JANT 한국항행학회논문지
Journal of Advanced Navigation Technology

기반 기술

J. Adv. Navig. Technol. 18(6): 569-575, Dec. 2014

안드로이드 플랫폼 기반에서 스미싱 탐지 및 차단을 위한 기술적 대응체계 연구

A Study of Technical Countermeasure System for the Smishing Detection and Prevention Based on the Android Platform

서 길 원 · 문 일 영*
한국기술교육대학교 컴퓨터공학부

Gil-won Seo · Il-Young Moon*

School of Computer Science and Engineering, Korea University of Technology and Education, Chungcheongnam-do 330-708, Korea

[요 약]

2009년 이후부터 스마트폰 및 태블릿 PC의 사용자 수는 기하급수적으로 늘고 있다. 특히 성장의 중심에는 애플의 iOS와 구글의 안드로이드 OS가 있으며, 대부분의 스마트폰과 태블릿 PC 들이 이 두 OS 중 하나를 기반으로 하여 동작을 하도록 설계되어 있다.

그리고 이러한 스마트기기 사용의 증가는 시간 및 장소의 제약을 줄이는 사회 환경의 변화로 이어지고 있다. 그러나 이런 발전이 우리에게 편의성만을 제공하고 있지는 않으며, 오히려 과거에 비해 더욱 쉽고 빠르며 심지어 자신이 알지도 못하는 사이에 중요 정보를 유출할 수도 있고 금전적 피해로도 이어지고 있다. 대표적으로 초기의 피싱, 파밍에 이어 현재의 스미싱과 이를 변조한 큐싱 등 다양한 공격을 통해 금전적 피해 및 심각한 정보 유출 등이 발생하고 있다. 이에 본 논문에서는 스미싱 공격을 기술적으로 탐지 및 차단할 수 있는 대응체계를 제안하고, 제안한 방법으로 스미싱 공격을 100% 탐지하여 기존의 탐지 방법과 비교하여 성능이 우수함을 보였다.

[Abstract]

Since 2009 the number of users of smart phones and tablet PC is growing exponentially. In particular Apple's iOS and Google's Android OS are the heart of this remarkable growth, most of smart phone and tablet PC are designed to operate based on these two OS. Such increasing use of smart devices has led to changes in the social environment that allows, without the constraints of time and place. However, such development does not supply only ease to do something, even compared to past, financial fraud and information leakage are easier than before by variety of new types of attack for example phishing, pharming, smishing and qshing. So according to this paper, analyzes for smishing attack, propose a countermeasure system of the technical way and proved its higher performance compare to the existing method.

Key word : Android, Detection, Malicious app, Prevention, Smishing.

http://dx.doi.org/10.12673/jant.2014.18.6.569

Received 20 October 2014; **Revised** 24 November 2014
Accepted (Publication) 12 December 2014 (30 December 2014)

***Corresponding Author; Il-Young Moon**

Tel: +82-41-560-1493
E-mail: iymoon@koreatech.ac.kr

Ⅰ. 서 론

2009년 스마트폰 출시 이후 전 세계적으로 스마트폰 및 태블릿 PC를 사용하는 사람들의 수는 꾸준히 증가하고 있다. 이는 누구나 자신이 원하는 것을 언제든지 빠르고 간단하게 할 수 있다는 장점 때문이다. 특히 영국 ICrossing의 모바일 OS 시장점유율 보고서(2014.1)에 따르면, 이러한 증가세를 이끌어가는 두 축은 애플의 iOS와 구글의 안드로이드 OS 임을 알 수 있다[1].

그리고 이 자료에 따르면, 2012년 중반 이후부터 안드로이드 OS 계열의 스마트폰과 태블릿 PC의 시장점유율이 애플의 iOS를 넘어서고 있다. 이는 상대적으로 폐쇄적이고 제한적인 기반의 iOS에 비해 안드로이드 OS는 개방적이고 구글 플레이스토어를 통해 누구나 공유하기가 쉽다는 점이 큰 장점으로 작용한 것이 크다는 것을 의미한다. 즉, 개발과 공유의 용이성으로 안드로이드 OS의 시장점유율이 높아지고 있는 것이다.

