스미싱을 이용한 안전결제(ISP) 해킹 공격 연구

박인우, 박대우*

호서대학교 벤처전문대학원

Study of Hacking Attacks Secure Payment(ISP) with Smishing

In-Woo Park, Dea-Woo Park*

Hoseo Graduate School of Venture

E-mail : cowboyiw@daum.net, prof_pdw@naver.com

요 약

안전결제는 국내 최초의 PKI기반 전자서명방식을 적용한 신용카드 인터넷 결제서비스로 해킹 피해가 해마다 증가하여 2012년도에는 1억 8천만 원 이었다. 2013년도 들어 스마트폰을 이용한 스미싱(Smishing)이라는 피싱수법으로 인하여 피해가 급증하고 있다. 스미싱을 이용한 안전결제 시스템에 대한 해킹사고가 직접적인 금전적 피해와 개인정보 탈취를 야기하고 있다. 본 논문에서는 스미싱에 대해 분석하고 안전결제에 대한 해킹 공격을 연구하여 스미싱을 이용한 안전결제의 피해를 예방한다. 더불어 스마트폰을 통해 보다 안전하고 편리하게 온라인 결제를 할 수 있도록 하는 연구가 될 것이다.

ABSTRACT

Hacking damage is increasing year by year in the Internet payment service credit card applying the digital signature method of PKI-based first domestic, secure payment, was 180 million won in 2012. Revenues have soared for phishing that Smishing using smartphone after entering 2013. Hacking accident to the secure payment system using Smishing has occurred took over personal information and financial direct damage. In this paper, we analyzed for Smishing, to prevent the damage of secure payment using Smishing to study the hacking attack of secure payment. In addition, it would be studies to allow through the smartphone, online payment safer and more convenient.

키워드

스미싱, 안전결제(ISP), 해킹 공격,

Key word

Smishing, Secure Payment(ISP), Hacking Attack, Phishing.

Ⅰ. 서 론

작년인 2012년까지 안전결제의 해킹 피해가 해마다 증가하여 1억 8천만 원이었다. 스마트폰의 급격한 보급과 함께 컴퓨터 해킹뿐만 아니라, 스마트폰 해킹 해킹으로 인해 안전결제 피해 사례가 점차 늘어나고 있다[1].

더불어 최근인 2013년 시장조사업체 IDC가 발표한 자료에 따르면 전세계 PC 출하량이 지난해보다 상당히 줄어들었다고 한다[2]. 이것은 스마트폰과 태블릿 보급이 확산되면서 사람들이 PC보다 스마트폰을 더 많이 사용하기 시작한다는 신호로 PC 전성시대가 가고 스마트폰 전성시대가 오고 있음을 의미한다.

이와 같이 급증하는 스마트폰 사용자들을 겨냥한 스미싱을 이용한 안전결제 해킹공격으로 인한 피해사례가 점점 늘어나고 있으며, 특히 개인정보보호법 시행에 따른 개인정보의 보호를 위해서 스미싱을 이용한 안전결제 해킹공격을 분석 및 연구가 필요하다.

본 논문에서는 보안강화를 위해 시행되고 있는 스미싱을 이용한 안전결제 해킹공격을 연구한다.

Ⅱ. 관련연구

2.1 스미싱

스미싱(Smishing)은 2013년도 들어 새롭게 등장하였으며, 단문자서비스(SMS)와 피싱의 합성어로, 스마트폰을 이용하여 피싱 사기를 유도하고, 그림 1과 같이 스마트폰상으로 개인정보를 빼낼 수 있는 신종 사기 수법이다[3].

휴대폰 또는 PC로 웹사이트에 접속한 피해자는 바이러스 퇴치를 위한 애플리케이션을 무료로 다운받을 것을 권고받게 되나, 이 파일에는 트로이목마 바이러스가 포함되어, 다운로드 즉시 해커의 조종으로 개인정보가 유출되어 버린다.

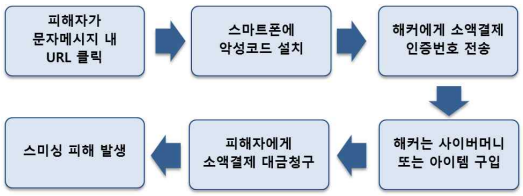


그림 1 '스미싱' 피해 단계

2.2 해킹공격 사례

스마트폰사용이 늘어남에 따라 스마트폰 해킹의 위협 또한 갈수록 커지고 있다[4].

