Journal of
Computer Science & Systems Biology

de Sampaio Ferreira, J Comput Sci Syst Biol 2016, 9:2
DOI: 10.4172/jcsb.1000218

Review Article Open Access

Proposal of a Cryptographic Application for Mobile Devices

Enza Rafaela de Sampaio Ferreira*

Faculty of Estacio, CEUT, Teresina, Piauí, Brazil

Abstract

The use of mobile devices is increasingly on the rise in our daily lives and many information is exchanged and stored on these devices. Thus, there are some risks that must be prevented as information leakage, installing malicious files one of the techniques used in the safety process is the encryption that through it, the cryptographic keys are created, ensuring a high level of protection the information. Soon this work comes with the proposal to show the development of an application to perform this security function, using the Blowfish algorithm, implemented on the Android platform, enabling the user data encryption of your devices.

Keywords: Mobile devices; Cryptographic application; Android platform; Data encryption; Blowfish algorithm

Introduction

The use of mobile devices is no longer a phenomenon considered new today, however the growing demand of using these devices is very large and is not likely to stop. Mobile devices most commonly used by people are mobile phones (cell phones, smartphones) due to the need that society imposes the individual be available 24 hours for contact [1]. With a simple mobile device, iPad, tablets and smartphone, you can connect a digital world, where several exchanges of information and data is increasing due to the large access the Internet made by these devices. A survey by GlobalWenIndex in 2014, in Brazil and around the world, showed the following statistics: points out that 80% of respondents have a smartphone and basically all of them owners have used the internet on their devices, and 75% used the last month service related to the survey date (www.correiobraziliense.com.br).

Mobile Computing

Concept

The notable expansion that has occurred in this decade in the areas of cellular communication, wireless local area networks and satellite services enable information and data can be accessed and used there anytime and anywhere. The current growth in the personal computer market, leads to realize that in a few years, hundreds of millions of people will have a laptop, palmtop or some kind of PDA. Whatever the type of mobile device, most of them should have the capacity to communicate with the fixed part of the network and other portable devices. In this computing environment is given the name of mobile computing or nomadic computing [2].

This computing emerges as a fourth revolution, preceded by the great centers of processing of the sixties data, the emergence of the terminals in the seventies and computer networks in the eighties. Considered a new paradigm, mobile computing allows users to access services regardless of where they are located, or change of location providing mobility. By reducing the cost of devices, mobile computing has become viable not only for the corporate segment, but for people in general.

Mobility

The main feature of mobile computing is mobility, taking advantage as the traditional computing works with more static. Then, the mobile computing main purpose would provide users with a computing environment, comprising a set of services comparable to those existing in a static system computers but allowing mobility [3]. So technology advances and become part of the life of the new generation and various professionals who are used these media to keep themselves informed in real time. Soon have high end appliances is a way to be connected with computerization, not to mention that they come with many features, together practicality that allows you to have the scope of information in your hands.

Some issues fairly well resolved in traditional computing remain open in mobile environments, such as problems ranging from channel speed, through interference of the environment and the mobile unit location until the battery life of this unit.

Safety

A recent research in Brazil, says the country is fourth in the world in smartphones, affirmation that allows you to have sense of proportion in which it reached the remarkable presence of such mobile devices in our country and the world [4]. However, this advance may pose a major security risk, since data and confidential information may be traveling on networks that are considered unsafe and could also turn out to be accessed by unauthorized persons. In addition to personal use (due to practicality and convenience), has increased the use by many companies for their employees, giving them the opportunity to access and manipulation of internal data via smartphones. This condition provided by the companies gives the employee greater freedom, and also the privilege flexibly access [5]. But all this ease comes followed by a major problem: the risks that the use of improper or even malicious way can bring to the end user.

The mobile users are aware that this is not a fully reliable service and we can also say that a portion lacks the necessary care in deciding which applications to install on your Android smartphone or a recognized antivirus. Currently, it can be said that one of the main security threats involving mobile devices lies in the user himself who inadvertently ends up clicking on malicious links and thereby installing malware on your device.

