Combined hardware and cryptographic user data protection in personal computer systems and networks

Adnan Ramakić[1], Zlatko Bundalo[2]

[1]University of Bihać, Bosnia and Herzegovina
[2] University of Banja Luka, Faculty of Electrical Engineering, Banja Luka, Bosnia and Herzegovina
adnan.ramakic@gmail.com, zbundalo@etfbl.net

Some methods for combined hardware and cryptographic protection of user data in personal computer systems and networks are described and considered in the paper. It is given an overview of the main types of cryptography, described ways of key distribution and the most known cryptographical algorithms at the beginning of the paper. Then the paper presents and describes practically implemented system of usage of cryptographic algorithms and protection of user data on the personal computer. It is solution that has been developed in Java programming language which combines hardware and software protection and can be also used in personal computer networks. It allows users to protect data by encrypting data files using one of cryptographic algorithms and protection of any user data from a computer using symmetric or asymmetric cryptography. The software is intended for use of only authorized users with appropriate user personal data.

One effective solution of practically implemented system which uses combined hardware and software to protect user data in personal computers (PC) and PC networks is presented in the paper. As the hardware protection is used a USB memory device as a hardware key which contains user data. Without the USB device access to the program and user data protection is impossible. The software is realized using Java programming language which is platform independent. The program can protect user data using symmetric and asymmetric cryptography algorithms as well as any type of data from PC of user. Also program gives option of digital signature, key generator and hash function. User's data are stored in database on PC. Administrator of the system performs manipulation of user's, storing user's data on USB memory device etc. Administrator can also add additional options to a program. In this way the program is specific only for one computer, one USB device and one user.

1 Introduction

Data security is one of the most important requirements and elements in modern computer systems. In implementation of any computer and information system one of the most important items is security or safety.

According to NIST (National Institute of Standards and Technology, The NIST Computer Security Handbook) computer security is defined as the protection provided in information system in order to achieve the applicable objectives of preserving the integrity, availability and confidentiality of information system resources (including hardware, software, firmware, information/ data and telecommunications). This term defines three key objectives which are the essence of computer security: confidentiality (confidentiality, privacy), integrity (data integrity, system integrity) and availability [1]. When it comes to security it should be noted that security is a process, not a product and there is no absolute security. Another important aspect when it comes to security is the human factor. It would be wrong to assume that all attacks are coming from the outside because a substantial part of the attacks comes inside.

It is needed to protect important data whether it is an ordinary user or a company. One effective solution is to develop and establish own user data protection system based on application of cryptographic methods.

2 Cryptography

The words "cryptography," "cryptology," and "cryptanalysis" are commonly interchanged. However, each has a slightly different meaning. The common beginning "crypt" comes from the Greek language for "hidden." The ending "grapy" refers to writing. So the first word in the list means "hidden writing" and generally refers to establishing a system for transmitting secret massages. The encrypted string is call a "cipher" or "ciphertext". Cryptanalysis refers to an analysis of hidden text, or ciphers, to expose what is hidden. Cryptology is made up of the two components "hidden" and "study" and refers to the study of hidden writings or secret massages [2-5]. Accordingly cryptography or cryptology is a modern scientific discipline based on applied mathematics. It is used in the banking industry (ATMs, Internet banking), computer communications (e.g. security and privacy on the Internet) and many other areas where privacy and data security is very important and necessary [3-5]. When it comes to the types of cryptography there are symmetric and asymmetric cryptography and a hybrid that combines the previous two.

2.1 Symmetric and asymmetric cryptograpy

The main characteristic of symmetric cryptography is the identity of cryptographic keys used in the encryption and decryption [3]. The most common practically used symmetric cryptography algorithms are AES, 3DES, Blowfish, Twofish, RC4, Cast5, IDEA [4]. With this type of cryptography the biggest problem is in the secure distribution of keys, i.e. how to deliver secret key to a recipient. The problems of secret key distribution are solved by Whitfield Diffie and Martin Hellman in 1976. introducing asymmetric cryptography [3].

Asymmetric cryptography uses a pair of keys, i.e. so called public and private key. The public key is publicly available information while the private key is kept secret and is only available to the owner of a pair of keys. Encryption is done using a public key while decryption is performed with the help of the private key. The most commonly used asymmetric cryptography algorithms are RSA (Rivest, Shamir and Adleman), Diffie-Hellman, DSS, and Elgamal [4].

