# 안전한 금융 서비스를 제공하기 위한 스마트폰 보안에 관한 연구+

강수영*, 이기정**, 박종혁**
*안철구연구소, **서울과학기술대학교
e-mail: bbang814@ahnlab.com, kaksy78@naver.com, jhpark1@snut.ac.kr

# A Study on Smart Phone Security to Provide Secure Finance Services

Soo-Young Kang*, Ki Jung Yi**, Jong Hyuk Park**
*AhnLab. Inc. and **Seoul National University of Science and Technology

요 약

스마트폰은 자체 메모리 및 연산량이 PC보다 훨씬 낮고 빠른 속도의 서비스를 제공해야 하기 때문에 보안에 대한 기술 구현이 부족한 상태이다. 또한 악의적인 공격 기술이 점차 발전하고 있고 새로운 해킹 기술이 급증하고 있어 보안 대책이 필요한 실정이다. 또한 금융 분야와 같이 사용자의 자산에 위협을 줄 수 있는 분야에서는 특히 보안 대책이 반드시 강구되어야 한다. 따라서 본 논문에서는 스마트폰을 이용한 금융 서비스 환경에서 발생할 수 있는 보안 위협에 대하여 알아보고 이를 대응할 수 있는 보안 기술에 대한 방안을 제안하고자 한다.

## 1. 서론

IT(Information Technology) 기술이 발전함에 따라 사용자들은 이동 시 서비스 제공에 대한 요구가 증대하게 되었으며, 이를 충족시키기 위하여 서비스를 제공 받기 위한 단말기가 급속도로 발달하게 되었다. 또한 IT 기술 발전은 네트워크의 고도화 및 대역폭을 확대하고 범용 OS(Operating System)의 고도화를 통한 단말기 사용 진입 장벽을 낮게 만들었다. 이러한 환경에서 사용자를 만족시키고 다양한 서비스를 제공하기 위하여 가장 적합한 단말기로 휴대폰이 선택되었으며, 휴대폰은 통화 및 문자 서비스뿐만 아니라 PC(Personal Computer)와 같은 기능을 제공하는 스마트폰으로 재탄생하게 되었다. 스마트폰은 최근 가장 이슈가 되고 있기 때문에 많은 표현으로 정의되고 있으나, 표준 정의는 되어 있지 않지만 PC와 같은 기능과 다양한 고급 기능을 제공하는 휴대전화로 사용자에게 응용 프로그램 개발자를 위한 표준화된 인터페이스와 플랫폼을 제공하는 완전한 OS 소프트웨어를 실행하는 단말기이다. 또한 인터넷 뱅킹, 메일, 인터넷, 전자책, 내장형 키보드나 외장 USB(Universal Serial Bus) 키보드, VGA 단자를 갖춘 고급 기능을 제공할 수 있는 소형 컴퓨터라 볼 수 있다.

스마트폰은 기능만 다양한 것이 아니라 하드웨어에 탑재되는 OS도 다양하게 개발 및 사용되고 있다. 심비안은 1980년에 개발된 OS로 단말기와 스마트폰을 위한 오픈소스 기반의 운영체제로 현재 실제 시장 점유율 중 가장 큰 비중을 차지하고 있는 운영체제이다. RIM(Research In Motion)에서 개발된 블랙베리는 2002년 개발된 운영체제로 멀티태스킹이 가능하며 자바 및 타 시스템과의 연동 및 호환이 자유롭다는 장점을 가지고 있다. 애플에서 개발된 아이폰 운영체제는 가장 개방되지 않은 운영체제로 다양한 어플리케이션을 동작할 수 있도록 지원되고 있으며, 사용자의 요구에 따라 어플리케이션을 개발하여 사용할 수 있도록 마켓을 형성하고 있다. 마이크로소프트에서 개발된 위도우 모바일은 아이폰 운영체제나 안드로이드가 나오기 전까지 보편적으로 사용되고 있는 운영체제로 사용자 요구에 충족할만한 속도 및 기능을 지원하지 못하여 사용량이 점차 줄고 있는 운영체제 이다. 구글에서 개발된 안드로이드는 개방형 플랫폼으로 사용자들이 필요한 서비스를 제공받기 위한 어플리케이션을 직접 개발하여 사용할 수 있도록 지원하고 있으나, 개방형 플랫폼이기 때문에 다양한 위협에 노출되어 있다.