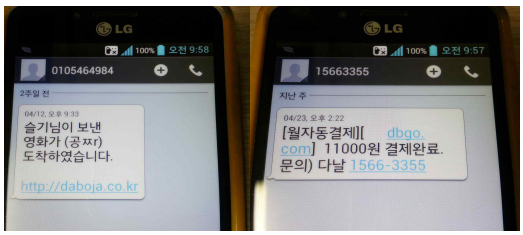


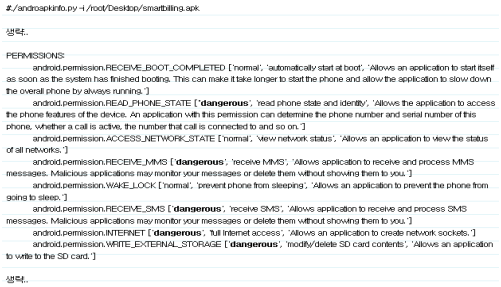
그림 2 호기심 자극하는 스미싱 해킹공격 사례

스미싱에 악용되는 해킹공격 사례는 다양하다. 대표적인 것이 그림 2와 같이 SMS로 호기심을 자극할만한 문구를 쓴 뒤 악성코드가 숨겨진 인터넷 URL을 함께 보내오는 경우이다.

Ⅲ. 스미싱 이용한 안전결제 해킹공격 분석

3.1 스미싱 이용한 안전결제 해킹공격 분석

스미싱 공격은 문자 매세지 내 인터넷 주소를 클릭하게끔 하여 악성코드를 자동 설치하고, 해커에게 소액 결제 인증번호를 전송함으로써 해커가 게임 아이템 및 사이버머니를 결제할 수 있다. 그로 인해 소액 결제 대금이 청구되는 것이다. 그림 3은 androapkinfo.py를 이용하여 smishing.apk의 API권한을 살펴본 모습이다.



```
#./androapkinfo.py -i /root/Desktop/smartbilling.apk

생략..

PERMISSIONS:
        android.permission.RECEIVE_BOOT_COMPLETED ['normal', 'automatically start at boot', 'Allows an application to start itself as soon as the system has finished booting. This can make it take longer to start the phone and allow the application to slow down the overall phone by always running.']
        android.permission.READ_PHONE_STATE ['dangerous', 'read phone state and identity', 'Allows the application to access the phone features of the device. An application with this permission can determine the phone number and serial number of this phone, whether a call is active, the number that call is connected to and so on.']
        android.permission.ACCESS_NETWORK_STATE ['normal', 'view network status', 'Allows an application to view the status of all networks.']
        android.permission.RECEIVE_MMS ['dangerous', 'receive MMS', 'Allows application to receive and process MMS messages. Malicious applications may monitor your messages or delete them without showing them to you.']
        android.permission.WAKE_LOCK ['normal', 'prevent phone from sleeping', 'Allows an application to prevent the phone from going to sleep.']
        android.permission.RECEIVE_SMS ['dangerous', 'receive SMS', 'Allows application to receive and process SMS messages. Malicious applications may monitor your messages or delete them without showing them to you.']
        android.permission.INTERNET ['dangerous', 'full Internet access', 'Allows an application to create network sockets.']
        android.permission.WRITE_EXTERNAL_STORAGE ['dangerous', 'modify/delete SD card contents', 'Allows an application to write to the SD card.']

생략..
```

그림 3 Smishing.apk의 API권한의 소스

androapkinfo.py에서 확인한 API권한 정보를 보면 알 수 있듯이, android.permission.INTERNET, android.permission.Receive_MMS, android.permission.RECEIVE_SMS, android.permission.READ_PHONE_STATE, android.permission.WRITE_EXTERNAL_STORAGE API 권한이 악의적으로 사용될 수 있는 API이다. 즉 APP이 SMS/MMS를 조작할 수 있는 권한, APP이 인터넷에 액세스할 수 있는 권한, APP이 개인 정보에 액세스할 수 있는 권한이다[5].

