ACTA TEHNICA CORVINIENSIS – Bulletin of Engineering
Tome VII [2014] Fascicule 2 [April – June]
ISSN: 2067 – 3809

[1.] Adnan RAMAKIĆ, [2.] Zlatko BUNDALO

DATA PROTECTION IN MICROCOMPUTER SYSTEMS AND NETWORKS

[1.] University of Bihac, Bihac, BOSNIA & HERZEGOVINA
[2.] University of Banja Luka, Faculty of Electrical Engineering, Banja Luka, BOSNIA & HERZEGOVINA

Abstract: The possibilities and ways for data protection in microcomputer systems and their networks are considered and described in the paper. The overview of the most important threats and attacks on security of microcomputer systems and networks is given first. Then, the possibilities and ways for protection of those systems and data are described. Finally, the paper provides a detailed description of one actual practically implemented system of cryptographic protection of data on personal computers which represents the combination of hardware and software protection.
Keywords: microcomputer system, data protection, security of data and systems, attacks and threats on security, hardware protection, software protection, cryptography

INTRODUCTION

Safety or security od the microcomputer systems, information systems, software, generally speaking user data is one of the most important and the most present problems in computer technology and computer industry. The most important issue is how to secure the data from unauthorized use. Computers, dominantly microcomputer systems are used in almost all spheres of human life, from private to the business. Since existing computer systems, there are people who want to violate their security what at the end leads to damage and loss of user data. The first step in computer and network security is to formulate a realistic assessment of threats to the system. It should have a clear picture of the dangers in order to prepare defense [1].

Safety or security can be defined as the degree of protection from some danger, damage, loss, etc. In security and protection of microcomputer systems and network several principles are now established as the basic postulates:

- Security is a process, not a product, service or procedure but contains them with a lot of elements and measures which is carried out continuously.
- There is no absolute security or absolutely protected systems.
- With the different methods of protection it should have in mind the human factor with all the weaknesses [2].

ATTACKS AND THREATS ON SECURITY OF MICROCOMPUTER SYSTEMS & NETWORKS

Classification of attacks & threats to security

There are several threats to computer and information systems. According to the classification by NIST (National Institute of Standards and Technology) threats to computer and information systems can by divided into [3]: errors and failures, fraud and theft, sabotage by employees, loss of physical and infrastructural support, hackers, malicious software (malware) and threats to user privacy.

Types of attacks & threats to security

In order to adequately assess the security needs of an organization and pick an efficient way to select security products, policies, procedures and solutions, each manager in a company who is in charge of security, must have systematic way of defining requirements about security and one categorized approach, which ensures that these requirements are met. One approach is to consider the following aspects of information security and data [4]:

- Security attack - Any action that endangers the security of information.
- Security mechanism - The mechanism that detects an attack and that the system recovers from the attack.
- Security service - A service that enhances the security of the system for processing and transmitting data. Security service includes the use of one or more security mechanisms [4].

In fact, attacks may be defined as actions that are aimed at endangering the security of information and computer systems and networks. There are several kinds of attacks that can be classified into following four categories: interruption (an attack on availability), interception (an attack on confidentiality), modification (an attack on integrity) and fabrication (an attack on authenticity) [4].

Threats can be classified into passive and active. Passive does not directly affect the behavior of the system, while active can affect the behavior and functioning of the system. Passive attacks refer to eavesdropping and surveillance, tracking information, but without modification. Active attacks made changes to the content or information flow. Passive would be the disclosure of message content and traffic analysis. Active include masking, spoofing, replay - repeat network traffic, modification of message content and denial of service.

The most important attacks and threats are: Denial of service (DoS attack), Buffer overflow attack, Malicious programs (Malware) – Viruses, Worms, Trojan Horse, Spyware, Adware, Backdoor, Rootkit, Bootkit, Spoofing, Phishing, Sniffing and so on.

METHODS OF DATA PROTECTION IN MICROCOMPUTER SYSTEMS & NETWORKS

There are several approaches and division for methods of protection. According to some authors, there are four groups of protection methods that include: cryptographic methods, programming methods, organizational methods and physical methods [4]. Many authors consider this division outdated and use schemas based on ten domain of security defined by the organization (ISC)² (International Information Systems Security CertificationConsortium).

