A study of message security system on Smartphone-based for message security threat prevention

SuckJoo Hong*, Hae-Gill Choi**

*Corporation of Industrial Educational Programs, Mokwon Univerity, #88 Doanbuk-ro, Seo-gu, Daejeon, 302-729, Korea
sjhong@mokwon.ac.kr

**Corresponding Author, Deptment of Digital and Media Technology, Kyung Hee Cyber University, 1 Hoegi-Dong, dongdaemun-Gu, Seoul, 130-701, Korea
hgchoi@khcu.ac.kr

Abstract. With the latest number of smartphone users having exceeded 20 million, smartphone use is growing rapidly thanks to their openness as a mobile communication platform enabling the operation of a wide range of applications or apps. However, such rapid spread of smartphones is also creating the optimal condition for malicious code programs that are being spread exclusively targeting smartphones and enabling negative functions, such as hacking and violation of users’ privacy.

The latest known online fraud schemes, including pharming and smishing, have incurred significant amounts of money in damage, as such programs infiltrate into the user’s financial as well as personal information. As the focus of smartphone-based mobile and electronic infiltration is being put more on the users of such gadgets, users are being requested to come up with more aggressive measures for protecting personal information security. Notwithstanding the importance of such protection, users are being faced with the limitation in their aggressive blocking of electronic violations of their personal information as committed in multiple channels. This makes it necessary to build a secure mobile environment that can help minimize the leaks in personal information and the financial damages incurred on users.

This study aims to address the message security system capable of protecting the critical information and property of users to help prevent any leaks in the personal information and the financial damages that could result from smishing. Such protection can be offered by analyzing the text messages, prior to users’ checking of them, by scanning any malicious information contained therein, and by implementing necessary security measures based on the results of such scanning, including blocking or deleting of the message concerned.

Key words: smishing, mobile security, malicious codes
1 Introduction

As the use of smartphones has increased rapidly in Korea and elsewhere around the world, threats/risks associated with mobile security in smartphones, etc., have also increased to such that the smartphone security has become a big issue. Hence, more attention has been given to security in the mobile environment.

Equipped with OS (Operating System), smartphones offer to users services quite similar to the ones offered by desktop PCs (Personal Computers). Likewise, similar security threats possible to realize on desktop PCs are being recognized on smartphones as well.

The reason why malicious codes are found in smartphones is that smartphones are capable of engaging in voice-activated communications as well as in Web-based communications. Additionally, the spread of malicious code programs has become far easier through the use of ultra-high-speed wireless communication networks. Other reasons contributing to the rapid increase in the spread of malicious codes in smartphones include: expansion of access to Wi-Fi and Wibro, expansion of wireless browsing, improvement in performance of mobile phones, personalization of mobile phones and support for e-Approval systems, and open platforms embraced by smartphones.[1]

Back in 2012, the number of smishing malware identified was 29, whereas the number between January and August 2013 totals to 2,433, an 84 times increase. Of the 725 smishing malware detected last month, the ones that can actually cause financial damages are 252, accounting for 34.8% of the total number of smishing malware.[2]

This study intends to address the security issue regarding smishing malware that is causing significant damages to users in various ways. To this end, the study introduces the user-friendly and easy-to-use method/system that is capable of blocking smishing-induced infiltration by allowing the users to analyze the incoming text messages, to determine if they are malicious to their mobile system, and if yes, to have the smishing malware blocked from their system.

2 Related studies

2-1. Security trends in smartphones

The vitalization of mobile infrastructure and the smartphone market does not offer to users the positive effects only. The mobile device has embraced the general-purpose OSs due to the increase in open platforms and introduction of app stores, which results from the full-scale competition now in progress in the smartphone market. Such use of the general-purpose OSs has made it easier to create malicious codes for mobile devices, and so created mobile codes are highly portable due to the use of general-purpose OSs, thus increasing the scale of mobile attacks and the extent of damages therefrom.
The above-mentioned threat to mobile security has made it necessary to ensure safer smartphone service environment both in Korea and abroad and to build a defense system against the possible security threats proactively. To this end, research has been conducted on internal security technology for mobile devices as well as on technologies for remote security control, support for safer e-Approval services, and verification of mobile applications distributed through app stores. [3]

2-2. Security trends in smishing

Regarding the solutions to prevent smishing programs, independent analysis technology and mobile security control capabilities have been put to use comprehensively, based on the top-grade database (DB) on malicious code programs, including the latest malicious apps that had been identified in Korea as well as hundreds of thousands of externally created and distributed malicious apps that had been collected. Such approach to mobile security avoids simple checking of Android-based malicious apps for installation authorization. Hence, the risk of misdiagnosing similar patterns has been minimized, while increasing the actual efficacy of detecting the new variants of smishing malware.

