

Boomerang: An Anti-theft and security android application

(Jaypee Institute of Information Technology)

Rishabh Jain
(rishabh.jain9196@gmail.com)

Aditya Bakliwal
(abakliwal12@gmail.com)

Tarun Agarwal
(agarwaltarun4@gmail.com)

Ambalika Sarkar
(ambalika.sarkar@jiit.ac.in)

Abstract

With the advent of modern technology in this era, we have seen some significant progress in the life of a common man. It has made lives simpler and easier. But with the increasing technological advancement, the security threats have also increased. Hence, we need to look beyond the favourable aspects and try to be as safe as possible while using these technologies.

The same is the case with mobile technology. These days, android devices come in a very wide range. People are very affectionate towards their phone, but are least aware of the dangers that it may pose. This is where Boomerang kicks in. This application helps its users to try and prevent any mishap or find their lost android device by providing various features.

1. Introduction

Boomerang is an anti-theft and security android application that helps its users to secure their android devices against minor threats. Nowadays android devices come in various price brackets. Despite the great advancement in the mobile development field, there is very little that we can do when we find ourselves in a position that our phone is stolen or lost. Sometimes our phone is left on silent profile when it is lost and it creates a big problem in finding it. Many times some people try to break into our devices, without our permission. To secure our device, this application, provides some features that might come in handy. Although, it does not guarantee to return your phone to your doorsteps or to catch the person responsible, this application will certainly increase the

chances. It boasts of a strong and secure database based on Google's Firebase. It offers various security features, such as, locating the phone activating alarm mode or ringer mode via messaging. It further provides a list of all the permissions of all the applications in the device. It also features pattern security settings and signal flare.

2. Proposed System

This application uses some starting activities to sign in the user. It provides the user with the functionality to register the user to the online database if not already registered and to log in if the user has already registered. The user also has the option to sign in either via their Google or Facebook accounts using their respective tokens. After signing in, the user is presented the mandatory option to fill in the profile. After that with a navigating drawer. The components of the navigation drawer are as follows.

2.1 Messaging options

This part of the application uses the messaging feature of the device. Firstly, the application requests the user to set a password for operating the phone via messaging. This password resets itself after the user signs out for security reasons. The messaging feature comprises of three different options – Ringer Mode, Alarm Mode, and Location Mode.

The Ringer Mode helps the user to change the profile of his/her device from silent mode or vibrate mode to ringer mode. The Alarm Mode helps the user to ring an infinite alarm and can be stopped by force closing

the application by going to the settings of the device. The Location Mode helps the user to get the device's current location via a link that redirects onto the Google Maps.

To activate any of the mode, it needs to be checked in the settings. Now the user can send a message from any number to the device in the format: "password" + <space> + "keyword", where the password is the password that the user entered for messaging options and the keywords are, RINGER (for Ringer Mode), ALARM (for alarm Mode), and LOCATION(for Location Mode). This application uses a Message Broadcast Listener to receive messages and Knuth Morris Pratt algorithm for matching the received message with keywords.

2.2 Application Permissions

This feature of the project allows user to manually view the permissions that are being used by the applications that are installed in their smartphones. It helps the user to check if the permissions are actually needed or not, if not, then one can uninstall the undesired application from their devices. The basic purpose is to provide user the knowledge about different applications, about what they are accessing and what they are transmitting. This helps the user to identify if they have malware applications installed on their device.

This feature uses package manager of android to load the applications. Further, it uses Asynchronous task to load the list in the background.

2.3 Signal Flare

This feature allows user to automatically get the device's current location to the emergency contact number of the user whenever the device's battery is below by a particular level.

To activate this feature, the signal checkbox needs to be checked. Then using the seek-bar, the user can set the cut-off battery percentage to activate the signal flare. It uses a Battery Broadcast Listener to listen to the change in battery levels using many intent filters to monitor the same. Some of the intent filters used are: BATTERY_CHANGED, BATTERY_LOW, BATTERY_OKAY, and POWER_CONNECTED.

2.4 Password Security

One of the most fascinating feature of the application, allows user to keep an eye on anybody who is using their devices without having user's prior knowledge.

It monitors the user's passwords that is set on the lock screen and counts the number of attempts. When the number of wrong attempts matches the number entered by the user, the application launches the front camera and automatically captures the user's image. The user's image is then sent to the registered email as a warning that a user who is unaware of the password has tried to unlock the device.

