PROBLEMS WITH INFORMATION SECURITY ON MOBILE DEVICES

Veselka Stoyanova, PhD

National Military University “Vasil Levski”, Artillery, AD and CIS faculty, Shumen

veselka_tr@nvu.bg

Abstract: *The current report takes a look at possible problems with information security on mobile devices, analyzes them and suggests some of the possible solutions. We're taking a look at problems with transfering information between mobile devices and how this information can be received without letting people outside the conversation get access to it*

Keywords: EDUCATION, COMPUTER GRAPHICS, IMAGE

1. *Introduction.*

With the advances in technologies and mobility of users, many of us carry with us devices, which a few decades ago existed only in science-fiction books, and only a few years ago, nobody thought that they will offer the functionality that the common user uses today.

In connection with this ubiquitous and necessary mobility comes the question, are the mobile devices and data of their users secure. There are risks of different nature about the security of information on mobile devices.

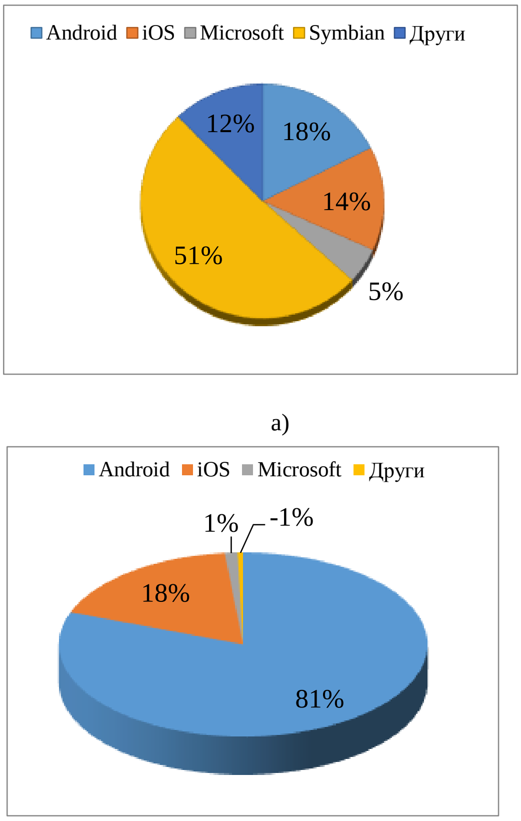
Providing information security is linked with identifying threats and pinpointing the possible solutions for providing informational security of data and apps of users in a given environment, it's necessary to aim the efforts of dealing with the problems in different categories

Given the fast growth of the smartphone market, mobile software developers suggest many applications, which let you hide information in different concealing objects [2], and a part of them are free to use. We must note the fact that owners of Android devices for 2015 are 17,2% of the total market share, for iOS being 14,1%, Microsoft at 4,9%, and Symbian was a complete monopoly for that period with it's 50,2% of the smartphone market. In 2017 things look a little different, Android has taken the lead with it's record 80,7%, iOS having 17,7%, Microsoft at 1,1%, other OS at 0,5%, and Symbian is no longer available (figure 1).

1. *Model of measuring security of information*

All of these facts lead to the conclusion that we're in the era of smartphones and the conveniences they offer, the transfer of confidential messages will be supported and the whole process of communication and data delivery will be accelerated. The whole process of secret communication will be unnoticeable and natural, and dangerous in terms of data leak security due to the fact that it'll be an almost instant process of just one touch on the screen.

The interesting part is the analysis of security of data shared in the computing cloud. Cloud technologies have a lot of pros as to be considered as the best solution by many IT organisations, the biggest of which is being able to pay only for the used resources therefore reducing costs or even eliminate the investments in IT structure. According to organisations like “Cloud Security Alliance (CSA), Cloud Computing Information Assurance Framework (ENISA), Information Security Forum (ISF) etc. part of the major threats to informational security of users in the cloud space are connected to: user authorization, data ciphering, physical safety of hardware, malicious traffic etc. [3].



a)

b)

fig. 1. Market share of devices used in a) 2015 and b) 2017

The Bulgarian Institute for Standardization suggest multiple standards for informational security. On figure 2, you can see a model of measuring security of information [1].

Using the model of measuring security of information, you can define the stages, through which you have to go when securing information, which are the informational necessities and methods of measuring. Measuring results influence the process of controlling the security of information and for the effectiveness of defence be analysed. The model thus presented is relative to and the problem connected to information security on mobile devices.

