I. J. Computer Network and Information Security, 2013, 5, 1-8
Published Online April 2013 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2013.05.01

Security Software Green Head for Mobile Devices Providing Comprehensive Protection from Malware and Illegal Activities of Cyber Criminals

Zhukov Igor, Mikhaylov Dmitry, Starikovskiy Andrey, Kuznetsov Dmitry, Tolstaya Anastasia,
Zuykov Alexander
National Research Nuclear University "MEPhI", Moscow, Russia
zhukov@inbox.ru, mdmitry@mephi.ru, userandrew@rambler.ru, kuzn.dmitry@gmail.com, polynna@yandex.ru,
avzuykov@gmail.com

Abstract **—** This paper deals with the description of the threats to mobile devices and suggests the security software that provides comprehensive protection of personal data and mobile telephone from malware and illegal activity of cyber criminals. The developed security software Green Head protects personal smartphones of majority of brands from spam, viruses and unauthorized access. It is an innovative software product ensuring information security of mobile phones from all currently existing threats that today does not have any full analogs. Green Head security software warns the user about wiretapping, which keeps professional and personal confidential information intact. The developed security software is universal for people using mobile phones in professional and personal life because any stored information is protected from various attacks.

Index Terms — Security software Green Head, malware, wiretapping, spam, cyber criminal

I. Introduction

Today a mobile phone has become an integral part of our everyday life. Mobile phones have become more than just a way of making and receiving calls and sending massages. They can be "smart" and used as a personal computer, for quick access to the Internet and to transfer and download data via the Net.

Nowadays there are more than 6 billion mobile phones in the world [1]. With the growing number of mobile phone users, the problem of information security becomes rather significant.

Mobile malware is now very much a reality and a growing threat. With the increasing functionality the number of cyber criminals and malicious software is growing as well.

If a mobile device has been infected by specially designed malicious software a cyber criminal can make calls, send massages, wiretap private telephone talks, change settings of a device or ever block it, and finally steal money. Moreover, it can be difficult for user to know whether the device has been infected or not because all the manipulations with a mobile phone can be hidden [2], [3], [4].

The paper is organized in the following way:

- introduction telling about main tendencies in the field of mobile technologies;
- description of common attacks on mobile devices without proper level of antivirus security, namely Malicious mobile applications, Phishing pages, Fake messages, Wiretapping, Danger of files transmitted via Bluetooth, Virus websites, Payment for free services;
- description of the developed security software for mobile devices that provides comprehensive protection from malware and illegal actions of cyber criminals;
- conclusion.

II. Common attack on mobile phones

At the present moment, security threats to a mobile device include the following [2]:

- access to wireless transmission networks (Wi-Fi, Bluetooth, GSM, mobile Internet access technologies – GPRS, EDGE, 3G) to obtain harmful content or send confidential data without the user's authorization and, possibly, spend money from the user's account by making calls or sending massages using paid mobile services;
- access to personal data without the user's authorization in order to send them to a third party or to use them in an illegal manner. Personal data include the contact list, massage content, and other confidential information;
- unauthorized access to video and audio recording functions (camera and microphone). Such activities may be used for audio or video eavesdropping;

- screen freeze. The application presents a sort of a Screen Lock similar to Windows WinLock programs (the screen is blocked with a prompt to send paid massages or transfer money to receive the unblocking code);
- unauthorized access to other features on the mobile device – vibration, speaker, backlighting – in order to disturb the device's normal operation.

Hereafter we would like to consider attacks that may affect a mobile device with insufficient level of security provision.

A. Malicious mobile applications

Mobile phones are getting more and more functional, thus, the diversity of mobile applications is also increasing. For some devices such applications, for example games, are placed on the official resources, however, a lot of applications are freely available in the Internet. Often they may contain malicious code. And it is not enough to install applications only from the official website, since even they can be harmful, for example, the "new version" or addition to the popular application [5].

The most malicious applications are that request more rights than they need to perform their functions. In other words, it is obvious that calculator does not need to identify user`s location and work with messages. Such applications can initiate calls, turn on and off camera, microphone or discharge the battery with no reason, change the settings of a device and even block it.

Mobile applications can be sophisticated but the cyber criminal can easily insert a malicious code in popular game [6]. The user downloads a game, install it and at the same time the smartphone becomes infected.

