안드로이드 기반 스미싱 방지 시스템 설계 및 구현

장래영* · 배정민* · 정성재** · 성경*** · 소우영*

*한남대학교 컴퓨터공학과, **(주)스컴씨엔에스, ***목원대학교 컴퓨터교육과

Design and Implement of Anti-Smishing System based-on Android

Rae-Young Jang* · Jung-Min Bae* · Sung-Jae Jung** · Kyung Sung*** · Woo-Young Soh*

*Hannam University, **Sky Computing C&S, ***Mokwon University

E-mail : rene402@hnu.kr, bjmin86@nate.com, posein@naver.com, skyys04@mokwon.ac.kr, wsoh@hnu.kr

요 약

최근 안드로이드 기반의 스마트폰을 대상으로 한 해킹기법중 가장 활발한 것은 스미싱(Smishing)이다. 스미싱은 SMS, MMS등 문자메세지를 이용한 새로운 해킹기법으로 사용자에게 악성코드애플리케이션(이하 악성앱)을 다운로드할 수 있는 주소가 포함된 메세지를 보내 개인정보를 수집하거나 스마트폰을 제어하고, 특히 사용자가 알지 못하게 통신사의 소액결제 서비스를 이용하게 하여 최대 30만원에 달하는 소액결제 사기피해를 유발시킨다. 스미싱은 다양한 유형의 문자메세지를 통해 사용자가 피해를 입을 수 밖에 없게 한다. 본 고는 대표적인 스미싱기법과 그 피해형태에 대해 알아보고, 예방법과 근본적인 해결책을 제시하고자 안드로이드용 스미싱방지 시스템을 설계및 구현해보았다.

ABSTRACT

Lastest Smishing is one of the hacking techniques target on the Android smartphone. Smishing using the SMS message is a new hacking techniques. smishing sends a message to the user included trojan address. It collects personal information and to control smartphones. In particular, without the user's knowledge of the retail payment service provider uses the service. It caused damage worth up to 300,000 won. It damage to users through different types of text messages. This paper Smishing typical methods and types are described in damages. This paper are described in damages and type by Smishing. This paper propose preventive and fundamental solution. We designed and implemented a anti-smishing system for android.

키워드

Smishing, Android, Phishing, Trojan, Anti-Virus

Ⅰ. 서 론

휴대폰 산업은 지속적인 발전 성장 단계를 밟아왔다. 우리나라에 스마트폰이 도입된 시기는 불과 3~4년밖에 되지 않았지만 이제 스마트폰이 아닌 휴대폰을 찾아보기가 어려운 정도로 스마트폰은 대명사화 되었다. 최근 구글코리아의 '한국모바일소비자의 이해(Our Mobile Market)'이라는 조사결과에 따르면 우리나라의 스마트폰 보급률은 73%에 달하고 이는 조사대상 43개국중 가장 빠른 성장률을 보이고 있다. 또한, 대상자의 82%가 스마트폰을 매일 이용함으로 답하였고 63%는 외출시 반드시 스마트폰을 소지함이라고 조사되었다. 이제 많은 사람들이 실생활에서 스마트폰을 사용하고 있다고 단정지을 수 있게 되었다. 이런 현상과 함께 단점들도 부각되고 있는데 그 중 하나가 스미싱(Smishing)으로 인한 금전적 피해다. 스미싱은 특히 안드로이드(Android)를 운영체제로 사용하는 스마트폰에서 주로 발생하고 있는데 그 이유는 오픈소스(Open Source)를 지향하고 애플리케이션(Application, 이하 앱)이 별다른 제재없이 마켓에 등록되고 제3의 장소에서도 손쉽게 다운로드와 설치가 가능하기 때문이다. 본 고에서는 스미싱 해킹기법과 피해유형을 알아보고 그에 따른 예방책을 알아본다. 또한, 원천적으로 피해를 방지할 수 있는 애플리케이션을 구현해보았다.

II. 본 론

2.1 스미싱(Smishing)

스미싱은 문자메시지를 뜻하는 SMS(Short Message Service)와 피싱(Phishing)의 합성어로 문자메시지를 이용해 사용자에게 금전적인 피해를 입히는 새로운 사기 수법이다[2]. 일반적으로 사용자의 호기심을 자극하는 문구로 클릭을 유도하거나 지인의 결혼식, 돌잔치같은 경조사 안내 메시지 또는 경찰청, 우체국등 국가기관을 사칭하는 메시지등 일명 사회공학기법을 활용해 사용자들이 자칫 속아 넘어가도록 한다. 스미싱으로 인한 피해는 스마트폰의 보급과 더불어 기하급수적으로 증가하고 있다. 정보공개센터에 따르면 2012년 경찰청에 접수된 스미싱피해는 2100여건, 피해액은 5억6900만원에 달하며 2013년 상반기에는 18000여건, 피해액 35억 3천만원으로 조사되었다[3]. 올해 조사기간은 상반기임을 감안하면 2013년 스미싱에 의한 피해가 얼마나 심각할지 수준을 짐작케하고 있다.

