Android Mobile Guardian System Security Architecture for Handset and Data Security

So-Ra Han and Mason Noah

Abstract--- *Nowadays, usage of smart phones are rapidly increasing and turning out to be our second memory bank, which contains mostly sensitive personal information. Access to this information by others violates our privacy. In order to overcome this concern, the requirement for developing a software solution that would secure private information was essential. On the other hand with more people switching to other smart phone for various activities, securing the old devices has now turned out to be a high priority. Mobile Guardian System for Android is one such application for the purpose of protecting the Android Smartphone against such information thefts. The Mobile Guardian System for Android incorporates security architecture that support both handset and data security.*

The Android device is being exploited since both of its fame and the capability for the code to be open-source. This is in contradiction of other phones, like the iPhone, which would not permit for open source application development and would not go in favor of the objectives of the overall project.

To conclude, the application provides best features and utilities that would become quite popular with Smartphone users. These features come with enhanced performance, separation of logic from display, ease of administration, predominantly, the ease of use.

I. INTRODUCTION

BEFORE the advent of Smartphone there was a massive use of cellular phones. However the only advantage of cellular phones was that they were cheap and easy to use. But the cellular phones come with lot of limitations. Finding a lost cellular phone is not so convenient. There are hardly any features to ensure privacy of the user. In spite of availability of INTERNET services like mobile tracker for tracking a phone there usability is limited because of privacy concern, so it is not possible to find the user name and address. Off lately some handset devices started providing facilities for recovering lost phone but with the limitation that it had to be enabled manually. So the need to address this issue was felt. Unfortunately, developing application for the regular phones is not easy because of the proprietary issues. Hence android was chosen as the platform. Take-up of Google's Android Smartphone operating system is growing at a tremendous rate worldwide, and we can now see just how quickly this is happening, thanks to a number of Android activations around the world. Android was listed as the best-selling Smartphone

platform worldwide in Q4 2010 by Canalys with over 300 million Android devices in use by February 2012. According to Google's Andy Rubin, as of February 2012 there are over 850,000 Android devices activated every day. Given the increased sophistication, features, and convenience of these smart-phones, users are increasingly relying on them to store and process personal information.

II. POSSIBLE THREATS IN MOBILE DEVICES

A. Limitations of Nonsmart/Regular Phone

Regular phones come with a lot of limitations. The current available features in them may not be sufficient to protect them effectively. A person may find it quite difficult to find his/her lost phone with the limited features made available in the devices. A very few feature phones support GPS making it difficult to track the phone. Privacy breach of received messages is inevitable. Eavesdropping is unavoidable since there is no way to encrypt an important message. If at all a mobile phone has the feature of mobile tracker it has to be activated all the time. Many a times a phone can be located using the IMEI number. But it is not so feasible since there are lot many overheads involved. There could also be a case when your phone gets misplaced locally and is in silent mode making it difficult to track it down. Thus it can be stated that losing a phone (expensive or cheap one) could mean plethora of problems since it contains your vital data.

B. Why Android?

Out of the curiosity to address the above issue, the need for developing a solution that could help in tracing a lost phone and protect its content was felt. However developing applications for regular phones is not possible because of the proprietary issues. The regular feature phones do not allow or support third party applications hence making any kind of experiment completely impossible. On the other hand most Android devices allow you to use applications published by third-party developers, making practical implementation of ideas easier for the developers. Thus android platform was chosen for the development

III. SOLUTION- MOBILE GUARDIAN SYSTEM

Mobile Guardian System was developed with the sole intention of addressing the above issue in phones. As mentioned there are very limited ways and facilities available for protecting your handset and data in it. Mobile Guardian System is an intelligent application which ensures safety of your phone and data in a number of ways. Comprising of four main modules, the anti theft feature of the phone makes it possible to retrieve the longitude and latitude of your lost phone. Backed by its efficient ability to display maps, viewing

So-Ra Han, Kangwon National University, Korea.

Mason Noah, University of Michigan, United States.

