Android SMS Security Application

Isa Chang, Professor Chao-Li Tarng
Department of Electrical Engineering, San Jose State University, San Jose, California 95192

Introduction

This project addresses the concerns of SMS based security with the Android platform. The idea is to have a filter which prevents SMS messages with malicious URLs from entering the inbox of the Android phone. Prior to entering the inbox, the SMS message is quarantined when the URL is extracted from the message and cross-referenced with a database that is filled with malicious URLs. Any suspicious texts are also thrown away.

Why Engage in SMS Security?

- Android OS Platform has increased in market share since 2013 [1]

	2012		2013		
	Units (M)	Market Share	Units (M)	Market Share	Growth in 2013
Android	517	70%	813	79%	57%
iOS	136	19%	153	15%	13%
Windows Phone	16	2%	33	3%	105%
BlackBerry	33	4%	19	2%	-42%
Symbian	23	3%	1	0%	-96%
Others	9	1%	8	1%	-15%
Total	**734**	**100%**	**1,027**	**100%**	**40%**

Table 1. Android Market Share

Android SMS Security Concept

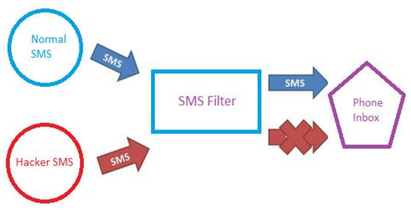

Figure 1. Concept Diagram for Android App

What Are We Preventing?

One type of SMS attack is known as “Contact Hi-Jacking” where the hacker can steal the victim’s contact info simply by sending a “word bomb”[2].

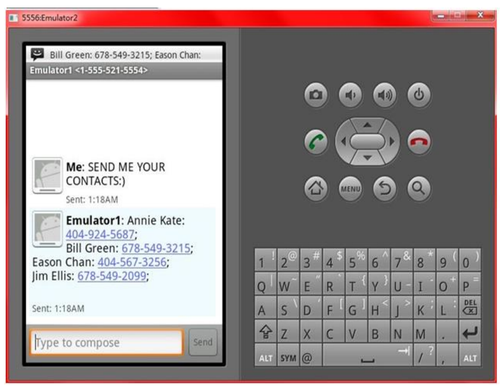

Figure 2. SMS Contact Theft

- The same concept can be applied to malicious URLs sent through text messaging.
- Hacker can program URL to send any information once it is clicked
- We prevent that URL from ever entering the inbox, prevents is the best solution!

Design Approach

Three Main Stage of Android SMS App

- Design of User Interface
- Design of Check Phish Function & Filter
- Design of Database for Information Storage

Android SMS App User Interface

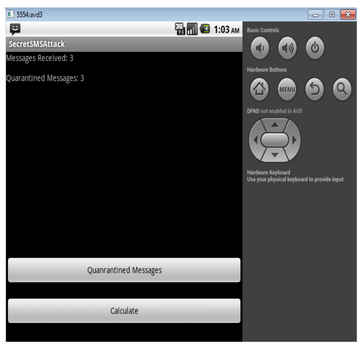

Figure 3. Front End of App

User Interface allows the user to display the number of messages filtered and received. The filtered messages can also be viewed by clicking “Quarantined Messages”

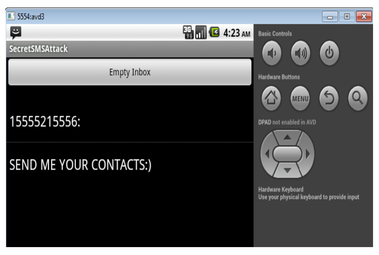

Figure 4. Displaying Filtered Messages

The user is also able to delete the message by clicking the “Empty Inbox” button once they are finished viewing the message, this prevents the URL from being clicked and potentially causing damage. [4]

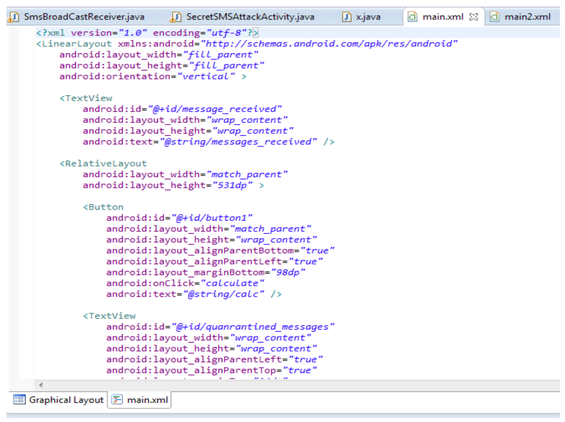

Figure 5. Coding the Graphical Layout

Design of CheckPhish & Filter

- “Check Phish” function is used to extract, store, and send any URLs that enters the user’s mobile device
- Upon sending to phishtank.com, a cross-referencing is done to see if the sent URL matches with any malicious URLs stored in the phistank.com database, if so, the message is automatically filtered [3]
- The filtered message are not allowed in the inbox, they are stored in a remote location where the user can only access them through this app. This prevents any accidental clicking of the malicious URLs.

