안드로이드 환경에서 SMS 피싱 행위 탐지 기능 설계

안성환°, 민재원*, 박민우*, 정태명**
°*성균관대학교 전자전기컴퓨터공학과
**성균관대학교 정보통신대학
e-mail:{shahn, jwmin, mwpark}@imtl.skku.ac.kr°*, tmchung@ece,skku.ac.kr**

Design of SMS Phishing Detection Mechanism in Android Environment

Sung-Hwan Ahn°, Jae-Won Min*, Min-Woo Park*, Tai-Myoung Chung**
°*Dept. Electrical and Computer Engineering, Sungkyunkwan University
**College of Information and Communication Engineering, Sungkyunkwan University

● 요 약 ●

스마트폰 보급은 현대인들에게 시간적, 공간적 제약에서 벗어나 언제 어디서나 무선 인터넷을 사용하여 모바일 뱅킹, 결재, 증권거래 등 원하는 서비스를 이용할 수 있게 해주었다. 사용자들은 이를 이용하여 다양한 정보들을 검색, 저장, 이용한다. 그러나 무선 인터넷의 순기능과는 반대로 최근 모바일 기기의 보안취약점을 이용한 악성애플리케이션 및 각종 공격으로 사용자 개인정보탈취의 위협이 증가하고 있다. 사회공학공격의 일종인 피싱(Phishing)은 신뢰받는 기관을 사칭하여 만들어놓은 가짜사이트에 사용자로부터 자신의 개인정보 및 금융정보를 입력하게끔 유도하여 사용자정보를 탈취하는 방법으로 최근 SMS를 이용하여 정부 및 금융기관을 사칭한 문자를 보내 피싱사이트로 접속을 유도하는 피해사례가 증가하고 있다. 본 논문에서는 국내 피싱사이트의 유형을 분석하고 피싱사이트로 접근을 유도하는 방법 중 하나인 SMS를 이용한 피싱을 방지 할 수 있는 시스템을 고안한다.

키워드: 안드로이드(Android), 피싱(phishing), SMS(Short Message Service), 사회공학공격

I. 서 론

2008년 아이폰의 보급과 함께 스마트폰이 널리 세상에 알려지기 시작했고 그 이후 스마트폰은 누구도 예상하지 못할 정도로 빠른 보급률을 보였다. 스마트폰의 최대 장점인 언제 어디서나 인터넷을 이용하여 간단한 업무를 볼 수 있는 기능은 현대인들의 생활에 많은 변화를 가져왔다. 게임, 일정관리, 금융, 인터넷, 음악, 비디오 등 각종 애플리체이션이 출시되어 생활과 밀접한 연관을 맺고, 이러한 스마트폰 사용의 증가는 무선 인터넷의 사용을 급격하게 증가시켰다[1].

하지만 현대인의 일상생활을 편리하게 해주는 무선 인터넷 사용자의 증가와는 반대로 무선 인터넷상에 입력 및 저장되는 사용자 개인정보를 탈취하려는 목적의 다양한 해킹시도 및 악성애플리케이션도 빠르게 증가하고 있다.

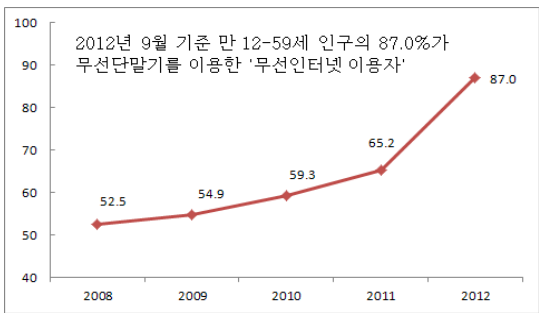

그림 1. 무선 인터넷 이용률 변화 추이

이러한 기법 중 하나인 피싱은 정부 및 금융기관 등 신뢰할 수 있는 기관의 웹 사이트를 사칭하여 무선 인터넷 사용자로 하여금 사용자의 개인정보 즉, 주민번호, 신용카드번호, ID, Password, 보안카드, 정보탈취를 위한 악성앱 설치 등 개인정보 및 금융정보를 탈취하려는 악의적인 목적을 가진 사회공학공격의 일종이다. 피싱사이트는 최근 정부 및 금융기관 등을 사칭하여 스팸메일, SMS, 보이스피싱 등 다양한 방법을 이용하여 피해자의 접속을 유도한다. 본 논문에서는 다양한 피싱사이트 접속 유도 방식 중

SMS를 이용한 방식에 대하여 문자 메시지 및 피싱사이트의 특징을 이용하여 피싱가능성을 실시간으로 분석하여 피싱 공격으로부터 벗어날 수 있는 시스템 구현 방안을 제시한다.