***Corresponding author:** Enza Rafaela de Sampaio Ferreira, Faculty of Estacio, CEUT, Teresina, Piauí, Brazil, E-mail: enzasampaiof@hotmail.com

Received January 22, 2016; **Accepted** February 12, 2016; **Published** February 16, 2016

Citation: de Sampaio Ferreira ER (2016) Proposal of a Cryptographic Application for Mobile Devices. J Comput Sci Syst Biol 9: 033-037. doi:10.4172/jcsb.1000218

Android

The volume of users accessing the Internet through mobile devices is so much that is almost surpassing the use of normal computers. And with great emphasis on mobile growth, appears Android.

Android is an open platform geared for mobile devices developed by Google and is currently maintained by the Open Handset Alliance (OHA). It was on November 5, 2007 the company made public the first Open Source development platform for mobile devices based on the Java platform with Linux OS.

According to IDC (International Data Corporation), Android is present in 85% of smartphones in more than 190 countries around the world, and its sales surpass the competitors, making it the most widely used platform in the world. Google says that every day more than one million users adhere to their devices to Android, both the advantages already mentioned, such as the ease of use of this operating system, which has its basis precisely designed to meet all types of users (www.andoidpro.com.br).

Encryption and Security on Mobile Devices

Information security is associated with attributes they wish to preserve data, systems, or any other resources that have some value to the individual. Broadly, information security involves requirements directed to the guarantee of origin, transit and use of information, in order to ensure all steps that make up their life cycle. Thus, the development of an application, security should not be treated as a process, but as part of the whole development. Practice safety comes down to providing confidentiality, integrity, availability and, according to some literature, authenticity and irreversibility.

As you increase the number of applications in the market, there is growing concern about the vulnerability and the occurrence of malicious attacks. Thus, it is motivating the implementation of techniques aimed at ensuring the information and the quality of services offered by applications, and help developers to incorporate such safety practices, are these: authenticity, confidentiality, integrity, availability and irrevocability.

Malicious attacks the mobile devices

According to a study conducted by Juniper Networks (American IT company), over 90% of malicious attacks on mobile targets the Android operating system. The study takes into account the period from March 2012 to March 2013, it recorded the amount of 276.259 malicious applications. An increase of 614% compared to the period of 12 months prior.

The study showed that approximately (73%) of all malware exploit vulnerabilities in mobile payments. Another survey, conducted by Kaspersky Lab, a company specializing in creating software that protects the malware, recorded that 99% of new mobile malware are made for Android. Most malware (63% in this case) try to invade the devices SMS system to try to confirm subscriptions and divert money from customers without the operator suspicious.

Encryption

Although the Android platform segregate applications stored on a device by assigning a UID (user-id), which ensures a certain level of protection in data sharing and access permissions, the use of techniques that add higher levels is necessary security [6]. The standard model of Android access may not be enough to protect the security risk and reliability, due to the possibility of a user has total system manipulation or in cases where the data is stored on external media such as SD cards, which are situations where the information may be accessible to any other device able to access this media.

Types cryptographic systems

A cryptographic system then is a set of techniques that allow us to make incomprehensible a given message, so that only the true recipient can decipher the same, thus obtaining the original text [6]. These techniques for preventing such attacks come in two forms, symmetric and asymmetric, which can be used alone or in combination. In the case of the keys (both symmetrical as asymmetrical), the security level is measured in number of bits, that is, the more bits are used, the harder it is to break the encryption by brute force. E.g., If we have a 10-bit encryption, there will only 2^{1o} (or 1024) protection keys, however, in using 64 bits, the number of possible keys reaches approximately 20 × 10 ^ 18 keys, a very high number to be broke.

The first invented cryptographic systems were symmetric encryption type, or secret key. Systems in which there is only one encryption key, and the encryption and decryption processes are symmetric [6]. Algorithms that use symmetric encryption have the advantage of being faster. Since one of its disadvantages is the use of the same key both to encrypt and to decrypt the data. Therefore, all parties that send and receive the data must know or have access to the encryption key. For example, by using symmetric encryption, an organization can be reasonably certain that only persons authorized to access the shared encryption key can decrypt the ciphertext.

