International Journal of Soft Computing 11 (1): 1-3, 2016
ISSN: 1816-9503

The Role of Software Telephone Bugs in Mobile Security

[1]Zhukov Igor, [2]Mikhaylov Dmitry, [2]Kharkov Sergey, [2]KholyavinVitaliy and [1]Nasenkov Igor
[1]Concern Radio-Electronic Technology, Ltd., Moscow, Russia
[2]MEPhI (Moscow Engineering Physics Institute), National Research Nuclear University,
Kashirskoe Highway 31, 115409 Moscow, Russian Federation

Abstract: Nowadays mobile device manufacturers offer customers not only devices for calling and sending text messages but also multi-functional smartphones with much broader capability. They can store and process a lot of data that may be breached by theft or data leakage. This study deals with the overview of the main attacks that can be performed using the vulnerabilities of a mobile device with inserted software bug. This bug can force the phone to send text messages, make calls on paid numbers and record them, get access to private information (list of contacts, text) as well as harm the operating system. Researchers also provide the basic recommendation the following of which will protect the user from the unlawful action of an intruder using the malicious logic. The overview can be used to improve existing mobile security means.

Key words: Software bug, malicious logic, mobile device vulnerabilities, unauthorized access, action

INTRODUCTION

Personal mobile devices with growing functionality have become an integral part of our everyday life influencing complexity of modern mobile networks with increasing the number of users and base stations. Modern information technologies are constantly being developed. The probability of an attack by fraudsters on a mobile device is inevitable increased. Hackers were writing deleterious software codes and "infecting" mobile devices not so long ago (Pu *et al*., 2014). But now viruses are being concealed from users. Viruses are being integrated in popular applications and games. Moreover, they can control your device or even block it (Mikhaylov *et al*., 2013; Liang *et al*., 2014).

The development of the open-source operating systems is a reason for appearance of many open-source projects and applications. Nowadays a malefactor can easily write an application, sending text messages from your mobile device to paid numbers. However, this functional can be integrated in games or calculators. Then owners of mobile devices will have no information about the threat. Such application can secretly send messages and delete all information about this action from a journal of connections (Mikhaylov *et al*., 2013).

It is possible for a malefactor to get a confidential data, damage information, block a mobile device with the help of software bugs (Mikhaylov *et al*., 2013, 2012; Mikhaylov and Yu, 2011; Inoue *et al*., 2012). This study presents the main attacks that may be performed by the intruder using the software telephone bugs (or malicious logic) inserted into the mobile device.

The study can be used to enhance the mobile security. Researchers also provide some protection rules to eliminate the malicious logic harmful actions.

POSSIBLE VULNERABILITIES

The software bugs are invisible parts of software giving an opportunity to interfere in functioning of a mobile device. The malicious logic is often used as "interceptors" of passwords and traffic. What is more, it can be used as conductor for viruses. It is impossible to detect such software bugs by standard antiviral means. They can be detected by special test programs only. The scheme of the attack can have the following view (Fig. 1).

Licensed software which is checked by manufacturer of an operating system/a mobile device does not guarantee that there are no undocumented functions, committing illegal actions in relation to users. Moreover, Google and Apple keep information about user's location and Wi-Fi identifiers (Mikhaylov *et al*., 2011). It is enough to visit special site, enter MAC-address and you can see where the person is.

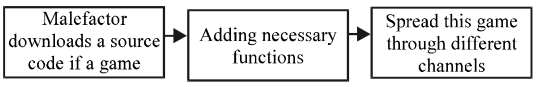

Fig. 1: The scheme of the fraudsters attack

Corresponding Author: Zhukov Igor, Concern Radio-Electronic Technology, Ltd., Moscow, Russia

Special software bugs for deliberate attacks are often added. Malefactors can remotely control their work. Parameters of the malicious logic are changed and an intruder can use owners of mobile devices in fraudulent schemes. Android.Anzhu is the program which can change configuration of software bugs and manage your smartphone.

Android.Anzhu is a back door program which is installed by an attacker in user's mobile device for following access. Trojan has a lot of functions one of which is the accumulation of users personal information including geolocation coordinates and IMEI (International Mobile Equipment Identify).

A malicious program, installed in screen off and lock is a famous application which is used for screen locking and phone switching off in one touch without "on/off" button. After installation the additional icon for running the program in service mode, configure screen off and lock is created at the screen of mobile device together with icon of the program.

Android.Anzhu can change, add or delete favorites in browser of the mobile device. Moreover, it can install different applications without user's permission. Android.Anzhu can change system privileges. Intruders can use owners of mobile devices in fraudulent schemes, placing links to malicious sites in software bugs (or changing attributes of the software bugs) (Mikhaylov *et al*., 2013).

Android.Anzhu can track changes in Android system journal. For example, it can obtain information about events, linking with starting and opening different windows in applications.

One more threat is malicious programs which are masked as usual applications. After installing and running such applications start sending expensive text messages without user's permission.

Intruders can use different software (for instance Android.DreamExploid, Android.SmsSend, Trojan-SMS.AndroidOS.FakePlayer, Trojan.spy.4android, Android.Adrd, Android.Geinimi, Android.Walkinwat) for attacks with hidden texts. It is masked or integrated in popular applications (in a popular game, for example).

In the process of installing such program can request permission to send messages. However, this information is often ignored by users. They can agree with all program features without reading terms of agreement. Many "additional features" can be in installed application. Thus, information about sending texts may stay without user's attention.

