Conference Paper

Information Protection Tools for Android-based Mobile Devices

Rubtsov O. E.[1] and Norkina A. N.[2]

[1]National Research Nuclear University MEPhI (Moscow Engineering Physics Institute), Master, Kashirskoe shosse 31, Moscow, 115409, Russia
[2]National Research Nuclear University MEPhI (Moscow Engineering Physics Institute), Candidate of Economic Sciences, assistant professor, Kashirskoe shosse 31, Moscow, 115409, Russia

Abstract

Presently, the issue of protecting information and personal data contained in mobile devices is of vital importance. The use of cutting-edge powerful smartphones presented by manufacturers as a substitute for personal computers, laptops and tablets, stresses the need for utilizing both built-in free information protection features and special antivirus software manufactured by recognized global developers. The article reveals the effectiveness of using built-in information protection tools for Android-based mobile devices and presents a comparative characteristic of similar tools applied with the help of up-to-date antivirus software.

Keywords: mobile devices, information, personal data, cyber threats, Android-based, viruses, protection of information (information protection), smartphones, security.

Corresponding Author:
Chicherov K. A.
kirill.chicherov@me.com

Received: 11 December 2017
Accepted: 20 January 2018
Published: 13 February 2018

Publishing services provided by Knowledge E

Selection and Peer-review under the responsibility of the FinTech and RegTech: Possibilities, Threats and Risks of Financial Technologies Conference Committee.

1. Introduction

Today, when personal computers, tablets and all other mobile devices are more important than ever, it is smartphones that are rapidly gaining momentum as being important for any person's life irrespective of his or her social status and financial standing and increasingly preferred by advanced users. Due to their high performance and portability, smartphones can be a substitute for any mobile device. At the moment, one simply cannot imagine his or her life without modern mobile devices, particularly in light of the growing use of user communication tools (social networks, all kinds of messengers, etc.) installed on smartphones by default.

2. Material and Theoretical Bases of Research

According to statistics, at the end of 2016 smartphones were used by more than 2 bln people all over the world, or 25% of the world population. Statistics-based

projections show that by the end of 2020 the number of users may grow by at least 20%.

All mobile devices, including tablets and smartphones, contain massive amounts of information, including strictly confidential user data, with the leak of such information posing a grave threat to its owner. Ever-increasing cyber threats, high virus danger, and current vulnerabilities in operating systems stress a crucial significance of reliable protection of personal data and all the information contained in mobile devices.

There exists quite a number of sensitive information protection tools, from free features built-in by default to specialized antivirus software. Built-in features are capable of protecting user's contacts, correspondence and calls, social network accounts and all files and folders both in the device and the plug-in SD card.

By default, Android-based mobile devices offer six various protection (device lock) tools provided in Settings, Security and Lock Screen menus, with each of them having its own advantages and disadvantages:

1. Lock Screen Pattern is one of the most convenient and popular tools for protecting personal data from being seen or read by third persons. This tool employs a unique visual pattern, i.e. a finger-drawn line connecting, in a chosen sequence, nine dots of the square appearing on the screen. This combination represents a protection key, however its reliability in future depends on the number of selected dots and the complexity of the pattern. Yet this method has a material deficiency: the user leaves his or her fingerprints on the screen and the latter needs to be thoroughly cleaned, while to ensure proper security the user has to engage at least five dots offering over 7,000 combinations.

2. Visual tracking feature to unlock the device; however the device may be unlocked using the owner's photo or that of another person looking like the owner.

3. Voice-based identification which requires the owner's speech pattern to unlock the device. Still, the device can easily be unlocked when the owner's voiceprint is used, sometimes in combination with the photo. This tool cannot be considered a reliable one due to significant vulnerabilities and unlocking potential.

4. Use of a signature as a key word (to be entered three times). However, most of the users choose their names as a key word, and any intruder can easily unlock the device even if he or she has minimum information on its owner.

5. Password entered as a 4-digit PIN code; considered the most effective tool for ensuring device security and protection. And again, the device can easily be

unlocked since many users choose first digits of their birthdates for PIN codes. Also the PIN code or the password can be recognized by tracking the fingerprints the owner leaves on the screen.

Many smartphone developers suggest owners use their fingerprints as a protection means. However, if the finger is cut or the finger cushion is dirty, the device will remain locked. If this is the case, the owner may alternatively enter the PIN code.

Given major disadvantages of built-in smartphone features, third party applications are recommended, with Emoji being the most popular of them and developed specifically for Android-based mobile devices. Its basic idea lies in setting a specific sequence of smiley faces at the moment of the first run, and such sequence will serve as a specified authorization key to unlock the device. After each lock-up, the sequence of smiley faces (up to eight) changes, and unlocking the device using fingerprints or breaking a rapidly changing sequence of smiley faces can be a challenge. No doubt, this application has an obvious advantage over all built-in free features.

