International Journal of Application or Innovation in Engineering & Management (IJAIEM)
Web Site: www.ijaiem.org Email: editor@ijaiem.org
Volume 3, Issue 3, March 2014 ISSN 2319 - 4847

Secure Instant Message and Location Sharing System for Android using Cryptanalysis

Sushant A. Patinge[1], Pravin D. Soni[2]

[1]ME (CSE) Scholar, Department of CSE, P R Patil College of Engg. & Tech., Amravati-444602, India
[2]Assitantant Professor, Department of CSE, P R Patil College of Engg. & Tech., Amravati -444602, India

ABSTRACT

The recent surge in popularity of smart hand held devices, the Google Android operating system as one of the dominate technology trends for the smartphones is virtualization platform that provides an application oriented services to smartphones infrastructure. Android devices have appeared so strongly and, since then, the number of applications available for this operating system has exponentially increased, Google already has its Android market where applications are placed and offered to the smartphone users. Due to the gain in popularity of android based smartphones, has given a new challenges in protection of end user privacy. The current android-based Location and text message sharing system is work only single user perspective to share the information with other user having poor user interface that user can't manage to understand easily. In the paper describe to overcome the drawback of the current developed system that provides the secure communication using MD5 and SHA-1 algorithms of the user data like text message and user location by developing healthier user interface that can easily managed to understand by the end user.

Keywords: Android, App Inventor for Android, MD-5, SHA-1.

1. Introduction

The smart gadget life-cycle has evolved drastically in recent years. [1] These new generations of the smart gadget devices such as the iPhone and Google Android devices are powerful enough to accomplish most of the tasks that previously required a personal computer.

Among them, Google Android has been gaining popularity and its market share in the mobile operating system market is rapidly increasing. According to Gartner (2010),[2] Android is poised to become second worldwide mobile operating system in the nearer future. Android is a widely anticipated open source operating system for smartphones. Developed by the Open Handset Alliance (visibly led by Google) initially release in September 23, 2008.[3] It provides a base operating system, an application middleware layer, a Java software development kit (SDK), and a collection of system applications.[4] Android phones ship with a rich array of built-in activities including different applications developed under the android platform or the application framework provided by the android. In July 2010, Google announced the public beta release of the App Inventor for Android (AIA) visual programming environment.[5]App Inventor for Android (AIA) provides a platform to develop the new set of applications in the open source environment of Android operating system.

Android based smart phones applications and internet; people are sharing information with other people but they are not sure that information is securely transmitted or not, these proposed system deals with secure transmission of information with each other within the network. The main objective of this proposed system, on the highest level, is to communicate with a PHP server that stores the information sent through the android device in encrypted form and vice-versa which finally establish a secure two way communication between android device and web server.

2. Related Works

Adding text messaging functionality to mobile devices began to gain traction in the mobile communication services community in the early 1980s. The first action plan of the CEPT Group GSM was approved in December 1982, requesting "The services and facilities offered in the public switched telephone networks and public data networks should be available in the mobile system. [6] This plan included the exchange of text messages either directly between mobile stations, or transmitted via Message Handling Systems widely in use at that time. The first proposal which initiated the development of exchanging information or sent message to the user was made by a contribution of Germany and France into the GSM group meeting in February 1985 in Oslo. [7] Initial growth was slow, with customers in 1995 sending on average only 0.4 messages per GSM customer per month. In 2013, 6.1 trillion text messages were sent. [8] This translates into 193000 SMS per second. [9] It is commonly used by financial institutions, airlines, hotel booking sites, social networks, and other organizations sending SMS from their systems to their customers. According to research in 2013, A2P traffic is growing faster than P2P messaging traffic. [10]

Over the years several approaches and solutions presented considering the secure exchanging of message thorough client and webserver. The various researches have been done and are going on location based project and in the same ratio various applications have been developed on location-based and message sharing system. [11]As the amount of user deal to

exchange the information with other people to store the large amount of data the existing system cannot support the centralized database. Sensitive data may also be leaked accidentally due to improper disposal or resale of storage media. [12] Diesburg et al. [13] surveys, summarizes and compares existing methods of providing confidential storage of data but it cannot support the secured communication between the user application and the webserver. Ramesh Shrestha, Yao Aihong et al. [11] developed location and message sharing system for Android Platform. In the present location based services, the works are mainly focused on how to handle the location, how to display Google map on android devices and finally about classes and functions used for location services.