표 1. 국내 스미싱 피해 금액

년도	사건건수	피해액(천원)
2012	2,182	569,000
2013상반기	18,143	3,530,000

스미싱의 피해과정을 살펴보면 다음과 같은 단계로 이루어진다.

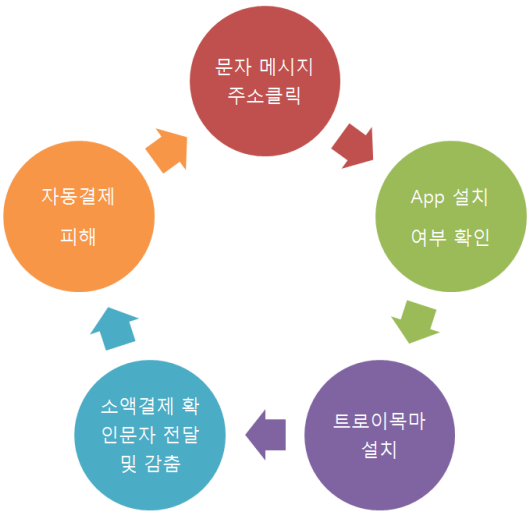

그림 1. 스미싱 피해 유도 과정

1단계 사용자가 문자메시지를 통해 전송된 웹페이지 주소를 클릭했을 경우 감춰져있던 안드로이드 앱 설치파일이 다운로드 되고 2단계 애플리케이션을 설치할지 여부를 묻는 과정을 거치게 된다. 이 단계에서 사용자가 습관적으로 확인버튼을 클릭하는 순간 3단계 트로이목마 프로그램이 사용자의 스마트폰에 설치되게 되고 해커의 서버로 스마트폰의 정보가 전송되어진다. 소액결제서비스에 사용자의 정보를 이용해 결제를 시도하고, 4단계 결제 여부를 묻는 확인 문자가 사용자의 스마트폰으로 전송되지만 이미 잠식된 트로이목마앱이 정상적인 문자메시지를 가로채 다시 해커의 서버로 전송하게 된다. 그 결과 5단계 자동적으로 결제가 되고 결제여부는 사용자가 모르는 상태로 대부분 다음 요금고지서를 통해 알게되어 피해사실을 인지하게 된다.

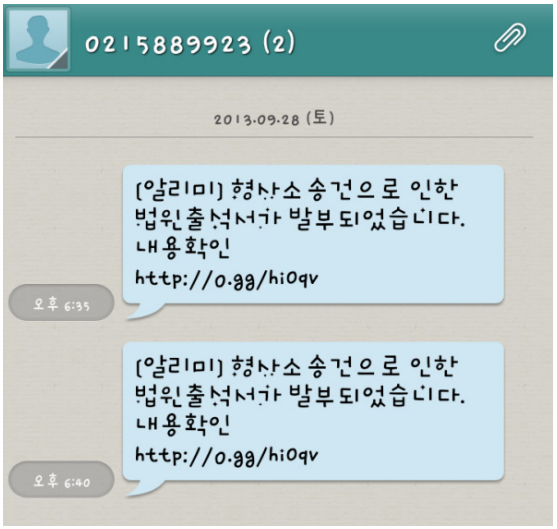

그림 2. 스미싱 시도 문자메시지

III. 예방과 대책

3.1 소액결제범위 축소

가장 대표적인 피해예방법이며 근본적인 방법이라 할 수 있다. 이동통신사의 고객센터를 통해 스마트폰 소액결제 한도를 최소화해놓는 방법이다. 이를 통해 비록 스미싱앱을 설치하였더라도 결제한도가 낮거나 없어 실질적으로 피해가 없게 하는 방법이다. SK텔레콤, KT, LGU+ 모두 고객센터 상담원을 통해 한도를 설정할 수 있고 KT의 경우 온라인홈페이지에 접속해 사용자가 직접 한도를 지정할 수도 있다. 그러나, 정작 소액결제가 필요한 상황에서도 이용을 할 수 없는 불편함이 있다는 단점이 존재한다. 평소 소액결제를 사용하지 않는 패턴이라면 적당한 방법이다.

