithm consists of the following main stages:

- The biometric system records a sample of the user's biometric traits using a reader.
- Individual traits are extracted using a software algorithm.
- Traits are also stored in the database along with other identifiers.
- For authentication, it is necessary to present the original of the biometric trait, which is compared with the data from the database using a matching algorithm.
- The system opens access only if the compliance rating has exceeded the previously set threshold.

Biometric authentication is based on the principle of reading of anatomical and behavioral traits of a person: fingerprints (palm prints); scanning of the eye retina (iris); geometry and thermogramm of the face; –voice features; keystroke dynamics.

Fingerprint authentication is performed using special scanners. Retina and iris authentication is considered as the most fault-tolerant with minimal errors, but has not been used for a long time due to its high cost and complexity.

One of the most secure authentication methods is the iris scan. The eye tissue, which is genetically individual for everyone, is used as a source of identification. During research, medical scientists found that pigment spots are formed on the iris in case of eye diseases. To solve this problem, scanners use black and white images. The eye is focused with the help of recording equipment at a distance of up to one meter [6,7]. Then the device forms about 250 identification points on the eye cornea. Authentication takes place by comparing the scanned points with a reference that is stored in the database.

Authentication by face geometry and thermogramm is based on the recognition of a person by his external features (shape of the nose, skull, facial features) and is divided into two categories: 2-D and 3-D face recognition. 3-D face recognition is considered as the most effective method.

Facial thermogramm authentication is based on infrared scanning of the blood vessels on the face and creation of a thermal map. The main advantage of this method is that the vascular system does not depend on body temperature and remains unchanged, even if conspiracy methods were used or plastic surgery was performed.

Voice authentication is performed by comparing the speaker's voice with data from the database. There are several authentication methods: text-independent; text dependent on static passphrase; text dependent on dynamic passphrase.

There is handwriting and keystroke dynamics authentication. During development of handwriting

authentication systems, it is necessary to take into account external factors affecting a person's condition. Therefore, a large error is allowed. It increases the likelihood of hacking or forgery of the identifier.

Storage of biometric data in the relevant database (in accordance with the Federal Law "On Personal Data") is quite expensive. It is also a disadvantage of this methods.

Two-factor authentication is a combination of two or even three factors. In the most situation it is a pair of factors: to know something and to have something; to know something and to be someone. From a security point of view, this method is more efficient than using a single authentication methods.

4. Features of the action algorithm of virus on flash drives

According to statistics, today the Internet is the main breeding ground for viruses, and removable storage devices hold the second place. And the leading among them by a large margin are flash drives (USB sticks), which have the ability to repeatedly rewrite and replenish files without any additional effort. In addition, flash drives have a larger amount of memory than those known before and use more advanced data management algorithms, which is why they are of such interest to attackers.

In addition, sometimes the user cannot even remember where and when he connected a flash drive in order to download a particular picture or program. However, when a computer user inserts a flash drive into the system unit of this device, the antivirus program can display a whole list of picked up malicious programs, which can often be removed only after the drive is completely formatted.

The algorithm of the virus is carried out along the following path: an infected electronic computing device or workstation is exploited by an intruder in order to steal someone else's access codes and passwords to the main and service services of the site that can migrate, this situation also applies to USB connectors and Flash drives [8]. In this situation, the infection is carried out sequentially from the workstation to the flash drive connected to it.

If the virus detects the possibility of joining the global network, then it will immediately perform an operation to transfer previously recorded information with access codes and passwords to the global Internet, further infecting other elements of the network environment. To enable the operation to start sending a virus when a flash device is connected, the malicious program overwrites Autorunners (special files named autorun.inf) on the specified drive, which contains a description of the current applications that are a connecting link for starting autoloading when connecting the media.

The Autorunner describes the direction to the malicious program, namely to the code that must be executed, as a rule, it is a certain file (“EXE”) with a specific name. As a rule, the "Autorunner" file and the EXE file do not have a visual reflection in the optimal settings of operating systems, including Windows, since their attributes have the "system" or "hidden" status.

The security issue of flash drives is still open. There are many effective methods that can significantly reduce the possibility of infection of a flash drive.

One of the options is to disable autoload, since some viruses are registered only when the system tries to open removable drive automatically. The absence of autorun in this case does not activate the virus and it will not "settle" on the flash drive. Another even more radical option is to create hidden files with a "zero" size. Usually, viruses that spread through flash drives create a hidden file with a specific name, which does not cause suspicion in the user.

For example *autorun.ini, autorun.inf, recycler*, etc. And if user creates files with such names in advance, then the virus will simply have nowhere to register and it will “unhook” you.

The third possible protection option is to prohibit writing to the drive root, and use a separate folder (folders) for writing files. However, this option is directly possible only for the NTFS file system.

If user does not take this problem seriously enough, then there is a risk of infecting user's computer with the picked up virus, which is a much more serious problem.

