

AndroLocker: Detecting Brute Force Attack on Android Smartphone Lock Screen

Ariff Affandi Bin Azman
University Kuala Lumpur
Malaysian Institute of Information Technology
Kuala Lumpur, Malaysia
ariffaffandi93@gmail.com

Dalilah binti Abdullah
University Kuala Lumpur
Malaysian Institute of Information Technology
Kuala Lumpur, Malaysia
dalilah@unikl.edu.my

Abstract— Nowadays, android smartphones are acting like a computer. It can be used to create and store information, data, and documents. This devices become very popular because it provide a large number of utilities for handheld devices. Based on this situation, an application named AndroLocker is created to detect if intruder trying to brute force the smartphone lock screen. This application will capture the image of the intruder and will alert owner of the smartphone on their email.

Keywords—Android; Brute force; Lock screen; Alert.

I. INTRODUCTION

Android based smartphones has become a very important part of our life. Smartphones change the way of communication by providing an advantage of communicating with anyone virtually through voice and video conversation, create and receive text messages, and email. Nowadays, android smartphones are acting like a computer. It can be used to create and store information, data, and documents. This devices become very popular because it provide a large number of utilities for handheld devices. Android operating system is an open-source platform that is why there are many utilities has been developed. Smartphones can be stolen easily because of its small size. The information such as organization or personal details that are stored in the phone memory can be easily exposed and be shared to the public. In this project, my aim is to develop an application named AndroLocker to detect when intruder trying to brute force the smartphone lock screen. This application will capture the image of the intruder and locate the GPS location and will alert owner of the smartphone on their email.

II. LITERATURE REVIEW

A. Detection

In general, detection is the extraction of particular information from a larger stream of information without specific cooperation from or synchronization with the sender. In this project, the development of this application will have the

functionality that can detect the brute force attack on android smartphone

B. Brute Force

In cryptography, brute force attack is an attack that consist of an attacker trying many passwords or passphrases with hope to bypass any secure device or login webpage correctly. The attacker will try all possible password or passphrases until the correct one is found. Brute force attack may be used by attacker to crack encrypted data or by security analyst to test an organization security.

The one example of type of brute force attack is dictionary attack. Techopedia (2017) explains in their website page that a dictionary attack is a technique or method used to breach the computer security of a password-protected machine or server. A dictionary attack attempts to defeat an authentication mechanism by systematically entering each word in a dictionary as a password or trying to determine the decryption key of an encrypted message or document. Dictionary attacks are very often successful because many users use basic and ordinary words as password. These words can be easily found in a dictionary such as English dictionary.

C. Android

Android is a mobile based operating system that are developed by Google based on the Linux kernel. It is used by several smartphones and tablets such as Sony Xperia, Samsung Galaxy and Google Nexus One. Android's user interface is mainly based on direct manipulation (human-computer interaction style), using touch gestures such as swiping, tapping and pinching to manipulate on-screen objects along with a virtual keyboard for text input.

The Android operating system (OS) is open source, meaning that developers can modify and customize the OS for each phone. TechTerms (2016) explains in their website page that Android phones typically come with several built-in applications and also support third-party programs. Developers

can create programs for Android using the free Android software developer kit (SDK). Android programs are written in Java and run through a Java virtual machine JVM that is optimized for mobile devices. The "Dalvik" JVM was used through Android 4.4 and was replaced by Android Runtime or "ART" in Android 5.0. Users can download and install Android apps from Google Play and other locations.

D. GPS Tracker

A GPS tracking unit is a device that normally carried by a person or moving vehicle that uses the Global Positioning System to track its precise location. The recorded location data can be stored in the tracking unit, or it may be transmitted to a central location database, or Internet-connected computer, using a cellular (GPRS or SMS), radio, or satellite modem embedded in the unit. This allows the asset's location to be displayed in real time.

