PRINT: ISSN 0972-0073 ONLINE: ISSN 2456-6802
Anthropologist, 17(1): 37-43 (2014)
DOI: 10.31901/24566802.2014/17.01.05

Developing a Security Software for Android-based Systems ("Secand")

Ozgur Can Karaduman[1], Suleyman Kaygisiz[2], Ali Buldu[3], Kazim Yildiz[4] and Daghan Cetinol[5]

[1]Faculty of Technical Education, Marmara University, 34722, Turkey
E-mail: [1]<ozgurcan_karaduman@hotmail.com>, [2]<suleymankaygisiz@msn.com>
[3]<alibuldu@marmara.edu.tr>,[4]<kazim.yildiz@marmara.edu.tr>
[5]Koc System, 34700, Turkey
E-mail: daghan.cetinol@kocsistem.com.tr

KEYWORDS Security for Android. Retrieving GPS Coordinates. Reading SMS. Secand

ABSTRACT In this study, an application has been developed in the Eclipse environment for android that is used to locate the stolen mobile devices with turned on status. If an user send a Short Message Service (SMS) to our device from another phone as soon as we notice that our device is stolen, the designed application, which the name of "Secand" was given by us, will detect the password within this SMS and understand that our phone is stolen. Our application must be continuously running in the background in order to detect this incoming SMS. After our application detects the password within SMS, it will retrieve Global Positioning System (GPS) coordinates of our device and send these coordinates to us via SMS. Secand must have all GPS and SMS related authorizations for all of these operations. If it is assumed that the thief is on the move after the first GPS coordinates are sent, our application must send the coordinates of device in certain frequencies. This range of time can be set by the user. Such details can be activated optionally by the user after Secand application is installed to the device.

INTRODUCTION

Last decade computer aided smart systems have found a wide application to make easier human life, for instance instructional materials (Baytak and Hirca 2013), software development (Yilmaz 2013; Kabaca 2013), mobile navigation systems(Wang 2013) e-learning applications (Köse et al. 2013; Vural 2013) etc. Recently, Android can be accepted as one of the most popular smart system for computer based applicaitons.

Android is a linux, which is a computer operating system assembled based mobile operating system with open source code, developed by google, open handset alliance and free software community for mobile devices (smart phones, personal digital assistants, tablets, etc.) (Nedircom 2013).

Android is built on linux core. The middleware, libraries and Application Programming Interface (API) have been written in c programming language for this mobile operating system. Applications are running on apache backbone that contains java compatible libraries (Wikipedia 2013). Android uses Dalvik Virtual Machine (DVM) in order to run compiled java code. There is a significant feature here that differentiates DVM from Java Virtual Machine (JVM).

JVM is a stack machine. Commands are received from the point indicated by stack pointer through the main memory. However DVM is a register machine and retrieves commands directly from the registers available within microprocessors. It performs mathematical transactions with too many interim results pretty fast (Ogutmen 2012). Google has benefited from the possibilities offered by microprocessors in the most suitable way thanks to this structure that it has developed.

While Nokia was taking solid steps in mobile phone market in 2000s with symbian operating system, Apple released first i-phone in 2007 and quite impressed people with touch screen, chic design and high quality software. Suddenly the mobile world attracted all attention. I-phone was growing so fast that it has started to outpace all other phones in the market. Then android showed up as a competitor to i-phone (Sel 2011).

Google had acquired Android Inc. in July 2005 and established a small start-up company in Palo Alto. There were rumors that Google will penetrate into mobile devices market. Today there

Address for correspondence:
Kazim Yildiz
Marmara university
Technical education faculty(34722)
Istanbul, turkey
Telephone: +90 (216) 336 57 70
E-mail: kazim.yildiz@marmara.edu.tr

are more than 700,000 applications running on android operating system. One of the most important reasons of having such high number of applications is undoubtedly the open source code structure of this operating system, which allows so many programmers to work on the applications that improve functionalities of devices (Tibken 2012).

MATERIAL AND METHODS

Mobile Phone Theft in Turkey

Similar to the entire world, mobile phone was started to be used widely also in Turkey after 1990s. While there were only 80,000 mobile phone users in 1994, this number has reached 8 million in 2000 in Turkey. At the end of December 2005, total number of mobile phone line subscribers, to which three national service providers (Avea, Vodofone and Turkcell) were offering mobile phone services, reached 43.4 million (Yildiz 2006). According to 2011 data of www.worldbank.org, 89 of every 100 persons are using mobile phone in Turkey (World Bank 2013).