II. 관련 연구

1. 국내 동향

한국인터넷진흥원(KISA)에 따르면 국내 기관을 사칭한 피싱사이트 발견 건수가 2006년~2010년까지 총 20건에 불과하였으나 2011년에는 1,849건, 2012년 1분기에만 1,218건으로 폭발적으로 증가하는 추세를 보이고 있다. 사칭하는 기관으로는 검찰·경찰 등 사법기관에서부터 최근에는 금융감독원, 시중은행 등 금융기관까지 그 범위를 넓혀가고 있다[2].

표 1. 국내 피싱사고 발생 현황 (단위: 건)

구분	06	07	08	09	10	11	12'1
건수	4	2	2	4	8	1849	1218

초기 피싱사이트 접속 유도 방식은 피해자에게 직접 전화를 걸어 보이스피싱을 통해 피싱사이트로 접속을 유도하여 피해자가 개인정보 및 금융정보를 입력하도록 하는 방식을 사용하였으나 최근에는 은행과 같은 금융기관의 홈페이지와 유사하게 피싱사이트를 구축한 이후 불특정 다수에게 '보안승급', '보안강화', '보안프로그램 무료배포' 등의 문구를 삽입한 SMS를 보내 해당 사이트로 접속을 유도하여 개인정보 및 금융정보를 탈취하는 방식이 급증하고 있다[3].

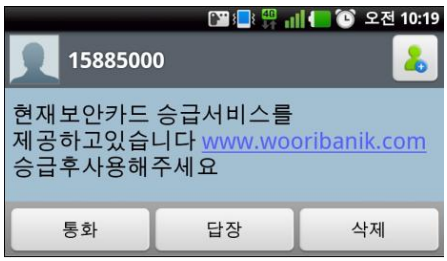

그림 2. 피싱사이트 접속 유도 SMS의 예

2. 국내 피싱사이트의 구축 방식

국내 피싱사이트의 대표적인 구축 방식은 다음과 같다.

- 이미지 방식

신뢰할 수 있는 기관 및 금융회사의 홈페이지를 캡쳐한 이미지 위에 링크를 추가 하는 방식

- IFRAME 태그방식

IFRAME 태그를 통해 정상적인 링크들 사이에 피싱페이지가 링크된 부분을 추가

- 정상사이트 복사 방식

정상사이트의 소스를 복사하여 모든 메뉴 및 게시글의 링크를 피싱페이지로 설정한 외관상 정상사이트와 가장 흡사한 모습을 가짐

- 팝업 방식

1차 페이지에 정상사이트의 링크와 신뢰할 수 있는 기관의 링크로 위장한 팝업페이지 링크를 함께 놓아 사용자에게 개인정보 및 금융정보 입력을 유도

- 악성앱 다운로드 링크 방식

스마트폰 사용자를 노려 신뢰기관은 사칭하여 악성앱을 다운로드 받게 하는 형식

위 5가지 방법 이외에도 최근 자동화 툴로 자동으로 피싱 사이트를 만드는 방법도 알려져 피싱사이트 및 피싱으로 인한 피해가 지속적으로 증가할 것으로 예상된다[3][4].

3. 기존 피싱사이트 탐지 방안

금융보안연구원에 보고된 금융보안 리포트에 의하면 기존 피싱사이트 탐지를 위한 방안은 3가지가 있다.

첫 번째 수집된 피싱사이트에 대해 DB로 구축하여 블랙리스트 기반으로 탐지하는 방법이다. 이 방법은 오탐율이 낮고 구현이 쉬운 반면, 새롭게 발견되는 피싱사이트를 탐지할 수 없다는 문제가 있다.