The existing mobile vaccines are created such that they are capable of detecting malicious apps known to Korea and elsewhere around the world, requiring relatively large resources to carry out the said function. In more recent years, more focus has been put on minimizing the data input required for real-time monitoring, thus successfully making the system as light and small as possible. Also, the problems with battery consumption and resources occupation have been solved, allowing expecting a smishing-exclusive security solution(s) that contributes in significant way to user convenience and security improvement.

3. Smishing security strategies and solutions

3-1 Smishing security system diagram
① Security DB server
- Security DB server to (a) collect information about smishing-caused damages (cases) and (b) control and update the collected information such that it can be used by malicious message scanning apps.

② Malicious message scanning app
- A software program that automatically handles malicious codes according to the security policy, by analyzing incoming messages (senders’ phone No., malicious URLs, unrecognizable No., etc.) and submitting any problems detected to the security server.
- If an unwanted message has been received, a manual function capable of blocking or deleting such message is provided.

③ Social network-based security ranks DB
- A DB to apply security ranks to and control such individuals who send malicious messages using the addresses stored in smartphones.

④ System management, statistics server
- A server to collect the information on each user from the social network-based security rank DBs and to analyze any big data and carry out overall statistical functions and management thereof.

3-2 Procedures for blocking malicious messages

① Malicious message scanning

② Message scanning
  - Determine whether or not it is a malicious message by comparing the malicious information updated on the user’s smartphones.

③ Implementing security policy
  - Scan the message to verify whether it is malicious. If it turns out malicious, implement the security policy and rules to have it blocked, deleted, etc.
  - If it turns out a normal, non-malicious message, do not implement the
security policy.

4. Security server update
   - In cases where malicious information is searched during message scanning, search the information by comparing it against the security server’s malicious information DB. To this end, this update ability registers and controls the latest malicious information.

4 Smishing security module design

4-1 Smishing blocking module

The following flow chart illustrates the overall flow of the process wherein an incoming message is analyzed to determine whether or not it is malicious to the system and whether the message needs to be blocked or deleted.

1) Malicious message-read module

To ensure security against smishing, it is necessary to have system abilities that will determine the presence of malware before exposing the initial incoming message to the user. If the message turns out malignant, such abilities will block the messages
from entering the system.

This study proposes a method for detecting the URL details via text message search, which are entered in the system as linked to the message. That is subject to analysis to determine whether or not it is malicious. The proposed method also blocks any and all messages that match the information from malicious URL database.

Through the smishing URL pattern analysis, common URL patterns will emerge. Hence, to reduce overloads in the search engine and smartphone, the following information describes how to search the common string and to block unwanted URLs promptly:

2) Message filtering module
This section defines the rules that allow the user to have the messages handled either manually or automatically, after reading the malicious information. The rules include the blocking, deleting and enabling of the telephone No. and malicious message filtering abilities.

In this paper, however, definition is to be provided only for the malicious message filtering to ensure blocking of smishing malware.

1) Definition of malicious message filtering rules
   - Block malicious URLs:
     Ability to block the URLs via search through the previously stored malicious sites BD, if they are found on the list of such sites
   - Allow malicious URLs:
     Ability to allow the sites if they are not included in the previously stored malicious sites DB
   - Revise blocking/allowing malicious URLs:
     Ability to switch from the blocking to allowing ability against the stored malicious DB information, as well as ability to manually register the previously blocked URLs

5 Conclusion

With the extremely rapid growth in the smartphone market, security threats such as malicious programs and smishing malware that target smartphones, too, are on the rise. As for smartphones, it is a particularly serious issue because the phones carry
large amounts of sensitive personal information, meaning any breach of security would lead to serious problems.

Recently, smishing malware is disguising itself as a message sent from someone whom the user can trust or from trusted businesses, thus requesting the user to expose his/her personal information. Smishing malware also change itself in various forms — stealing from users all of their SMS (Short Message Service) information; deleting the normally stored banking apps from the smartphones and installing malicious apps instead, thereby stealing the financial information of the users.

Such prevalent and imminent security threats have inspired the present researcher to study strategies for ensuring smartphone security against threats from smishing malware. For this study, a method was examined that analyzes the information contained in the incoming messages and blocks the information depending on their malicious/non-malicious characteristics. Additionally, such method is expected to be utilized as basic tool for determining the smartphone-based smishing patterns and information, blocking malicious information and developing automated analytical systems.

For future studies to realize the proposed idea as described in this study, it would be necessary to examine the pros and cons of the proposed method and to continue to study other strategies collectable for examination. Lastly, optimization of analytical technologies shall be studied as well to apply such technologies previously studied to the current smartphone environment.

References