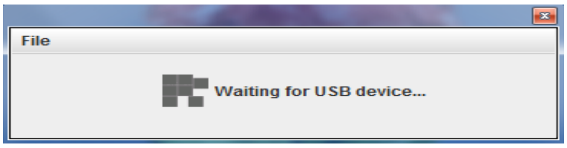
In addition to the two mentioned cryptographies there is a combination that is called hybrid cryptography. Hybrid cryptography involves the use of asymmetric and symmetric cryptography in which the algorithms of asymmetric cryptography are used for secure exchange of keys for symmetric cryptography. After exchanging keys further encryption is with one of symmetric cryptography algorithms. The main reason for such a combined use of cryptographic algorithms is to exploit the advantages of each of them, especially the fact that the symmetric cryptography is significantly faster than asymmetric, while asymmetric makes it easy to establish encrypted communications using public key [4].

3 Description of practically implemented system for user data protection

Practically has been realized solution that consists of hardware and software protection of user data that are stored on personal computers (PCs) and computer networks. Hardware protection is provided by a USB memory device as a hardware key. This USB device contains data specific for some specific user. Without USB device access to program and data protection is impossible. The program works only while USB device is in USB port of PC. When the program starts it checks for the USB device and if it is plugged in USB port it verifies user data on this device. If this data are correct and the user has permission to access the program this step of checking is done. After that the user still has to enter username and password. If this credentials are correct the user can use the program, otherwise no.

The program has been implemented using the Java programming language. The Java programming language is widely used. Its main advantage is the independence of the platform which is the main reason for its use in the realized system for data protection. Based on this, it easily can work and be used on various platforms such as Windows, Linux, Mac etc. The data about users (usernames and passwords) are stored in Microsoft SQL Server 2012 database. Instead of Microsoft SQL database it can also be used some other database as MySQL, Oracle, PostgreSQL etc. The progam can be easy adjusted to use some of this databases.

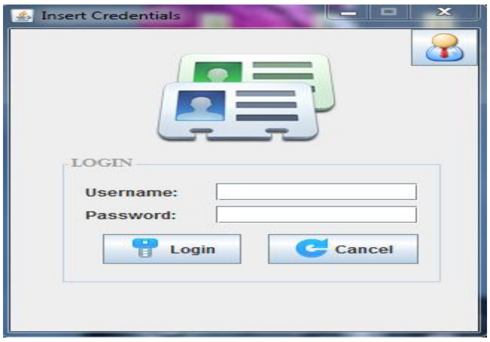
The Figure 1 shows the first frame after starting the program. This frame is showing until the USB device is inserted in the USB port of PC.



Waiting for USB device...

Fig. 1 Waiting for USB device

Once the USB memory device is inserted into the USB port the program starts verification of user data stored on this USB device. If verification is passed the user must still enter username and password. It is shown in Figure 2.

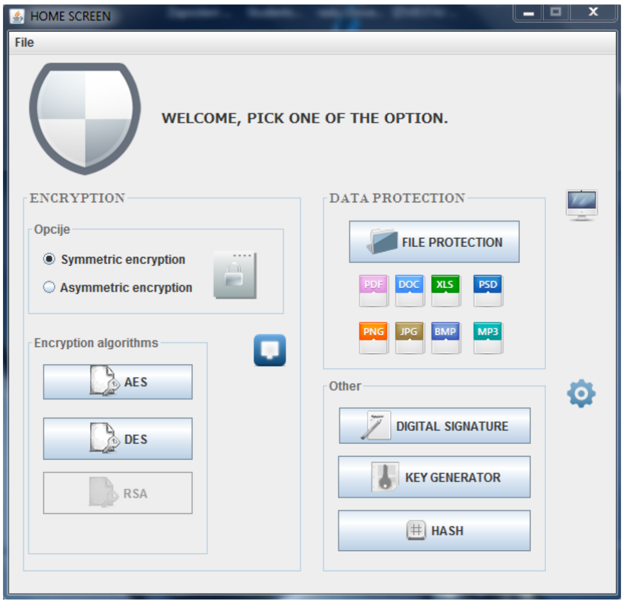


Username:

Password:

Fig 2. Login form

This user data are stored in database as mentioned before. After this step and successful verification of username and password the main frame of the program is shown. This is illustrated in Figure 3.



WELCOME, PICK ONE OF THE OPTION.

● Symmetric encryption

○ Asymmetric encryption

Fig 3. The main frame of the program

As Figure 3 shows the program can protect user data on different ways. The program offers possibilities for encryption of data using symmetric and asymmetric cryptography algorithms (AES, DES and RSA), protection of any files stored on PC, e.g. word documents, pdf documents, pictures, music (mp3 etc.), digital signatures of files and so on. File protection options allow 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. 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 stored on PC and also can be sent over a network or other form of distribution. If someone wishes to perform decryption the procedure is similar. This is illustrated in Figure 4.

