ANALYSIS OF SECURITY IN MOBILE COMMUNICATION SYSTEMS

[1]Jumakulov F.K., [2]Rayimov F.T, [3]Rahimov J.N, [4]Yusupov Y.T.

[1,2] Master's degree students of the department of "Radio-technical installations and systems" of Tashkent state technical university

[3]Teacher at the department of "Radio-technical installations and systems" of Tashkent state technical university

[4]Associate professor at the department of "Radio-technical installations and systems" of Tashkent state technical university

https://doi.org/10.5281/zenodo.7643742

Abstract. *The article deals with the problem of ensuring the information security of mobile devices. The method of analysis of this problem based on the basic threats to information security is applied. The result of the study is a cumulative conclusion about the reliability of mobile devices in terms of their security to information security threats.*

Keywords: *information security, mobile devices, privacy.*

Introduction

Currently, mobile devices are becoming the main devices in the life of a modern person, primarily for accessing Internet resources. At the end of 2011, personal computers were inferior in sales to mobile devices, and in the United States and Western Europe, the number of smartphone sales exceeded the number of sales of traditional mobile phones in the second quarter of 2012. The number of mobile subscribers is approximately 5.7 billion people, while the number of mobile device users is 792 million, but this number is growing very rapidly. Analysts at International Data Corporation predict that the volume of mobile device shipments will reach one billion copies from 2016 [1].

The number of features provided by mobile devices is much greater than that of traditional mobile phones: they have a pre-installed mobile operating system (IOS, Android, Windows Phone, etc.) and can work with both mobile communication networks and Wi-Fi and Bluetooth wireless technologies, thanks to which users can download and run third-party applications using the Internet. Other features of mobile devices include support for the multimedia messaging service (MMS) and the presence of built-in sensors: a gyroscope, a GPS signal receiver, an accelerometer, as well as a microphone, a high-resolution camera and a speaker. The emergence of a number of information security problems is explained by the increasing popularity of mobile devices. In 2014, the number of descriptions of Android threats increased by more than 2 times [2].

Threats to information security

Consideration of the problem is supposed to begin with the basic threats to information security. As applied to mobile devices, they do not undergo changes.

Let's identify the main threats to information security:

– Threats to privacy. They consist in unauthorized access to confidential information.

– Threats to integrity. These threats mean any deliberate transformation of the data contained in the information system.

– Accessibility threats. Their implementation leads to a complete or temporary inability to access the resources of the information system.

All the listed threats are relevant for mobile devices [3]. They store a huge amount of confidential data. The reason is that a mobile device is a powerful tool for generating and storing confidential information. Due to its compactness and non-stationary use, it is convenient to use it for such purposes. The mass application makes mobile devices a convenient target for intruders.

Security threat model for mobile devices

We will develop a model of threats to the security of a mobile device. Most often, the threat implementation scheme for a mobile device looks like this. An attacker develops and publishes an application with malicious code in the app store or on a website on the Internet. The user downloads and installs this application. During installation or operation, the application requests access to certain operating system resources and uses them for its own purposes.

Resource leakage can occur through any communication channel.

Let's form a model of security threats. In the above scheme, there are three main levels:

– Resource level. These are memory, sensors, microphone and camera. Malicious programs through the privilege system try to gain access to them and manipulate the information coming from them.

– Communication level. These are Wi-Fi, Bluetooth, mobile communication networks, Micro USB ports and memory card slots. Any of these channels can be used by a malicious program for self-distribution and for the dissemination of information obtained at the resource level.

– Application level. In fact, these are all mobile device applications. At this level, malicious applications are embedded on a mobile device under the guise of ordinary ones.

This threat model describes the entire lifecycle of a malicious program on an end device. The damage caused by the actions of a malicious program can vary from insignificant to significant, for example, it can be expressed in a decrease in performance and sending spam, or, for example, leading to the fact that the user will not be able to use the basic functionality of a mobile device and will incur financial losses.

Attackers are usually interested in resources containing vulnerable data – when malicious code is introduced into a mobile device under the guise of a program, it, using a privilege system, tries to gain control and access to such resources. For example, a virus can change the memory management on the device, in which case it will not be possible to delete it without full recovery. Mobile devices use microSD memory cards as additional memory, and an attacker can gain access to their contents. Confidential information is also provided by various sensors on a mobile device, such as a GPS receiver, gyroscopes and accelerometers. The GPS sensor provides information about the current location, and this information can be used without the user's desire. The camera and microphone of the mobile device can also be used in hidden mode. Data leakage can occur via Wi-Fi or Bluetooth communication channels.

If the virus has gained full control over the mobile device, then it is able to fully spy on the owner of the mobile device.

Classification of attacks for mobile devices

The main categories of malware are: viruses, Trojans and spyware. Viruses are often disguised as games or other software downloaded by the user to a mobile device. The specifics of viruses for mobile devices are not much different from viruses for personal computers. The main task of Trojans and spyware is to collect various kinds of information using the sensors of a mobile device, and then transfer this information to unauthorized persons [4].