그림 3. KT의 온라인 소액결제 차단

3.2 기기설정을 통한 예방법

대부분 안드로이드 악성코드는 정상적인 마켓을 통해 유통되지 않기 때문에 이런 경우 설치시 경고메시지와 함께 설치가 되지 않는다. 하지만, 필요에 의해 기기설정에서 그런 과정이 생략되었다면 다시 되돌려 주도록 한다. 기기마다 조금씩 다르지만 일반적으로 환경설정, 보안, 기기관리 순으로 메뉴를 찾아 들어가면 '알 수 없는 소스'에 관련된 설정값이 있다. 알 수 없는 출처의 앱 설치 허용에 체크가 되어있는지 확인후 체크되어 있는 경우 해제하여 준다. 이런 경우 제3의 서버를 통해 배포되는 임의의 악성코드를 설치과정에서 예방할 수 있다. 하지만, 은행권같은 금융관련 앱이나 사내 보안앱같은 경우 마켓을 통해 배포되지 않는 경우도 있어 사용상 주의가 필요하다.

그림 4. 알 수 없는 소스 체크해제

3.3 백신프로그램 설치

최근 스마트폰용 백신프로그램도 다양하게 개발되고 있다. 기존 PC용 백신개발 벤더들의 모바일 진출이 활발하게 진행되어 유명한 PC용 백신들이 많이 모바일용으로 제공되고 있다. 믿을 만한 업체의 백신프로그램을 설치해 사용해주면 완벽하게 스미싱을 차단할 수 없지만 많은 도움을 받을 수 있다. 하지만, 이런 백신프로그램으로 가장한 악성코드도 있기때문에 설치시에 각별한 주의가 필요하다. 보통 안드로이드 마켓의 심사는 애플의 그것만큼 철저하지는 않기때문이다. 백신 설치시 다른 사용자들의 사용기를 참고하여 믿을 만한 프로그램인 확인하여야 피해를 예방할 수 있다.

IV. 구현 애플리케이션

구현한 앱은 스미싱 방지 본연의 기능에 충실하고자 하였다. 안드로이드폰에 문자가 왔을 때 이를 인식하고 제어하기 위해서 브로드캐스트 리시버를 사용하였다. 기본앱은 메모리에 상주하면서 문자메시지가 수신된 경우 발동되게 하였다. 안드로이드는 문자 수신시 android.provider.Telephony.SMS_RECEIVED 를 브로드캐스트한다. 문자 수신을 제어하기 위해 브로드캐스트 리시버에 android.provider.Telephony.SMS_RECEIVED를 인텐트 필터로 등록한다. 이때 인텐트필터에 android.prioriry를 낮은 수를 주어 우선순위를 높인다. 이 경우 안드로이드 기본 SMS앱보다 먼저 수신된 문자를 받아볼 수 있다. 또한 매니페스트 파일에 RECEIVE_SMS로 문자 수신 권한을 동록해 주어야 한다. 문자가 수신되면 intent.getExtra().get 을 통해 문자메시지 정보를 추출하고 createFromPdu API 를 통해 SmsMessage 객체를 얻어 데이터를 분석한다. 이를 통해 웹페이지로 유도하는 문자코드가 있을 경우 스미싱유도로 의심해 this.abortBroadCast(); 를 지정해주어 수신을 원천차단한다. 이 경우 안드로이드 기본 SMS앱뿐만 아니라 다른 SMS을 제어하는 앱에서도 수신을 하지 못하게 되어 사용자로 하여금 설치하게 하는 오류를 방지하게 하고자 하였다.

V. 결 론

스마트폰은 젊은 층의 전유물로 머물고 있지 않다. 전연령층에 걸쳐 대부분 스마트폰을 이용하게 되고 있는 상황이며, 그에 따라 기기에 익숙하지 않은 사용자를 고려해야 하는 것은 당연하다. 현재 스미싱피해는 기하급수적으로 늘어나고 있는 형편이지만 다행히 그에 따른 대비책도 널리 퍼져가고 있다. 본 고를 마무리할 때 즈음 특정 이동통신사는 스미싱피해방지를 위해 자사 통신망(3G/LTE)을 이용해 스미싱의심주소로 접속하려 하는 경우 경고메시지를 보여주기도 하고, 다양한 스미싱방지앱들도 무료로 배포되고 있다. 구

현 방식은 다르더라도 널리 스미싱방지앱들이 보급되어 사용자들의 피해를 줄이기 위해 통신사, 제조사, 보안업체, 개발사들의 관심이 필요하다. 추후 본 연구과제를 확장해 개발서버와 연계해 스미싱의심메시지의 경우 서버정보와 실제 다운로드 되는 파일이 설치파일인지 분석해 오탐의 범위를 줄일 수 있는 기술과 사용자로 하여금 원한다면 접근할 수 있는 선택을 할 수 있는 등 다양한 기법연구를 하고자 한다.

참고문헌

[1] 구글코리아블로그,
http://googlekoreablog.blogspot.kr/
[2] 사이버경찰철,
http://www.police.go.kr/portal/main/contents.do?menuNo=200287
[3] 정보공개센터,
http://www.opengirok.or.kr/3632
[4] 박헌재, 안드로이드를 지배하는 통신프로그래밍, 프리렉, 2011
[5] W. Frank, Android in action, Insight, 2013