According to June 2012 data of International Telecommunication Union, the number of mobile phone subscriptions throughout the world reached 6 billion at the end of 2011 (International Telecommunication Union 2012). This number exceeded 67 million in Turkey in 2013, which means that almost everyone has a mobile phone. However the number of mobile phones is 168 million, that is, 2.5 times more than the number of subscribers, according to 2012 data. When we compare this number with the country's population, it is seen that the number of mobile phones per person is more than two. As mobile phone is so widely used, its theft is a significant problem in Turkey.

As it can be seen from Table 1, the number of notices for lost or stolen mobile phones was increased to 32,775 in 2012 from 27,843 in 2010. These notices were made by phone to information and notification center. Considering the fact that there are many stolen mobile phones, of which a notice has not been made as the International Mobile Equipment Identity numbers of phones are not known widely, while examining this table, we can clearly see that mobile phone theft is a quite significant problem in Turkey.

Table 1: Notices for lost and stolen (per year) (Bilgi Teknolojileri Kurumu 2012)

Period	*No. of confirmed notices*	*No. of non-confirmed notices*	*Total*
2010	24.096	3.747	27.843
2011	29.060	3.610	32.670
2012	29.184	3.591	32.775

When a notice for a stolen mobile phone is received, the data provided by the person who has submitted the notice are transmitted to the operator of Global System for Mobile Communications (GSM) and the device is disabled for communication after such data are confirmed.

When the device is queried with its IMEI number through official website of Mobile Device Registration System located at http://www.mcks.gov.tr/tr/ihbarsorgulama.php, after the notice was made, it is seen as 'device notified as stolen'. After the notice was confirmed, the status of device is changed to 'stolen device'.

As it is written above, the device is disabled only for communication if the notice is confirmed. It is stated at the official website of Mobil Cihaz Kayit Sistemi that *our organization is neither responsible for finding the stolen, usurped or lost phones nor for returning them to their owners* (Mobil Cihaz Kayit Sistemi 2013). This system does not have any feature or functionality for finding the device.

Basics of Android Based Mobile Phone Security Application, Named *"Secand"*

This paper describes the application that was developed to locate android based smartphones, whose use has also started recently in Turkey, in case the smartphone is stolen. Initially we have to state that the application will be active when the device is turned on. In other words, this application is developed by assuming that the device is still turned on and user's Subscriber Identity Module card is still available on the device after the device is stolen. As none of the applications that have been developed for android based smartphones are running when the mobile phone is turned off, this application will also not run.

As it is seen in Figure 1, when the user of smartphone notices that his/her phone is stolen

and sends a SMS to the stolen phone from another phone, this application would detect the password within the SMS and send current GPS coordinates back to the phone, from which a SMS is sent. This application would not only send GPS coordinates of stolen smartphone but also, at the user's discretion, would be able to switch the front camera of smartphone on in order to take a picture and send this picture to the counter party as a multimedia message system or lock the phone.

The application must have some permission to perform the tasks that were determined by the user. These permissions are the ones that many application needs to improve the functionality of android based devices. In Figure 2 operation of application can be seen.

There is not a single list of permissions for android- based devices. The list given in the website of android developers, located at http://developer.android.com/reference/android/manifest.permission.html can be used to list permissions required for applications running on an android based device (Android Developer 2013). For example, Secand application must listen incoming SMS continuously to understand that smartphone was stolen. In order to be able to listen incoming SMSs, our application must have the necessary permission in androidmanifest. xml file, located in our application, as it can be seen in the following code example:

<uses-permission
android:name=*"android.permission.RECEÝVE_SMS"*/>

When we want to install such applications that need permission to android-based devices, android operating system asks the user whether the permissions needed by the application are granted or not. Thanks to this feature, we can understand the operations that malware intend to perform on our smartphone and ensure the security of our device by not allowing them to do so. The screen for allowing our application to listen incoming SMSs while our application is being installed to our smartphone can be seen in the Figure 3.

Similar to the access to SMS, our application must have necessary permissions in order to be able to retrieve current GPS coordinates of smartphone and, if requested by the user, to switch front camera on, take a picture and send this picture as mms. One can use the website of android developers specified above in order to see the details and same type of utilizations of these permissions (Android Developer 2013).

