UDC 004.056.53

L.M. KUPERSHTEIN, O.P. VOYTOVYCH, V.A. KAPLUN, S.O. PROKOPCHUK
Vinnytsia National Technical University

THE DATABASE-ORIENTED APPROACH TO FILES PROTECTION IN ANDROID OPERATION SYSTEM

This article is dedicated to methods and means protection of information security threats which are specific for mobile systems. In the article main ways of information security violations in mobile devices with Android operation system (OS) are considered. There are also samples of existing methods and means of information securing from confidentiality and integrity violation threats. The complex approach on securing data files of the Android OS devices is proposed. This approach is oriented on database usage. Such approach allows you to save encrypted files in the database to save them from the confidentiality violations. It also provides you with the integrity safety by saving the hash-number of the file in the database. The protection system architecture from unauthorized file access of the Android OS was developed. The system consists of three main modules for applying data protection: hashing module and encryption module, each of them interacts with the database module. The hash module generates a hash value of the selected files and stores them in a database. Hash values need to further protect when remove the file to check whether the content has not been changed. Encryption module is intended to encrypt the content of files. Password for encryption key generation is stored in the database. After saving the encryption key, the bit array of file is also being stored in the database, and file is being deleted from the permanent memory of mobile device. During the decoding, password is being entered again, and if it equals to the password, which is saved in database, then file decrypts. Using the hash value, file integrity check is being performed and file is being recovered it in the same folder, which it has been removed from. The scheme of database securing based on the TOTP-service. The proposed approach will provide the stable protection of the data on the mobile devices with Android OS.

Keywords: database, data protection, information security threat, mobile device, Android OS.

Л.М. КУПЕРШТЕЙН, О.П. ВОЙТОВИЧ, В.А. КАПЛУН, С.О. ПРОКОПЧУК
Вінницький національний технічний університет

ПІДХІД ДО ЗАХИСТУ ФАЙЛІВ НА ОСНОВІ БАЗ ДАНИХ В ОПЕРАЦІЙНІЙ СИСТЕМІ ANDROID

Проаналізовано можливі загрози для файлів даних на мобільних пристроях під керуванням операційної системи Android. Проаналізовано методи та алгоритми шифрування та хешування даних для застосування їх щодо захисту даних в операційній системі Android. Розроблено програмне забезпечення для мобільних пристроїв під керуванням ОС Android, яке включає набір методів захисту даних, а саме хешування, шифрування та захист бази даних.

Ключові слова: база даних, захист даних, загроза інформаційній безпеці, мобільний пристрій, операційна система Android.

Introduction. The popularity of mobile operating systems is growing rapidly, as well as the number of devices which are using these operating systems. Today, smartphones and tablets perform a large number of tasks both in everyday life and in business. This is the implementation of money transactions, communication via VoIP telephony, geolocation determination, presentations viewing, creation and editing of various documents, photo and video shooting and many other tasks. However, with the increasing demand for mobile devices, the number of intruders who wants to access confidential information also increases. Therefore, the question of protecting communication devices based on mobile operating systems is currently very acute.

You need to be cautious when storing the information, because it can be stolen or altered by intruders. That is why the development and use of an effective system that will ensure reliable protection of information from threats of confidentiality and integrity is relevant.

Android OS security system. Android is the mobile operating system, which was ranked first in global sales in 2016 [1]. The usage of operating systems (OS) in percentage representation is shown in Fig. 1.

Android OS security system was being improved with each version. Almost every system update includes Security Patch, which eliminates certain vulnerabilities of the system. However, the security system underwent significant changes when the Android 6 Marshmallow OS [2] was released. In this version, the approach to granting of rights to applications has been changed. So, when installing the program from the application store, it became unnecessary to provide all the access rights that the application needs for the work, as it was before. Granting the application all permissions, the user very often did not understand what they are for.