3.2 스미싱 공격 피해 분석

해커가 스미싱 공격을 위해 사용자에게 보낸 SMS를 통하여 설치한 악성 앱을 실행시키면 그림 4와 같이 "점검시간입니다. 불편을 드려서 죄송합니다"라는 문구로 가장하여 사용자를 안심시키고 실제로는 악성코드가 설치되어 SMS 탈취 서비스가 동작하고 있다[6].

그림 4 SMS를 통한 악성 앱 설치 후 실행 화면

해당 악성앱을 설치를 하게 되면 그림 5와 같이 빨간색 표시된 URL로 스마트폰 사용자의 전화번호를 해커의 서버로 전달을 한다.

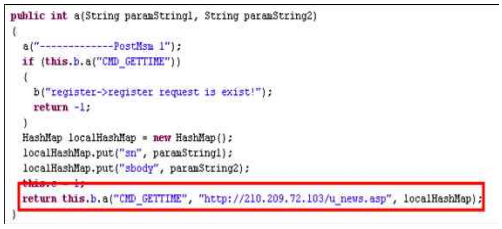


그림 5 해커에게 전달되는 모습

또한 그림 6과 같이 와이어샤크를 통하여 해커의 서버로 스마트폰 사용자의 전화번호를 전송하는 것을 확인할 수 있다.

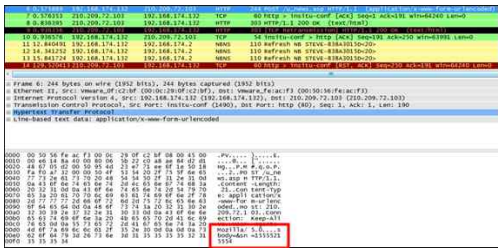


그림 6 와이어샤크로 확인된 모습

Ⅳ. 스미싱을 이용한 안전결제 보안대책

4.1 통신사 측 보안대책

해커에게 스미싱 공격을 당했더라도 각 통신사 고객센터 또는 통신사 인터넷 홈페이지를 이용하여 휴대폰 소액결제를 원천적으로 차단을 하면 방지할 수 있다[7]. 표 1은 3사 통신사들의 안전결제 차단 방안을 나타낸다.

[표 1] 3사 통신사의 안전결제 차단 방안

통신사	KT	SKT	LGU+
고객센터를 통한 소액결제 차단 방법	[1] 114을 눌러 '5'번, 그리고 '1'번을 순차적으로 눌러 KT 모바일 고객센터로 연결 -> [2] 상담원과 통화하여 오프라인결제 • 무선결제 • 청구대행 • 본인인증차단 등을 선택적으로 신청하여 소액결제 차단 -> 완료.	[1] 자신의 스마트폰으로 114로 통화버튼을 눌러 SKT고객센터로 연결 -> [2] '3'번을 눌러 상담원과 연결 -> [3] 소액결제 모두 차단 -> 완료.	[1] 자신의 스마트폰으로 114를 눌러 전화를 하면 LGU+ 고객센터로 연결 -> [2] '0'번을 눌러 상담원과 연결 -> [3] 자동결제 • 인증결제 모두 차단 -> 완료.

4.2 정부 측 보안대책

1) 법제도 개선 대책

- 명시적 동의자에게만 통신과금서비스 제공
- 운영규정 마련을 통한 이용자 보호 수준 제고
- 통신과금 이용 세부사항 명시를 위한 약관 개선

2) 자율규제 및 모니터링 강화

- 통신과금서비스 제공자의 자율 안전조치 강화
- 스팸 모니터링과 연계하여 악성코드 배포 방지
- 통신과금 위해요소 공동대응 체계 구축
- 통신과금서비스에 대한 이용자 이해 증진

3) 공동 대응 체계 구축 및 홍보 강화

- 통신과금 위해요소 공동대응 체계 구축
- 통신과금서비스에 대한 이용자 이해 증진

이번 보안대책의 시행을 통해, 통신과금서비스 시장의 건전한 성장기반을 구축하고 이용자 보호 수준을 한층 높일 수 있을 것0이라 본다[8].