DOI : 10.9756/BJIEMS.8323

location of your Smartphone can become much easier. The module also notifies a trusted person in case a different SIM is inserted in the handset besides the one asserted as the trusted one in the beginning. At times the data in phone could be much more valuable to a person rather than the handset itself. In such a case Mobile Guardian system allows you to remotely lock the phone or alternatively wipe the data in it rendering it useless and thus preventing its misuse by another person.

Another module of the phone which is concerned with the data security helps you sort your incoming messages on the basis of some important keywords preset in the application. Also one can assert certain numbers to be private so that messages from those particular numbers will get stored in another password protected database. One of the plus points of this module is its ability to send an encrypted message and decrypt the same using a key. Based on a secure AES algorithm, the chances of eavesdropping and theft are minimized. Mobile Guardian System also makes it possible to change the mode of your phone remotely. The data backup (to a remote server) and restore feature is an added advantage making it a high end application.

IV. DESIGN REQUIREMENTS

Mobile Guardian System will be supported on all android phones having Android OS v2.2(Froyo) and above. The minimum CPU speed needed is 600MHz. Internet connection is a must for supporting map and data backup/restore facility. GPS support is also needed for location based services.

V. MODULE DETAILS

The application Mobile Guardian System for Android comprises of four main modules:

A. Anti Theft

Losing an android phone can be a bad thing, since they are so expensive, and carry so much information. Anti Theft is a module that will help you track your android phone if it has been lost or stolen. Anti Theft module has following features:

- **SIM Change Notification:** SIM change notifier is a service that sends a message to the number provided by the phone owner in case the thief tries to change the SIM. It has a high priority since it helps the owner track his phone using the information sent via the message. As soon as the thief changes the SIM a message will immediately sent to the number provided by the owner of the phone consisting of details which will help the owner track his phone
- **Remote GPS Tracking:** GPS location provider lets you know the exact longitude and latitude of your handset. If your phone is stolen you can easily get the exact location of your phone remotely by sending a predefined keyword set by owner previously in the AntiTheft settings. You can easily view the phone location in the map ones you get the response of your message.
- **Remote Phone Lock:** This feature helps you to lock your phone remotely by sending message to your phone. A predefined message is sent to your phone

which locks your phone and disables access to it. Thus in this way you can deny access to any foreign users/thief to access your private data.

- **Remote Data Wiping:** Similarly you can remotely wipe all the contents that could be private and confidential just by sending a specific message.

B. SMS Filter

SMS Filtering helps in maintaining your private and confidential messages. Your important messages are stored in a separate private box which requires your authentication to access the private box.

Filtering-It is done on the Basis of

Private Contact List

A Private Contact List is created and all the messages received from these numbers will automatically be placed into your private box.

Keywords

A keywords list is created. On encountering any word from the keywords specified the message will automatically be placed into your private box

Encryption /Decryption of Message

One can encrypt a message using a specific key and send this encrypted message to the specified receiver. Message will be decrypted at the receivers end using the same key. This ensures security of your important and confidential message. Encryption and decryption techniques are based on AES algorithm.

C. Mode Toggler

This feature helps you to change the mode of your phone from silent to loud in case it gets misplaced. A predefined message is sent to the handset which changes the mode of the phone and lets you track your phone.

D. Data Backup/Restore

This feature helps you to backup your data on to a server. You can backup your contacts, SMSs and Photos. The data can be restored back whenever required.

VI. IMPLEMENTATION

Architecture Diagram

Mobile Guardian System is based on Android version 2.2 (and higher). It has been successfully run on Galaxy S2, Samsung Pop, Galaxy Y and many other android devices. Using our application, one can protect his/her personal information along with the device. Our system is extensible to add the feature of Bluetooth firewall. In the following, we explain in more details about the system implementation (module wise).