When one launch the application for the first time, it will be seen that none of the tasks are selected by default. Since there is not any task to be performed by default, the letters of tasks available under the *'yapilacaklar'* (to do) section on the home screen will be displayed in red. The user should click *'gorevler'* (tasks) button

Fig. 1. Simple operation logic of the application

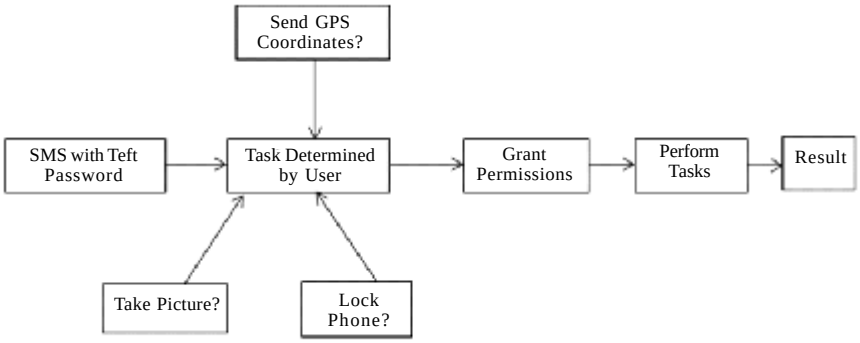

Fig. 2. Operation of application

on the application's home screen to visit *'gorevler'* (tasks) screen and select the tasks that he/she wants to be performed. When the tasks are selected and the application's home screen is returned, it will be seen that the tasks to be performed are written in green whereas the tasks that are not going to be performed are written in red. In order to demonstrate how this service works, screenshots of our application have been taken from our smartphone and these screenshots are displayed in Figure 4.

The *'ayarlar'* (settings) button on the application's home screen is clicked to visit *'ayarlar'* (settings) screen and necessary settings other than tasks are made on this screen. For instance, the text to be entered into the text box, called *'sihirli kelime'* (magic word), would be the password that our application will identify to understand that smartphone is stolen. The user of smartphone should send this password as soon as he/she notices that smartphone is stolen in order to start predetermined tasks. This password (magic word) is '1234' by default. User can change this password in any manner he/she requests.

Fig. 3. The screen for approving permissions while installing the application

When *'nasil kullanilir'* (how to use) button on Secand application's home screen is clicked, general information on how our application is operating and how it can be used are given. *'Ana menu'* (main menu) button, which is also available in other sub screens, can be used or 'back' key of our android based phone can be used to return to home screen.

When *'kapat'* (close) button, one of the two buttons available at the bottom of application's home screen, is clicked, Secand will be closed. In this case, even if the password indicating that Secand smartphone was stolen is received, the tasks will not be performed since it is turned off. However if *'gizle'* (hide) button is clicked instead of *'kapat'* (close) button, we will exit from the application and in such case Secand application will not be turned off and will continue to be running on the background. So, if smartphone is stolen, our application will detect the password sent by the user and perform the expected tasks.

The application will perform the tasks as soon as the SMS that contains the password for stolen smartphone is received. It will retrieve GPS coordinates, match these coordinates with the names of cities and districts and convert them to SMS format. Then it will send this SMS to the user of SIM card, from which the password was sent. If 'resim cek' (take picture) task was activated, the application will turn our smartphone's front camera on and take a picture and send this picture to the counter party in mms format. This

Fig. 4. Application's home screen

'resim cek' (take picture) task would be useful if the person that has stolen the smartphone is using the phone and looking at the phone's screen at that time.

The user must grant necessary permissions to the application during installation in order to allow the application to perform these tasks. Secand provides receive_SMS permission for detecting incoming SMSs and access _fine_ location permission for retrieving GPS coordinates and the user must allow them during the installation (Narman 2012). Codes of some permissions, defined in androidmanifest.xml file of our application are given below.

```
<uses-permission android:name=" android.permisssion. access_fine_location">
<uses-permission android:name="android.permission.access_coarse_location">
<uses-permission android:name="android.permisssion.internet">
<uses-permission android:name="android.permission.read_phone_state"/>
<uses-permission android:name="android.permission.send_SMS"/>
<uses-permission android:name="android.permission.receive_SMS"/>
<uses-permission android:name="android.permission.read_SMS"/>
<uses-permission android:name="android.permission.write_SMS"/>
<uses-permission android:name="android.permission.receive_mms"/>
<uses-permission android:name="android.permission.write"/>
<uses-permission android:name="android.permission.vibrate"/>
<uses-permission android:name="android.permission.write_external_storage"/>
```

It is also possible to access "permissions" tab, located on lower left corner of the screen, quickly through android mainfest eclipse when our .xml file is open (Tac 2011). In Figure 5 application's task screen can be seen. User can be selected one of the task from there.

Figure 6 shows selecting tasks on application. User can be choose all of the tasks of whatever. For example in this screen one and three number of the tasks are selected.