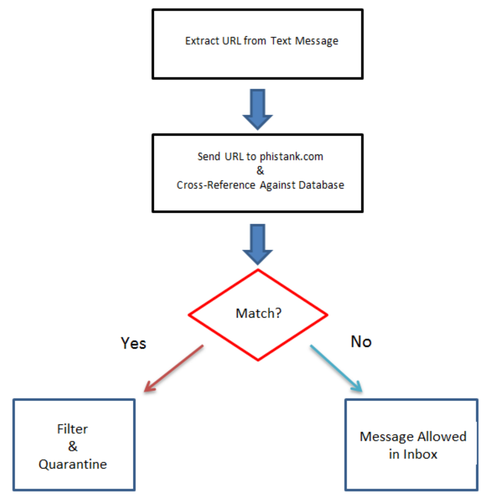

Figure 6. Block Diagram of Back End

Results

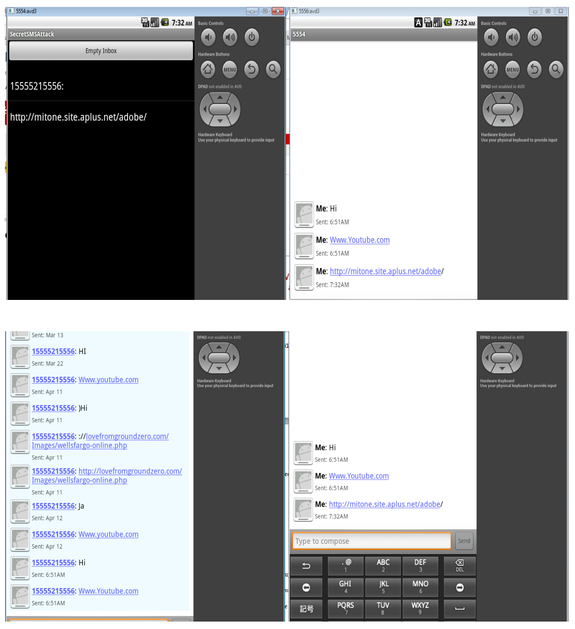

Figure 7. Malicious URL is Filtered

- Malicious URL is chosen from phishtank.com
- Hacker (Right Emulator) sends the malicious URL
- Android App (Left Emulator) filters the URL since it found a match in phishtank.com database. The message is stored in a remote location
- User has the option to delete all quarantined messages
- The message does not show up in the app user’s SMS inbox as it has been filtered, thus preventing the user from accidently clicking any unwanted URLs

Conclusions

The Android SMS App successfully filters any text which may have malicious URLs. By using the Phishthank.com database, any mobile device using this app can be sure that no intentional harm will come. Future plans involve adding more databases to increase likelihood of successful defense. The main philosophy is that “Prevention is the Best Solution”. Why try to solve the problem after it has appeared, let’s try stopping it before it happens!

Key References

[1] CCS Insights. "Global Smartphone Market Analysis and Outlook: Disruption in a Changing Market." *CCS Insight Report* (n.d.): n. pag. *For Those Lenovo Who Do*. CCS Insights, June 2014. Web. 16 Apr. 2015.

[2] Qian, Kai, Prabir Bhattacharya, Minzhe Guo, and Li Yang. "SMS Threat/Attack Lab Activity(Eclipse Mobile Security Labware.“ SMS Threat/Attack Lab Activity(Eclipse) - Mobile Security Labware Google Sites, n.d. Web. 19 Apr 2015.

[3] Misra, Anmol. *Android security attacks and defenses*. Boca Raton, FL: CRC Press, 2013. Print.

[4] Prayaga, Lakshmi, and Jeffrey Hawthorne.*Android App Inventor for the absolute beginner*. Boston: Cengage Learning PTR, 2013. Print.

Acknowledgments

We thank Professor Chao-Li Tarng for providing valuable guidance, suggestions, and providing the topic of Android Based Security for the project..

For further information

Please contact *isachang1990@gmail.com* for more information. The source code & demo can be provided upon request. Validation from Professor Chao Li Tarng may be needed prior to providing any information.