하지만 운영체제가 다양화되고 있지만 이에 따른 보안 기술이 부족하고 스마트폰 해킹 기술이 발전하고 있어 많은 위협에 노출되어 있다. 특히 금융 분야와 같이 사용자의 자산과 직결되어 있는 분야와 사용자의 개인 정보가 요구되는 분야는 사용자의 자산 피해와 프라이버시 침해에 대한 문제가 발생하여 이에 대응할 수 있는 보안 대책이 반드시 강구되어야 한다.

+"본 연구는 지식경제부 및 정보통신산업진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음" (NIPA-2010-C1090-1031-0004)

## 2. 스마트폰 금융 서비스 보안 위협

스마트폰은 유연한 서비스 제공을 목표로 하여 개발된 디바이스로 보안에 대해 미흡한 연구가 진행되었다. 따라서 금융 서비스를 제공받는 환경에서 안전한 스마트폰을 사용에 다양한 위협이 발생하고 있다.

스마트폰은 기존 휴대폰과 다르게 오픈마켓을 통한 서비스의 다양성을 제공하기 때문에 오픈마켓에서 검증되지 않은 애플리케이션을 통해 위협을 받을 수 있으며, 아직 스마트폰용 백신이 활발히 적용되고 있지 않아 무방비 상태로 노출되어 있는 실정이며, 스마트폰을 이용한 보안 위협은 다음 <표 1>과 같다.

<표 1> 스마트폰 보안 위협

| | 스마트폰 보안 위협 |
|---|---|
| 1 | 악성코드 감염으로 인한 다양한 복합 보안 위협 |
| 2 | 기기 오동작 및 파괴로 인한 사용 불가의 보안 위협 |
| 3 | 분실, 도난 및 악성코드 감염에 따른 정보 유출 및 프라이버시 침해의 보안 위협 |
| 4 | 불법 과금, 도청, 스팸 발송, 피싱 등 사용자가 원하지 않는 보안 위협 |
| 5 | 불법 위치 추적으로 인한 프라이버시 침해 보안 위협 |
| 6 | 금융 서비스 위협 및 서비스 거부 공격을 통한 사용자 자산 침해 보안 위협 |

## 3. 스마트폰 금융 서비스 보안 대책

위와 같이 스마트폰 보안 위협 요소들이 발생하며, 스마트폰 보편화의 걸림돌이 되고 있다. 특히 스마트폰을 분실했을 경우 발생하는 개인 정보 노출, 프라이버시 침해 문제는 심각한 수준이다. 또한 최근 스마트폰에서 폰뱅킹과 인터넷 뱅킹 해킹 문제가 실질적으로 발생하여 앞으로 스마트폰에 대한 보안 위협이 점차 다양해질 것으로 예상되고 있다. 따라서 이러한 문제들을 개선하고 스마트폰 보안 문제가 발생하지 않도록 예방하기 위해서는 다음과 같이 스마트폰 보안 수칙을 준수해야 한다.