B. Phishing pages

Many people use mobile phone in order to access the Internet without worrying about the device safety. Networks contain a lot of so-called "phishing" pages that replicate the well-known resources changing, for example, only one letter in the address [7].

Phishing is the act of attempting to acquire information such as usernames, passwords, and credit card details (and sometimes, indirectly, money) by masquerading as a trustworthy entity in an electronic communication. Phishing is typically carried out by email spoofing or instant messaging and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one. [2], [8].

After visiting such a webpage the phone is infected, or a person enters their username and password to access the resource sending it to attacker. The smartphone user may even lose money on his or her bank account if erroneously sending credit card details to a cyber criminal.

C. Fake messages

Nowadays the use of fake messages to attack unprotected mobile phones is getting very popular. A person receives messages from a well-known phone numbers, or on behalf of the mobile operators that are actually sent by hackers.

For example, each person has contacts like "mum" or "dad". This peculiarity can be used by a fraudster. He may write "mum" in the sender`s address and the mobile phone user will perceive the massage as one sent from his relatives.

Such a technique is used by fraudsters to mislead the victim and to persuade him or her, for example, to send a message to a certain number to get a discount on mobile communication, or even something more serious. If a person replies they can not only lose private information and money but also have their phone infected by malicious software [9].

The problem lies within the impossibility for the phone user to detect a fraud number without special software but it is quite possible for cyber criminal to fake the sender's name.

D. Wiretapping

A mobile phone can be used by hackers to wiretap personal phone conversations. It is not even necessary to infect the smartphone with malware [10].

The cyber criminal can secretly put the microphone of a device on even if the telephone itself is switched off. After that he can wiretap confidential information.

E. Danger of files transmitted via Bluetooth

Bluetooth is a wireless data exchanging technology. And a lot of viruses are spread via Bluetooth. Data transfer channel itself is secured, but attackers can play on the users' credulity and curiosity.

If Bluetooth is turned on in visible mode the mobile phone can suddenly receive a request to accept the file. It is quite possible that the file contains a virus that will infect the device [11], [12].

Such attacks are widely spread in public places: shopping malls, subways, universities, museums, cafes, etc.

F. Virus websites

Nowadays viruses that infect websites are getting sophisticated. Today they also aimed at users of mobile devices.

When viewing infected computer resources via a personal computer browser, a person will not mention something strange. But once they visit it from a smartphone the device will be immediately redirected to a fraudulent page.

Usually, at this page the user will be offered to download critical software updates, or check the safety devices. But attackers will just write off money from the account. In both cases the user of the phone loses money [2].

This kind of viruses can "live" on websites for a long time. The owners will stay in dark about it because they are likely to visit it from PCs. This peculiarity makes such viruses dangerous and tenacious.

G. Payment for free services

Almost all cellular operators provide services – the ability to subscribe to any information (weather, jokes, etc.) The point is that a person enters their number on a

website of a service supplier who in turn communicates with the mobile operator and asks to send to the user a message with a confirmation code.

Once the user receives the confirmation code, he or she types it at website of a provider and then the code is sent to a mobile operator. If the code is correct – then the mobile phone is successfully subscribed to the mailing list. After that a defined amount of money will be written off the account.

However, this scheme may be used by fraudsters.

Most users believe that the money will not be written off until they personally send a message, so they easily type the phone number and a confirmation code on the fraudulent site. However, after that procedure they lose money without being provided with any service [13], [14].

III. Comprehensive security provision for mobile phones

As we can see from the information mentioned above the number and complexity of malicious software is growing from day to day. Security software is available today for protecting personal computers (e.g., desktop and laptop computers) against at least some forms of malicious software. Mobile phones are also susceptible to malicious software. At least in part because of the wide range of functions that may be performed by smartphones, there is a wide range of possible types of attack by malicious software or other forms of interaction [5].

That is why it is vital to develop software that is aimed at protecting special features of mobile devices. For this purpose Green Head security software has been designed. It is an innovative software product ensuring information security of mobile phones from all currently existing threats that today does not have any full analogs.

In a general aspect, Green Head is the security software providing complex protection of a personal mobile device (and the user) on a number of directions. It comprises comprehensive protection from malicious software, counterfeit massages with substitution of number, unauthorized interception, wiretapping and also compromises of private data.

The security software easily adapts to the characteristics of popular operating systems for mobile phones and emerging “new items” from developers of viruses and other malicious programs.