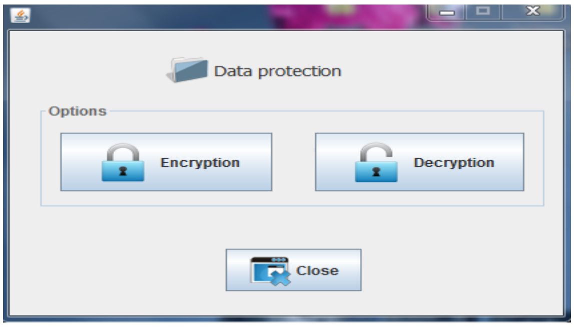


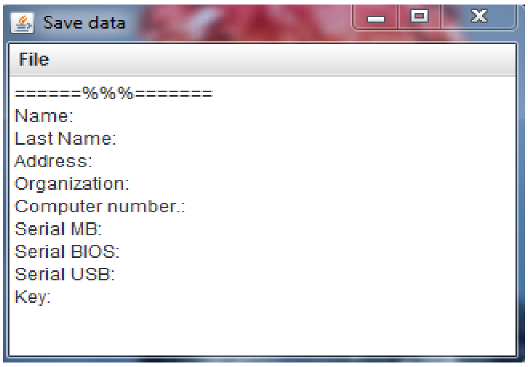
Fig. 4 Document protection

As mentioned before the program has also option of digital signature. The frame is similar to the frame shown in Figure 4. 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.

This program can also generate keys that can be used for various purposes and also compute a fixed hash for any file from computer using SHA-256. The procedure is similar to the procedure of File protection, only in this case there are options for creation and verification of digital signature instead encryption and descryption in previous case.

In this program there is also an administrator panel which allows administrators to manage with users and program usage. Administrator can add, delete, edit, view, search the users and write user data on USB device, adding some specific options to the program, e.g. addition security that the program when starting is checking and serial number of USB device, serial number of Motherboard of computer, BIOS number and so on. This is optional. The user data that are stored on USB memory devices are shown in Figure 5.

The user data are inserted from the Administrator and for them are calculated hash. This hash is stored on user's PC and USB device and program is checking this hash. Administrator also performs registration of users. It should be noted that the administrator's data (username and password) are not stored in the database as well as for other users but are placed in the program by using the hash function and the salt addition. The Figure 6. shows the Administrator panel.



======%%%=======
Name:
Last Name:
Address:
Organization:
Computer number.:
Serial MB:
Serial BIOS:
Serial USB:
Key:

Fig 5. User data

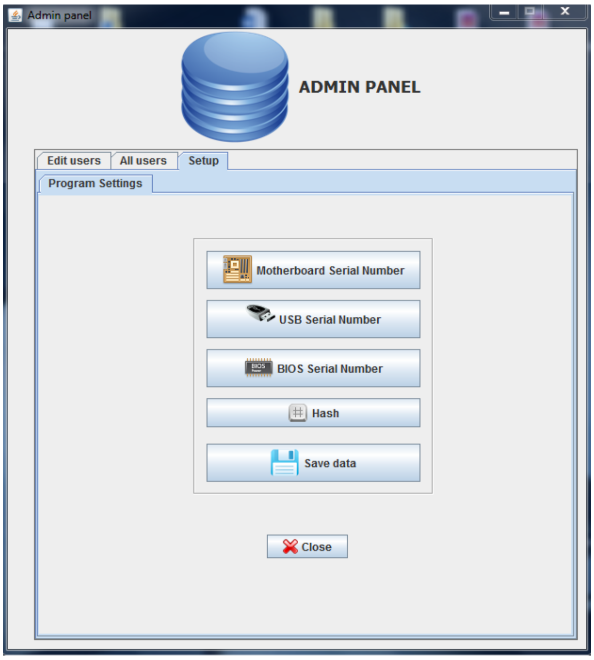


Fig 6. Administrator panel

As an illustration, below is shown a part of code for managing users.

```
public boolean spremiKorisnika() {
  boolean jeSpremljen = false;
try {
String sql = "INSERT INTO tblkorisnik (ime, prezime, adresa, korisIme, lozinka, godine) VALUES (?, ?, ?, ?, ?, ?)";
PreparedStatement ps = c.prepareStatement(sql);
ps.setString(1, ime);
ps.setString(2, prezime);
ps.setString(3, adresa);
ps.setString(4, korisIme);
ps.setString(5, lozinka);
ps.setString(6, godine);
if (!ps.execute()) {
 jeSpremljen = true; }
ps.close();
c.close();
} catch (Exception e) {
System.out.println("Error" + e.getMessage()); }
return jeSpremljen; }

public boolean pretraziKorisnike() {
 boolean jeNadjen = false;
 try {
 String sql = "SELECT *FROM tblkorisnik WHERE sifra =
?";
PreparedStatement ps = c.prepareStatement(sql);
ps.setInt(1, sifra);
ResultSet rs = ps.executeQuery();
if (rs.next()) {
 jeNadjen = true;
 sifra = rs.getInt(1);
ime = rs.getString(2);
 prezime = rs.getString(3);
 adresa = rs.getString(4);
 korisIme = rs.getString(5);
 lozinka = rs.getString(6); }
ps.close();
c.close(); } catch (Exception e) {
System.out.println("Error" + e.getMessage());
} return jeNadjen; }

public boolean obrisiKorisnika() {
boolean jeObrisan = false;
try {
String sql = "DELETE FROM tblkorisnik WHERE sifra = ?";
PreparedStatement ps = c.prepareStatement(sql);
ps.setInt(1, sifra);
if (!ps.execute()) {
jeObrisan = true; }
ps.close();
c.close(); } catch (Exception e) {
System.out.println("Error.The data are not deleted." +
e.getMessage()); }return jeObrisan; }

public boolean azurirajKorisnika() {
boolean jeAzuriran = false;
try {
String sql = "UPDATE tblkorisnik SET ime = ?, prezime = ?,
adresa = ?, korisIme = ?, lozinka = ?  WHERE sifra = ?";
PreparedStatement ps = c.prepareStatement(sql);
ps.setString(1, ime);
ps.setString(2, prezime);
ps.setString(3, adresa);
ps.setString(4, korisIme);
ps.setString(5, lozinka);
ps.setInt(6, sifra);
if (ps.execute()) {
jeAzuriran = true;}
ps.close(); c.close(); } catch (Exception e) {
System.out.println("Error. Edit is not possible. +
e.getMessage()); }return jeAzuriran;}
```

4 Conclusion

In times of fast Internet and data availability to every part of the globe exposure of the data to potential threats is very large. The question is how to protect important data. The solution is to develop and establish one own system for user data protection based on application of cryptographic methods.

In this paper is described one example of implemented system which uses hardware and software to protect user data in PCs and networks. As the hardware part of protection used is USB memory device key. Without the hardware key user data protection is impossible. The software part of protection is realized in Java programming language which is platform independent and easily can be used on Windows, Linux, and Mac. The program can protect user data using symmetric and asymmetric cryptography (AES, DES and RSA) and any type of data from user's PC, e.g. word documents, pdf documents, music and picture documents and so on. Program also provides option of digital signature, key generator and hash function. User's data are stored in database on PC. Iin this case it is Microsoft SQL Server 2012, but it also can be used databases MySQL, PostgreSQL and so on. Administrator of the system performs manipulation of user's, storing user's data on USB memory device key etc. Administrator can also add additional options to a program such as checking of serial number of USB device, motherboard of computer, BIOS and so on. In this way the program is specific only for one user, one computer, one USB device.

The realized and described user data protection system for PCs and PC networks is simple and cheep. But, it gives possibility for very good and effective data protection and appropriate protection for many practical applications depending on the user needs. The system has more different possibilities using different cryptographic algorithms for user data protection on PC systems and in PC networks. Using the developed data protection system it is possible to establish different ways for data protection for different user groups and for different purposes. It can be used different cryptographic algorithms for protection of data with different levels of importance for user. Also, it can be used different cryptographic algorithms for data protection for different user groups in PC networks. All this gives possibility to effectively and simple organize and establish needed level of data protection in PC systems and PC networks.

References

[1] W. Stallings, "Cryptography and network security principles and practice", Fifth edition, Prentice Hall, 2011.

[2] L. M. Batten, "Public Key Cryptography, Applications and Attacks" , John Wiley & Sons, Inc., Hoboken, New Jersey, 2013

[3] https://security.carnet.hr/vise-o-sigurnosti/enciklopedija/kriptografija/

[4] https://sigurnost.carnet.hr/assets/Dokumenti/Uvod-u-kriptografiju.pdf

[5] http://sigurnost.lss.hr/images/dokumenti/lss-pubdoc-2011-10-020.pdf