So, first of all, to protect the own computer from viruses that got on the flash drive, user must disable autorun on all drives connected to the computer.

5. Issues of vulnerability of FAT32 and NTFS file systems of flash drives against malicious software

The second aspect of computer security is the task of direct protection of the flash drive from infection. Since a flash card is actually a container for transferring files from one computer to another, we can say with confidence that a flash drive is infected only through an already infected computer, when files are transferred through this container.

To work with external drives, you can use one of two possible systems: FAT32 and NTFS. Let's take a closer look at these two systems.

As it is known, the use of the FAT32 system that is focused on working with various versions of Windows operating systems is standard for flash drives . A feature of this system is the limitation imposed on the file size - no more than 4 GB.

The FAT 32 system itself has low requirements, this is especially evident in the need to use a small amount of RAM, while the speed of this system as well as the efficiency of working with large files are very high. In addition, with this system, the wear of information carriers is also low, since the read-write heads of the hard disk are produced in fewer quantities.

The FAT 32 system also has disadvantages, they are manifested in the vulnerability of the security system from existing failures, in reducing the efficiency of working with huge files; setting a limit on the volume of files and corresponding sizes, the absence of normal information processing speeds when performing the fragmentation operation, slow synchronization when interacting with directories that store a significant amount of information [9].

Thus, a high level of safety of small files is most suitable for the FAT32 system, this is due to the fact that the system does not have unnecessary components, while a sufficiently high and productive speed of information processing and working with files prevails. The minimal risk of existing disc wear is also an advantage of this system.

Describing the characteristics of NTFS, it is worth to note that the advantages of this system are the relatively high speed of access to small information, the absence of boundaries and obstacles on the capacity of the data storage, the absence of the effect of data fragmentation on the file system, high safety of information and system structure, high performance characteristics during processing of the large information.

Talking about the shortcomings of the NTFS system, it is worth canceling that this system requires a much larger amount of RAM compared to the FAT32 system. And data fragmentation also makes it difficult for the system to work with medium-sized file directories. Moreover, compared to the FAT32 system, NTFS has a relatively slow performance speed [10].

During use of the NTFS system, we have a number of additional capabilities, since within the framework of the file system itself, security settings are provided, that is, we have the ability to simply prohibit writing to the root of our flash card and create a separate folder (or folders) where all data can be recorded.

Thus, we have two possible options: leave the media on the native FAT32 file system or switch to the NTFS file system. In the first case, it is necessary to use the specifics of the FAT32 system. The task is as follows - to prevent the virus from creation of the *autorun.inf* file on the USB flash drive. Previously, this problem has been solved quite simply - user had to create a directory with *AUTORUN.INF* name. and set its attributes as "Read only" and "Hidden". These steps have prevented the creation of a file with the same name. A modern virus can easily change the rights, delete a file and write a new one.

There is a slightly more sophisticated way that most viruses have not yet learned to bypass. The idea is as follows: create the *AUTORUN.INF* directory [11,12]. If the directory is not empty, then it can be deleted only by deleting all the content. And this is very simple, however, in the case when the directory contains files with names that are incorrect for FAT32, the task becomes impossible for modern viruses.

It is the principle of protection that forms the basis of our algorithm, the software implementation of which creates on the USB flash drive the *AUTORUN.INF* folder with invalid local UNC paths.

UNC – is a format for recording the path to a file located on a remote computer. It has the following

form: \\ *server* \ *share* \ *path*, where *server* is the name of the remote host. This option of accessing files can also be used for the local machine, in this case, instead of server user need to type "?" or «.», and specify the path to the file with the drive letter.

For example as follows: *\\?\C:\ folder\file.txt*. The idea is that using *UNC* paths and standard console commands, it is possible to create files even with names that are not allowed by the file system.

Let's create a simple bat-file, the algorithm of which creates an incorrect *autorun.inf* folder and several incorrect folders in it. Next, it creates a configuration file in the folder itself and places its' icon there (this icon will serve as an identifier). In other words it will be a folder that will look like an icon, and the path to this folder is written in the configuration file with hidden attributes. What does it give us? With this method, each time the flash drive is opened we can know whether our *autorun.inf* file has been changed or not (if it was changed than it means that the drive is infected).

The disadvantage of this method is that although the folder cannot be deleted, it is possible to rename it, and this gives attackers a chance to write their *autorun* to the flash drive. But if user insert his flash drive and did not see his icon than it means that a virus has settled on the flash drive with a 100% probability.

The next step is as follows. To protect the computer from an already infected USB flash drive, the autorun must be disabled. In our opinion, the most convenient way is to do it through the register [13].

Esentially this method replaces the contents of the *autorun.inf* file with a value from the registry, which is specially set as empty/invalid. This leads to the fact that if the *autorun.inf* file is registered on the disk, then it is perceived as empty.