하지만 이러한 안드로이드 OS의 장점이 오히려 문제점으로 돌아오고 있다. 바로 iOS 기반에 비해 월등히 많은 악성 앱의 수이다. 이 역시 안드로이드 OS를 기반으로 한 개발과 공유의 용이성 때문으로 파악해볼 수 있다. 그리고 이러한 문제점을 가장 잘 보여주는 것이 최근의 스미싱 공격사례라 할 수 있다. 그리고 이러한 스미싱 공격에 따른 피해를 줄이기 위해 차단한 악성 앱의 수가 급증하였다[2].

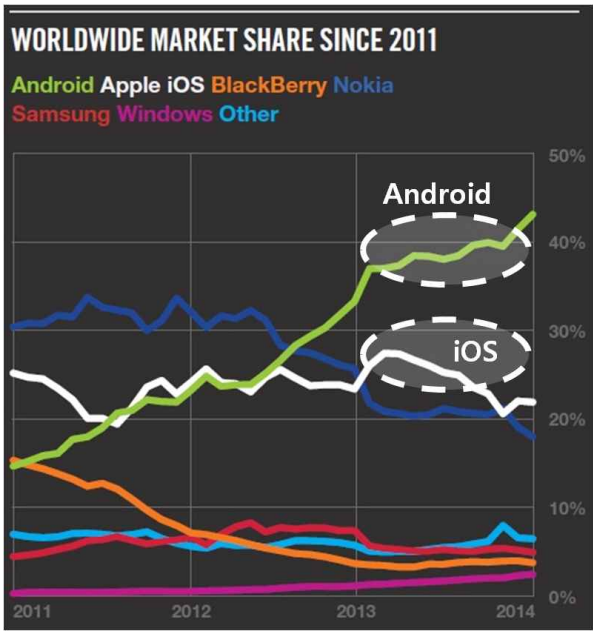

그림 1. 2011년 이후 전 세계 스마트폰 OS별 시장점유율
Fig. 1. Worldwide market share since 2011.

표 1. 스마트폰 금융사기 통계
Table 1. Smartphone financial fraud statistics.

	2012년	2013년	계
악성 앱 차단 수	17	1,688	1,705

스미싱은 간단하고 빠르게 불특정 다수 혹은 특정 누구를 선정하여 금융사기를 벌일 수 있다는 특성이 있다. 즉, 금융거래, 쇼핑 등의 행위를 간단하고 빠르게 할 수 있다는 것과 불특정 다수에게 문자, SNS 등을 활용하여 악성 앱을 쉽게 공유할 수 있는 것이 금융사기의 피해를 키우는 환경적 요인일 수 있다.

반면, 이를 예방하기 위한 현재까지의 노력은 매우 낮은 수준에 불과하다. 출처를 알 수 없는 앱의 설치를 막기 위해 개인의 단말기 내에서 일일이 옵션을 설정하거나, 소액결제를 차단 혹은 최소화하도록 통신사를 통해 관련 설정을 적용하는 것, 그리고 스스로 조심하는 것 이외에는 현실적 대안이 별로 없었다. 그나마 요즘의 사회적 이슈로 인해 일부 스미싱 방지를 위한 앱이 개발되어 어느 정도 피해를 줄이고자 노력 중에 있다.

이에, 본 논문에서는 스미싱 시도를 탐지하고 차단함으로써 스미싱으로 인한 피해를 예방하기 위한 기술적 방안을 제시하고자 한다.

Ⅱ. 기존 연구

2-1 스미싱의 개요

1) 개념

스미싱은 SMS와 phishing의 결합어로서, 문자메시지를 응용한 연결 수단을 이용하여 피싱하는 방법을 말한다. 공격자는 스마트 기기에 사회공학적인 문자메시지 등을 발송하여 소액결제, 자동결제, 금액이체 등 다양한 금융 사고를 유발한다[3].

스미싱은 악성코드가 삽입된 앱인 악성 앱을 사용하고, 악성 앱은 자신의 목적을 달성하고자 사용자 모르게 실행이 되는 것이 일반적이다. 이러한 악성 앱의 실행에 의해 사용자는 정보유출 및 금전적 피해를 당하게 된다. 더욱 큰 문제는 이러한 악성 앱이 자신의 스마트 기기에 설치 및 실행되고 있다는 것 자체를 모르는 경우가 대부분이라는 것이다.