4.3 스마트폰 사용자 측 보안대책

스마트폰 사용자들은 기본 설치되어 있는 모바일 백신 앱은 정기적으로 업데이트는 필수적으로 해야 하고 발신처가 명확하지 않은 곳으로부터 전달되는 SMS의 인터넷 주소는 되도록 클릭하지 않는다, 그림 7과 같이 구글 플레이나 이동통신사 앱 장터에서 스미싱 해킹 무료방지라는 S-GUARD라는 앱을 다운받아 예방하는 것이 좋다.

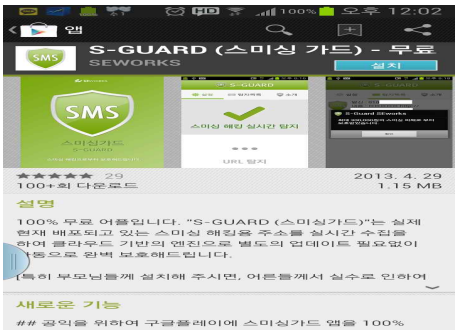


그림 7 S-GUARD 앱의 모습

이 앱 같은 경우는 실시간으로 스미싱 해킹용 주소를 실시간 수집을 하여 클라우드 기반의 엔진으로 별도의 업데이트 필요없이 자동으로 예방해준다.

또 다른 방법으로는, 그림 8과 같이 확인되지 않은 앱이 스마트폰에 설치 되지 않도록 스마트폰의 보안설정을 강화하는 방법이다.

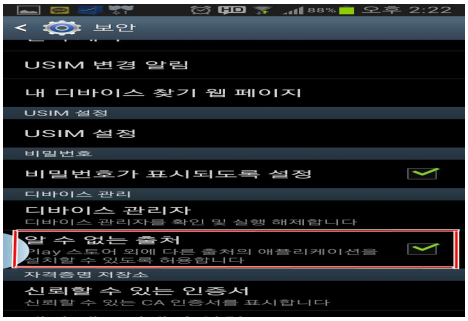


그림 8 스마트폰의 보안 설정 강화 화면

① 환경설정 -> ② 보안 -> ③ 디바이스 관리 -> ④ 알 수 없는 출처에 체크가 되어 있을 경우 해제를 하면 된다.

이와 같은 방법으로 스마트폰 사용자들은 스미싱 해킹공격으로부터 예방할 수 있다.

V. 결 론

스미싱 해킹공격에 대한 스마트폰 사용자들의 피해사례가 급증하고 있고, 안전결제 시스템에 대한 해킹사고가 직접적인 금전적 피해와 개인정보 탈취를 야기하고 있다. 이에 대비하기 위해 스미싱을 이용한 안전결제 시스템의 해킹 공격을 조사 및 연구 그리고 분석 하였다.

향후 연구에서는 스마트폰에서 스미싱 및 URL 탐지 기능이 강화 되는 연구와 아직 특별한 보안조치가 없는 QR코드를 악용해 이루어질 수 있는 해킹공격 연구를 하여야 할 것이다.

참고문헌

[1] 한국경제, "안전결제 해킹 '충격', 피해액 1억 8천…게임사이트 정보 도용", http://www.hankyung.com/news/app/newsview.php?aid=201212042411x&ltype=&nid=&sid=010610&page=1&rss=r, 2013년.

[2] TATTER&MEDIA, "급증하는 스미싱 피해, 올바른 대처 방법은?“ http://logfile.tistory.com/1340?_best_tistory=trackback_bestpost, 2013년.

[3] 경찰청 사이버 테러대응센터, “스미싱의 대처방법”, http://www.netan.go.kr/, 2013년.

[4] 박대우, 서정만, 'Phishing, Vishing, SMiShing 공격에서 공인인증을 통한 정보침해 방지 연구', Vol 12, No 2, pp. 171-180, 2007년.

[5] TickTalk, '아웃백 소액 결제 사기(스미싱)에 사용된 smartbiling.apk 분석', http://darksoulstory.tistory.com/210, 2013년

[6] '4월호 보안 뉴스레터', 2013년.

[7] http://www.symantec.com/norton/. 2013년.

[8] KISA, '인터넷 침해사고 동향 및 분석월보', 2013년, 3월.