In addition, for safety reasons the *autoplayhandlers* branch of the registry shall contain a prohibition on autorun of all file types (except double-click processing and context menu autorun). The last one means that a well-known pop-up window which offers to open a USB flash drive, listen to music, etc. will appear but no files will be able to start in automatic mode.

Another more radical option is to completely fill the USB flash drive with empty files. In other word it will not be possible to write a single byte of information directly to the USB flash drive.

If we need to write something to a USB flash drive, then this is done by a special program that will automatically write the file to the USB flash drive without deleting the information we need, and besides, it will check and, if necessary, fill the entire volume of the flash drive.

Considering the NTFS file system it shall be noted that one of the protection methods will be a software setting to prohibit: changing and writing files; deleting all files; create or copy files or folders to the root of the flash drive.

6. Findings

Corporate computer networks have become very important for analysts of the information market, since today there is a tendency for the growing development of information security threats. This is due to the proliferation of mobile banking and account management services, the availability of communication facilities (smartphones, communicators, tablets) and personal data, the accumulation of electronic resources, the widespread use of cloud computing, the desire of Russian companies to keep trade secrets and the reluctance to invite appropriate specialists and the need for revision and customization. universal "box" solutions.

Considering that flash drives are often used on computers of corporate computer networks, the following algorithm seems rational: format the specified drive; create a folder in the root, in which all operations on files and directories will be carried out in the future; deny everyone access to the root. If a flash drive is used more often on a home computer, then the home computer is chosen as the worker and full access is given to it. All others are banned from recording. In addition, by combining these two methods, you can create, for example, such a flash drive, for which access to the root is present only on the home computer, and on all others, it is allowed to use the folder that was previously created in the root.

References

[1] Ilin S 2020 Protection of USB flash-drives against viruses (In Rus.) http://www.windxp.com.ru/articles61.htm
[2] 2020 Viruses elimination "Kaspersky lab fan-club forum" (In Rus.) http://forum.kasperskyclub.ru/index.php?showtopic=8920)
[3] Bereza N V Current trends in the development of the global and Russian markets of information services *Inzhenerniy vestnik Dona* **2** URL: ivdon.ru/ru/magazine/archive/n2y2012/758/ (accessed: 22.12.2019)
[4] Vasilenko K A, Zolkin A L, Abramov N V and Kurganov D O 2020 Enterprise data processing networks: authentication and identification procedures *Infocommunication technologies* **18(1) (**Samara: Povolzhskiy State University of Telecommunications and Informatics) p 61-7
[5] Vasilenko K A, Zolkin A L, Abramov N V and Kurganov D O 2020 Features of flash drives information security *Infocommunication technologies* **18(2) (**Samara: Povolzhskiy State University of Telecommunications and Informatics) p 200-6
[6] Vasilenko K A, Zolkin A L, Abramov N V and Kurganov D O 2020 Malicious software in computer networks *Intenational Market Institute periodical* **2** (Samara: International market institute) p 108-11
[7] Morozova T, Akhmadeev R, Lehoux L, Yumashev A, Meshkova G and Lukiyanova M 2020 Crypto asset assessment models in financial reporting content *typologies Entrepreneurship and Sustainability Issues* **7(3)** 2196-212 doi: 10.9770/jesi.2020.7.3(49)
[8] Morozova T, Akhmadeev R, Lehoux L, Yumashev A, Meshkova G and Lukiyanova M 2020 Crypto asset assessment models in financial reporting content typologies *Entrepreneurship and Sustainability Issues* **7 (3)** 2196-212 doi: 10.9770/jesi.2020.7.3(49)
[9] Yumashev A V, Koneva E S, Borodina M A, Lipson D U and Nedosugova A B 2019 Electronic apps in assessing risk and monitoring of patients with arterial hypertension *Prensa Medica Argentina* **105(4)** 235-45
[10] Dzhangarov A I, Suleymanova M A and Zolkin A L 2020 Face recognition methods *IOP Conference Series: Materials Science and Engineering Krasnoyarsk Science and Technology City Hall of the Russian Union of Scientific and Engineering Associations* (Krasnoyarsk, Russia) 42046 DOI: org/10.1088/1757-899X/862/4/042046
[11] Tormozov V S, Zolkin A L and Vasilenko K A 2020 Setting training and testing of the long short-term memory neural network for pattern identification task *Industrial ACS and controllers* **3** (in Rus.) (M.: Scientific & Technical Literature Publishing House "Nauchtehlitizdat") p 52-7
[12] Faizullin R V and Hering Sh 2019 The model of data aggregation from clustered devices in the internet of things Intelectual *Intelligent systems in production* **17(4)** 156-62
[13] Zhukovskyy V, Zhukovska N, Vlasyuk A and Safonyk A 2019 Method of forensic analysis for compromising carrier-lock algorithm on 3G modem firmware *IEEE 2nd Ukraine Conference on Electrical and Computer Engineering UKRCON 2019 Proceeding* p 1179-82, 8879941