Journal of Theoretical and Applied Information Technology
31st May 2015. Vol.75. No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

OVERVIEW ON IDENTIFICATION OF MARKS OF SUBSCRIBER SECRET LOCATION TRACKING IN WIRELESS COMMUNICATIONS NETWORKS

MIKHAYLOV DMITRY[1], ZHUKOV IGOR[2], ZUYKOV ALEXANDER[1], BORUCHINKIN ALEXANDER[1], FILIMONTSEV ALEXANDER[1], KALINTSEV NIKOLAY[1], LUKYANENKO LEONID[1], YOKHIN MIKHAIL[1],

[1]National Research Nuclear University "MEPhI" (Moscow Engineering Physics Institute)
Kashirskoe highway 31, 115409, Moscow, Russian Federation
[2]Concern radio-electronic technology, Ltd.

E-mail: i.zhukov@kret.com, mr.mdmitry@gmail.com, avzuykov@gmail.com, boruchinkin28@ya.ru, asfeliks@mail.ru, nick.ingenium@gmail.com, suvereign@mail.ru, MNYokhin@mephi.ru

ABSTRACT

As mobile devices are getting an integral part of our everyday life they store and process data that can be of great importance for the user. Another problem with the development of mobile Internet and means of wireless communication is tracking. All the movements and activities of the mobile phone owner can be secretly tracked by both – criminals and mobile service providers. The article addresses the issues of online service market occupation and stationing servers in the USA; disorienting of users and hidden settings of a mobile phone; third-party data collection applications; malware and secret modules in open systems; foreign components and maintenance; passing data security; system integration; indirect equipment identification and data remainence. The described in the paper overview can be used to improve existing mobile security means, eliminating the vulnerabilities and ensuring more detailed protection from intruders.

Keywords: *Applications, Location, Mobile Operating Systems, Software And Instrument Bugs, Tracking, User`S Data Security.*

1. INTRODUCTION

Mobile phone has become an integral part of modern life. According to network providers' statistics, 99.99% of the population of different age and social groups has mobile phones, and more than half of them own two or more devices [1].

Modern mobile phones have high functionality and are used to access the Internet for e-mailing, social networking, playing online games, watching movies and listening to music, finding your location and routing, etc. A smartphone can store a lot of data that may be breached by theft or data leakage.

The fact that modern mobile devises has a great number of vulnerabilities is highlighted in many scientific papers. For example, Mas'ud et al propose a general mobile malware behavior model that can contribute in identifying the key features in detecting mobile malware on an Android Platform device [2]. Gelenbe and his team present in [3] novel security technologies for seamless service provisioning in the smart mobile ecosystem improving mobile network security through a better understanding of the threat landscape. In [4] the review of malicious mobile applications, phone bugs and other cyber threats to mobile devices is provided. The issue of enforcing the security within mobile devices using clouds and its infrastructure is presented in [5].

Although companies, developing security software, have been creating protection means for mobile devices, they still cannot reach the complete security. This happens because mobile security threats are emerging every day and it is difficult to foresee the way it will be performed. That is why it is necessary to constantly carry out studies to identify new threats in order to use this information during the development of new protection means.

This article focuses on the mobile phone vulnerabilities and main tendencies in mobile technologies that can lead to subscriber secret location tracking in wireless communications networks. The paper also presents the identification marks of these unlawful actions that can be used to enhance the mobile security.

Journal of Theoretical and Applied Information Technology
31st May 2015. Vol.75. No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

The results of this overview can be implemented by the security software manufactures to improve existing information protection means, remove the vulnerabilities and ensuring more thorough protection from intruders.

2. ONLINE SERVICE MARKET OCCUPATION AND STATIONING SERVERS IN THE USA

Mobile operating systems market leaders are Google Android and Apple iOS [6]. Both they and Microsoft Windows Phone, which is rapidly gaining popularity, are developed in the USA; RIM BlackBerry – in Canada. This suggests the USA to become in the near future the country, where the vast majority of the mobile operating systems manufacturers are registered.

Google and Microsoft are winning the majority of market segments of Internet services – email services, search engines, cloud storage, social networks, enabling the synchronization of any data, on-line supervision of documents, tasks and meetings, multimedia and content portals, billing systems, translators, own Internet browsers, as well as desktop operating systems and loads of applications.