The security software controls and alerts unauthorized access to the wireless information transmission channels, prevents from downloading malicious content and protects user’s data from being sent to the third parties and its improper use. Green Head detects malicious application at the moment it is trying to perform an undesirable actions. This allows preventing adverse effects on the system. Database is updated every time when program updating is performed.

Green Head security software comprises three main products:

- Green Head Antispam reliably protects user from receiving unnecessary and malicious information, performs the functions of protection against attacks with the forgery of the number and other types of mobile fraud.
- Green Head Antivirus monitors the activity of the installed applications, protecting users from malicious actions that can endanger the security of mobile devices. The basis of Green Head Antivirus is a unique method of proactive protection.
- Green Head PROcontrol provides confidentiality of conversations. It also protects from malware massages and from switching the camera or microphone on by malicious apps. PROcontrol affords to hide contacts. It has SOS button, antitheft option and file encryption. Green Head PROcontrol includes the first two products.

The main application provides the user with a list of all modules available for downloading and starting, and is responsible for their activation, updating, and password-protected running.

Except the main functions, the Green Head user can supplement them with options. The user can activate all possible options or only some of them depending on the need.

A. Antivirus protection

Android has become one of the most popular platforms on the IT market [15]. It is programmed in the Android system that when installing an application the user has to confirm permissions for using the mobile device's functions; but users actually do not know exactly why the application needs any particular rights and in the majority of cases they simply pass over this information.

The problem is complicated by the fact that Android provides neither clear functional division of certain groups of permissions, nor well-developed documentation on them. Besides, the installation dialog in some Android versions does not help the user concentrate on the permissions requested. This module's primary objective is to assist the user in controlling applications' access to potentially dangerous functions on mobile devices in real time in the context of the threats mentioned above [16].

Each Android application operates under its own Linux account (on the shell level) and runs as an individual process within its own Dalvik virtual machine [17]. Thus, direct interaction between processes and penetration of a process to the memory space of another process become impossible, including access to data of another process. Interaction between active applications and joint use of data is very limited and regulated by the application providing data during its installation.

The Android system basically prevents the creation of “classic” computer viruses that embed their code in the memory space of other processes and install themselves as system modules, as well as propagate themselves through data communications networks (since it is impossible to run a malicious application setup process on a remote device) [19].

Green Head Antivirus uses absolutely new approach to protection against malicious applications. Previously, files were scanned for a malicious applications' code

based on the existing virus database. Such protection called signature analysis has a fundamental defect – even the slightest change of a malicious application's code makes it unidentifiable to the antivirus until the code is included in the signature database. As a result, antivirus software using such protection is only able to identify widespread malicious applications, and they are vulnerable in the context of new threats that may be a mere modification of the old ones.

Green Head Antivirus software is based on a proactive protection idea the main task of which is to identify security threats in real time by monitoring applications' activities related to potentially dangerous operations (data transfer, positioning, massages transmission, outgoing calls, user data reading and use of built-in functions of the telephone – camera, microphone) and to prevent them by blocking such processes and providing a warning to the user.

Installation packages of the Android-based applications (.apk) contain compiled Java code for JVM Dalvik and compiled resource files [17], [18]. When monitoring an application, the Antivirus software modifies the .apk file by embedding its code into it to enable the Antivirus to receive notifications about potentially dangerous processes, inform the user, and suppress them. Once the .apk file has been modified, the Antivirus suggests re-installing the application in order to apply the modifications made.

B. Spam prevention and verifying validity of massage sender number

Green Head Antispam protects mobile device from receiving malicious, fake and useless information. The Antispam module checks incoming messages for:

- fake or potentially fake number/sender's name with the respective notification to the user;
- presence of the sender's number in the user's black/white list or presence of a part of the message (in black list only) with suppression of such a message (staying outside the system);
- presence of the sender's number on a fraudster list with suppression of such a message;
- presence of unwanted content in the message (links to harmful websites, fraudulent scams or spam) with a notification given to the user.

Sender number validation is a unique function of Green Head Antispam. It protects the user from many threats which may result from third parties' ability to send their messages in other mobile subscribers' names and in the operator's name.

At the present time, mobile operators do not validate the delivered messages, and the mobile phone software makes fraud easier by applying overly broad comparisons when searching numbers in the phonebook.