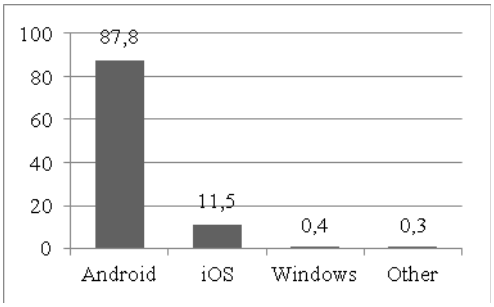

Fig. 1. Diagram of the OS usage on smartphones

As a result, some applications performed the functions of malicious software (malware), and the owner of the smartphone did not even know about it. Therefore, in the new version of the system, the user is authorized to grant epy rights to certain function when he wants to use a certain functionality of the program. This approach is called Runtime Permissions and it has clearly increased the security of the system. Now the user can prohibit the use of permissions, if he does not understand what they are for, and the developer must explain why the application needs certain permissions. In Fig. 2 the diagram of the different versions of the Android OS usage is shown.

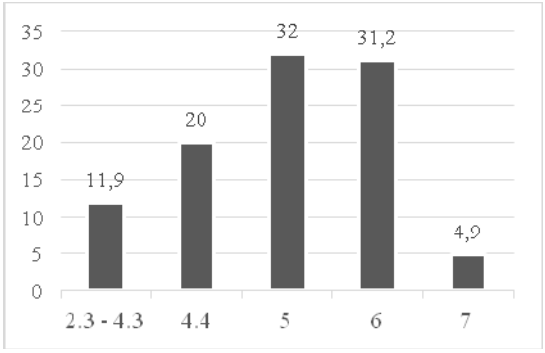

Fig. 2. Android OS versions usage

Fig. 2 is shown that now users are using not the latest versions of the OS. It means that a large part of them can easily be exposed to negative effects [3].

Attackers are creating a lot of malware to bypass the protection of mobile operating systems. We can conventionally distinguish the following classes of malicious software:

- SMS-Trojans (Android.SmsSend family). The purpose of these programs is to send SMS messages to paid numbers [4].
- Trojan programs of various functionalities working in superuser mode, which can perform any malicious actions, namely the removal and modification of data, the theft of confidential information, the performance of spam mailing, conducting network attacks as a bot and the like.
- Commercial spyware, which is used to monitor users. So, depending on the class and cost, you can meet them with the following functionality: interception of incoming and outgoing messages and calls, audio recording of the environment, tracking coordinates or collecting statistics data, including other programs data.
- Advertising modules, which developers use to monetize applications. In general, they do not pose a threat, the user moves on an advertise and developer receives money [5].

The most dangerous malware in our opinion is Trojan programs, as they can violate the integrity, confidentiality and availability of data on the mobile device [6].

The threats for data of mobile devices with Android OS appeared along with the appearance of the first mobile devices. Therefore, starting with the first versions of the OS, the development of software to protect against threats began.

The software for data protection in Android OS, which is currently available on the market, mainly provides such protection: data encryption, data hashing, setting passwords for the software of the mobile device, the usage of encrypted containers. Some software is protecting data only with the passwords, some only encrypts it. Also, there is software that creates encrypted storages, but they are being protected only with a password or are not being protected at all [7]. On the market there is a significant number of software data protection tools, among which can be distinguished such tools as: Andrognito, AppLock, KeepSafe, Vault, LUKS Manager, EDS Lite. The software provides the ability to encrypt and hash data, protect them with a password, hide data, create encrypted disks [8]. Software tools such as AppLock, KeepSafe and Vault are almost identical in functionality, they all protect software and data by setting a password. The best of these applications is the Vault, which, in addition to password protection, has a "false password" function for entangling an attacker and has a ‘hiding in the network’ function. But hiding the network opens up data for new threats.

Programs such as LUKS Manager and EDS Lite are hiding data in encrypted containers or disks. Both programs are using the AES algorithm for encryption [9]. EDS Lite has several advantages over LUKS Manager. Firstly, it is support for volumes created by the TrueCrypt utility. Considering the fact that TrueCrypt works on all major desktop platforms, this advantage becomes very significant. Secondly, this program doesn’t need Root access to work.