Asymmetric or public-key encryption systems are systems in which the encryption process using a public key, but the decryption process uses a different key, said private key. These keys are known as a key pair. Asymmetric encryption is considered more secure than symmetric encryption because the key used to encrypt data is different from that used to decrypt them. Soon, because asymmetric encryption uses more complex algorithms than symmetric, and because asymmetric encryption uses a key pair, the encryption process is much slower compared to the symmetrical types [6].

Encryption algorithm blowfish

Blowfish is a symmetric key algorithm of free distribution, developed by Bruce Schneier in 1993, whose main characteristics the fact of having several key sizes, ranging from 32 to 448 bits [7]. It is a cryptosystem acceptable only in applications where the key does not change often, for example, a communication link or cipher data file. It is significantly faster than DES and IDEA when deployed on 32-bit microprocessors with large cache data such as Pentium and PowerPC.

This algorithm has been well accepted in many applications, it has not been studied much. To date it has not yet been notified no breach of it. In fact, what I have found was a bunch of keys that can be detected, although they cannot be broken. For these reasons, this algorithm is gaining popularity and growing.

The encryption is made in it through an interaction function 16. Blowfish has great efficiency with today's microprocessors. The cipher text is made in 64 or 128-bit block in which bits are not processed separately, but in 32-bit groups. In order to increase its efficiency, was chosen to use in the making of this algorithm for simple functions such as XOR, addition and modular multiplication.

The algorithm consists of two parts, which were the expansion of key and data encryption. The first is the transformation of key subkeys

in a total 4168 bits. The second consists of 16 stages and each of these is made a dependent permutation, dependent key and a replacement key and data. In addition to the simple functions already mentioned, the algorithm also works with cryptographic structures called "S-boxes" and "Network Feistel" [7].

Motion for an Encryption for Mobile Application

This work proposes an application for mobile devices based on the Android platform, with the function of performing data encryption and information available on the internal storage and SD card of the same. Therefore, seeing the need to ensure greater security the information in the device, the user will have the option to encrypt and decrypt, using a password, ensuring greater safety to the process.

For creating such a proposal had to be specified steps, such as implementing the Algortimo Blowfish in the Java programming language, application development on the Android platform and application prototype showing their specified features.

Implementation of the blowfish in java

The Blowfish encryption algorithm is the most widely used in Java programs. This is probably due mainly to the fact that patent free. The algorithm as has been shown in previous chapters uses keys that make its secure encryption. Thinking about the development of this proposal, it was used for the most important functions that will be encrypt and decrypt files on a mobile device. Watching the line of code passing below that shows how the algorithm was created, with all its classes and functions: From all classes created, will come to the main one being the formation of the program menu which defines and calls all the features ever created for algorithm execution as we shall see below (Figure 1).

Then, with the implementation of the algorithm can make the encryption or decryption of any file located on your computer, as shown Figure 2.

Designing and creating applications androids devices

Currently mobile devices are one of the fastest growing computer systems and with them the development of applications aimed at various segments, has accompanied this growth. But developing an application for these devices requires physical resources such as CPU, memory, screen, and environmental resources related to system usability. The development of such applications for devices has a more specific meaning is related to developed desktop.

To develop the project we used the Android SDK, which is a development tool that provides a set of APIs required to develop applications for the Android platform using the Java language.

Application prototype crypto+

The Crypto+ application, developed in the design of this work, is installed for proper testing on the mobile device Sony Xperia SP, 2G RAM, C5303 model, Android version 4.3 and version number 12.1.A.205. Just below follows the print screen, where the implementation of application functionality as Encrypt is shown, look for a file to be encrypted in the directory, enter the password and perform the action (Figure 3).