When using online services, it is obligatory, one way or another, to create accounts, enter personal data, agree with privacy policy and license agreements that users usually do not read.

Many of the services of one particular company, such as Google, – according to privacy policy again – are interrelated. That allows linking, for example, the history of search queries, bookmarks in browser, photos in the cloud and contacts synchronized with the mobile phone. Even if a user once entered false information, sooner or later somewhere else he or she enters the mobile phone number – for example, for two-factor authentication – or credit card details to pay for goods.

It is also worth noting that many users create the same or similar passwords on various Internet portals.

3. DISORIENTING OF USERS AND HIDDEN SETTINGS OF A MOBILE PHONE

Internet services and applications are designed so that it is very difficult for user to learn how to remove all "unnecessary ticks" to cancel particular data synchronization or to deny providing reports that contain identifying information (see Figure 1).

Some ticks are likely not to be noticed at all – they are only displayed when the user runs the program at first time. For example, on many Android phones user can "decouple" attached Gmail account from the device only by reset to factory settings, which is very troublesome as private and work information is kept on the phone.

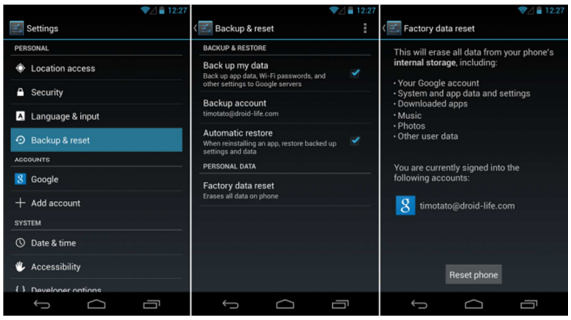

Figure 1: Backups [7].

For data synchronization it is also needed to use online services or programs for personal computer that contain a lot of specifications regarding ability to send data tacitly to third parties (see Figure 2).

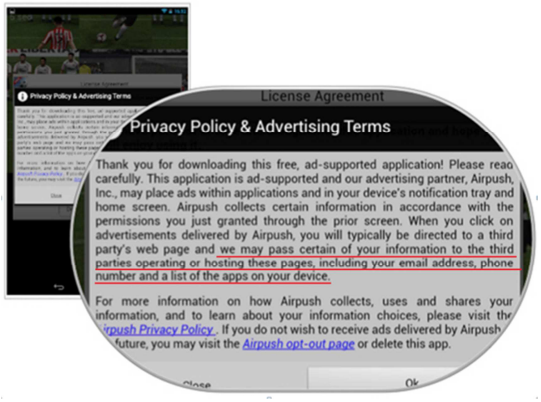

Figure 2: Terms Of Data Sending In Private Policy [8].

For instance, information may be tacitly transferred to a personal computer when a mobile phone is connected to it by USB.

For example, the use of Apple devices is based on a music store iTunes. When the iPhone or iPad is synchronized with the computer, iTunes automatically copies the full backup of data stored in the device to the hard disk. The backup archive is updated every time, not only by the fresh content, contacts and applications that have been downloaded or modified since the last synchronization, but also by geolocation and navigation data base of the mobile phone. [9]

Journal of Theoretical and Applied Information Technology
31st May 2015. Vol.75. No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Another example is using browser exploits to retrieve information about a user's location by means of HTML5 [10].

4. THIRD-PARTY DATA COLLECTION APPLICATIONS

Popular programs (for example, the Angry Birds game) are installed on the device in most cases through online shopping of mobile applications, where user should have an account (on Android it is the e-mail, which cannot be deleted without resetting the phone).

All programs have their own system of users and devices identification in order to prohibit copying applications, impede piracy and comply with license of the developer. Usually it is the standard identification by app store; the application is bound to a unique device number and account.

However, application developers often send to their servers more information than necessary (see Figure 3).

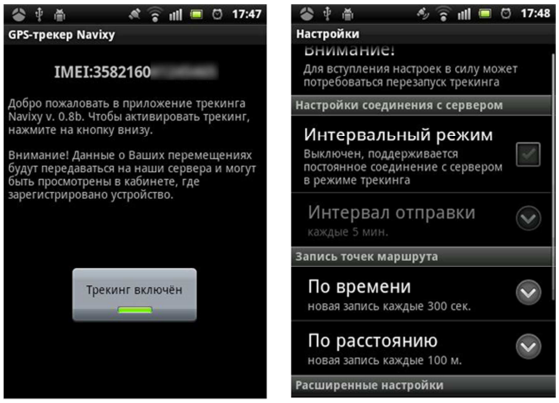

Figure 3: Tracking Application [11].