After task are selected screen of the application can be seen in Figure 7. User has chosen one and three. So in the screen one and three number of the tasks are green. And red task is not selected for this application.

Fig. 5. Application's tasks screen

Fig. 6. Selecting tasks on the application

Fig. 7. After tasks are selected

OBSERVATIONS AND DISCUSSION

The application, named 'secand' (security for android), that have developed, contributes a lot to the efforts for locating stolen android based smartphones. As it can be seen in Table 1, more than 30,000 notices were made in 2012 in our country for lost and stolen phones. However mobile device registration system, which was developed as a precaution, can only disable these devices for communication. In other words, it does not have any function for locating and finding the stolen devices. Therefore the application that we developed is very important. Secand application's functions, such as notifying GPS coordinates of the stolen phone in city and district format, switching the device's front camera on and taking a picture and sending such picture in mms format, improve the functionality of application.

ACKNOWLEDGEMENTS

This work is supported by Koc System Data and Communication A.C.

REFERENCES

Android Developer. Manifest Permission. From <http://developer.android.com/reference/android/manifest.permission.html> (Retrieved on March 13, 2013).

Baytak A, Hirca N 2013. Prospective teachers' lived experience on computer-based instructional materials: A phenomenological study. *Anthropologis*t, 16(1-2): 97-109.

Bilgi Teknolojileri Kurumu 2012. Cagri Merkezi Trafik Bilgileri. From <http://www.btk.gov.tr/kutuphane_ve_veribankasi/istatistikler/2012-EKBHCDI.pdf> (Retrieved on March 16, 2013).

International Telecommunication Union 2012. Itu Releases Latest Global Technology Development Figures. From <http://www.itu.int/net/pressoffice/press_releases/2012/70.aspx#.uux-0hwqwwa> (Retrieved on March 20, 2013).

Kabaca T 2013. Using dynamic mathematics software to teach one-variable inequalities by the view of semiotic registers. *Eurosia Journal of Mathematics, Science and Technology Education,* 9(1): 73-81.

Kose U, Koc D, Yucesoy SA 2013. Design and development of a sample "Computer Programming" course tool via story-based e-learning approach. *Educational Sciences: Theory and Practice*, 13(2): 1235-1250.

Mobil Cihaz Kayit Sistemi 2013. Kapatilan Cihazlar. From <http://www.mcks.gov.tr/tr/KonuDetay. php?BKey=39> (Retrieved on March 17, 2013).

Narman AE 2012. *Android Programlama*. Istanbul: Kodlab Yayin Dagitim.

Nedircom 2013. Android Nedir? From <http://android.nedir.com/> (Retrieved on March 11, 2013).

Ogutmen N 2011. *Android*. Istanbul: Kodlab Yayinlari.

Sel V 2011. Android Tarihi Infografik. From <http://androidturkey.net/2011/08/15/android-tarihi-infografik/> (Retrieved April 1, 2013).

Tac M 2011. *Android Programlama*. Istanbul: Dikey Eksen Yayin.

The World Bank 2013. Mobile Cellular Subscriptions. From <http://data.worldbank.org/indicator/it. cel. sets.p2? order=wbapi_data_value_2011+wbapi_data_value+wbapi_data_value-last&sort=asc> (Retrieved on March 15, 2013).

Tibken S 2012. Google Ties Apple With 700,000 Android Apps. From <http://news.cnet.com/8301-1035_3-57542502-94/google-ties-apple-with-700000-android-apps/ > (Retrieved on March 15, 2013).

Vural OF 2013. The impact of a question-embedded video-based learning tool on e-learning, e-learning approach. *Educational Sciences: Theory and Practice*, 13(2): 1315-1323.

Yildiz M 2006. Kamu siyasalari acisindan cep telefonu teknolojisi ve mobil devlet. *Hacettepe Universitesi Iktisadi ve Idari Bilimler Fakultesi Dergisi*, 24: 241-263.

Yilmaz Z 2013. Usage of Tinker Plots to address and remediate 6th grade students' misconceptions about mean and median. *Anthropologist*, 16(1-2): 21-29.

Wang TS 2013. Design and assessment of joyful mobile navigation systems based on TAM and integrating learning models applied on ecological teaching activity. *Eurosia Journal of Mathematics, Science and Technology Education*, 9(2):191-200.

Wikipedia 2013. Android (Iºletim Sistemi). From <http://tr.wikipedia.org/wiki/android_(iºletim_sistemi)> (Retrieved on March 13, 2013).