2) 스미싱 공격 절차

악의적인 목적을 가진 공격자가 공격 대상에게 이벤트, 무료쿠폰, 대출, 사진송부, 범법행위 처벌 안내 등 매우 기발하고 다양한 방식의 메시지를 SMS로 전송한다. 이 때 이를 수신한 스마트폰 사용자가 흥미를 느껴 해당 메시지에 포함된 링크를 접속하게 되면, 사용자의 의지와 관계없이 사용자의 스마트폰에 악성코드가 포함된 악성 앱이 설치되고, 이를 이용하여 사용자의 인증정보를 확보하거나 직접 소액결제를 유도하는 등의 행위를 할 수 있다[4].

최근에는 스미싱 공격을 위한 다양한 사회 공학적 기법의 발전과 더불어 공격에 사용되는 악성 앱 역시 점점 진화하고 있다. 공격용 앱 외에도 다운로더 앱을 추가함으로써 이를 제거하더라도 최종적으로 악성 행위를 수행하는 앱이 제거되지 않고 사용자 몰래 계속 활동한다[5].

그림 2. 강화된 스미싱 공격 절차
Fig. 2. More powerful smishing attack flow.

2-2 국내 스미싱 피해사례 및 대응 현황

1) 국내 피해사례

스미싱 피해 유형은 다음의 몇 가지 사례가 있다.

첫째, 결제정보 메시지를 발송하는 방법으로 공격자는 거짓 메시지를 발송하여 고객센터에 전화통화를 걸도록 유도한 후, 환불 목적의 인증번호를 요청하여 사기결제에 사용한다.

둘째, 청첩장이나 돌잔치를 사칭하는 메시지를 발송하는 방법으로 공격자는 사용자의 지인으로 사칭하여 모바일 청첩장이나 돌잔치 초대를 가장한 문자메시지를 발송하고, 사용자가 메시지에 포함된 URL을 연결할 때 악성 앱이 설치됨으로써 정보유출, 금융피해가 발생한다.

셋째, 공격자는 사용자에게 친숙한 유명 패스트푸드의 쿠폰이 제공되었다는 문자메시지를 발송하고, 사용자가 메시지에 포함된 URL을 연결하도록 유도한다.

넷째, 공격자는 경찰청, 우체국, 법원 등을 사칭해 법원등기 발송, 형사소송 참고인 조사 송환 등의 문자메시지를 발송하여 사용자가 메시지에 포함된 URL을 연결하도록 유도한다[2].

2) 스미싱 대응 현황

스미싱 공격의 목적이 사용자의 개인정보나 금융정보 탈취도 있겠으나 궁극적으로는 금전적 이득을 위한 것이라고 볼 수 있다. 직접적인 것은 소액결제, 계좌이체, 금융거래 시 필요한 각종 인증정보가 될 것이며, 그 외 개인정보는 고객정보의 수가 곧 경쟁력이 되는 대부업체, 보험업체 등으로 팔려나갈 수 있을 것이다. 그렇기에 관련 법령 개정 및 지연인출제도, 대포통장 관리시스템 등을 시행한 바 있다[6].

하지만 이러한 관리적 측면의 보완만으로는 완벽히 사용자를 보호할 수 없다. 따라서 개인용 스마트 기기의 설정 적용 및 통신사의 소액결제 서비스 최소화 등 기술적/관리적 개선책을 함께 적용함으로써 그 피해 정도를 줄이고자 하였다.

그러나 개인용 스마트 기기의 설정 적용을 수작업으로 해야 하는 번거로움과 특수한 경우 정상적인 앱 설치를 해야 함에도 불구하고 구글 플레이스토어나 기타 인증 받은 앱 마켓이 아닌 특정 기업에서 자체적으로 온라인에 등록하고 다운로드 할 수 있도록 한 경우 사전에 적용한 안전장치를 다시 해제해야 하는 문제가 있다. 그리고 이 안전장치를 해제하여 관련된 앱을 설치한 후 다시 이를 적용해야 함에도 불구하고 놓치고 넘어가 무방비 상태가 되는 경우도 발생할 수 있다.

스미싱 피해가 심각해짐에 따라 각 통신사 및 보안전문 업체에서 자체적으로 혹은 제휴를 통해 스미싱 방지용 앱을 개발, 배포하기 시작하였다[7].

하지만 이들은 검사 방식과 검사 시점의 문제점을 갖고 있어 보완이 필요하다.