In order to discover a fake contact name, the address is compared to all possible transliterations of contact names (if a name is entered using Latin letters, the address is compared to it). For example, if a person receives a message from someone named Petya or Petja, and they have Petr in a contact list (including last name or other words in the Name field), the program will give the following warning: "Sender uses a fake name!"

If there are no matching names, it is checked if the phone number is recorded in the address. If it is a number, the following warning is given:"Sender's name is fake!"

General algorithm for incoming message processing is presented in Fig. 1.

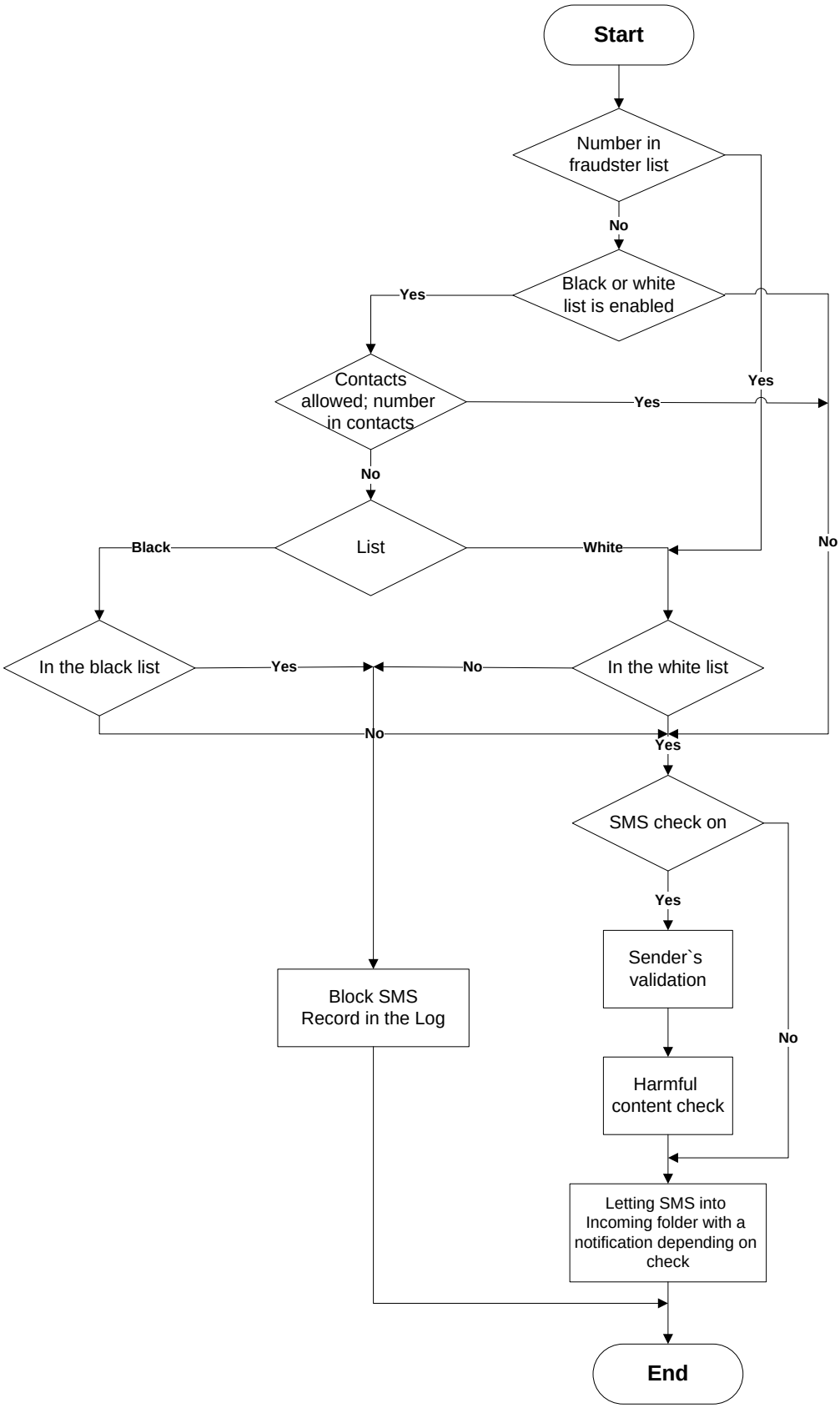

Figure. 1. General Algorithm for Incoming Message Processing

There is also a feedback function making it possible for users to send unwanted messages that were not identified by the Antispam module to the developers for inclusion in the database and to the mobile operators for recording fraudster numbers on the black lists.