3. System Implementation and Working

As our main area of discussion is android application security hence we will try to overcome some of the shortcomings of the various present messaging and location sharing system. In this system when user want to communicated with the other user or the group of user then during mutual communication the security is the more important issue that overcome in the proposed system. Proposed system mainly consists of three modules which are listed below

1) Login Module:

In this module of system the must valid user name and password for login to the application that helps to identify the user. The valid user only login and access services like messaging and location sharing. Each user has its own user id and certain permission that helps to access the full features of the application. If the user login with its android based smartphone then the IMEI number is used to uniquely identify of that particular user. The all user data will be stored in the database in encrypted form using the different cryptographic algorithms like MD5 and SHA-1.

2) Messaging Module:

This module is used to send the message to the other users that are present in contacts and provides the secured communication between the users. It also helps to form the groups that help the user to communicated more than one person at a time. Maintain the different group of user to share information within the particular groups only. In the proposed system provides the feature to maintain the group for the specific users that can communicated within a particular group only and gives the accuracy of information within a group.

3) Location Module:

The main Objective of this module is to share the location with the different users if the user wants to share it. The GPS system will used to capture the location of the user and make available to the other users. The user location information is also stored in the database in the form longitude and latitude that help user secure its information from unauthorized person

1. The proposed system implement the better user interface for the android device as well as web server that easy to achieve the high level interaction between user and application and application and web server.
2. It also achieved the goal of portability of different version of android operating system. The system will work on different version of android operating system with give level of application programming level (API).

4. Conclusion:

This paper introduced a security service for Smartphone's, which offloads the secure message transfer and location sharing between the user and webserver. As Smartphone's are very much popular the different kind of application for the information exchange and location sharing but it violated the security on the certain level that causes the loss of information and misuse of it by unauthorized user we introduce a new approach to deal with security while exchange information between users using different algorithms.

References:

[1] Zhaohui Wang, Rahul Murmuria, Angelos Stavrou, "Implementing and Optimizing an Encryption Filesystem on Android", 2012 13th IEEE International Conference on Mobile Data Managament, pp. 52-62.

[2] "Granter", Available:http://betanews.com/2011/02/09/gartner-android-smartphone-sales-surged-888-8-in-2010, [Online; accessed 28-sep-2013].

[3] "Announcing Android Sdk 1.0 Sdk, Release1", Available: http://android-developers.blogspot.in/2008/09/announcing-android-10-sdk-release-1.html. [Online; accessed 25-sep-2013]

[4] William Enck, Machigar Ongtang, and Patrick McDaniel, "Understanding Android Security", 2009 IEEE Security & Privacy, pp. 50-57.

[5] Margaret Butler, "Android: Changing the Mobile Landscape", 2011 PERVASIVE Computing, Available: www.computer.org/pervasive, [Online; accessed 24-Sep-2013].

[6] "3GPP Specification detail", Available: http://www.3gpp.org/ftp/Specs/html-info/0340.htm, [Online; accessed 06-Sep-2013].

[7] "GSM document 19/85", Available: http://en.wikipedia.org/wiki/ETSI, [Online; accessed 06-Sep-2013].

[8] "The Rise of 3G", Available: http://www.itu.int/ITU-D/ict/material/FactsFigures2010.pdf, [Online; accessed 06-Sep-2013].

[9] "Timeline global SMS per second 2007 - 2010", Available: Statista.com, [Online; accessed 05-Sep-2013].
[10] "Why SMS is still King", Available: http://clicksumo.com/sms-is-still-king, [Online; accessed 05-Sep-2013].
[11] Ramesh Shrestha, Yao Aihong, "Design of Secure Location and Message Sharing System for Android Platform",2012 IEEE International Conference on Computer Science and Automation Engineering, pp. 117-121.
[12] Zhaohui Wang, Rahul Murmuria, Angelos Stavrou, "Implementing and Optimizing an Encryption Filesystem on Android", 2012 13th IEEE International Conference on Mobile Data Managament, pp. 52-62.
[13] S. M. Diesburg and A.-I. A. Wang, "A survey of confidential data storage and deletion methods," *ACM Comput. Surv.*, vol. 43, pp. 2:1–2:37, December 2010

AUTHOR

Mr. Sushant A. Patinge.
Received Bachelor's Degree in Information Technology from Pune University in 2011 & Pursuing Master Degree In CSE from P.R. Patil College of Engg. Amravati-444602

Prof. Mr. Pravin D. Soni
Received the Master Degree in Computer Science from VJTI, Mumbai in 2011. Working as Assistant professor in Department of Computer Science and Engineering at P. R. Patil College of Engg. Amravati-444602.