이를 극복하기 위한 두 번째 방법은 유사도메인을 통한 탐지로 도메인에 일정한 패턴이 존재하는 경우 키워드, 패턴 검색 등을 활용하여 피싱사이트 유무를 판별하는 방법이다. 유사도메인 탐지 방식은 오탐율이 적고 피싱사이트 서비스 초기에 발견 할 수 있는 장점이 있으나 유사도메인을 사용하지 않는 도메인의 경우는 탐지하기 어렵다.

마지막으로 HTTP 트래픽 분석을 통한 탐지 방법으로 피셔(Phisher)가 피싱사이트를 구축할 때 정교하게 꾸미기 위하여 정상사이트(원시사이트) 정보를 정상사이트 웹 서버에 요청할 때 유입되는 링크 요청 내의 HTTP Referer 헤더 값에 피싱사이트 URL, IP 정보가 남게 되는 것을 이용하여 탐지하는 방식이다. 이 방법은 정상사이트 정보를 링크하는 피싱사이트에 대해 100%탐지할 수 있고 피싱사이트 피해가 구체화 되기 전 파악이 가능하지만, 정상사이트의 링크를 포함하지 않는 경우는 탐지가 불가능하다[3][4].

III. 본 론

앞서 살펴본 바와 같이 다양한 피싱사이트 탐지 방법은 인터넷진흥원등 관계기관에서 피싱사이트를 인지하고 해당 사이트를 차단하는 형태로 스마트폰 사용자에게 피싱사이트로 접근을 유도하는 SMS 수신 시점에는 해당 문자가 피싱을 유도하는 것인지 판단할 수 없다. 따라서 관계기관이 피싱사이트를 인지하고 차단하는 시스템 외에 사용자가 능동적으로 피싱사이트임을 파악하고 이를 회피할 수 있는 시스템이 필요하다.

본 논문에서 제안하는 시스템은 국내 스마트폰 사용자가 가장 많이 사용하는 모바일OS인 구글의 안드로이드 플랫폼을 기반으로 한다.

스마트폰에 수신되는 SMS를 분석해 피싱 위협을 방지하는 시스템을 구성하기 위해 안드로이드 플랫폼에서 이벤트를 처리하기 위한 브로드캐스트 리시버를 이용한다. 브로드캐스트 리시버는 브로드캐스트 된 인텐트를 기다리는 애플리케이션의 요소이며, 시스템은 인텐트를 기다리고 있는 모든 브로드캐스트 리시버에게 이벤트를 전달하고 리시버는 순서대로 인텐트를 처리한다. 브로드캐스트 리시버가 대기할 수 있는 인텐트는 전화, 문자수신, 사진 촬영, 배터리상태, SD카드삽입 등이다[5]. 기본적으로 브로드캐스트 리시버는 어떠한 동작도 하지 않지만 필요한 경우 백그라운드에서 원하는 이벤트를 핸들링할 수 있으며, 동작이 오래 걸릴 경우(통상 10초가 지나면 브로드 캐스트 리시버는 시스템에서 강제 종료 된다. 따라서, 수행시간이 짧은 간단한 역할을 수행) 서비스를 시작하는 형태로 다양한 역할을 수행할 수 있다.