Green Head specialists, who maintain the server, receive notifications about all messages that have accumulated a certain number of complaints from different users, verify them and, if the massages are confirmed to be malicious, the sender's number is added to the black list automatically. When databases are updated next time, the number is uploaded to all clients.

C. Protection against wiretapping

This module ensures the user's protection against unauthorized eavesdropping on conversations. The following unique functions are supported:

- protection against undetected enabling of the phone's microphone by malicious applications for eavesdropping on the user's and the user partners' conversations;
- protection against the recording of phones calls by third party software installed on the phone;
- protection against imitation of the cellular operator's base station.

The application's functionality is based on the concurrent operation of the tracking modules for phone conversation recording, recording of conversations of the user and the user's conversation partners, and tracking of virtual cells (fake base stations).

General algorithm for the wiretapping security module (base stations checking) is presented in Fig. 2.

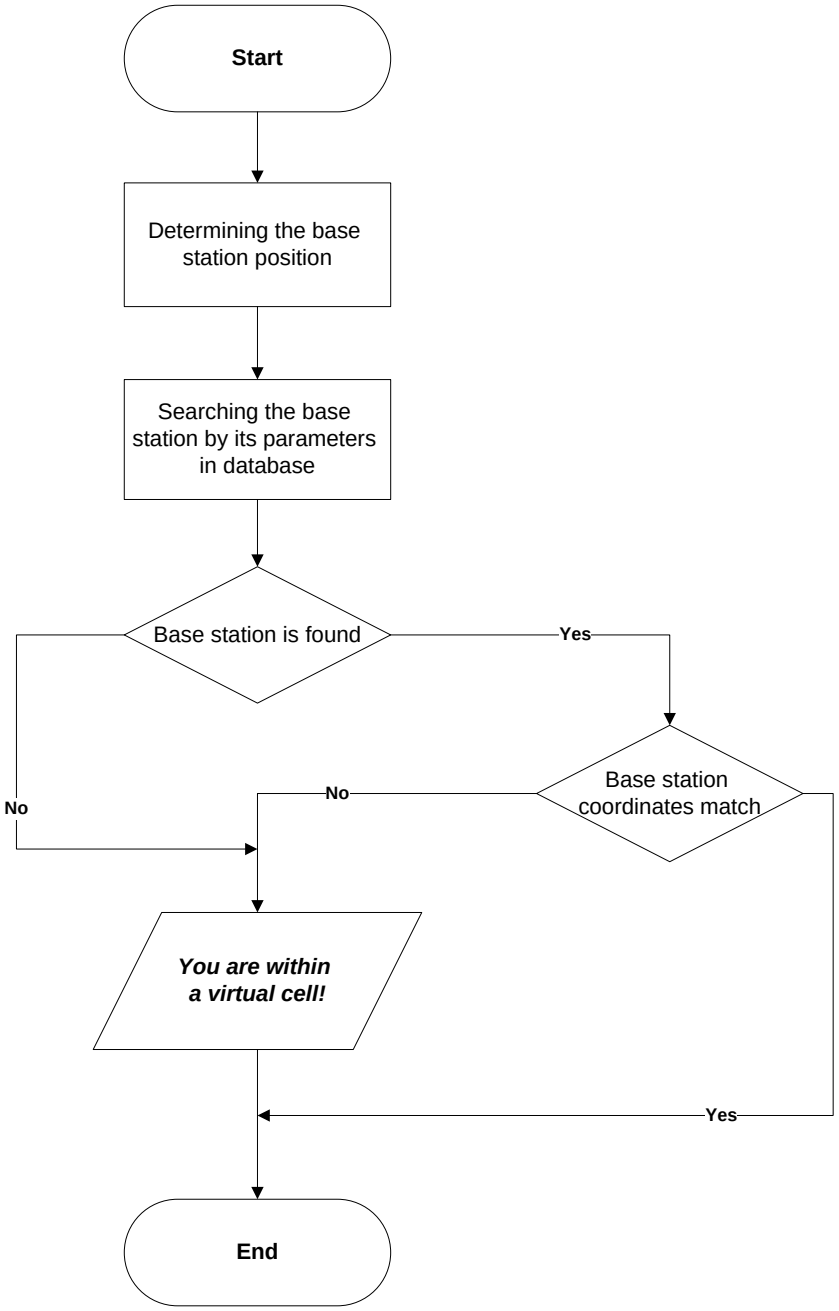

Figure. 2. General Algorithm for the Wiretapping Security Module (Base Stations Checking)