In addition, the information is frequently updated, as mobile Internet is unlimited in many tariff plans now and switched on all the time, for example, to communicate in social networks.

Since mobile phones are used as navigators, GPS is often enabled in settings, which allows applications to get the exact user's location. But even without a GPS location coordinates accurate enough for public interest can be got through cell towers or by using the gyroscope and inertial reference system.

Security policy in the operating systems is designed so that the user skips notifications (for example, OS Android) that applications access any system resources – getting location coordinates, sending SMS-messages to paid numbers, etc.

5. MALWARE

The decompiling process of applications for operating system Android is relatively simple. This fact makes the program`s algorithm accessible for hackers, who can easily find some bottlenecks of the program. For example, they may examine the encryption algorithm to extract necessary data and literals from the code. Due to the simplicity of code extracting, now it is possible directly on a mobile device. At the same time even a calculator can get an access to installation package of the third party application.

If the device is rooted, the access to the files of installed applications including passwords and important identifiers that promotes "bugging" of personal data can be easily obtained (Figure 4).

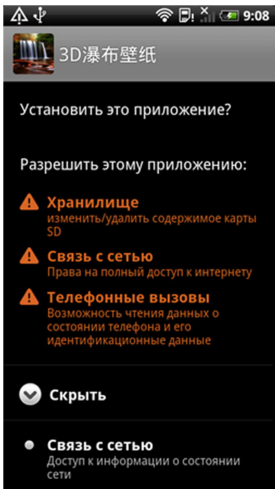

Figure 4: Tracking Application [12].

Furthermore, due to ease of retrieval of the program algorithms and changing of its functionality [13], as well as lack of proper moderation of applications on Google Play, it has become probable for Android to distribute clones of popular apps that pass every log-in and password entered, inter alia, to third parties.

6. SECRET MODULES IN OPEN SYSTEMS

The claim that Google Android is an open operating system is not completely true. Back code of "bare" operating system is really accessible to anyone, but mobile device manufacturers add their own set of system modules with closed back code and often tacit data collection function (news about bookmarks in Android and iOS continually appear in the media [9], [14-16]).

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

System software cannot be deleted by standard actions and the system stops working altogether after the intervention of experienced "hackers", as many secret modules are necessary for correct work of devices, while in order to replace them with the standard "open source", recompilation of the operating system, a very complex procedure, is necessary. Also the hardware components and software drivers are closed for them.

7. FOREIGN COMPONENTS AND MAINTENANCE

Today, the vast majority micro-chip and the components of mobile devices are produced abroad, which does not exclude hardware and software bugs. Moreover, in Russia there is no technological capacity for modem production, and it is an integral part of any cell phone.

Mobile operators' equipment also largely comes from abroad and poorly controllable elements in the radio access subsystem – the base stations – through which all traffic of subscribers connected to them flows may also be bugged. It is proved by extra traffic from base station subsystem to the third-party servers.

Russia lacks specialists in core equipment of mobile operator; most of the work (installation, configuration, and repair) is performed by foreign suppliers. Therefore even if equipment has been installed without active bugs, they could be activated during repair work.

8. PASSING DATA SECURITY

Found that popular online services do not encrypt traffic (including the authentication process leaving log-in and password to flow openly over the network), or do it with errors, making it easy to decipher the data. Safety is very badly thought out, especially that of the third-party applications. A major software companies usually spend too little time on security, as a rule, in order to release the product to the market as soon as possible ahead of the competition.

Not only frauds, but also authorities can collect identification data in networks. For example, they can be sniffing wireless connections or use special programs on the cross connect equipment. Even in case of proper encryption there are vulnerabilities and weaknesses of algorithms, such as reduced cryptorezistability of A5/2 cipher (stream cipher algorithm which is used to protect the data transmitted between the phone and the base station) in Russia.

9. SYSTEM INTEGRATION

Currently there is a tendency to improve the quality of services provided. However, as known, technological development and the introduction of new services leads to new threats, while increase in number of independent parts of the system pro rata with the level of its vulnerability as a whole. GSM/3G network is deployed as widely as the Internet, but is being much less analysed due to greater secrecy.