Ⅲ. 스마트 차단 시스템

3-1 악성 앱 탐지 및 차단

SMS에 포함된 링크를 통해 악성 앱이 설치된다는 것에 초점을 맞추어, 사용자가 최초로 앱을 설치할 때 해당 앱의 고유한 ID 값을 암호화하여 DB에 저장하고 이때의 앱의 명칭과 고유한 ID 값을 식별정보라 칭하였다. 이 식별정보를 이용하여 보유한 앱의 업데이트본이 출시되어 업데이트를 진행하거나 앱을 재설치 할 경우 해당 앱의 고유 ID에 대한 식별정보를 비교하여 앱의 안전성을 검증할 수 있다.

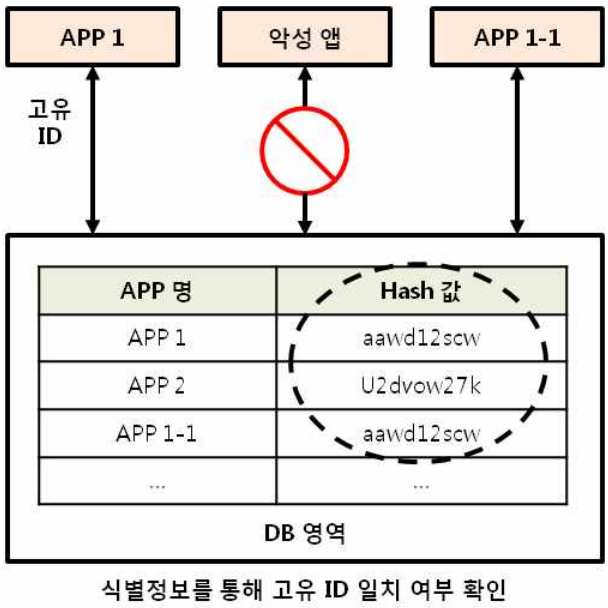

그림 3. 악성 앱 탐지
Fig. 3. Detecting malicious app.

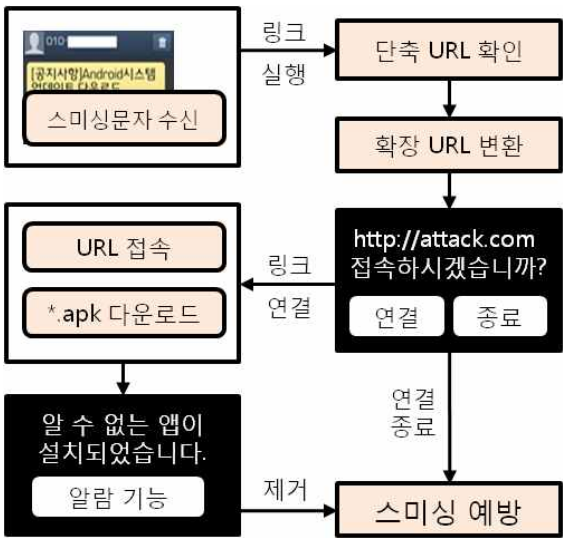

그림 4. 스미싱 대응 흐름도
Fig. 4. Smishing handling process flow.

3-2 악성 URL 탐지 및 차단

SMS를 통해 제공된 URL을 접속하는 것 자체를 줄임으로써 URL 검증 단계에서부터 스미싱 공격을 예방하고자 하였다. SMS를 통해 제공된 URL로의 접속을 시도할 경우 해당 URL의 전체 URL 정보를 사용자에게 알림으로써 사용자는 이를 보고 1차적으로 해당 링크로의 연결을 수행할지 여부를 판단할 수 있다. 만약 해당 URL로 접속을 하더라도 접근한 사이트에서 OO.apk 형태의 패킹된 앱을 다운로드 받는다면 사용자에게 "알 수 없는 앱" 설치가 진행되었다고 다시 한 번 경고를 제공하여 사용자는 자신의 기기에 무엇인가 설치되었음을 인지하고 후속 조치를 진행함으로써 스미싱을 예방할 수 있다.

3-3 스마트 차단 시스템

1) 개요

본 논문에서 제안하고자 하는 스마트 차단 시스템은 악성 URL과 악성 앱을 탐지하고 차단하는 것이 핵심으로, 사용자와의 2회에 걸친 상호작용을 통해 URL 접속과 앱 설치 여부를 확인하여 사용자 실수에 의한 악성 앱 설치를 예방하고자 하였다.