Protection system architecture. To protect files in the Android operating system the approach is offered, which consists of comprehensive protection, which includes file content encryption, file hashing, saving files in a secure database (DB). This approach will provide reliable protection of data files on a mobile device from the threats of integrity, availability and confidentiality. Data protection system architecture in the Android operating system is shown in Fig. 3.

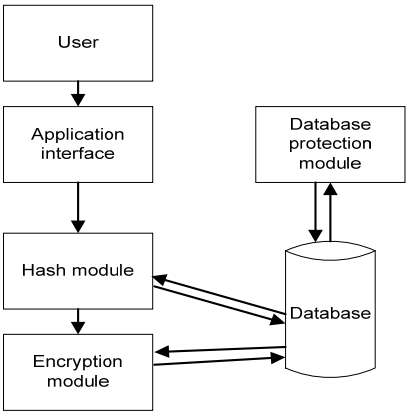

Fig. 3. Protection system architecture

The system consists of tree modules for applying data protection: hashing module, encryption module, each of them interacts with the database nodule. The hash module generates a hash value of the selected files and stores them in a database. Hash values need to further protect when remove the file to check whether the content has not been changed. Encryption module is intended to encrypt the content of files. Password for encryption key generation is stored in the database. After saving the encryption key, the bit array of file is also being stored in the base, and file is being deleted from the permanent memory of mobile device. During the decoding, password is being entered again, and if it equals to the password, which is saved in database, then file decrypts. Using the hash value, file integrity check is being performed and file is being recovered it in the same folder, which it has been removed from. Databases in Android OS are hidden from users without root access. If the mobile device has root permissions, you can view the DB using a special software. Therefore, to protect the database after recording data, database is being encrypted.

Hash-module. Hashing is a conversion of input data array of arbitrary length into the output bit string of fixed length. Such transformations are also called the function of hashing or hash-function [10].

Hashing is used in the following cases:

- the construction of associative arrays;
- searching for duplicates in data set series;
- construction of unique identifiers for data sets;
- calculation of data (signal) checksum to further error identifying in them (which happened accidentally or intentionally introduced) which are happening during the saving and/or transmission of data;
- while saving the passwords in protection systems in hash-code form (password recovery by the hash-code requires a function that is reversed in relation to the used hash-function);
- electronic signature development (in practice, a “hash-image” of the message, not the message itself is often being signed).

The best-known hashing algorithms are the following [10, 11]: JH, HAVAL, Keccak, MD5, SHA-3.

The data, which is stored in the permanent memory of the mobile device, can not only be stolen, but can be also modified. In order to know about the change of file content by extraneous persons, hash-values of files can be generated. SHA3 is the most reliable algorithm. It can be used to create hash-functions with arbitrary length of output, stream cypher, key generation function from password, authentication codes of messages, crypto-persistent generator of pseudo-random numbers with entropy pumping from an external source and with internal state deleting [12].

Following actions in the hash module are performed:

- the file is being chosen;
- file content gets converted into a bit array;
- hash value based on the bit file array is generated;
- hash-value is converted from decimal to hexadecimal;
- obtained hexadecimal hash-value is saved to the database table.

The hash value is being generated to generate it again when protection is removed from the file, and compare it with the one stored in the database, to know whether changes were made to the contents of the file.

Feedback process requires the following actions:

- from the list of protected files in the database, the one which is necessary to remove protection from is chosen;
- file content is transformed into a bit array;
- based on a bit array, the hash-value is generated;
- hash-value is converted from decimal to hexadecimal;
- obtained hexadecimal hash-value is compared with the saved in the database one.

Thus, the module allows a mobile user to check the data integrity.

Crypto-module. To construct the encryption module, usage of symmetrical encryption is offered, because asymmetrical encryption is designed to encrypt data, which is transmitted between users. On mobile device a very

large number of files will not be encrypted, so the worry for the safety of a large amount of keys is not necessary.

The most famous and reliable symmetric encryption algorithms are AES and DES. DES algorithm uses a key with 56-bit length for encryption. AES uses a keys with length of 128/192/256/512-bit [13]. AES algorithm is fastest and it uses some of the most persistent keys. Therefore, AES is chosen to implement encryption module.

