Bluetooth Security Lock for Android smart phone platform

[1] Khaled Alghamdi, [2] T. Oh, [3]B. Stackpole

Abstract— The project is to make an Android application which triggers a screen lock with a PIN when the device is disconnected from another Bluetooth device. This application will run in the background normally and constantly monitor the Bluetooth connection of the device. As soon as it catches a change in Bluetooth connectivity state, it will trigger a lock screen to protect the device.

Keywords: Bluetooth, Security, protection, power conservation.

1. Introduction

Today, mobile applications act as an important tool to increase the efficiency of the work. From personal to commercial use, these apps assist us in a number of different ways. Smart phones have a number of connectivity features like Bluetooth, WI-FI, RFID, etc which can be utilized into useful applications. For instance, creating applications that use Wi-Fi and Bluetooth services to establish ad-hoc networks between devices. Such as applications can inform whenever a specific device connects to the network and automatically perform a specified action. Conversely, automated actions can be performed whenever a device disconnects from this network. By triggering such pre-specified reaction for each occurrence, these applications can act as powerful scheduled systems.

The application that the author proposing has a similar concept, along with enhanced security features.

2.1 Related works:

People use mobile devices in their daily lives more than any other technology available today. People use them as an alarm clock, a dairy, a contacts detail book, a computer, a calculator and the list goes on. People can also use a mobile device as a radio, media player, and a camera easily without any issues. Basically many features of different devices have been merged into this one device called mobile device. A mobile device can be a mobile phone or a latest version of a tablet or iPad. These devices are available at different costs in the market. Mobile service providers have made it very easy to send text messages via mobile phones devices.

[1]K. Alghamdi is currently pursuing MS degree program in Networking and Systems Administration at Rochester Institute of Technology, E-mail: kyadg@hotmail.com
[2] T. Oh is an associate Professor at the Rochester Institute of Technology, Email: thoics@rit.edu
[3] B. Stackpole is an associate Professor at the Rochester Institute of Technology, Email: wrsics@rit.edu

Over 70 percent of the world's population now uses mobile phones [1]. Children use mobile devices more than having books around them. Apple has sold over 60 million phones worldwide and Android is currently activating 160,000 devices a day. These statistics make the significance of mobile devices much clear. Since the mobile devices carry such a large variety of data, it is very much important to protect this private data as well. Nobody wants his or her personal lives to be invaded by a hacker or a thief. Therefore, the authors are going to focus on the mobile device protection.

2.2 Wireless Security Issues:

As demonstrated in by R.H Hamid, the data transmitted between mobile devices wirelessly can easily be accessed by any one of the users on that network because no walls or buildings can obstruct radio waves [2]. Without proper security measures being taken, anyone can access private and confidential information or data being transmitted over a wireless network.

Mobile devices are much cheaper than the computers or laptops, which make them a beneficial way for doing business, but losing data within the device can be more expensive than losing the mobile device itself. Therefore, the author has this access control idea in order to save user's data from being stolen. Some mobile devices have biometric access control while others have heavy password protected systems. There is no standard access control technique being used in mobile devices, which makes the data security on mobile devices of low priority. According to [2], up to 90% of the mobile devices don't have appropriate security systems.

2.3 Bluetooth Proximity-Based Access:

As mentioned in [3] by Credant Technologies, Bluetooth proximity-based access is a unique and elegant solution to the most commonly-- known problem of mobile device security. It senses the proximity of a user based on Bluetooth technology and secures the device if an authorized user is no longer within range. Locking down a system based on a time delay is considered good practice. But what if the user is driving and wants the directions

for a certain place and the device gets locked again and again? In this case, a user would have to re-authenticate the device repeatedly. Potentially creating a hazardous driving condition and possibly leading to a collision.

3.1 Approach

The authors will be developing the application for Android operating system using the Android SDK. The application will be compatible with Android version 2.3 Gingerbread and the development will utilize the. Android plug-in for Eclipse as well. The documentation for Android the SDK Bluetooth API from the Android Developers website will be used extensively. Various Bluetooth devices such as Bluetooth headphones and keyboards will be used for Bluetooth connectivity with the device.