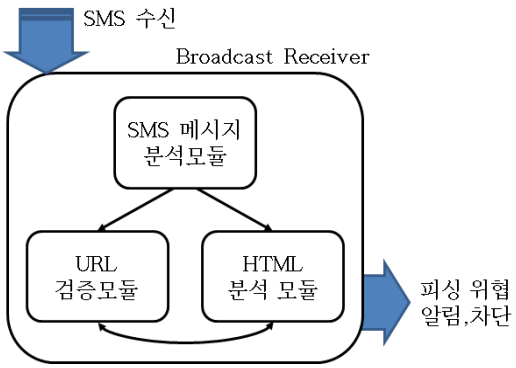

그림 3. SMS 후킹 기반 피싱 차단 시스템

[그림 3]의 시스템은 3개의 모듈로 구성되어있으며 SMS가 수신되어 브로드캐스트 리시버가 동작하면 SMS메시지 분석 모듈로 해당 이벤트의 내용을 전달하여 SMS를 분석하는 역할을 담당한다. 이 모듈은 메시지 발신지, 메시지 내용 (URL, 특정 문자열 삽입) 등을 분석하여 URL과 특정 문자열이 존재하지 않을 경우 일반적인 SMS 수신절차로 전달하고, 기관명과 URL이 삽입되어있는 경우 URL검증 모듈로 전달한다. URL검증 모듈에서는 실제 기관(기업)명 URL과 메시지에 삽입되어있는 URL을 비교하여 피싱사이트임을 판별한다. 마지막으로 HTML 분석 모듈은 수신된 메시지에 기관명이 없고 URL만 삽입되어있는 경우 해당 URL의 웹페이지를 분석하여 피싱사이트일 가능성을 판단한다. 국내 피싱사이트 제작 유형과 별도로 정보탈취 및 악성애플리케이션을 다운받도록 유도하기 위한 특성은 [표 2]와 같다.

표 2. 국내 피싱사이트의 특성

① 사용자의 신뢰를 얻기 위해 웹페이지 타이틀에 기관명 삽입
② 금융정보 탈취를 위한 정보를 수집하기 위해 입력을 위한 텍스트 박스가 과도하게 많음 (예: 보안카드 번호 35개)
③ IFRAME 태그 및 이미지에 정상사이트 URL 참조
④ 최초 URL 접속 시 다운로드를 위한 페이지로 Re-Direction
⑤ 웹페이지 내에 활성화 버튼이 1개 존재

HTML 페이지 분석으로부터 기관명 및 정상사이트 참조 등으로 URL 인한 정보를 추출하게 될 경우 URL검증 모듈로 전달하여 이를 확인하고, 정상사이트에 대한 URL정보를 찾을 수 없을 때에는 페이지 분석을 통해 피싱사이트일 가능성을 판단한다. 세 개의 분석 및 검증 모듈로부터 결과가 정상적인 웹페이지로 판단된 경우 특정한 동작 없이 종료하고, 그렇지 않은 경우 피싱사이트일 가능성이 있음을 알리는 알람을 띄워 사용자가 피싱 공격의 위협으로부터 벗어날 수 있게 하여, 사용자의 개인정보를 안전하게 지킬 수 있다.

Ⅳ. 결 론

최근 피싱사이트는 유사도메인, 보이스피싱 등과 같은 다양한 사회공학 기법과 융합하며 그 방식이 날로 지능적이며 교묘해지고 사용자가 인지하기 어렵도록 진화하고 있다. 또한, 피싱사이트 자동화 툴의 등장과 피싱사이트 거래가 암암리에 이루어지는 등 피싱사이트가 폭발적으로 증가하고 있어 적절한 대응을 하지 않을 시 시간이 지날수록 그 피해규모가 커질 것으로 예상된다. 한국인터넷진흥원(KISA) 및 관계기관에서 피싱 피해를 막기 위해 방지 및 탐지 방법, 신고사이트를 만들었으나 일반 사용자들에게 널리 알려지지 않아 뚜렷한 효과를 보이고 있진 않다. 본 논문에서 제안하는 시스템은 안드로이드 플랫폼 스마트폰 사용자에게 SMS 수신 즉시 메시지 내용 및 웹페이지를 분석하여 피싱사이트 가능성을 판단하고 이를 통해 피싱 공격의 위협이 있음을 알리고 회피할 수 있도록 도와준다. 그 결과 사용자가 피싱에 대해 능동적으로 대처할 수 있으며 나아가 한국인터넷진흥원(KISA) 및 관계기관에서 구축해놓은 기존 시스템인 유사도메인 검색 시스템, 피싱사이트 신고 기능, 트래픽 모니터링 시스템에서 분석한 결과 DB 등과 연동하여 사용할 경우 더욱 효율적으로 피싱 공격을 방지 할 수 있을 것으로 예상된다.

참고문헌

[1] Korea Internet & Security Agency (KISA), “2012 Survey on the Wireless Internet Usage”, Dec. 2012.

[2] Korea Internet & Security Agency (KISA), “Phishing Activity Trends Report”, Press report data, Apr. 2012.

[3] J. H. Sa, Financial Security Agency, Issue Report, vol.

2011-020, Nov. 2011.
[4] Young ho Sim, Financial Security Agency, Issue Report, vol. 2012-06, Aug. 2012.
[5] S. H. Kim, “Android Programming Complete Guide”, Banbit Media, pp.1129-1152, 2010.