SMS Security for Android

Brijesh Rathod

Project Partners: Isa Chang, Kanwalpreet Dhindsa
Department of Electrical Engineering, San Jose State University, San Jose, California 95192

Introduction

Implementation of this security application can protect the phishing attacks delivered through SMS. Since it’s a background application, the user is not intervened or prompted.

The world has seen many dangerous cyber security attacks and the worst effects of it. Phishing can be the first phase of any cybersecurity attack. It is used to gather sensitive information from users. So, stopping phishing can be a good start minimizing the risk of security attacks.

Android is the most used mobile OS in the world and since it is open-source, it is more prone to attacks too. As a small step securing mobile space, we made security application for Android.

There are many ways users are delivered and taken to the phishing sites. One way is via SMS messages. Usually, user has to see the link in the browser to come to know that the link is a phishing one via anti-virus services if the phishing source is detectable by the service.

This application does not even let the user see such kind of phishing SMS. It accesses the SMS and checks whether it is dangerous or not and if it is, it quarantines it and the user gets notified about the phishing SMS.

Implementation

There are mainly two parts of implementation. Getting the SMS before the default Android messaging service and detecting that the SMS contains phishing URL.

For this, the application runs a background service that monitors all the incoming SMS and processes it before they are given to default Android messaging service.

This is done using a child class to the BroadcastReceiver() classs which is the default messaging service. We override its onRecieve method which defines what to do when an SMS is received.

The application processes the SMS and look for a URL. If there is one, it is checked that whether it is a phishing URL or not.

To detect whether it is a phishing URL or not, crowd-sourced intelligence is used. Phishtank is one of the largest and best community for threat-sharing. It is a community for detecting phishing sources.

Phishtank also provides an API for developers to use the data gathered in the community. The team used it to check with the crowd-sourced threat intelligence and to detect the phishing URL.

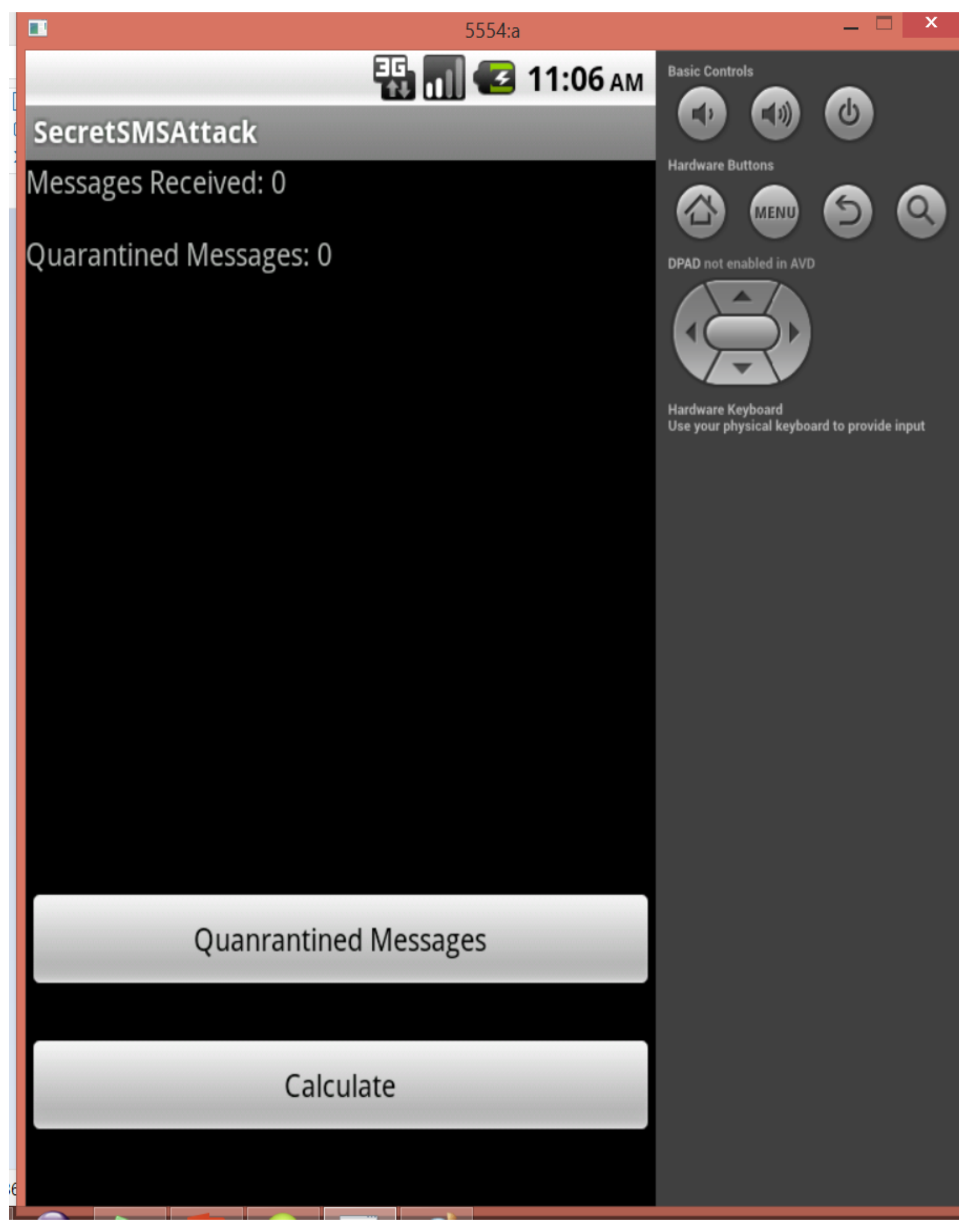
The API provided by Phishtank is used to do this. The URL received is sent to the API as per the API requirements.