3.2 Block Diagram:

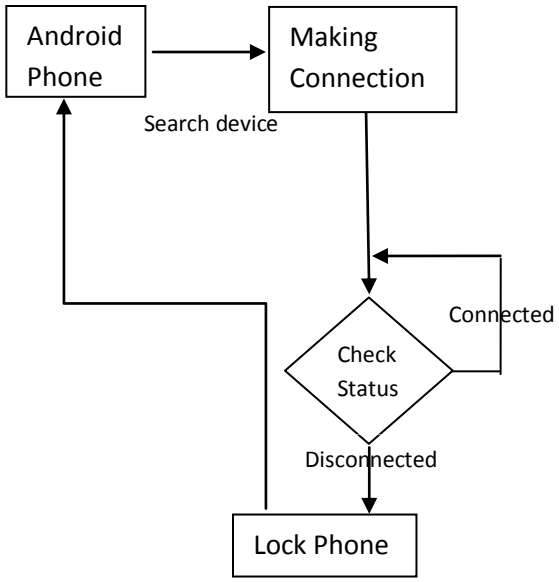


Figure 1: Lock Algorithm

4. Implementation Setup

Development in Android requires installation of Android SDK that is easily available from android website "http://developer.android.com/sdk/index.html". Along with the SDK, android platform tools and android tools are also necessary for developing applications in android. The latest version is Android API level [14].

Android development environment is available for and supports both Windows and Mac operating systems. For the development of this application the authors selected the Windows version. For the Integrated Development Environment (IDE). Eclipse, a free open--source product, was chosen. Android has an Eclipse plug-in called ADT that integrates the Android SDK with Eclipse.

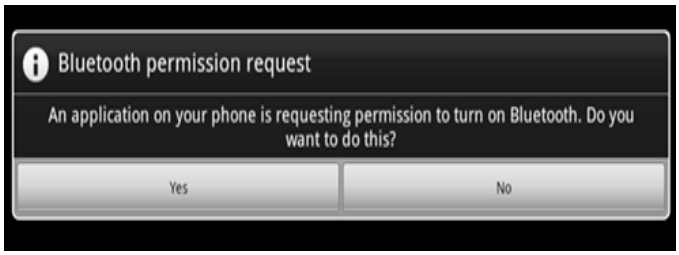
Android virtual simulators for Android Éclair, Froyo, Honeycomb and Ice Cream Sandwich were used for development and testing purposes. [4]

5. The Experiment

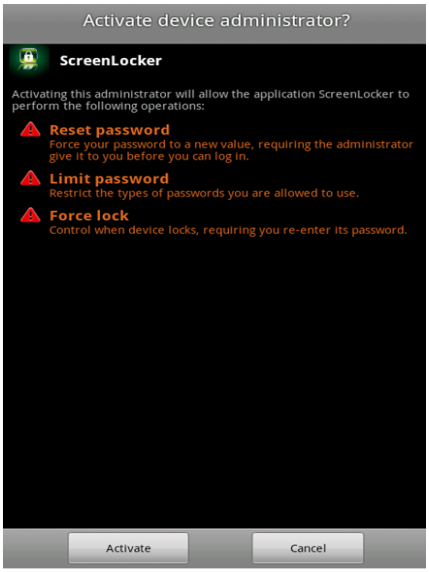
The veracity and the utility of the application were determined by means of some random experiments. The most interesting was coupling of the Android device with a headphone.
The real-time scenario was formulated and the application was put into its rigors.

A user was asked to connect his/her phone to a Bluetooth enabled headphone and start listening to songs. The application was started and configured. The device was kept in a different room and the user moved about with an intention to break the connection as result of low proximity.

The user has to turn ON the source "Android" Bluetooth so it can pair with another Bluetooth device. Once the devices are paired the connection now is up between two devices.