It is also worth noting that due to non-compliance of connecting SS7 (signalling system N7) networks to the Internet with safety requirements, vulnerability characteristic for the Internet becomes a problem for SS7. That is, as the result of vulnerable and relatively safe network interaction, final system is usually more vulnerable.

Vulnerabilities of SS7 can be used for fraud, eavesdropping, network failures organizing, targeted attacks and more dangerous intrusion into the system. SS7 network of mobile operators around the world are related, which in case of inter-state cyber warfare is a potential danger for communications in peacetime and during hostilities, as well as terrorist attacks.

The problem of SS7 security is underestimated in Russia, the legislative and regulatory framework lays behind the rapid growth of technology and business solutions when it comes to security. At the same time attack methods become more sophisticated, intruders' motivation increases. Even easy to fake falsification of the SMS-message sender can not only mislead people but also initiate actions such as management of various electronic devices and services. [17] For example, vulnerable banking services is a threat to users' account and the "smart home" managed by the third party – a threat to his life.

As 3G network is now not available everywhere all the mobile phone modems also work with more vulnerable GSM-standard which is very advantageous to attackers. Nowadays fraud-aimed equipment that creates a device capable of exploiting GSM vulnerabilities and listening to GSM-traffic gains in popularity. It is a false base station similar to mobile operator's base stations (often referred to as virtual cells).

10. INDIRECT EQUIPMENT IDENTIFICATION

There are a lot of unique identifiers in mobile devices that can be easily extracted by means of

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

software. IMSI is a SIM-card ID, IMEI is a mobile device ID, MAC addresses of Wi-Fi and Bluetooth modules can also be counted among the identifiers of user's mobile device.

Operating systems and system software developers need to use many IDs to identify the user in order to control and provide the latest system updates, to collect statistics, as well as for growing in number geo-location services. Even if all "extra" programs are removed from the phone, information about the location of a subscriber can still appear in Google / Apple [5].

The fact is that mobile phones collect information not only about themselves but also about others devices (Wi-Fi access points, neighbouring cell towers, etc.). It is enough to switch on Wi-Fi for MAC-address of the phone to be passed along with approximate coordinates of nearby devices (in public transport such devices are very numerous).

Moreover, sending geolocation information often occurs with the consent of the user who does not know about the side effects of using Wi-Fi positioning. Thus, for example, Google "knows" not only location of the phone, but also of the user's home Wi-Fi router.

The way of the identification of devices and users at higher levels (cellular-service provider and cross connect equipment) is another example. To access to the Internet through the same access point you have previously done by an unprotected home laptop (which has already passed all the necessary information to third parties) is enough for these third parties to learn the ID number of a phone (at least its MAC-address) and to track the subscriber at any other place.

Another source of the precise information about location is the mobile base stations. Companies such as Google, have the database matching base station with its coordinates, while mobile devices locate not only the station they use, but also the nearby ones. The situation is similar to Wi-Fi access points. Also it is worth noting that to provide services mobile operators need to know the location of the caller as well as his or her identifier. This information passes through foreign equipment in the radio access subsystem, and cross-connect subsystem.

Nowadays mobile phones tend to be equipped with NFC-modules (Near Field Communication) that can read data from a classified area pass, bank card or ticket to the subway. This is a new channel of indirect identification of people – it is enough for one person to switch on NFC and walk along a subway car at rush hour.

Judging by the absence of the necessary software between the operating system framework and the Secure Element NFC in Android (which is necessary for secure key storage), Google aims to develop its own NFC-payments infrastructure through which mobile phones and Google will know manifold more information about users and their bank cards than they do now.

11. DATA REMANENCE

It happens that after removal of any information from a mobile device or a hardware component (eg, SD-card), the data remains on the device. As an ID of the mobile phone can be stored on the external memory card in a hidden file, new owner will be able to find out where it used to be, comparing the data on the card with its source.

Not only system, but also third-party applications (such as games) store identifying information on external media. When deleting Google account from a mobile phone the remote account information (e-mail) continues to be stored on it. A system log file of the Symbian contains information about all applications ever installed on the phone. Thus, information on the original user of the mobile phone can be found using files on the phone or an external device (SD card).