Encryption process in crypto-module consists of the following steps:

- file for encryption is chosen;
- password with length of 8 to 32 characters is entered;
- encryption key, based on the entered password is generated;
- converting the generated key in a secret key;
- file content is transformed into a bit array;
- bit array is encrypted using the secret key;
- key and the encrypted bit array are being saved in the database;
- file is being deleted from the permanent memory of the mobile device.

Thus, the encrypted file cannot be found using standard file manager.

Decryption process in crypto-module consists of the following steps:

- file that needs to be decrypted is chosen from the list of protected files;
- password for encryption is entered;
- entered password is compared with one which is stored in the database. If the passwords are not equal, the process is stopped, if they are the same, then the transition to the next step will be performed;
- encryption key, based on the entered password is generated;
- converting the generated key in a secret key;
- decrypting the massive using the secret key;
- writing the decrypted massive to new file and saving it in the folder which it was deleted from.

DB-module. It is necessary to use the database for effective functioning of the data protection system. It is necessary because we must hide encrypted files in a byte array, hash values of the files and the encryption password in it. Result of file encryption is being saved into the database and the file is being deleted from the place where he was located in memory. This will protect your data files from mobile threats such as stealing and modification of information, denial of access to the database, removing of information [14].

AES encryption algorithm is used to protect the database [15]. Encryption key is generated by the BKDF2 (Password-Based Key Derivation Function) algorithm, which is the standard for key-based password formation [16].

Database protection scheme shown in Fig. 4. TOTP-service interacts with the main components of the program. TOTP (Time-based One Time Password Algorithm) is sufficiently resistant to cryptographic attacks one-step authentication algorithm that is used to generate one-time time-based passwords [17]. Wherein there is not sustainable value, but certain period of time is being used, which is difficult to find out if there is no source codes of the program.

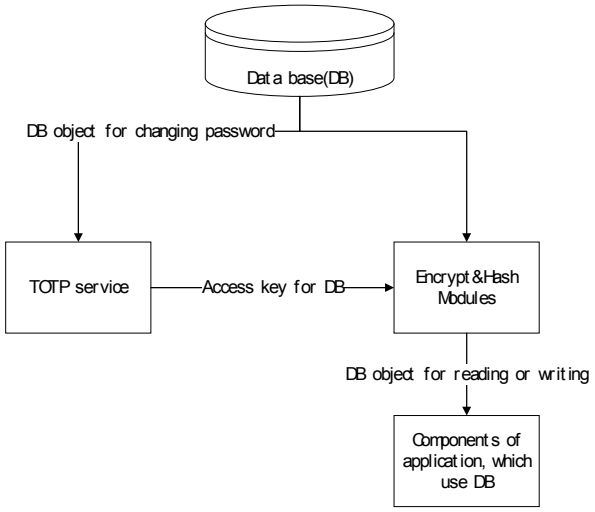

Fig. 4. Scheme of database protection

TOTP-service is connecting to the necessary components using binding mechanism [18]. This approach enables communication with service simultaneously, which in our case is very critical and important. After all, if you use asynchronous request, it may cause the conflict situation. For instance, service changes password to the database, along with the password change, database access password will be sent asynchronously.

A service that is always running in the background was implemented in database module. This service will generate a time-based access password for the database. When the program runs, sometimes password will change and application continues its work with newest access key. As a result, the database password will be changed and it will be very difficult for attacker to gain access to the database.

Implementation of the system. Using the Android studio was developed an application based on the

architecture of protection system. Android Studio is an integrated development environment (IDE) for Android. Android Studio replaces the ADT plugin for Eclipse platform. The environment was built on the source codes of IntelliJ IDEA Community Edition product [19]. In addition, the modern technology of reactive programming RxJava, which significantly increased the performance of the system and its flexibility, was used. Android Clean Architecture was used as the basic system architecture. This approach has improved the quality of code and provided the quick updates. The application uses three main classes: DBHelper, Secur and Unsecur. DBHelper is designed to work with the database records, for reading and clearing. In Secur class Secur all methods designed to protect files are placed, and Unsecur class stores the methods for protection removing. SQLCipher library used for database encryption. This library encrypts the database file and provides access to it only when you enter the correct key.