The need to protect mobile devices from all external cyber threats and mobile viruses, given their ever increasing propagation and the concern they represent for information security, should always be kept in mind. Mobile viruses are small programs breaking into a mobile device (smartphone, messenger) that record, corrupt or delete data or send it to other devices via Internet and SMS messages.

There exists a number of mobile virus varieties, among them a well-known Commwarrior MMS worm that is distributed via Bluetooth connections and MMS messaging without the device owner's knowledge and flattens the battery. Metal Gear Solid, camouflaging as a game setup file, searches for and deactivates antivirus software, which results in problems with further use of the device even after the virus has been removed. Mosquit sends SMS messages; Pbstealer, a harmful application, steals personal data of the device owner and forwards it to the Bluetooth-accessible device it finds; Sculler disables all functions of the mobile device and corrupts contact information in Contacts, making its future recovery impracticable.

Malicious software is designed and distributed for stealing personal data, sending paid SMS messages and calling 'partner numbers' without the owner's knowledge, and for fraudulent activities using the Internet banking system.

If this is the case, to protect personal data it is recommended to use specialized antivirus software developed by leading global cyber security manufacturers, including Symantec as one of the most renowned manufacturers offering Norton Security

antivirus application. According to the rating, reliable and efficient antivirus applications are also offered by Kaspersky Lab and Dr Web. Mobile operators offer proprietary network-based solutions, such as the MTS antivirus. For the purpose of securing a reliable protection for smartphones, software applications developed with due account for information security standards of major corporations, financial and banking organizations are employed. Antivirus applications offer the following functions: 'white' and 'black' number lists, blocking of alphanumeric combinations, antivirus screens, entire system scan, SD card files and folders scan, powerful web-based protection, automated updating and quarantine, use of cloud technologies, and state-of-the-art user support.

Widely occurring Bluetooth threats should also be mentioned as they represent all sorts of attacks and viruses that use Bluetooth connections to hack mobile devices and steal data contained therein. Those threats include BlueBug, BlueSnarf, BlueDump, DoS attacks, and Bluetracking.

As an efficient safeguard measure for users, mandatory regular updates of the operating system are recommended, however, they do not always provide a reliable protection of the mobile device. To protect against covert readouts and unauthorized data acquisition, the use of a customized application that verifies Bluetooth requests and notifies the device owner on any suspicious activity appears to be reasonable and appropriate. Thus, one may prevent a hacking attempt or an attempt to put the mobile device out of operation which may be performed via overflowing the buffer or reading out information on the services offered. Authentication requires additional control as well, taking into account all Bluetooth-related vulnerabilities and deficiencies of the process. Speaking about authentication, it should be mentioned that specific authentication of the headset is required, as the headset enables the intruder to illegally operate the device and wiretap. As an interesting solution and a protection means in this very case, a special Bluepot technology is offered. It creates the appearance of vulnerability in the mobile device and allows a retaliatory capability, such as rebooting the intruder's device or sending him or her falsified data. Additionally, each mobile device owner should pay attention to applications available whether in app stores or on the open Internet and use trusted sources only in a manner compliant with all application requirements.

3. Conclusion

Therefore, the use of features built-in by default, as well as of up-to-date antivirus software and specialized applications, can reliably protect Android-based mobile devices from an unauthorized access, identity theft, and all sorts of cyber threats and virus attacks.

Acknowledgements

This work was supported by Competitiveness Growth Program of the Federal Autonomous Educational Institution of Higher Education National Research Nuclear University MEPhI (Moscow Engineering Physics Institute).

References

[1] Zhilin, V.V., Drozdova, I.I. Key Methods of Modern Mobile Device Protection // Molodoy Uchenyi. – 2017. – No. 13 (147). – P. 41–44.

[2] Zavyalov, I.A., Safonenko, N.V. Methods of Protecting User Data Contained in Mobile Devices from Covert Remote Data Reading via Bluetooth Connections // Issues of Automation and Management within Technical Systems / Collection of Articles of the International Technical Conference edited by M.A. Shcherbakov. – 2013. – P. 336–338.

[3] Sidorova, M.A. Protection of Data Contained in Android-Based Mobile Devices // Scientific Journal. 2017. – Vol. 2. – No. 6 (19). – P. 35–40.

[4] Zakharchuk, I.I., Veselov, Yu.G., Eremeev, M.A. Issues of Protecting Mobile Personal Devices from Informational and Technical Interference // Engineering and Computer Technologies. 2012. – No. 5. – P. 20.

[5] Kurmanbay, A.K. Protection Tools and Benchmarking Study of Information Security for Mobile Devices // Contemporary Decision-Making Technologies in Economy. 2015. – P. 97–99.

[6] Borzykh, Yu.A. Current Methods of Personal Data Protection in Mobile Devices // Emerging Information Technologies and Systems. 2015. – P. 192–194.

[7] Anisimov, M.A. Issues of Protecting Mobile Devices from Malicious Applications // Education. Science. Academic Personnel. 2013. – No. 2. – P. 168–170.