Security Methods for the Mobile Android Platform TJHSST Senior Research Project Computer Systems Lab 2009-2010

Sam Rush
Period 4

October 29, 2009

Abstract

Mobile technology is rapidly evolving to the point where customers who buy a phone with a two year contract feel compelled to upgrade before the contract expires. Yet, mobile phones have not yet experimented with biometrics to any large scale. This project will integrate biometric technologies with the Android mobile platform. As smartphones continue to hold more and more personal information, including emails and other forms of private communication, the demand for security is growing. This project aims to protect a phone using only biometric security measures.

Keywords: biometric security, mobile development, Android

1 Introduction

The cell phone industry is rapidly growing. In recent years there has been a mass shift from traditional cell phones with twelve key dual-tone multi-frequency keypads to “smartphones” with touchscreen displays. In the last six years, the United States has been migrating to 3rd generation (3G) cellular networks in the form of HSPDA and EVDO, which both carry a bandwidth potential of about 2 Mbit/s[4]. In comparison, the average household internet connection in the United States is 6.8 Mbit/s according to SpeedTest.net. This new technology has created a large demand for security, especially on phones capable of full internet and email. On the Android operating system, the only available security is called the pattern unlock seen below.

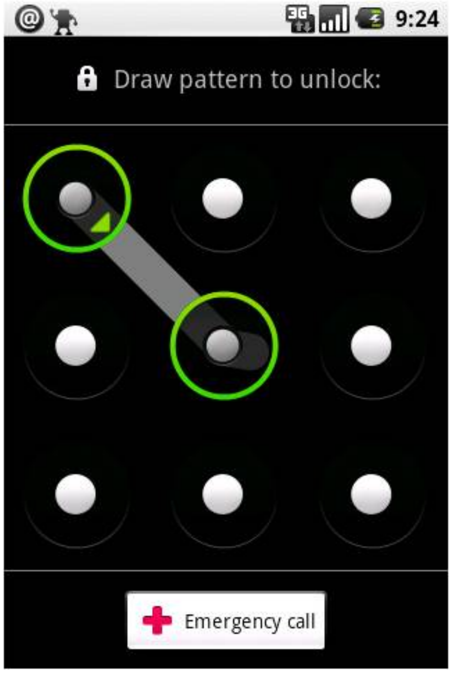

Figure 1: The pattern unlock consists of connecting a preset pattern of dots by dragging your finger across the screen.

The goal of this project is to allow the addition of alternative unlocking methods.

2 Background

2.1 Android

On October 21st, 2008, Google and the Open Handset Alliance released their new open source mobile phone operating system. The purpose of Android was to create a flexible, upgradeable phone which encouraged develeopment. The first phone to use Android, released alonside with the operating system, was the HTC Dream, also known in the US as the T-Mobile G1 and the Android Developer Phone (ADP). This project has exclusively used the HTC Dream and HTC Dream emulator provided by Google.

2.2 CyanogenMod

A user under the name CyanogenMod has created an immensely popular modified version of Android. This version allows for much easier development for the phone’s integrated features such as the Browser or, in this case, the lock screen. CyanogenMod is still based on the Android framework, similar to how Kubuntu, Xubuntu, and several others are operating systems based on the Ubuntu framework. This project will be developed and run under the CyanogenMod system.

3 Development

3.1 Languages

This project is not as straightforward as algorithmic development, since requires both modifications to the operating system as well as development of an application. The operating system is based on linux, and will require modifications to files written in C, Python, Bash, and possibly assembly. The application will require knowledge of Java.

3.2 Testing

Android provides free virtual devices along with their Software Development Kit (SDK). Unfortunately, I am not able to utilize touch or camera input from that interface so much of the testing requires a physical Android device. For this, I will use my HTC Dream.

3.3 Rooting

Android, while open source, does not appear on phones with full user rights. In other words, the owner of the phone is not free to do whatever he wants with the operating system, just as only the root account on linux machines is able to do whatever it pleases. However, to make modifications of the operating system, one must "Root", or gain access to, their phone. To do this, the phone's operating system was downgraded from version RC33 to RC29. Then, a root telnet session was opened and the root account was unlocked. Then, the CyanogenMod ROM was installed on the phone.

4 Expected Results

If the project is completed successfully, a user will be able to lock their phone using a variety of biometric and other input techniques, guarding against exposure of sensitive information.

4.1 Distribution

Upon successful completion of the project, the application will be distributed to the Android community.

5 Preliminary Results

There are no preliminary results as of this time.

6 Final Results

There are no final results as of this time.

References

[1] Chaudhuri, Avik. “Language-based security on Android.” Association of Computing Machinery: n. pag. PDF file.

[2] “The Developers Guide.” Android Developers. Open Handset Alliance, n.d. Web. 27 Oct. 2009. <http://developer.android.com>.

[3] Online posting. Dream Development - XDA Developers. N.p., n.d. Web. 27 Oct. 2009. <http://forum.xda-developers.com/?forumdisplay.php?f=448> .

[4] “Cellular Standards for the Third Generation”. ITU. 2005-12-01 <http://www.itu.int/osg/spu/imt-2000/technology.html#Cellular%20Standards%20for%20the%20T