A. *Anti Theft*- A service is tasked to check for the SIM change event and start the tracking activity. Settings that a user is expected to do are:

- Setting the numbers to which notification will be sent after the occurrence of SIM change event.
- Setting the trusted SIM Serial number.
- Setting the keywords for getting the location of the device, wiping data remotely and locking the device remotely.

On detecting the SIM change event the service would send the notification containing location (latitude and longitude) of the device, SIM number and various other details which would allow user to track the device easily. A link will also be provided using which one can locate the device on map.

A class extending Broadcast receiver class is used to check for the SMS containing the keywords that are set by the user. On receiving the keyword corresponding event is performed. SQLite database is used to store the keywords.

B. *Sms Filter*- For filtering sms on the basis of keywords and contact numbers Broadcast receiver class is used that checks the incoming message for the private numbers (set by the user) and the keywords (set by the user). Separate database is created in SQLite to store private SMS, numbers and keywords.

C. *Mode Toggler*- Keyword set by the user is stored in the database which is compared by the incoming message using Broadcast receiver class. If the keyword matches with the one in the message then the mode is changed from silent to loud. For serving this purpose audio manager is used.

D. *Data Backup/Restore*- This module helps a user to backup his/her contacts, photos and private SMSs. User needs to be registered on a remote server for using this feature.

VII. FUTURE ENHANCEMENTS

The Android Operating System has definitely made its mark in mobile OS history. The phenomenal and solid growth of android developers, lead the way to huge leaps in efficient mobile application development. It is expected that Mobile Guardian System for Android will be improved with enterprise level features and security.

It can be made more powerful by introducing following features which will ensure the best protection of each device and user privacy.

- *Tracing Path of Thief*: The entire path of thief can be traced by using Google map and GPS location. It can be done by sending the link of Google map on a

- particular cell phone or mailing that link on email-id.
- *Data Backup of SD Card on email-id:* SD card data backup can also be done on users local email-id. Can add additional feature of restoration of data from email when required or in case of data loss.
- *Bluetooth Firewall:* User will be alerted whenever any application installed on the device tries to turn on the Bluetooth. Certain devices can be set as trusted ones allowing easy communication between them and maintain logs of past communications via Bluetooth.
- *Real-Time Reporting of Possible Malicious Apps:* Proving security against malicious applications. Authenticating applications before getting installed.
- *Centralized IT provisioning:* Androids deployed in a corporate environment can be centrally managed by IT Administrators wirelessly. This will enable IT Departments to send out important security patches, update standard android programs, and enforce password and connection policies.

VIII. CONCLUSION

Android is a software stack for mobile devices such as mobile telephones and tablet computers developed by Google Inc and the Open Handset Alliance. Android consists of a mobile operating system based on the Linux kernel, with middleware, libraries and APIs written in C. Android uses the Dalvik virtual machine with just-in-time compilation to run compiled Java code. In Simple terms Android is the operating system behind +40% smartphones and 10-20% tablet market. Android provides the unique opportunity for one and all to have a custom phone for him.

Backed by these features we have developed an application, The Mobile Guardian System for Android which will help android phone users to secure their phones from various security problems like data security and handset security. This application is combination of various modules such as antitheft and mode toggler which deals with handset security and SMS privacy, data backup which provides data security.

Nowadays phone is not just a device to make a call or send a message, it stores all your important stuff like contacts, photographs etc. Here is our application, The Mobile Guardian System for Android containing such amazing features always ready to find or guard your phone from various security problems

REFERENCES

- [1] Nicolas Gramlich, "Android Programming with Tutorials", dev.org-Community, 2011.
- [2] R. Meier, "Professional Android application development", 2010.
- [3] Google Groups, Android Discussion Groups, <http://code.google.com/android/groups>.
- [4] "Google Projects for Android". code. google.com. Google Inc. 2011.
- [5] V. Nguyen, "Android Community", <http://androidcommunity.com>.
- [6] <http://droidapplications.org> for ideas
- [7] <http://www.developer.android.com> for downloading android-sdk and Google APIs.
- [8] <http://www.market.android.com> for getting the ideas of existing android application.