Tracking modules for phone conversations and conversations of the user with the user's conversation partners have black and white lists of applications that are allowed or prohibited to perform recording, respectively. Applications from the black list are automatically suppressed (only for Android 1.6 and 2.1 OS versions).

Tracking module for the virtual cell uses databases of cellular operators' bases stations and several algorithms for identification of a fake base station.

D. Hiding contacts

This module is used to store information about selected contacts, as well as messages and calls diary records with them, in a hidden mode. Contact hiding is used to prevent unwanted access to the user's valuable contacts.

This module makes it possible for the user to hide all information about selected contacts with the ability to view them again, send messages and make calls to the numbers of the hidden contacts using the module only.

Once a contact has been hidden, correspondence with such contact and call records will be hidden as they appear, thus, the contact will remain hidden even if a message arrives from him while the phone is controlled by someone else.

E. Theft protection

The theft protection module protects the phone and user`s data against theft via the following methods:

- device locking;
- deletion of user data;
- sending the device's location information (from the thief's number as well).

The theft protection functions can be enabled automatically when the device's SIM card is changed or manually by sending a controlling message.

F. Checking microphone and baseband processor current status to detect hidden audio transmission

A mobile device is capable of unauthorized sending data in response to an external controlling command. The baseband processor is periodically queried if there are any active calls or auxiliary services initiated by the network using AT (attention) commands in order to check its current status and detect connections hidden from the user.

Microphone is checked on the subject of sending data to the baseband processor to control its current status. The user will be notified if there are any unauthorized connections.

Specific features of the system include checking current status of the microphone and baseband processor to detect an unauthorized operation by means of external controlling commands and notification of the user about hidden audio transmission.

G. SOS button

SOS button is widget for a smartphone's home screen for quick sending of a predefined text and device coordinates to a preset number. In a dangerous situation, the person will only need to press the widget and confirm sending. Hence, only send and delivery status notifications will be displayed. They will remain in the notification line until removed by the user. This minimizes the required operations with the phone making it possible to send the message secretly.

Transmission of algorithm is as follows: the user confirms SOS sending; massage with a predefined text will be sent immediately; then, while the message is being delivered successfully, the device starts waiting for location data from the Google server (using cell towers - with large inaccuracy; using Wi - Fi access points - with average inaccuracy) and from the built - in GPS (with high precision). If the phone is within the network coverage zone or there are Wi - Fi access points nearby (if Wi - Fi is enabled), the coordinate data arrives almost immediately, while the GPS may be getting started and looking for satellites for several minutes; therefore, the coordinates will be sent to the preset number as they become available.

When new coordinate information is received, they are checked if more precise coordinates had already been sent. The message is sent after waiting for 5 seconds in case more precise coordinates arrive. The device will wait for information about the coordinates until the coordinates with an inaccuracy radius of less than 30 meters are received, or after waiting for 5 minutes.

VI. Conclusions

This paper is devoted to description of security software Green Head providing comprehensive protection from all current types of malware and cyber criminals` actions. Green Head software detects dangerous application at the moment it is trying to perform an undesirable actions. This allows preventing adverse effects on the system. A software implemented method for mobile device security system comprising: controlling third party applications executing on the device, including executing modified versions of the application that include security code, and validating communication at the device, including validating massage communication.

References

[1] Amanda Wills. The World Will Soon Have More Phones Than Humans. 2012. URL: http://mashable.com/2012/07/19/more-phones-than-humans.

[2] Zhukov Igor, Mikhaylov Dmitry, Ivashko Andrey. Mobile phone protection from attacks. Moscow. FOILIS, 2011. -192 pages.

[3] A.G. Beltov, I.Yu. Zhukov, A.V. Novitskiy, D.M. Mikhaylov, A.V. Starikovskiy. Security issues of mobile devices. Safety of information technologies. "Mobile communication security ", 2012, №2. P 5-7.