1. 애플리케이션을 설치하거나 이상한 파일을 다운로드한 경우에는 반드시 악성코드 검사를 한다.
2. 게임 등 애플리케이션을 다운로드할 때는 신중하게 다른 사람이 올린 평판 정보를 먼저 확인한다.
3. 브라우저나 애플리케이션으로 인터넷에 연결 시 이메일이나 문자 메시지에 있는 URL은 신중하게 클릭한다.
4. PC로부터 파일을 전송 받을 경우 악성코드 여부를 꼭 확인한다.
5. 백신패치 여부를 확인해서 최신 백신 엔진을 유지한다.
6. 스마트폰의 잠금 기능[암호 설정]을 이용해서 다른 사용자의 접근을 막는다. 잠금 기능에 사용한 비밀번호를 수시로 변경한다.
7. 블루투스 기능을 켜놓으면 자동 감염되므로 필요할 때만 켜놓는다.
8. ID, 패스워드 등을 스마트폰에 저장하지 않는다.
9. 백업을 주기적으로 받아서 분실 시 정보의 공백이 생기지 않도록 한다.
10. 임의로 개조 및 복사방지 등을 해제하지 않는다.

## 4. 결론

IT 기술이 진화됨에 따라 서비스를 제공받기 위한 다양한 디바이스 기술이 점차 진화되고 있으며, 최근 스마트폰의 보급으로 금융 서비스를 시간과 장소에 구애받지 않고 제공받을 수 있는 환경이 구축되고 있다. 스마트폰은 사용자의 사용 용도에 따라 다양한 서비스를 다운로드 받아 사용할 수 있어 사용하는데 확장성을 제공할 수 있으며, 이동 중에도 3G 망을 이용하여 자유롭게 네트워크를 구성하고 통신을 할 수 있기 때문에 보급률이 급증하고 있다. 그러나 스마트폰 보급이 증대되고 있는 금융 분야에는 특히 보안이 적용되야하는 분야임에도 불구하고 빠른 속도를 지원해야 됨에 따라 보안 구현이 시급한 실정이다. 또한 스마트폰에 대한 공격 위협이 본격화되고 클라우드 및 가상화 기술을 악용한 보안 위협이 증가될 것으로 예측되고 있어 보안 문제가 심각화 되고 있다. 기존 PC에서 발생하는 보안 문제가 스마트폰에서도 동일하게 발생할 수 있으며, 다양한 스마트폰의 종류와 플랫폼을 겨냥한 악성코드가 나타나고 있다. 특히 개인 정보를 노출하도록 하거나 스마트폰을 좀비 클라이언트로 만들어 DDoS 공격에 악용할 수 있어 심각한 문제가 되고 있다.

따라서 이러한 스마트폰의 보안 위협으로부터 안전하기 위해서는 스마트폰 보안 위협에 대하여 사용자가 인지하고 기존 PC에서 사용하는 것과 같이 스마트폰 백신 사용이 필요하다. 또한 스마트폰 보안 수칙을 준수하고 스마트폰 보안에 대한 사용자 의식 제고가 반드시 제공되어야 할 것이다. 스마트폰에 대한 보안이 적용된다면 금융 서비스 제공 환경에서 이동성에 따른 원활한 서비스 제공 및 편의성을 제공할 수 있는 강력한 디바이스가 될 수 있을 것으로 사료된다.

## 참고문헌

[1] Ahmed Alazzawe, Anis Alazzawe, Duminda Wijesekera, Ram Dantu, “A testbed for mobile social computing,” tridentcom, 2009 5th International Conference on Testbeds and Research Infrastructures for the Development of Networks & Communities and Workshops, pp.1-6, 2009

[2] Liang Xie, Xinwen Zhang, Ashwin Chaugule, Trent Jaeger, Sencun Zhu, “Designing System-level Defenses against Cellphone Malware,” Proceedings of the 2009 28th IEEE International Symposium on Reliable Distributed Systems, pp.83-90, 2009

[3] Xudong Ni, Zhimin Yang, Xiaole Bai, Adam C. Champion, and Dong Xuan, "DiffUser: Differentiated User Access Control on Smartphones," pp.1012~1017, 2009

[4] http://www.ahnlab.com, 안철수연구소 스마트폰 보안 수칙 10계명

[5] http://www.android.com/

[6] http://www.vmware.com/technology/mobile.html