There are many measures and solutions which are recommended to be used and applied, and not to rely on chance when securing confidential data, because in that case we can't talk about security or prevention of malicious users.

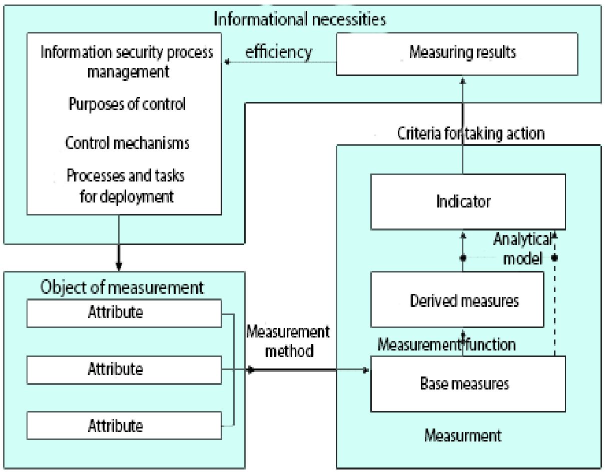


fig.2. Model of measuring security of information [1]

3. *Problems with the safety of information on mobile devices.*

Problems with the safety of information on mobile devices that may occur, can be different, like:

- Physical safety of devices and data;
- Authorization of user access to data;
- Separation of user data;
- Cyphering data and connections;
- Not using Fire Wall;
- Consuming fake service;
- When carrying personal belongings;
- Internet of Things, (IoT).

Physical safety and authorization of is of great importance to the safety of information. When using mobile devices increasingly big amounts of information are being concentrated on a small physical space. The information can be personal as well as or officers. Some standard measures which would prevent the possibility of information being received by unauthorized users are the biometric identification, by securing the screen and applications with passwords and codes, regular check of the device location, surveillance cameras etc.

Cyphering the data. It's suggested to cypher the communication channels and data. Usually when exchanging data over the web, internet providers can provide you with access to the data with a secure protocol HTTPS. When controlling data however, a problem may occur when the same key is used to cypher every account. This way the unauthorized spectator, getting access to the key could gain access to all the data too. A problem when cyphering data is the distribution of the keys. The most popular solution the provides cyphering of data and key management of keys is Trend Micro Secure Cloud, an upgrade of OTFE etc. in which a special technology is used that allows servers to be checked, to control access to locked data, to remove unnecessary data without a chance to be restored.

Bring Your Own Device, (BYOD).

The BYOD [7] trend is a threat which is connected with the security of official data and it's leak, the emergence of the possibility of company espionage and getting access to data. The risks for informational security of organizations grows with employees carrying personal smartphones, tablets, laptops etc. This fact occurs because of the possibility of not good enough management of the device, external manipulation of the software, installing of not well enough tested and unreliable for business applications.

The problems connected with the safety of information on mobile devices is conditional to the ability of using a different operating system. The question about the actual to this moment operating systems looks like this:

Security in Android OS:

The base of the Android platform is a Linux core, which is responsible for the drivers of the devices, for access to resources, for managing the electro-consumption and for other OS tasks [6].

It is accepted to divide the architecture of Android into four layers:

- Core layer (Linux Kernel);
- Implementation environment and library layer;
- Working framework of applications;
- Applications layer;

Android uses the ability of Linux which doesn't allow root access to the operating system and it is the basis of the security of the Android OS. When installing the device, every application gets a unique user ID (UID) and a group ID (GID) [5]. UID is used for identifying an application for the whole period of it being installed on the device.

Android is the preferred operating system of hacker attacks. Usually the infection is caused by malicious applications, which are offered in online stores.

In this OS while installing a given application it's permissions gets reviewed. All permissions, which are required by the application must be declared. Permissions represent access, which the application requires from the operation system so it can function properly. During the installation, the user can see a list of all permissions which are required by the application and can make an informed choice about the installation. A given application may require a permission to track your location by GPS, internet access, your contacts, developer tools, phone call register etc.

All Android applications are self-signed which means it's not required to sign the applications using a certifying body. The signature of the application represents the author.