12. CONCLUSIONS

As a conclusion it is worth saying that modern information technologies are making our life less private so it is important to circumspect especially in the sphere of information and mobile security. The provided in a paper overview of threats to mobile device user in case of location monitoring and breaching privacy can be used to improve existing mobile security means, eliminating the vulnerabilities and ensuring more detailed protection from attackers.

Moreover, this study can be taken in account during creation and update of the regulations governing the import and maintenance of foreign goods and technologies.

The study is underway to find more details about emerging threats to mobile devices.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

REFERENCES

[1] Russian mobile phone market. 2012. URL: http://myphoneblog.ru/2012/08/10/rynok-mobilnyx-telefonov-v-rossii/.

[2] Mas'ud, M.Z., Sahib, S., Abdollah, M.F., Selamat, S.R., Yusof, R., Ahmad, R. Profiling mobile malware behaviour through hybrid malware analysis approach. 9th International Conference on Information Assurance and Security (IAS), 2013. Pages: 78 – 84.

[3] Gelenbe, E.; Gorbil, G.; Tzovaras, D.; Liebergeld, S.; Garcia, D.; Baltatu, M.; Lyberopoulos, G. Security for smart mobile networks: The NEMESYS approach. International Conference on Privacy and Security in Mobile Systems (PRISMS), 2013. Pages: 1 – 8.

[4] Mikhaylov Dmitry, Zhukov Igor, Starikovskiy Andrey, Kharkov Sergey, Tolstaya Anastasia, Zuykov Alexander. Review of Malicious Mobile Applications, Phone Bugs and other Cyber Threats to Mobile Devices. Proceedings of 2013 5th IEEE International Conference on Broadband Network & Multimedia Technology (5th IEEE IC-BNMT 2013), November 17-19th 2013 Guilin, China. Pages 302-305.

[5] Anne, V.P.K., Rao, J.V., Kurra, R.R. Enforcing the security within mobile devices using clouds and its infrastructure. CSI Sixth International Conference on Software Engineering (CONSEG), 2012. Pages: 1 – 4.

[6] Android Extended Lead While Apple iOS Market Share Growth Paused. Gartner Says Worldwide Sales of Mobile Phones Declined 2.3 Percent in Second Quarter of 2012. Egham, UK, August 14, 2012. URL: http://www.gartner.com/it/page.jsp?id=2120015.

[7] How to reset Android to factory settings? NEXUS-DROID.RU, 2013. URL: http://nexus-droid.ru/408-kak-sbrosit-nastroyki-do-zavodskih-na-android-rukovodstvo-dlya-nachinayuschih.html.

[8] Graham Cluley. Fake Plants vs Zombies and other Android games infiltrate Google Play store, make money for fraudsters. Naked Security, January 21, 2013. URL: http://nakedsecurity.sophos.com/2013/01/21/fake-plants-vs-zombies-android-game.

[9] Mikhaylov D.M., Zuykov A.V., Zhukov I.Yu., Beltov A.G., Starikovskiy A.V., Froimson M.I., Tolstaya A.M. Vulnerabilities of mobile devises operating on Apple and Google systems. Journal "Specialized machinery and communication", №6, Moscow 2011. P 38-40.

[10] Ivaschenko T., Sidorov D. HTML5: viw through the prism of security. Hacker №12, 2010. URL: http://www.xakep.ru/post/54223.

[11] Tracking program for phones and tablets on Android. Gdemoi, 2012. URL: http://www.gdemoi.ru/news/2012/04/programma-treker-dlya-telefonov-i-planshetov-na-android.

[12] New Trojan downloader for Android. Doctor Web, 2012. URL: https://blogs.drweb.com/node/945.

[13] Ivanov P. Phone bugs and mobile devices` security. Information Security, №6, 2012.Apple and Google admit tracking the subscribers. 2011. URL: http://travelgps.com.ua/news/read/Apple_i_Google_priznali_chto_sledjat_za_polzovateljami.html.

[14] Apple and Google keep track over the users not only via phones but also via computers. 2011. URL: http://news.softodrom.ru/ap/b10226.shtml.

[15] Julia Angwin and Jennifer Valentino-Devries. Google's iPhone Tracking. The Wall Street Journal, 2012. URL: http://online.wsj.com/article/SB10001424052970204880404577225380456599176.html.

[16] Mikhaylov D.M., Zhukov I.Yu. Protection of mobile devices from attacks. Ed. By Ivashko A.M. Moscow: Foylisc, 2011. – 192 p.: ill.