After that, the user needs to touch on activate button to proceed. Once that happens a prompt comes up asking the user to enter the password required. After conforming the password the will start monitoring the connection.



The authors implemented the app in two cases. First, implementing the app when the connection is broke or lost. Second, implementing the app when the phone is out of the default distance or out of range. As a result of both situations, the application worked as expected ensuing security and power conservation.

6. The Results

When the user connects the Android phone with another Bluetooth device the app will constantly monitor the Bluetooth

connection of the device. When the connection broke or when the phone is out of the default distance the user's Android phone will be locked and protected by the user given password. The Bluetooth was also switched off.

Figure 2: Bluetooth switched OFF

The project currently has the functionality of detecting a Bluetooth device, connecting to it and locking the phone when the connected device is no longer available. Any Bluetooth enabled android device can be used for deploying running this application.

The phone's performance was fine and there was no freezing on the system while the app is running. In terms of battery live impact and standard issues the app didn't impact on the battery live and everything worked properly.

7. Conclusions

In this paper the framework for an Android application which ensures security has been touched upon. This application has a multifaceted functionality, in one hand it imbues the user with an option to restrict malicious attacks on his/her smart phone and on other hand its helps the user to resist unnecessary drainage of the battery.

This application requires an Android smart phone which can eventually connect to any Bluetooth device. A very low hardware requirement is a key to the success of this application. The user can connect the phone to any Bluetooth enabled device be it a laptop or a Bluetooth headphone. If the connection is terminated he/she won't have to worry about the security of the phone or wastage of energy

As soon as there are no proper security measures being taken, anyone can access private and confidential information or data being transmitted from a wireless network. Security issues should be taken into consideration especially for some mobile devices that don't have appropriate security systems.

A solution in the form of this application was built to result better security enforcement and less energy consumption. This Application provides an administrator interface that compels the user to set certain rules and abide by it and in turn ensures an overall security enhancement of the dangling blue tooth connection.

The developed app has provisions for more enhancement that will include in its stride various language support and multiple Bluetooth device connectivity. The user can also extend this developed solution to android supported tablets.

In the course of this application's development Android as an OS for handheld devices has shown its versatility and flexibility to enrich the user experience. The ease of development on Android platform and its open source feature will facilitate the development of more and more android apps aimed at different facets of usability and utility.

Finally, the app was built to monitor the connection frequently. As a result, the application worked as expected ensuing security features and power conservation. Also, there was no impact on the phone's performance and the battery life. The experiment succeeded to meet the requirements that guided its design and security.

Acknowledgement
The authors are grateful to those who will give their highly valuable suggestion and comments that lead to important improvement of this project.

Authors:
Dr. Tae Oh is an associate professor at the Rochester Institute of Technology, Rochester, NY USA. Professor Oh received a B.S. degree in Electrical Engineering from Texas Tech University in 1990 and M.S. and Ph.D. degrees in Electrical Engineering from Southern Methodist University (SMU) in 1995 and 2001, respectively. MANET, Sensor Networks, Telemedicine, Network/Cyber Security, Green Communications, and Scalable Modeling and Simulation are his current areas of research. Professor Bill Stackpole is an associate professor at the Rochester Institute of Technology, Rochester, NY USA. Professor Stackplo's research interests include mobile devices, network, and system security, computer and mobile forensics and Data Recovery.

References:

[1] Digital Buzz. [Online]. Available: http://www.digitalbuzzblog.com/2011-mobile-statistics-stats-facts-marketing-infographic/

[2] R. A. Hamid. (2003). Wireless LAN. Wireless Security Issues. [Online]. (1.4b). Available: http://www.sans.org/reading_room/whitepapers/wireless/wireless-lan-security-issues-solutions_1009

[3] C. Technologies. (2011). Bluetooth Proximity-based Access. [Online]. Available: http://www.credant.com/CREDANTBT/PROXIMITYACCESS/TB_0611W.pdf

[4] Android Developers. Bluetooth. [Online]. Available: http://developer.android.com/reference/android/app/Activity.html