Garmin (2017) explains in their website page that GPS satellites circle the Earth twice a day in a precise orbit. Each satellite transmits a unique signal and orbital parameters that allow GPS devices to decode and compute the precise location of the satellite. GPS receivers use this information and trilateration to calculate a user's exact location. Essentially, the GPS receiver measures the distance to each satellite by the amount of time it takes to receive a transmitted signal. With distance measurements from a few more satellites, the receiver can determine a user's position and display it electronically to measure your running route, map a golf course, find a way home or adventure anywhere.

E. Image Capture

Image is used in the broader sense of any two-dimensional figure such as a map, a graph, a pie chart, or a painting. Images can be rendered manually, such as by drawing, painting and carving. It also can be rendered automatically by printing or computer graphics technology, or developed by a combination of methods, especially in a pseudo-photograph (image that made by computer-graphics).

According to Encyclopedia (2017) website page, image capture is the process of obtaining a digital image from a vision sensor, such as a camera. Usually this entails a hardware interface known as a frame grabber, which captures single frames of video, converts the analogue values to digital, and feeds the result into the computer memory.

III. SYSTEM ARCHITECTURE

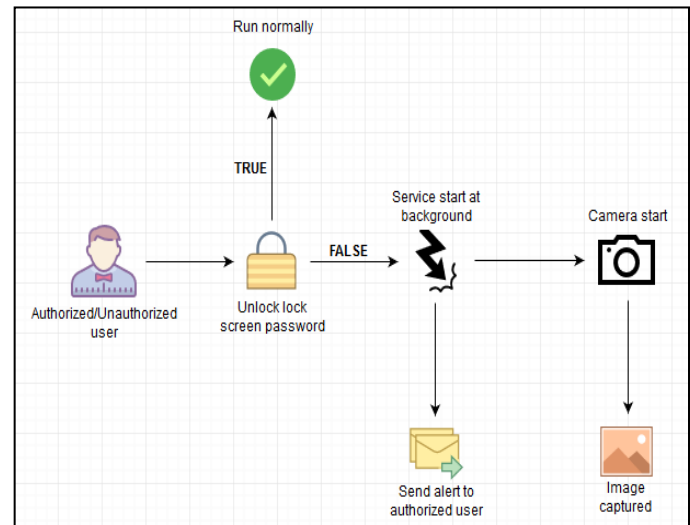


Figure 3-2: System Architecture Diagram

Figure 3-2 shown the system architecture diagram of this application. This diagram shows that the user will try to unlock the home screen password. If the password is correct, the user can do anything such as play music, messaging and calling. But if the user enter the wrong password more than three (3) times, there will be services that will start at background. That camera and GPS service will start and the camera will capture the image by using front camera while the GPS will trace the location. After that, there will be an alert emailed to the owner of the smartphone.

IV. DEVELOPMENT STAGE

A. Design Specification

i) Design Specification

a. Menu Screen Interface Development

The menu screen interface development is the first interface that user will see in AndroLocker application.

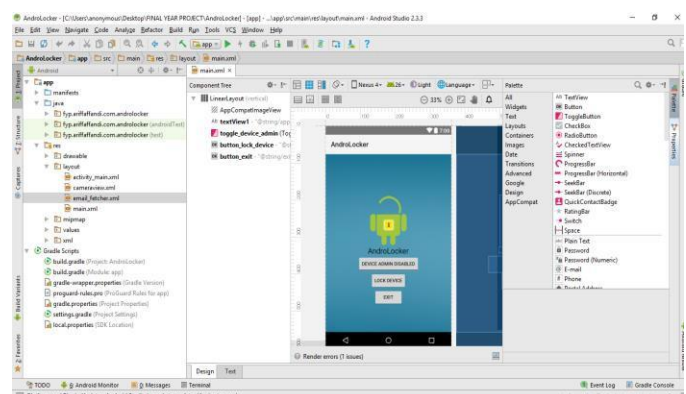


Figure 4-1: Menu Screen Interface Development

B. Functional Specification

After finish designing the menu interface, function for capture image, enabling device admin, detecting brute force and other information will be created. The function have been developed and tested for its usefulness as showbelow:

i) Menu Screen Function

Figure 4-2: Menu screen interface

The Figure 4-2 shows the menu screen interface for AndroLocker. For this project, user need to enable the device admin features and lock the device to make sure this application will function without any error.

ii) Device Administrator Function



Figure 4-3: Device Administrator interface

The Figure 4-3 shows the device administrator interface. User need to activate this feature to make sure that this application will run in background.