이 시스템은 앱들의 실행 및 변조 상태를 체크하고 서비스를 관리하는 smart protection과 DB 생성 및 관리, SMS 이벤트 수신 및 처리, URL 변환 등의 작업을 수행하는 smart protection service로 구성되어 있다.

2) 동작 원리

본 논문에서 제안하고자 하는 스마트 차단 시스템의 구성은 다음과 같다.

먼저 smart protection에서 변조 위험이 없는 실행 가능 앱의

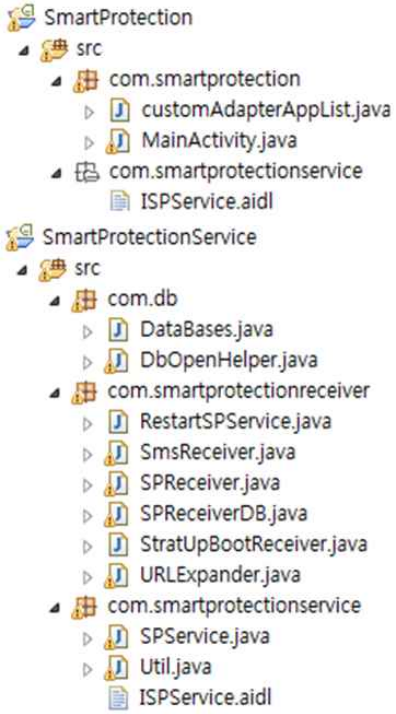

그림 5. Smart protection 구성 상세
Fig. 5. Smart protection detailed composition.

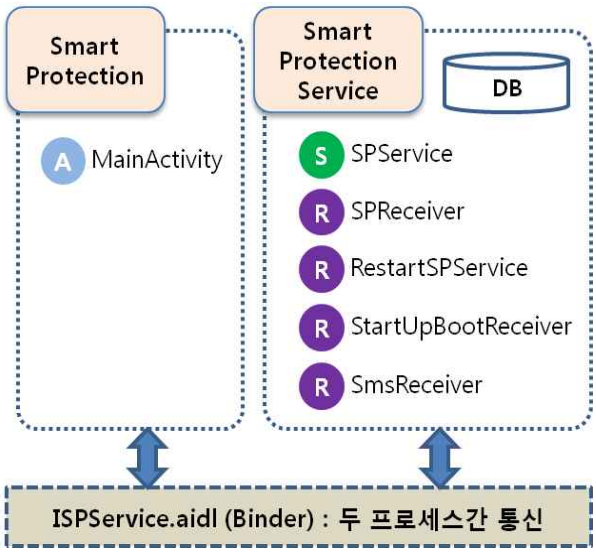

그림 6. 스마트 차단 시스템 구조
Fig. 6. Smart protection & service system architecture.

리스트를 보유하고 있다. 이 때 실행 가능 앱의 리스트는 spservice의 DB에 있는 정보를 참조하여 판단한다. 그 후 smart protection service가 가동되어 서비스가 잘 가동되고 있는지, 어떠한 행위가 이루어지고 있는지, 통신상의 문제는 없는지를 모니터링 한다. 이 smart protection service에는 크게 4가지의 모듈이 존재하며 각 모듈의 기능은 다음과 같다.

첫째, spreceiver는 패키지 앱이 추가(add), 제거(remove), 대

체(replace)되는 경우를 모니터링하고 로그를 생성한다.

둘째, restartspservice는 스마트 차단 시스템의 재기동 역할을 수행한다.

셋째, startppbootreceiver는 기기 가동 시 자동으로 스마트 차단 시스템이 실행되도록 하는 역할을 수행한다.

넷째, smsreceiver는 스미싱 문자를 수신하였을 때 해당 문자의 내용을 추출하여 URL이 있는지를 확인하고 검사하는 기능을 수행한다. 수신한 문자메시지로부터 URL을 검출하였다면 찾아낸 URL을 우리가 흔히 보던 일반적인 URL인 long URL로 변환하여 그 값을 사용자에게 보여준다.

3) 가동 결과

변조 악성 앱 탐지는 기존에 설치되어 있는 앱에 대한 리스트를 DB화하고 각각의 앱의 식별정보를 관리한다. 이후 사용자가 앱을 설치 및 삭제할 때마다 이 정보를 반영하며, 업데이트본이 나왔을 경우 이를 설치할 때 기존 앱의 식별정보와 비교하는 작업을 통해 교체 여부를 판별한다. 만약 기존에 있던 앱과 유사한 변조 악성 앱을 내려 받더라도 기존에 정의한 식별정보를 이용하여 특이사항이 있는 앱인지를 검사할 수 있다.