Security is the iOS operating system.

iOS is basically a version of Apple OS with specific characteristics linked with control of the devices for which it is designed. It's presented for the first time in 2007. [4] as iPhone OS – the operating system of Apples' mobile devices. It's later renamed to iOS, to underline the fact that it works on other Apple devices too. OS X and iOS are based on NeXTSTEP OS.

The model of security on iOS includes four layers:

- - Security of the device;
- - Security of data;
- - Security of the network;
- - Security of applications;

The security of the device aims to guarantee that a given device cannot be used by an unauthorized individual. The most common method of locking is with a PIN code or password. In the version for corporate users of iOS you are given the opportunity to set the minimal length, number of symbols to be used in the password and password history. Users can set extra settings to make the device automatically erase itself if a wrong password is entered too many times [10].

Security of applications is guaranteed using the Store, by starting them in the so-called "sandbox". The apps started in the "sandbox" cannot gain access to other apps or their data, neither can they gain access to system files or other resources. The size of the memory and processing time that can be used by the app are being limited and so is the access to files outside the app folder.

In addition to limiting the resources of a given device, to which an app can get access, Apple has turned on application signature to keep an eye on the binary code allowed to be started on top of it. For an app to be allowed to run on iOS, it has to be signed by Apple or have a certificate given by Apple.

Microsoft Windows operating system

Windows Phone is the successor of Windows Mobile. The most sold version of Windows Phone is Windows Phone 8.1. Windows

Phone 8.1 got released on the market in July 2014 [8]. OC Windows Phone 8.1 by it's characteristics is comparable to the latest versions of iOS and Android OS, supports multi-tasking with it's personal cloud service, online store and Twitter integration. The built-in browser is Internet Explorer 11. The successor of Windows Phone 8.1 is Windows 10 Mobile [9], which came in use on chosen Lumia series smartphones in February 2015. Windows Phone is designed to be secure. A lot of the security features are turned on by default. An example is the apps that can be downloaded from the Store, which are tested by Microsoft and cyphered to prevent the installation of dangerous software by mistake.

4. Conclusion

Mobile devices may look harmless when using them as regular phones, as access to news, social medias or for relaxation in the form of games or entertainment apps. In reality mobile devices are under a constant threat of personal data and information, in the form of different kinds of inquiries for access to the data and receiving permissions to use them, are threatened by receiving malicious software or even spy programs. Developers of the leading mobile operating systems understand the importance of the security of personal data and information, and set apart a large resource for development and improvement of the mechanisms of securing information on mobile devices.

Some suggestions that could be useful for security of information on mobile devices are:

- Locking the screen with a Pin code or password;
- Avoiding remote services like: remote lock, remote format, GPS localization etc.
- Encrypting data when passing it through open channels;
- Using anti-virus software which battle malicious software and to avoid problems with banking, paying bills and finance management.
- Using safe Wi-Fi networks and to avoid unreliable ones like in cafes, airports or other points of connection that can allow access to personal data.
- Updating the OS, the apps used by the users and all other programs.
- Regularly making back-up copies of the data.

Reference:

1. ISO/IEC 27004:2012 pp. 15.
2. Green T., Network World, http://www.networkworld.com/article/2291708/security/130370-15- FREE-steganography-apps-for-mobile-devices.html#slide1 Retrieved 08.03.2019г.
3. Halachev P., Problems with security of cloud services, E-Journal Mathematical Modeling and Computer Simulation Volume II, Number 6, Year 2014.
4. Honan, M. (January 9, 2007). "Apple unveils iPhone". Macworld. Retrieved January 16, 2019.
5. Savov, Vlad (January 28, 2014). "Chrome Apps are coming to iOS and Android". The Verge. Retrieved February 2, 2014.
6. Smartphone users worldwide 2014-2019, http://www.statista.com/
7. http://newhorizons.bg/blog/2014/01/information-security-threats-2014/
8. "Windows Phone 8.1 now available to developers". April 14, 2014. Retrieved January 14, 2019.
9. "Windows 10 won't launch on phones this summer". The Verge. Vox Media. Retrieved January 2, 2019.
10. Slavyanov, Kr., AN ALGORITHM OF FUZZY INFERENCE SYSTEM FOR HUMAN RESOURCES SELECTION TOOLS, SOCIETY. INTEGRATION. EDUCATION, Proceedings of the International Scientific Conference. Volume V,May 25-th-26th, 2018. 445-454 ISSN 1691-5887