V. TESTING AND RESULT

Testing in general is a process to finding out how its work and how well it works. It is processes to use to ensure the written coding and script actually does it is supposed to do. This process will use to evaluate whether the overall project's objectives are being fulfilled or not. Testing is done in order to provide better quality of product by find defect in the application system. Testing will be done using specific requirements to check whether the requirements of the user or client are being fulfilled or not.

To meet the objectives of AndroLocker, the testing has been done in University Kuala Lumpur – Malaysian Institute of Information Technology. The testing types has been conducted is Unit Testing, Functionality Testing and End-to-end Testing. It has been choose by the evaluator base on research and study in evaluating a suitable testing method. In the Rapid Application Development (RAD) have this kind of testing by asking the user opinion toward the application condition, interface and functionality.

A. End-to-end Testing

End-to-end testing is a testing method which determines whether the performance of application is as per the requirement or not. It is performed under real world scenarios like communication of the application with hardware, network, and other applications. The Table 5-2 below shows the result between different android versions.

Table 5-2: End-to-end Testing Table

No	Action	Expected Outcome	Android Version	Remark (Pass/Fail)
1	Enable device administration	Device administration interface will popup	Ice Cream	Passed
			Sandwich (4.0)	Passed
			Jelly Bean (4.2)	Passed
			Kit Kat (4.4)	Passed
2	Enter wrong password 3 times or more on lock screen	Brute force detected and triggered the camera in background	Ice Cream	Passed
			Sandwich (4.0)	Passed
			Jelly Bean (4.2)	Passed
			Kit Kat (4.4)	Passed
3	Capture Image	Image will be stored in phone	Ice Cream	Passed
			Sandwich (4.0)	Passed
			Jelly Bean (4.2)	Passed
			Kit Kat (4.4)	Failed
4	Send email in background	The user will receive the alert email	Ice Cream	Passed
			Sandwich (4.0)	Passed
			Jelly Bean (4.2)	Passed
			Kit Kat (4.4)	Failed

VI. PROJECT RECOMMENDATION

Several improvements can be added in this project for future development. Due to several weaknesses in this project, some modification and additional elements must include to make sure it improves. So, these are several recommendations to ensure the enhancement of the project can be done:

- Add own GPS Tracker in the application.
- Automatic detect default Gmail email addresses.
- Include image captured in alert email.

REFERENCES

- [1] Techopedia (2017). Dictionary Attack. Retrieve from <https://www.techopedia.com/definition/1774/dictionary-attack>
- [2] Techopedia (2017). Brute Force Attack. Retrieve from <https://www.techopedia.com/definition/18091/brute-force-attack>
- [3] TechTerms (2016, May, 16) Android. Retrieve from <https://techterms.com/definition/android>
- [4] Garmin (2017) About GPS. Retrieve from <http://www8.garmin.com/aboutGPS/>
- [5] Encyclopedia (2017, June, 19) Image Capture. Retrieve from <http://www.encyclopedia.com/computing/dictionaries-thesauruses-pictures-and-press-releases/image-capture>
- [6] TechAdvisor (2014, February, 04) How to use Android Device Manager. Retrieve from <http://www.techadvisor.co.uk/how-to/google-android/how-use-android-device-manager-3500315/>
- [7] Android Developer (2017) System Permission. Retrieve from <https://developer.android.com/guide/topics/permissions/index.html>
- [8] Android Developer (2017) Camera API. Retrieve from <https://developer.android.com/guide/topics/media/camera.html>