또한 SMS 내 스미싱 문자 탐지는 스미싱 공격으로 의심되는 SMS를 수신하였을 경우 전송된 URL의 실제 URL을 사용자가 쉽게 파악할 수 있도록 변환한다.

그림 7부터 그림 11은 본 논문에서 제안하는 스마트 차단 시스템의 기능들이 정상 동작하는지에 대한 결과를 보여준다.

```
Receive msg : android.intent.action.ADDED
addPackage ( ) - START
----------------------------------------
[add Package]
- APP Name       : Smart MSC Software
- Package Name : com.msc
- Hash Key       : MbzliaQxyST9XnrJSK94t++rPV4=
- Enable          : y
----------------------------------------
addPackage ( ) - END
Add package - com.msc
```

그림 7. Smart protection 서비스 - 앱 추가
Fig. 7. Smart protection service - app add.

```
Receive msg : android.intent.action.REMOVED
removePackage ( ) - START
----------------------------------------
[remove Package]
- Package Name  : com.msc
- Hash Key         : null
- Hash Key(DB)    : MbzliaQxyST9XnrJSK94t++rPV4=
- Enable           : d
----------------------------------------
removePackage ( ) - END
Remove package - com.msc
```

그림 8. Smart protection 서비스 - 앱 제거
Fig. 8. Smart protection service - app remove.

```
Receive msg : android.intent.action.REPLACED
replacePackage ( ) - START
Replace Package - Same hashKey!
----------------------------------------
[replace Package]
- APP Name       : Smart MSC Software
- Package Name : com.msc
- Hash Key       : MbzliaQxyST9XnrJSK94t++rPV4=
- Hash Key(DB)   : MbzliaQxyST9XnrJSK94t++rPV4=
- Enable          : y
----------------------------------------
replacePackage ( ) - END
Replace package - com.msc
```

그림 9. Smart protection 서비스 - 대체(식별정보 일치)
Fig. 9. Smart protection service - replace(same hash key).

```
Receive msg : android.intent.action.REPLACED
replacePackage ( ) - START
Replace Package - Changed hashKey!
----------------------------------------
[replace Package]
- APP Name       : Helloworld
- Package Name : com.helloworld
- Hash Key       : zSzNUBw13QFIQKq702krXvseuvY=
- Hash Key(DB)   : MbzliaQxyST9XnrJSK94t++rPV4=
- Enable          : d
----------------------------------------
replacePackage ( ) - END
Replace package - com.msc
```

그림 10. Smart protection 서비스 - 대체(식별정보 불일치)
Fig. 10. Smart protection service - replace(different hash key).

```
URL Filter(1 th) : http://goo.gl/Nh3zcx
isDataSchedulerEnabled():false
{"Long-URL":"http:\/\/www.koreatech.ac.kr"}
----------------------------------------
[Notification Information]
- Short URL      : http://goo.gl/Nh3zcx
- Long URL       : http://www.koreatech.ac.kr
- Notification ID : 1
----------------------------------------
- Title :
=> URL이 포함된 SMS
- Message :
=> Short URL : http://goo.gl/Nh3zcx
Long URL : http://www.koreatech.ac.kr
```

그림 11. Smart protection 서비스 - URL 검증
Fig. 11. Smart protection service - URL check and inspection.

3-4 기존 시스템과의 비교

한국인터넷진흥원(KISA)에서는 불법스팸대응센터를 통해 스미싱 주의 안내를 하고 있으므로 이를 활용하여 시중에 나와 있는 스미싱 차단 앱 중 안랩의 안전한문자와 본 논문에서 제안하는 스마트 차단 시스템을 비교하였다[8].

그림 12. 스미싱 문자현황 (KISA)
Fig. 12. Smishing SMS (KISA).

실제 발생한 스미싱 문자를 이용하여 테스트를 수행한 결과 제안한 방법인 스마트 차단 시스템에서는 모든 스미싱 문자를 사용자가 확인하고 의사결정을 할 수 있었던 반면, 안랩의 안전한 문자도 10개의 스미싱 문자 중 6개를 차단할 수 있었다.