The response is asked in JSON format and the data is extracted using JSON parser. If it’s verified phish URL, it is blocked and sent to the SQLite Database of Android which is displayed to the user. A counter for messages is also implemented.

Results

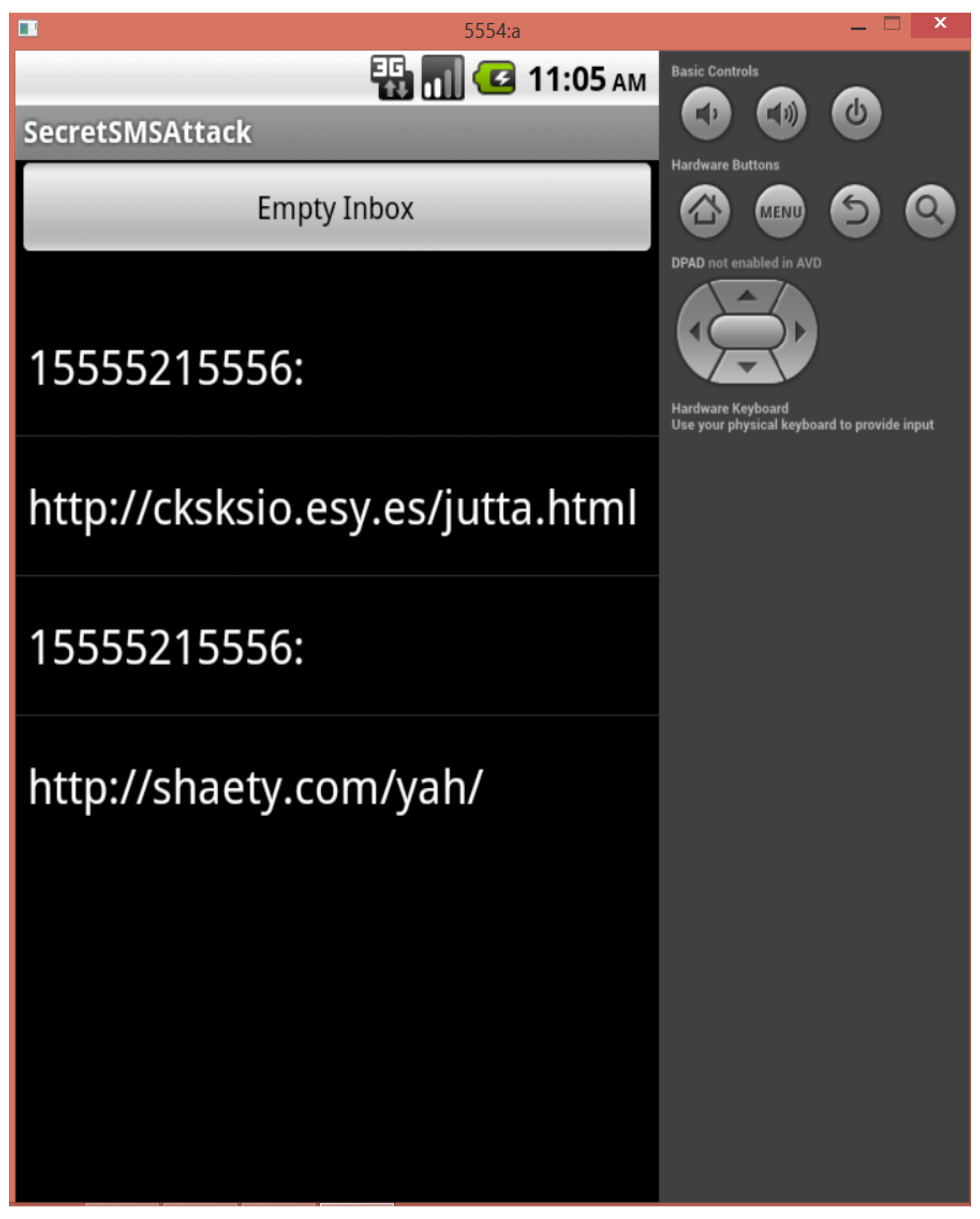
The Android Application was created successfully with successful phishing message detection in a way that user does not have to view it in the browser to get notification that it is a phishing site as proposed. Below are some screenshots of the application running on emulator.

Home Screen:



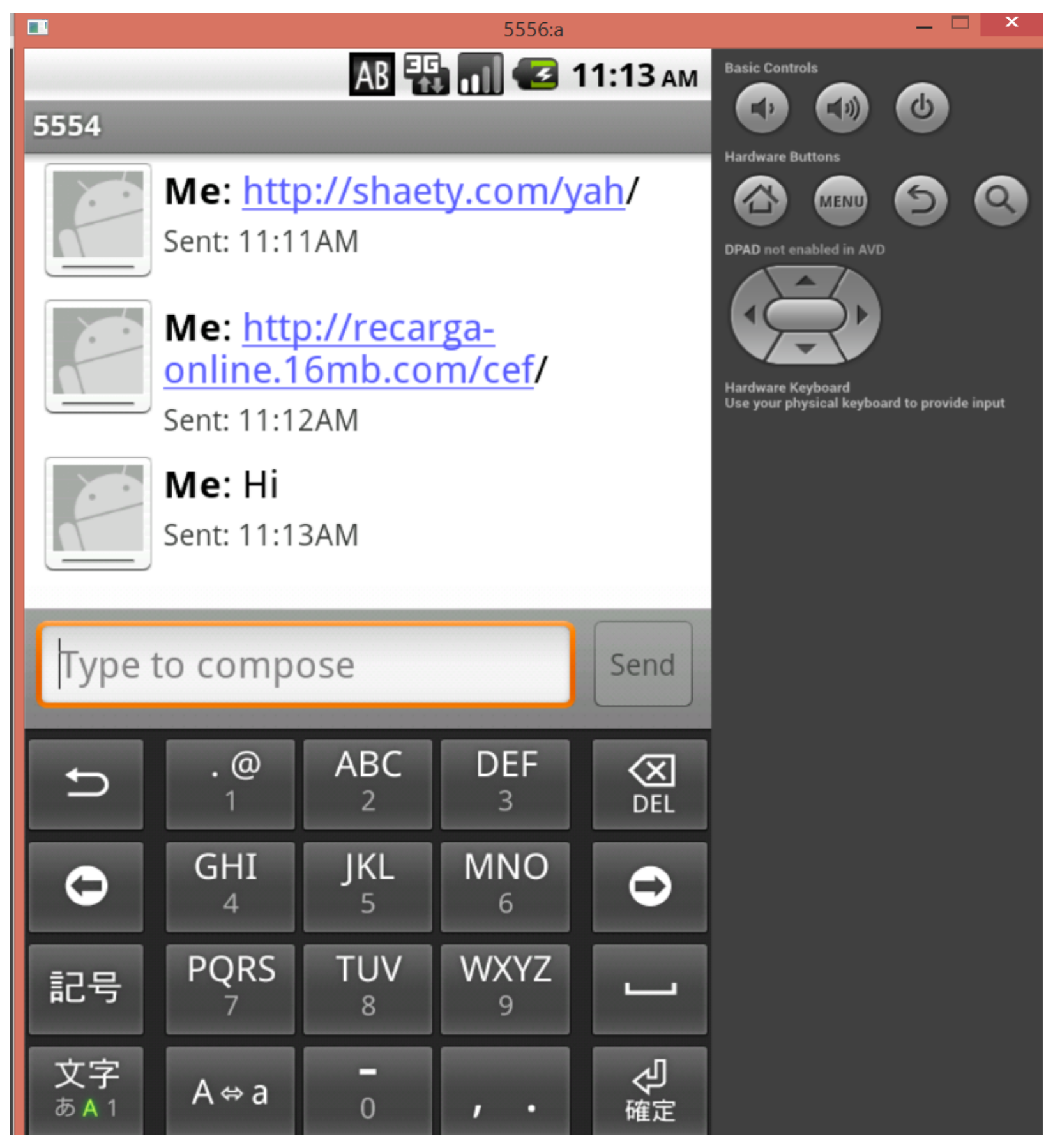
5554:a
11:06 AM
SecretSMSAttack
Messages Received: 0
Quarantined Messages: 0
Quanrantined Messages
Calculate

The Quarantined messages:



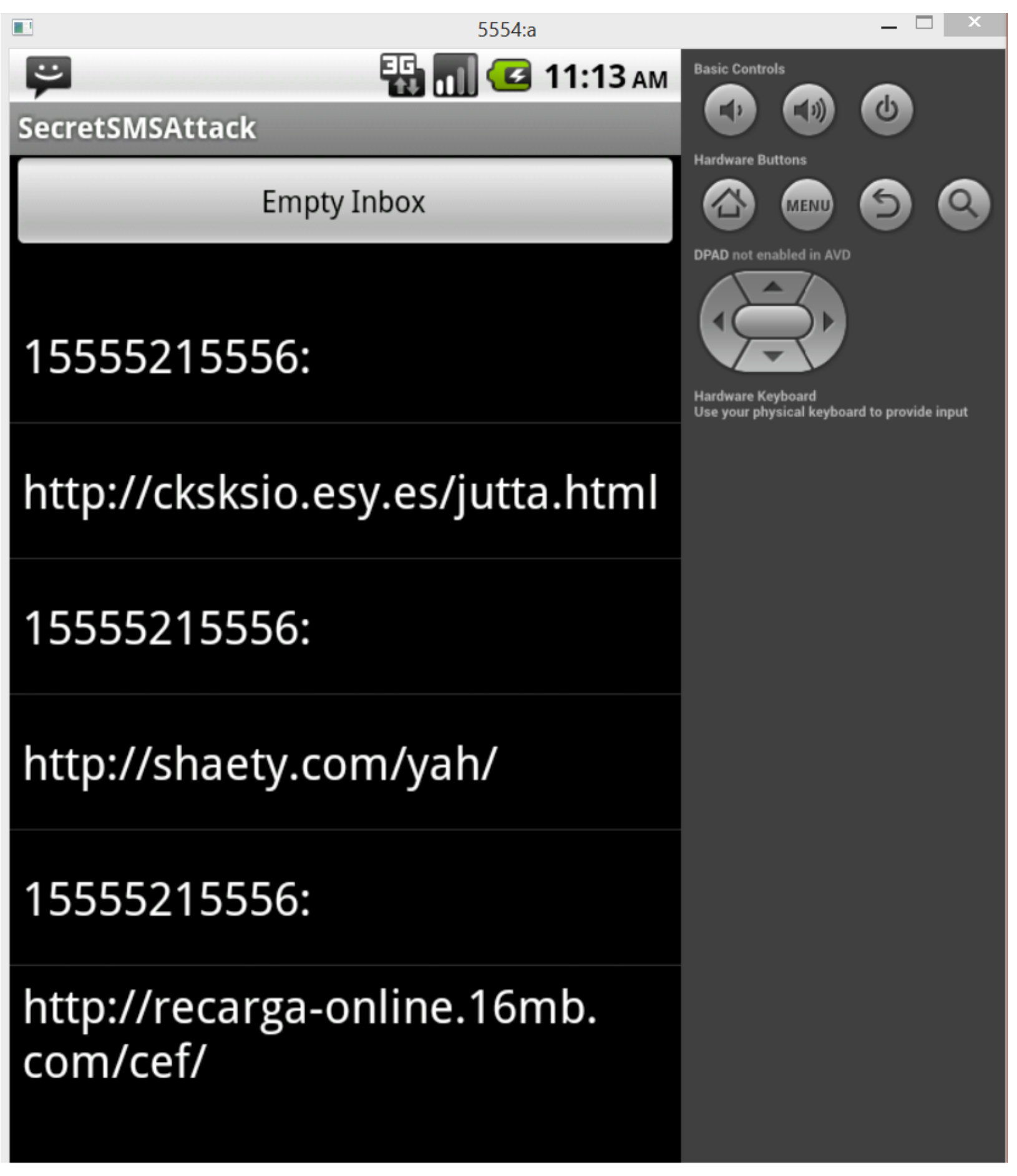
5554:a
11:05 AM
SecretSMSAttack
Empty Inbox
15555215556:
http://cksksio.esy.es/jutta.html
15555215556:
http://shaety.com/yah/

Now two messages are sent: one phishing URL and one normal message



5556:a
11:13 AM
5554
Me: http://shaety.com/yah/
Sent: 11:11AM
Me: http://recarga-online.16mb.com/cef/
Sent: 11:12AM
Me: Hi
Sent: 11:13AM
Type to compose
Send

The normal message is passed while the URL is in the quarantined messages list.



5554:a
11:13 AM
SecretSMSAttack
Empty Inbox
15555215556:
http://cksksio.esy.es/jutta.html
15555215556:
http://shaety.com/yah/
15555215556:
http://recarga-online.16mb.com/cef/

Conclusions

An Android application was successfully developed for blocking phishing SMS. The application also stores the quarantined messages in a database and keeps account of the received and quarantined messages. The application secures the device, the user's information and his contacts by creating an additional layer between the sender and inbox. The messages are first scanned by the application for the phishing URL before it goes to inbox and if it is safe, then only it lets the SMS go to the inbox. In this way, the application achieves its feature of blocking the phishing message without even disturbing the user. The application runs successfully on Android devices with all versions of the operating system.

Key References

[1] Adrienne Porter Felt, David Wagner. Phishing on Mobile Devices.

[2] Developer.android.com, 'Android Developers', 2015. [Online]. Available:http://developer.android.com/index.html.

[3] Phishtank.com, 'PhishTank | Join the fight against phishing', 2015. [Online]. Available: https://www.phishtank.com/.

Acknowledgments

The author would like to thank our project advisor Professor Chao-Li Tarng for his continuous guidance and encouragement. The author would also like to thank Professor Morris Jones and Professor Thuy Le for their guidance and support.

For further information

Please contact *brijesh17007@gmail.com*.