After application running the Trojan starts sending text messages in the background mode. The user's agreement is not requested. The program can send texts to the certain number.

One more problem for mobile device owners with preinstalled software bugs is a theft of passwords for mobile client-banks. It becomes possible because of Authentification System vulnerabilities. Moreover, the speed of services development and implementation plays much more important role than user's safety. Some banks have no two-factor authentification in their websites. The bug-application can send hidden message to set a new password. All intermediate service notices from the bank (for example, notice about password change) will be intercepted by the bug and removed from the system. Moreover, modern professional software bugs can circumvent two-factor authentification. In this case, the bug has a parser of incoming messages. This bug is searching for the necessary code and sends it to the bank. As a result, themoney is lost.

What is more, there are many spy programs (spyware) in the internet. Such a bug will obtain any confidential information about users and send it to the attacker for a modest sum of money.

The simplest method to integrate the malicious logic into application is its source code modification (Mikhaylov *et al*., 2012). The source code is often available in free programs but there are not many such programs nowadays.

However, the source code can be unavailable. In this case, the second variant is more appropriate. It is necessary to change .apk application file. .apk file is a usual zip archive including the code, the manifest, the digital signature and the resource files. The code stored in classes.dex file is more interesting. Dalvik virtual machine is used instead of Java in Android.

dex format is a format of files for Dalvik. An experienced virus writer can integrate a malicious code into a compiled code. It is possible to add new classes or change existing classes (to change logic of functioning). Classes .dex include a signature and a check sum as well. They should be changed after all manipulations (Mikhaylov *et al*., 2013).

Moreover, it is necessary to write Android Manifest.xml required changes (to add necessary resolutions or to announce added services). However, there are some difficulties because the manifest file in apkis encrypted. It is necessary to use the android-apktool utility for the manifest decoding.

The application is signed by other signature after changing the code and the manifest. Moreover, it is possible to automate software bugs integration and "infect" applications in devices. The software bugs are dangerous because they can include many features:

- Opportunity to send expensive text messages and make phone calls to paid numbers
- Call recording
- Access to personal information (contacts, messages)
- Damageoperating system and so on

Thus, even a harmless application or a game for mobile devices can be very harmful. A malicious logic gives malefactors an opportunity to remotely control an "infect" the device (for example, to run commands, to install different applications, to change settings in browser). Moreover, owners of mobile devices can unwittingly participate in fraudulent schemes.

MAIN PROTECTION RULES

To avoid troubles the user of a mobile device should be attentive and follow the simple rules including:

- Install applications only from the reliable sources or from the official websites
- Check permissions before installation (some dangerous permissions can be in "infected" application)
- It is not excessive to have an antivirus program on a mobile device
- Be attentive in regard of updates; if during the update installation an Android application the message is received telling that the process is failed, it is likely that this update is faked and it issigned by another signature

The method of the software telephone bugs deletion depends on the installation method. It is necessary to reprogram the read-only memory in the mobile device after malicious logic deletion. Bootable, driver, applied, masked bugs or imitation malicious logicshould be replaced by the software from reliable sources. If executable software bugs are detected, the user should remove the text of this malicious logic from the source software module and recompile this module.

CONCLUSION

The disclosed in the study main attacks using the software bugs show the diversity of negative effect that can be caused by malicious logic. This overview can be used by the security software manufactures in order to improve existing information protection means, remove the vulnerabilities and ensuring more thorough protection from intruders.

The study is still underway to provide more details about emerging threats to mobile devices and information stored and processed by them.

REFERENCES

Inoue, K., Y. Higo, N. Yoshida, E. Choi, S. Kusumoto, K. Kim, W. Park and E. Lee, 2012. Experience of finding inconsistently-changed bugs in code clones of mobile software. Proceedings of the 6th International Workshop on Software Clones, June 2-9, 2012, Zurich, Switzerland, pp: 94-95.

Liang, G.T., J. Wang, S.C. Li and R. Chang, 2014. PatBugs: A pattern-based bug detector for cross-platform mobile applications. Proceedings of the IEEE International Conference on Mobile Services, June 27-July 2, 2014, Anchorage, AK., Pages: 84-91.

Mikhaylov, D.M. and Z.I. Yu, 2011. Protection of MOBILE devices from Attacks. Foylisc, Moscow, pp: 192.

Mikhaylov, D.M., A.S. Smirnov, A.M. Tolstats and N.V. Kuznetsov, 2012. Using of phonebugs for mobile attack. Digest of annotations of the Kurchatov youth Scientific School.

Mikhaylov, D., I. Zhukov, A. Starikovskiy, S. Kharkov, A. Tolstaya and A. Zuykov, 2013. Review of malicious mobile applications, phone bugs and other cyber threats to mobile devices. Proceedings of the 5th International Conference on Broadband Network and Multimedia Technology, November 17-19, 2013, Guilin, pp: 302-305.

Mikhaylov, D.M., A.V. Zuykov, I.U. Zhukov, A.G. Beltov, A.V. Starikovskiy, M.I. Froimson and A.M. Tolstaya, 2011. The research of mobile vulnerabilities in apple and Google systems. Sci. Tech. J., 6: 38-40.

Pu, S., Z. Chen, H. Chen, Y. Liu and B. Zen, 2014. Threat analysis of smart mobile device. Proceedings of the 31th URSI General Assembly and Scientific Symposium, Auguest 16-23, 2014, Beijing, Pages: 1-3.