특히, 사용자가 의사결정을 하도록 함으로써 스미싱 문자가 아님에도 불구하고 오탐으로 인해 해당 SMS가 차단될 수 있는 상황에도 대응할 수 있으므로 본 논문에서 제안하는 스마트 차단 시스템의 성능이 우수하다고 볼 수 있다.

표 2. 성능 테스트 결과
Table 2. Performance test result.

	스마트 차단	안전한 문자
http://kudnesse.org	○	○
http://mxc.kr/15vi	○	X
http://asd.so/DWd	○	○
http://url.kr/CJSwkl	○	○
http://grep.kr/Q4S	○	○
http://nazr.in/siA	○	○
http://grep.kr/QC6	○	X
http://bit.do/pocda	○	○
homehanex.blogspot.kr	○	X
http://zxy.kr/1ty	○	X

※ ○ : 사용자에게 경고 제공 및 차단 유도
X : 특별한 반응이 나타나지 않음(미탐지)

Ⅳ. 결 론

본 논문에서는 앱을 활용하여 스미싱 공격을 효과적으로 탐지하고 차단할 수 있는 시스템을 구현하고자 하였다. 이를 통해 자신의 스마트 기기를 안전하게 사용할 수 있는 환경을 제공함으로써, 사용자의 실수 혹은 인지조차 못한 상태에서 발생할 수 있는 스미싱 공격의 피해를 낮출 수 있을 것이다.

본 논문에서 검증한 결과를 바탕으로 향후에는 사용자 영역에서 이루어지는 앱 형태의 대응이 아닌, 스마트 기기의 OS 커널 영역과 사용자 영역 사이에 모바일 가상화를 적용함으로써 이를 더욱 발전시킬 수 있도록 추가적으로 연구를 진행하고자 한다.

참고문헌

[1] iCrossing UK Ltd. Infographic: Android pulls in twice as many users as Apple's iOS [Internet]. Available: http://connect.icrossing.co.uk/infographic-android-pulls-in-twice-as-many-users-as-apples-ios_11372.
[2] E. H. Kwon, Policy materials: Electronic finance fraud

damage prevention guide, The National Assembly of The Republic of Korea, Seoul, Korea, Policy materials, 2013.
[3] D. W. Park, Guideline for countermeasures against smishing incident, Telecommunications Technology Association, Seoul, Korea, Technical Report TTAR-12.0017, 2013.
[4] H. J. Lee, "A study on the new types of crime using smart phone and the police counter measurements," *Korean Police Studies Association*, Vol. 11, No. 4, pp. 319-344, 2012.
[5] KISA Bohonara. Getting intelligent smishing malicious app! [Internet]. Available: http://boho.or.kr/upload/file/EpF387.pdf.
[6] S. J. Kim, A study on the detection of phshing sites using a similar domain search, Master dissertation, Sungkyunkwan University Graduate School of Information & Communications, Seoul, Korea, 2013.
[7] I. W. Park and D. W. Park, "A study of intrusion security research and smishing hacking attack on a smartphone," *Journal of the Korea Institute of Information and Communications Engineering*, Vol. 17, No. 11, pp. 2588-2594, 2013.
[8] KISA. Malicious URL info [Internet]. Available: http://spam.kisa.or.kr/kor/smishing/smishingWay.jsp

서 길 원 (Gil-Won Seo)
2005년 8월 : 한국기술교육대학교 인터넷S/W공학 (공학사)
2005년 8월 ~ 2013년 12월 : 삼성SDS(주) CERT
2014년 6월 ~ 현재 : 캐논코리아 비즈니스솔루션(주) 정보보호담당 및 한국기술교육대학교 컴퓨터공학과 공학석사 과정
※관심분야 : 정보보안 기획/운영/관리, 해킹 및 악성코드 분석

문일영(Il-Young Moon)
2000년 2월 : 한국항공대학교 항공통신정보공학과 (공학사)
2002년 2월 : 한국항공대학교 대학원 항공통신정보공학부 (공학석사)
2005년 2월 : 한국항공대학교 대학원 정보통신공학과 졸업 (공학박사)
2004년 ~ 2005년 : 한국정보문화진흥원 선임연구원
2005년 3월 ~ 현재 : 한국기술교육대학교 컴퓨터공학부 부교수
※관심분야 : 무선 인터넷 응용, 무선 인터넷, 모바일 IP