Among the most important methods of protection systems are included: cryptography, backup, antivirus solutions, antibootkit and antispyware, firewall, digital signature techniques, methods of protection against DoS attacks, the security services in the TCP/IP model (IPSec protocol, SSL/TLS protocol), IDS, IPS, SIEM systems, using the hardware key or dongle and so on.

DESCRIPTION OF PRACTICAL IMPLEMENTATION OF DATA PROTECTION SYSTEM ON PERSONAL COMPUTERS

Practical implementation of system for data protection on personal computers (PC) that is described here involves a program that performs encryption of user data. The program was developed in the Java programming language. This solution enables protection of any data (any document) from the computer using variety of cryptographic methods. It also uses hardware protection of the program from unauthorized use.

The hardware protection is implemented using USB memory device (stick) or USB flash drive. USB flash stick is very inexpensive, and allows storage of large quantity of data. The USB memory is used as a hardware key for the program. Therefore, the solution combines hardware and software protection. Program is intended for using on standard PC computers under Windows operating system. But, with some modifications it could be used on other operating systems. Its main advantages are simplicity, ease of use, low price and immediate protection level of user data, especially for applications that do not require a very high level of security. For conventional applications and less demanding users this solution represents simple, cheap and effective way of protection.

Using this solution any important file (document) on a PC can be encrypted. Thus obtained encrypted file is stored on PC and it can be sent over a network without concerning for its safety. It is impossible for someone else to unauthorized uses that file or any king of data encrypted with this program. Only after decryption process this data can be used.

The functioning of the program and its using is reflected in the following. When starting the program first appears welcome message which indicates that the program is running. After that, it is necessary to put USB flash stick into the USB port of a PC computer. For security reasons, it has no notes or indications for this step, but the user knows that it is a step that needs to be done. When the USB flash drive is in the USB port starting security checks defined in program. These checks include comparing XML files, one that is on the USB flash drive and another on a hidden location

on the computer. This file on computer is on secret location on HDD in order to prevent its locating and modification. Next check is existence of a hidden file (text file - .txt) on USB stick that is digitally signed, and elements of digital signature are at different locations on the USB flash stick and the computer. Very important is the way in which the program is connected to the USB flash stick and PC on which it is used. It is checking of serial number of USB flash stick and serial number of PC motherboard. In this way it is restricted using of program only with certain USB flash stick and on certain PC to protect program against unauthorized use. If any of these checks is not passed the program will not work and cannot be used. If all is well, if all checks passed, the next think is to input username and password. Passwords are stored using a hash function, using the SHA-1, with SALT supplement. Three wrong entries will result in deleting the XML file that is located in a hidden location on PC and thus all the checks will not be met and the program will no longer be operational. Implementation of the program on a PC can be accomplished in several ways. The first way is jar format on a computer. By clicking on it the program will run. Another way is to run executable file (.exe). Third, perhaps the most convenient way for the user is installation, which is identical to the standard installation program under Windows operating system. Clicking on the Install icon will open a box, and follow installation procedure.

After installation of the program its icon appears on the desktop as well as supporting documents in the Start menu. Clicking on the program icon it runs and begins with defined checks as previously described. If everything is correct, all the checks are met, it will open a login form as in Figure 1.

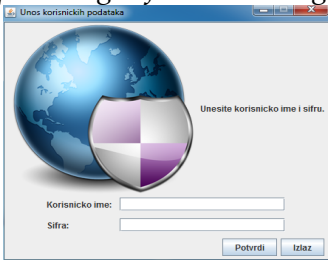

Figure 1. Login form

After entering correct user data (username and password) opens the main box as in Figure 2. Three incorrect inputs of user data result with overwriting one of XML file and program can't be used until program owner reinstall the program. Below is given code that is part of login method (loginMetoda) in class Login form, and after that the main box opens when entered the correct user data.

```
public Boolean login Metoda (String userTekst, String password) {
Boolean is Autorizovano = false;
String salted Password = SALT + password;
String hashed Password = generate Hash (salted Password);
String stored Password Hash = DB.get(userTekst);
If (hashedPassword.equals(storedPasswordHash)){
  isAutorizovano = true;
 }else{
  isAutorizovano = false;
 }
 return isAutorizovano;
}
```

The main dialog frame contains six buttons that allow selection of various methods for protection data. Follows a description of all methods.