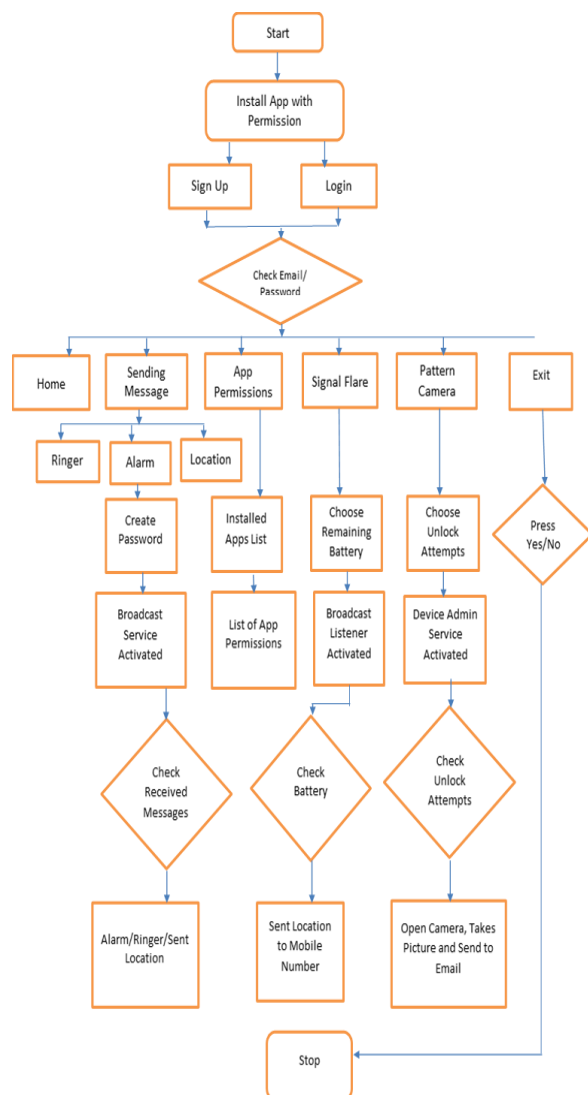


Fig 2.4.1 Flow Chart

3. Technical Background

This application uses various technical approaches in android to implement the features.

3.1 Android

Android is an open-source operating system which is developed by Google. This operating system is most popular in mobile devices, although it is making its way into various other categories. Currently Android holds a market share of approximately 70% leaving behind any popular mobile operating system.

Android's Play Store boasts of having over 2.5 million applications. It is also popular for the amount of customizability it offers. The amount of freedom given to the developers of android is still unmatched. This application is specifically designed to run on android devices.

3.2 Firebase

Firebase is an online database service provided by Google. It is secure and has many additional features. It is available for both mobile application development and web development. It provides a real-time database system and makes it easy to connect to the application. Furthermore, firebase is very versatile and adapts itself to the likes of the developer. It has an API that helps the application to store information in JSON format. Firebase also helps to login faster and in a more secure way as compared to the standard PHP API's. The JSON parsing is faster and easily compatible with android.

3.3 Broadcast Listeners

This application uses two broadcast listeners in the implementation of messaging and signal flare features. In the messaging feature, this application uses the Message Broadcast Listener which catches all the incoming messages and recognizes via KMP Search algorithm whether that message has a Boomerang keyword or not.

In the Signal Flare feature of this application, a battery broadcast receiver is used. This broadcast receiver is set to listen some battery activities such as Change in battery and charging the device. After the broadcast, the battery is compared with the stored value and then

it is decided that the location of the device has to be sent or not. Using broadcast listener, instead of keeping the application alive and monitoring the messages or battery itself, saves battery.

3.4 Fragments

Fragments are provided by android as sub-activities to reduce the load consumed up while loading activities. This application sports a user-friendly navigation drawer and each option in the drawer is linked to a fragment. Whenever the user clicks on any of the options, that respective fragment is loaded into the content view of the main activity. This helps to speed up the application and also helps the user to get a clean image of navigation.

3.5 Shared Preferences

Shared Preferences is a way in android to store a value in a file as a key-value pair. This can be retrieved as well as changed from any part of the application. This application has used shared preferences various times. To keep track of the navigation, to keep track of the selected values, or even to share data between any broadcast listener and a fragment, shared preferences are used. The shared preferences used in this application have been placed in the file named "data".

3.6 Device Administration

For in-depth monitoring of the device, the application needs to be declared as a device administrator. This is done so as to get access to the password security settings. It helps the application get access to more of the device's security features. The password security feature of the application uses Device administration to get the number of wrong attempts the user gets at the password.

3.7 JavaMail API

JavaMail API is a java based API that helps to send email in background with a set username and password. This application's password security feature uses this API to send the photograph captured by front camera to the registered email id. The email is sent via the official Boomerang id "boomerang.database@gmail.com". JavaMail API

provides the SMTP, Simple Mail Transfer Protocol which is used to send the emails.

4. System Architecture

System Architecture appertain to the overall layout of the application. It elucidates the flow of the activities involved during interaction of the user with the application.

The features of the applications are limited to users which are registered on the application. On opening the application, user first need to register for the application by entering email and password. Different validation checks have been implemented to maintain the flow, so that the no false information has is entered for the authentication. Registration can be done manually or by using Google or Facebook. The application is using the Google Firebase as the database for storing the details of the user. After the authentication, user is able to access the different functionalities of the application that are present in the navigation drawer.