Figure 4 shows how the encryption is done in the Crypto+ application by following the steps below:

Conclusion

With the growth of mobile devices increases every day their consumption and consequently the exchange of information resulting in the need for more security for their use, one of the biggest disadvantages of mobile devices. Therefore, the development of this work came innovate an application within the mobile computing

```
118    public void menuCryptagem(Scanner sc)
119    {
120        System.out.println("password : ");
121        String password = sc.next();
122        System.out.println("Nome do ficheiro de entrada para ser criptado : ");
123        String entrada = sc.next();
124        System.out.println("Nome do ficheiro de saida : ");
125        String saida = sc.next();
126        encriptar(password, entrada, saida);
127     }
128    /***
129     * Método criação de menu de decriptografia para usuário
130     * @param sc - atributo de entrada para leitura do teclado
131     */
132     public void menuDeCryptagem(Scanner sc)
133    {
134        System.out.println("password : ");
135        String password = sc.next();
136        System.out.println("Nome do ficheiro de entrada para ser desencriptado: ");
137        String entrada = sc.next();
138        System.out.println("Nome do ficheiro de saida : ");
139        String saida = sc.next();
140        desencriptar(password, entrada, saida);
141        if(tempoDecriptar!=0){
142            long somaTempos = tempoEncriptar+tempoDecriptar;
143            long porcentagemTempoEncriptar = tempoEncriptar*100/somaTempos;
144            long porcentagemTempoDecriptar = tempoDecriptar*100/somaTempos;
145            System.out.println("Levou-se: "+somaTempos+" milissegundos nas duas operações");
146            System.out.println("% do tempo total para Encriptar: " + porcentagemTempoEncriptar);
147            System.out.println("% do tempo total para Decriptar: " + porcentagemTempoDecriptar);
```

Figure 1: Code Party Blowfish java in Eclipse.

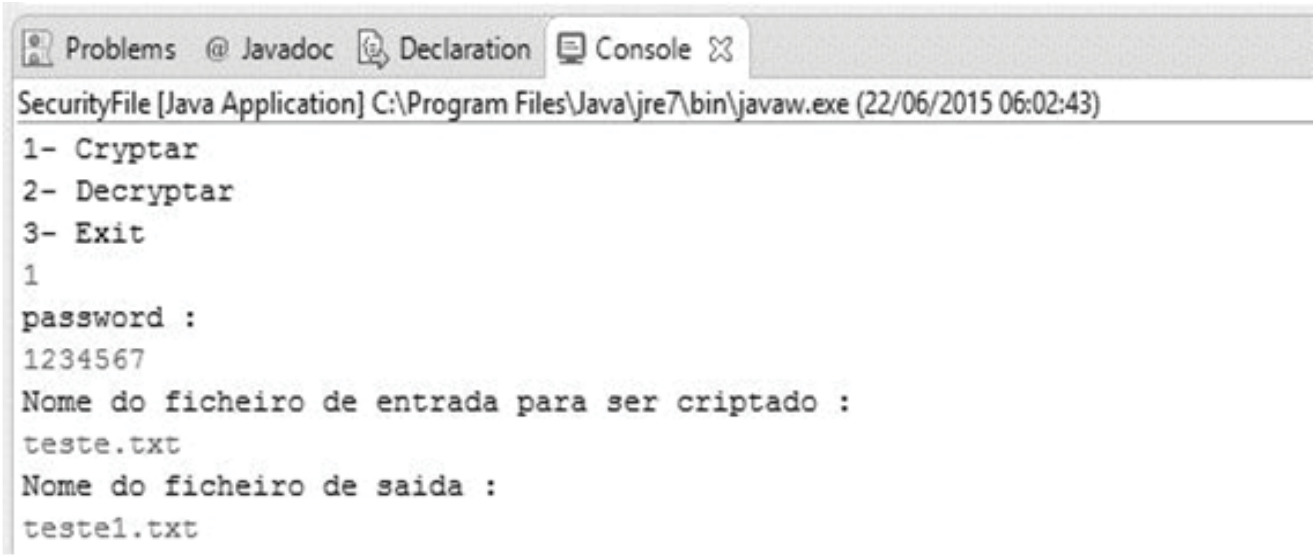

Figure 2: Code PartBlowfish java in Eclipse.

Figure 3: Encrypt Functionality in Crypto application+.

where the user could do the encryption of your files like photos, text documents, audio and video, such as use of passwords thus ensuring greater security for your information, since the means of security that the same has been shown in previous chapters is limited and once made, can never be undone.

Programming on the Android platform came as a key part of the creation process, which through the Android Studio software, can be implemented the algorithm and made application design creation, giving freedom of layout choices and the initial features thrown in the application crypto+, giving the opportunity to the users are encrypting your data with the use of passwords for each use and giving the option to keep or delete the working file, as well as the same are making the decryption, using the registered password, enabling the he keep or discard the file in question.