Summary. The market of mobile technologies was analyzed. The main types of malicious software for Android were defined. Application architecture and complex application, which improves the data protection, was developed. It consists of encryption module, hashing module and database module for data security improving in Android OS. This approach can significantly reduce the chance of threats of violations such as availability, integrity and confidentiality of a data.

References

1. “iPhone lost market share to Android in every major market” (25/11/2017) http://uk.businessinsider.com/apple-ios-v-android-market-share-2016-1.

2. “Malware alert! Android virus steals personal data including passwords” (25/11/2017) http://blogs.quickheal.com/malware-alert-android-virus-steals-personal-data-including-passwords.

3. “Vulnerability Statistics” (25/11/2017) http://www.cvedetails.com/product/19997/GoogleAndroid.html?vendor_id=1224.

4. “Anatomy of an Android sms virus” (25/11/2017) https://nakedsecurity.sophos.com/2014/06/29/anatomy-of-an-android-sms-virus-watch-out-for-text-messages-even-from-your-friends.

5. “Android ADB 8.0” (25/11/2017) Available: https://wincmd.ru/plugring/android _adb.html.

6. Voitovych O.P., Hurskyi M.V., Snigovyy D.S., Kupershtein L.M. Monitoring tool for Android operating system. Visnyk Khmelnytskoho natsionalnoho universytetu. Technical sciences. Khmelnitsky. − 2017. − Vol. 249, Iss 3. pp. 236-242.

7. “Top 5 Android security” (25/11/2017) http://www.digitaltrends.com/ mobile /top-android-security-apps.

8. “10 best security app for Android” (25/11/2017) http://www.androi dauthority.com/best-security-apps-android-687799.

9. Bellarel M. Introduction to Modern Cryptography / M. Bellarel, P. Rogaway. – California, 2005 (25/11/2017) https://www.nist.gov/news-events/news/2015/08/nist-releases-sha-3-cryptographic-hash-standard.

10. Konheim A. G. Heshing in computer science / A.G. Konheim. -New Jersey: Willey, 2010. – 406 p.

11. NIST. Plan for new cryptographic hash functions (25/11/2017) http://www.nist.gov/hash-function

12. “SHA-3” (25/11/2017) https://www.nist.gov/news-events/news/2015/08/nist-releases-sha-3-cryptographic-hash-standard.

13. Mahajan P. A study of encryption algorithms AES, DES and RSA for security / P. Mahajan, A. Sachdeva // Global journal of computer science and technology network, web & security. − 2013. – Vol. 13, Iss. 15 (25/11/2017) https://pdfs.semanticscholar.org/2878/4ff450d810ea2340bc0b059b74a2b601131b.pdf

14. Voitovych O. Investigation of simple Denial-of-Service attacks / O. Voitovych, Y. Baryshev, E. Kolibabchuk and L. Kupershtein // 2016 Third International Scientific-Practical Conference “Problems of Infocommunications Science and Technology (PIC S&T)”, Kharkiv, Ukraine, 2016, pp. 145-148.

15. Voitovych O. P. SQL injection prevention system / O.P.Voitovych, O.S.Yuvkovetskyi, L.M.Kupershtein // 2016 International Conference “Radio Electronics & Info Communications (UkrMiCo)”, Kiev, 2016, pp. 1-4.

16. “SQLCipher: Encrypted Database” (25/11/2017) https://guardianproject.info/code/sqlcipher.

17. Password-Based Cryptograpy Standard. – Camridge: RSA Laboratories, 2012. – 33 p. (25/11/2017) https://ru.scribd.com/document/268097645/PKCS-05-v2-1-Password-Based-Cryptography-Standard.

18. “TOTP: Time-Based One-Time Password Algorithm” (25/11/2017) https://tools.ietf.org/html rfc6238 .

19. “Android Studio” (25/11/2017) https://developer.android.com/studio/index.html.

Рецензія/Peer review : 9.05.2017 р. Надрукована/Printed :27.01.2018 р.
Рецензент: д.т.н., проф. Мартинюк Т.Б.