Under the App Permission Section, user can be able to view the permissions that have been taken by the already installed applications in the device. In the messaging Setting Section, user can be able to enable or disable the silent to ringer feature, the location tracker feature, or the ring alarm feature. The section also asks user to enter security password after enabling any of the feature. The user has to set the password again, if the user logs out from the application. Under the Signal Flare Section, user has been asked to set a minimum of battery range, so that the user has been informed with the device's last location once the battery has been dropped below that mark, via message or via Email. Finally, under the password security settings, the user can check/uncheck the feature and also fill in the number of wrong attempts.

5. Constraints

The phone should have an active internet connection for many features to work. The signing in and register feature of the Application is completely dependent on queries executed on online servers. Further, for the pattern security settings, internet is required to send the e-mail to the registered email id. Internet will also

be helpful in fetching more accurate location for the messaging feature.

The device should have GPS enabled for detecting the fine location of the device. It also should have a SIM card with some credit in it so as to facilitate the messaging feature. The device should have some decent amount of battery. The device must be protected via a security lock for the pattern security feature to work. All the requested permissions, must be provided for easy working of the application.

For Hardware specification, the device must sport at least a 1 GHZ processor along with at least 500mB of RAM. The device must also be above the required android version.

6. Juxtaposition

There are various anti-theft and security applications available on the play store for android devices. The best of them are: Prey and Lookout. While the Prey application is 100% free, Lookout has many premium features that are only available to paid users. Boomerang will always remain free and open-source. Here is a comparison of the free features between the three applications.

Features	Prey	Lookout	Boomerang
Ringer Mode	No	No	Yes
Alarm Mode	Yes	Yes	Yes
Location Tracking	Yes	Yes	Yes
Wi-Fi information	Yes	No	No
Signal Flare	No	Yes	Yes
Password Security	No	Paid	Yes
Backup Applications	No	Yes	No
Application Permissions	No	No	Yes
Antivirus	No	Yes	No

Fig 6.1 Comparison Table between Prey, Lookout and Boomerang

7. Future Scope of Study

This application is an anti-theft and security application which would have to tackle all the upcoming security threats.

7.1 Power-Button Override

A very important aspect of an anti-theft mobile system is not to let any unauthenticated user to switch-off the device. Therefore the application will provide the feature to override the power button before the security lock, so that the device cannot be turned off.

7.2 Wipe data

With this feature the user can wipe its internal memory, to avoid any data-theft from his/her device. Wiping data, although, will wipe everything on the device including our security application. Hence, this feature should only be used as a last option or when the user is inclined more towards data protection than device protection. This will be added under the messaging security of the application.

7.3 Video Recording

This feature can be used to record videos from a phone and send it via email to track the location of the phone. This will prove useful to identify the suspect or identify the location where the phone is being used. The audio file could be extracted to get more useful information.

8. Conclusion

This application is targeted at the general public, who want to protect their device. It helps the user to find

the phone when it is lost on silent profile, via the Ringer Mode feature. It helps the user to get the location of the phone or ring an alarm in the phone via just a message. It lists all the permission of the applications and leaves up to the user to decide whether an application could be a malware. It captures the photo of any unauthorized user trying to break into the device. This application helps the user to increase the chances of getting back their devices once they are lost or stolen. Hence, the name Boomerang. The application will be regularly updated and new features will be added as and when they see fit.

9. References

- [1]. K. Subha, Dr. S. Sujatha, "Anti-Theft Tracking System for Smart Phones", International Journal of Advanced Research in Computer Science and Software Engineering. ISSN: 2277 128X
- [2] Shweta Dhanu1, Afsana Shaikh2, Shweta Barshe3, "Anti-Theft Application for Android Based Devices", International Journal of Advanced Research in Computer and Communication Engineering Vol. 5, Issue 3, March 2016. ISSN (Online) 2278-1021 ISSN (Print) 2319 5940
- [3] [KMP77] D.E. Knuth, J.H. Morris and V.R. Pratt" Fast Pattern Matching in Strings" in *SIAM J. Comput.* **6**, 2 (1977) 323–350.
- [4] K.S. Kuppusamy1, Senthilraja.R2, G. Aghila3, MOBILE LOCATION ESTIMATION AND TRACKING FOR GSM SYSTEMS Vol. 4, Issue 5, June 2015
- [5] J.ManiBharathi, S.Hemalatha, V.Aishwarya, C.Meenapriya, L.Hepzibha Shekinah Grace, "Advancement in Mobile Communication using Android", International Journal of Computer Applications (0975 – 8887), Volume 1 – No. 7, 2010.
- [6] Chao-Lin Chen; Kai-Ten Feng; "Hybrid Location Estimation and Tracking System for Mobile Devices"