[4] Schmidt, A.-D., Schmidt, H.-G., Batyuk, L., Clausen, J.H., Camtepe, S.A., Albayrak, S., Yildizli, C., "Smartphone malware evolution revisited: Android next target?", Malicious and

Unwanted Software (MALWARE), 2009 4th International Conference on, On page(s): 1–7.
[5] Zhukov Igor, Ivashko Andrey, Mikhaylov Dmitry, Starikovskiy Andrey. Mobile technologies. Moscow: INFRA-M, 2012. - 206 pages.
[6] A.G. Beltov, I.Yu. Zhukov, D.M. Mikhaylov. Protection of mobile phones from attacks. Methods and tools of information security: 21st Scientific Conference June 24-29, 2012. - St. Petersburg, Polytechnic. University Press, 2012. - 191 p. P 43-44.
[7] Marco Cova, Christopher Kruegel, and Giovanni Vigna. There is No Free Phish: An Analysis of "Free" and Live Phishing Kits. 2nd USENIX Workshop on Offensive Technologies, 2008. URL: http://static.usenix.org/event/woot08/tech/full_papers/cova/cova_html.
[8] Phishing. Auburn University. URL: http://www.auburn.edu/oit/phishing.
[9] G.A. Evropeytsev, M.I. Froimson, G.A. Urvanov. Attacks on mobile phones using SMS-spam. Safety of information technologies. "Mobile communication security ", 2012, №2. P 14-16.
[10] A.V. Zuykov, D.M. Mikhaylov, A.V. Starikovskiy, M.I. Froimson. Wiretapping of mobile subscribers. Safety of information technologies. "Mobile communication security ", 2012, №2. P 11-13.
[11] Pikhtulov A.A., Mikhaylov D.M. Heuristic features of Bluetooth-virus for mobile devices. "Science and modernity - 2011": materials of XIII International Scientific Conference: in 3 parts. Part 2 / Ed. S.S. Chernova. – Novosibirsk: State Technical University, 2011. - 278 p. P 233-237.
[12] Xia Wei, Li Zhao-hui, Chen Zeng-Qiang, Yuan Zhu-zhi, "The Influence of Smart Phone's Mobility on Bluetooth Worm Propagation", Wireless Communications, Networking and Mobile Computing, 2007. WiCom 2007.
[13] T.R. Khabibullin, A.G. Beltov, I.Yu. Zhukov, A.V. Zuykov, A.S. Smirnov. Vulnerability of software for mobile phones and secure programming techniques. Safety of information technologies. "Mobile communication security ", 2012, №2. P 32-35.
[14] M.I. Froimson, A.M. Rapetov, N.V. Sychev. SMS-disorientation of mobile phone users. Safety of information technologies. "Mobile communication security ", 2012, №2. P 17-21.
[15] 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, Gartner, August 14, 2012. URL: http://www.gartner.com/newsroom/id/2120015.
[16] C. Collberg, C. Thomborson. Watermarking, Tamper-Proofing, and Obfuscation - Tools for Software Protection. Technical Report 2000-03. Department of Computer Science, University of Arizona, 2000.
[17] Sheng Liang, The Java Native Interface Programmer's Guide and Specification, Sun Microsystems, Inc. May 1999.
[18] David Ehringer, The Dalvik virtual machine architecture. Techn. report (March 2010), 2010 - davidehringer.com.
[19] Komatineni S., McLean D., Heshimi S. Google Android: Mobile Programming / / Pro Android 2. - 1st ed. - St. Petersburg, 2011. - 736 p.

Zhukov Igor, Doctor of Engineering Science, Professor. National Research Nuclear University "MEPhI", Moscow, Russia. Computer Systems and Technologies Department.

Mikhaylov Dmitry, PhD, associate professor of National Research Nuclear University "MEPhI". Computer Systems and Technologies Department.

Starikovskiy Andrey, teaching assistant of National Research Nuclear University "MEPhI". Computer Systems and Technologies Department.

Kuznetsov Dmitry, engineer. National Research Nuclear University "MEPhI". Computer Systems and Technologies Department.

Tolstaya Anastasia, graduate of National Research Nuclear University "MEPhI". Department of Management and Economics of High Technologies.

Zuykov Alexander, Ph.D. candidate of National Research Nuclear University "MEPhI". Computer Systems and Technologies Department.