Threats and attacks on a mobile device include phishing, spam, sniffing and data leaks.

A sniffer is a program or hardware-software device designed to intercept and then analyze, or only analyze network traffic intended for other nodes [5]. There are many ways to intercept information from mobile devices.

Spam – sending commercial and other advertising or other types of messages to persons who have not expressed a desire to receive them [6]. It can be distributed in MMS messages or using email.

Phishing is a type of Internet fraud, the purpose of which is to gain access to confidential user data - logins and passwords [7]. Most phishing attacks occur via email, social media, or MMS.

Data leakage is one of the most dangerous threats in cyberspace. It is the actions of individuals who managed to get legitimate access rights to information, which led to a violation of its confidentiality. Malware can steal personal information: location information, bank card data, contact list – and send them to an attacker. Data leakage from a mobile device violates the privacy of the user's personal life.

The user may not notice most of the attacks for a while, since they take place in a hidden mode.

Security issues

There are a number of properties that make it difficult to solve the problems of ensuring the security of mobile devices.

– Difference of user groups. Mobile devices are used for various purposes; therefore, security tools must be adaptable to the needs of each specific group of consumers.

– Difference of operating systems. Each operating system has its own security model features. Each version of the platform contains its own vulnerabilities, and all of them have to be taken into account.

– A large number of channels for information penetration and leakage. Each communication channel of a mobile device is a possible way of virus penetration under the guise of a legitimate application or leakage of confidential information.

– Risk of theft or loss of the device. When an unsecured device is stolen, an attacker gains practical full control over the data stored in it.

– Collecting information using built-in sensors. The number of potential attack options will increase with the increase in the number of sensors on mobile devices.

Having analyzed the higher-level problems, it can be noted that their cause is the desire of manufacturers to make the device as convenient and suitable as possible for each consumer.

Security measures

It should be noted that the most important functions of information security of mobile devices are authentication, integrity control and confidentiality.

Data synchronization with a personal computer contributes to the possibility of potential access to the file system of a mobile device. The security of confidential data on the device must be ensured by data encryption, as well as avoid storing information in plain text.

It is also necessary to monitor the integrity of not only the data, but also the system. Software integrity verification should be carried out by application stores to exclude the possibility of its modification by an attacker. Mobile devices should provide tools to protect the integrity of the system.

The mobile device should separate normal data from confidential data and provide the user with the opportunity to assign the appropriate status to confidential data. The advantage of this moment is saving computing power and battery life, and the disadvantage is the ability of an attacker to see which specific data the user prefers to hide. Encryption is the most effective method of ensuring the protection of personal data.

Along with encrypting the secret data that is stored on the mobile devices themselves, users should encrypt the contents of memory cards. The disadvantage of this method is the high load on the computing resources of the mobile device, it is necessary to rationally encrypt data in order to avoid a rapid drop in battery power.

An additional way to protect vulnerable information is to transfer data from mobile devices to cloud services. Suspicious activity can be detected by cloud intrusion recognition systems. The disadvantage of this method is the additional costs for service traffic and for the cloud service itself.

Summing up, it can be noted that the biggest responsibility for the safety of their data is borne by users of mobile devices. Comprehensive protection and reduction of the number of threats requires an integrated approach and interaction of manufacturers, developers, service providers and end users.

Conclusion

In the course of the study, the main threats to information security for mobile devices were identified, their model was built, possible security problems and measures to ensure the protection of confidential data were considered. It can be noted that the relevance of this problem is increasing every year, because the number of malicious programs is constantly increasing. Based on the possible measures to ensure protection, it becomes clear that at the moment a competent user security policy in relation to their confidential data plays a key role. The security model of mobile operating systems and the conditions for the distribution of applications need to be significantly changed and refined to prevent many problems in the future.

REFERENCES

1. Worldwide Smartphone Shipments Top One Million Units for the First Time - [Electronic resource]. Access mode: http://www.idc.com/getdoc.jsp?containerId=prUS24645514
2. Review of Android threats for 2013 from the company "Doctor Web" [Electronic resource]. – Access mode: http://www.freedrweb.com/show/?i=4211&c=19&lng=ru Gatchin Yu.A., Sukhostat V.V. Theory of information security and methodology of information protection. – St. Petersburg: St. Petersburg State University ITMO
3. Malware [Electronic resource]. – Access mode: http://ru.wikipedia.org/wiki/Malicious program Traffic Analyzer [Electronic resource]. – Access mode: http://ru.wikipedia.org/wiki/Анализатор_трафика
4. Spam [Electronic resource]. – Access mode: http://ru.wikipedia.org/wiki/Spam
5. Phishing [Electronic resource]. – Access mode: http://ru.wikipedia.org/wiki/Фишинг