Anyway, you can conclude that the objectives were achieved considering the issue at hand, through a well-defined methodology, not ruling out the possibility of new resources for improvements in their functionality and also the implementation of new shares.

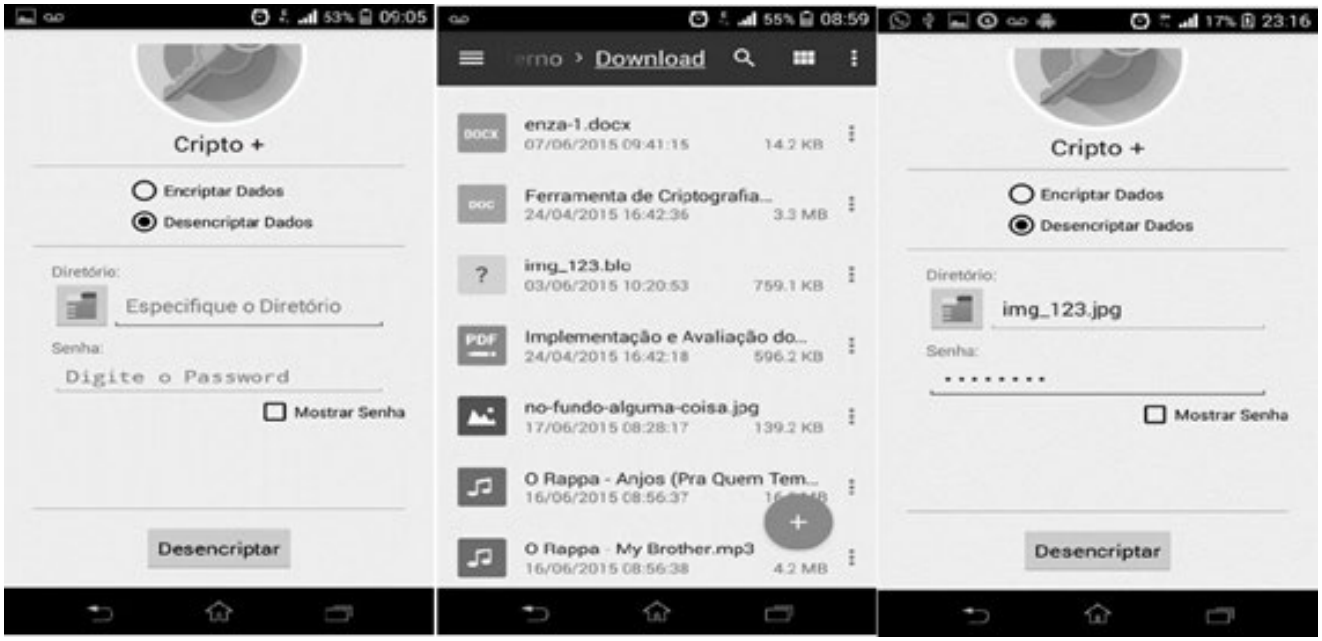

Figure 4: Functionality Decrypt in Crypto application+.

References

1. Moreira VF (2010) Encryption for mobile devices. Faculty of Technology of São José dos Campus.
2. Santana RC (2008) Mobile Computing, Historical Evolution. University of São Paulo Institute of mathematics and statistics.
3. Santos FRJ, Junior Manoel HB (2013) Mobile Devices as an eEducational Tool in Canindé-CE Municipality. Research Group in Applied Informatics Federal Institute of Education Science and Technology of Ceará - IFCE Caninde / EC, Brazil.
4. Alcântara CAA, Vieira ALN (2010) Mobile Technology : A Trend, A Reality. Docplayer .
5. Tonin GS (2012) Trends in Mobile Computing. USP, Institute of Mathematics and Statistics. Sao Paulo.
6. Torres TO (2014) Proposal Tool for Parallel Encryption. Teresina: CEUT.
7. Bugatti PH (2005) Monograph (Undergraduate Computer Science), Euripides University Center Marilia, Education Foundation Euripides Soares da Rocha, Marilia.