Document protection

Document protection allows protection of any document from computer. It is used symmetric cryptography where the same key is used for encryption and decryption of data. The procedure includes selecting a file (document) for encrypt/decrypt from PC.

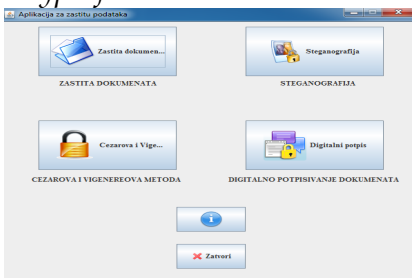

Figure 2. The main frame of the program

After selecting the file automatically is generated a key that is added to the document and then is necessary to enter desired name and extension under which document is stored on PC. In this way the document is protected and can be sent over a network or other form of distribution. If someone wishes to perform decryption the procedure is similar. It is necessary to select desired document from PC and then enter name and original extension of document, and key (the same that is used for encryption). In this way is performed decryption of document. The key is created

randomly in the range of numbers that cover the type Int. Any other key except the one with which is executed an encryption will result in a failed decryption. Figure 3 shows the framework for working with this part of the program.

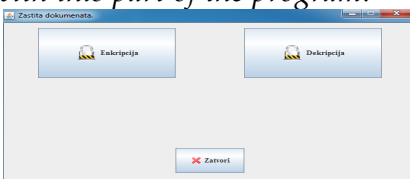

Figure 3. Document protection

Steganography

Great expansion of social networking and image sharing across the Internet, is led to idea of integration this type of protection. Idea is to hide a some text in an image. On a very simple way enters the text, loads an image in which want to hide the text, save it on PC, and procedure is done. Here it is used the principle of LSB (Least Significant Bit) where the least significant bit is substituted with bit of secret message.

Caesar Cipher and Vigenère Cipher

These two methods are widely used in the world of cryptography. They are integrated into the program for simplicity and fast encryption of short messages. Caesar cipher is one of the oldest methods where the letter of the text for encryption is changed with the appropriate letter. Vigenère cipher use series of Caesar ciphers based on key letters.

Digital signature

Digital signature is widely used in computer security. It is used for authentication of information. Its main purpose is the protection of author of the message, document or some other file from the possibility that someone else sends, published or otherwise. It ensures the authenticity, integrity, and secured recognition. Due to the increasing number of messages that are sent through the Internet, and often contain documents that are very important to the user, it is integrated into a program. Selecting this option in programs main box the user is in ability to generate and verifies digital signature of some document.

CONCLUSION

Safety or security of the computer, dominant microcomputer systems and information systems is one of the important issue of computer sciences. From this aspect, it is always necessary to carefully evaluate the relationship between investments in security and achieved effects. Here are analyzed the most important attacks and threats to the safety. Also are described best-known principles and methods of system protection, various aspects of protection and the most important methods of protection such as cryptography, firewall, digital signature techniques and security services in the TCP/IP model.

Presented practical example of protection implemented on PCs combines hardware and software protection. Software part of protection is realized in Java programming language. It combines different methods and performs cryptographic protection of desired documents from PC. As hardware part of protection is a standard USB flash stick. It contains information for specific user who is working with program. Without this USB flash stick the program cannot be used. Practically implemented system of protection is relatively simple and inexpensive, and allows obtaining medium level of protection. It uses a standard USB flash stick that is inexpensive and whose price is dropping. However, large capacity of USB flash stick allows to store large amount of data, related to a specific user, specific computer, computer network or any other. Described solution is flexible and can be easily customized for using on other operating systems with other methods of encryption.

REFERENCES

[1] *C. Easttom: „Computer security fundamentals“, Second edition, Pearson, 2012.*
[2] *http://de.napravisajt.com/web-server-administracija/sigurnosti-linux-mreza-i-servera.html*
[3] *„Sigurnosna politika“, CARNet CERT, Dokument CCERT-PUBDOC-2009-05-265 http://www.cert.hr/sites/default/files/CCERT-PUBDOC-2009-05-265.pdf*
[4] *http://mikroknjiga.rs/Knjige/SRSM/01_SRSM.pdf*

ACTA Technica CORVINIENSIS BULLETIN OF ENGINEERING
ISSN:2067-3809