The Journal of The Institute of Internet, Broadcasting and Communication (IIBC)
Vol. 14, No. 6, pp.267-272, Dec. 31, 2014. pISSN 2289-0238, eISSN 2289-0246

http://dx.doi.org/10.7236/JIIBC.2014.14.6.267
JIIBC 2014-6-38

모바일 앱 개인정보 침해현황 및 대응방안 (금융, 안드로이드 운영체제 중심으로)

Privacy Situation and Countermeasures of Financial Apps based on the Android operating system

김보*, 임종인**, 조용현***

Bo Kim*, Jong-In Lim, Yong-Hyun Jo*****

요 약 2014년 1분기 국내 스마트폰 기반의 모바일 뱅킹 등록고객 수는 4,034만명으로 2013년말 대비 8.5%(316만명) 증가했고, 하루 평균 거래액은 1조6276억원으로 집계되었다[1]. 또한 2014년 스마트폰 뱅킹 악성앱 발견건수는 1,440건으로 소액결제, 스마트폰 공인인증서 탈취, 정상적인 은행 앱을 악성 앱으로 바꾸는 등의 악성코드가 크게 증가한 것으로 나타났다. 이렇게 금융 스마트폰 앱 사용자수 및 거래액이 증가와 함께 스마트폰 악성코드 등도 늘어나면서 앱을 사용하는 금융소비자들에게 피해가 날로 확산되고 있다. 본 연구는 은행, 증권, 카드사들을 중심으로 금융 스마트폰 앱 설치 시 요구하는 개인정보 수집 권한에 대한 실태를 조사하였다. 이 결과를 토대로 개인정보 수집을 최소화 할 수 있는 방안을 제시하여 금융소비자의 개인정보를 안전하게 보호하고자 한다.

Abstract Customers who register at mobile banking service through startphone has 40Mil in first quarter of 2014, which was increased 8.5%(3.6Mil) compare to figure from end of year 2013[1]. Average 1 trillion 627.6billion won is dealing through smartphone banking in daily and three for increased psychological bullying caused by malignant code which change normality to malignant. The results of the analysis current state of affairs of personal information collection management authority required in finance smartphone app service and also recommend solution for protecting finance consumers plans to minimized collecting personal information in smartphone finance app service.

Key Words : Smartphone App, Mobile App, Privacy, Finance, Information Security

Ⅰ. 서 론

최근 모바일을 비롯한 다양한 스마트폰 기기의 확산으로 스마트폰 앱을 이용한 서비스의 중요성 및 관심이 급격하게 증가하고 있다. 기업은 모바일 서비스를 활용한 비즈니스 영역이 새롭게 창출하고 사용자들은 모바일 플랫폼을 기반으로 한 다양한 서비스를 이용할 수 있게 되었다. 스마트폰 사용자가 설치하는 앱은 평균 26개로 대부분 보안취약점에 대한 안내 또는 경고 없이 사용하고 있다[2]. 금융회사의 경우 계좌이체, 신용카드사용 등 전자금융서비스를 위한 상품으로 개발되었으나 외부 해킹에 의한 정보유출과 불필요한 정보 노출에 따른 사고

*정회원, 고려대학교 정보보호학과
**정회원, 고려대학교 정보보호학과 (교신저자)
***정회원, 정보안전포럼
접수일자: 2014년 11월 7일, 수정일자: 2014년 12월 7일
게재확정일자: 2014년 12월 12일

Received: 7 November, 2014 / Revised: 7 December, 2014
Accepted: 12 December, 2014
**Corresponding Author: jilim@korea.ac.kr
Dept. of Cyber Defense, Korea University, Korea

발생이 증가하는 등 다양한 형태의 위협이 존재하고 있는 상태다. 따라서 스마트폰 금융 앱이 이와 같은 위협에 노출되었을 경우, 금융 소비자들의 금전적 손실과 이에 따른 사회 공학적 문제가 크게 발생할 수 있다. 또한 최근에는 스마트폰 내의 손전등 앱 프로그램이 임의로 개인의 스마트폰 유심칩 정보나 기타 스케줄 등 개인정보를 침해하고 이를 외부에 제공한 사실이 방송 등 언론에 의해 공개되면서 스마트폰의 앱의 개인정보 침해가 심각한 수준에 이르고 있는 것으로 나타났다. 한국 ICT 추진협회에 따르면 스마트폰 이용자중 23%가 “본인의 개인정보가 유출될 것 같은 불안감이 있다”라고 조사되었고[3], 또한 스마트폰의 정보노출 문제점에 대해 72%가 “자신의 동의 없이 이뤄지는 개인정보 수집”을, 68%가 “형식적인 개인정보 취급방침”에 문제가 있다는 조사결과 나왔다[4]. 보통 스마트폰 앱 프로그램 개발과정에서 보면, 종종 불필요한 프로그램 명령어로 인한 악의적인 외부 해킹이나 정보노출에 취약한 경우가 종종 발생하고 있다[5]. 이것은 기업 내부에서 보안통제가 되어야 하는데 아직까지 프로그램 기능에 대한 오작동여부 등을 위주로 테스트하고 보안과 관련된 통제 활동은 많은 기업이 생략하고 있기 때문이다.

최근 스마트폰 문자메시지 등에 악성코드를 심어 문자 메시지를 확인, 클릭시 스마트폰 내부의 개인 및 금융정보를 탈취하는 스미싱(SMS+Phishing)이 기승을 부리면서 이를 통한 신용카드 부정사용 결제 사건이 지속적으로 발생하고 있다. 최근 소비자들은 본인의 개인정보에 대한 보안을 중요시 하고 있다. 이에 따라 지난 2008년 개인정보보호법이 제정되었고, 이 기준에 의하면 개인정보의 수집, 이용, 제공 등에 대해서는 본인의 동의가 있어야 가능하게 되어 있으며, 사업자는 개인정보의 최소 범위 내에서만 수집하도록 한정하고 있다. 그러나 스마트폰 앱에서도 그러한 기준으로 운용되고 있을까? 현실은 그렇지 않다. 이것은 기존의 개인정보보호법 내에 개인정보취급방침이 일반적인 PC 환경에서 사용자들이 웹브라우저 등을 이용할 때 수집되는 정보를 선택항목(쿠키, HDD Sirial, Mac Address 등)으로 구분하고 있어 스마트폰 앱도 유사하게 취급되기 때문이다. 그러나 스마트폰는 일반 PC와는 조금 다른 구현방식이다. 따라서 본 연구에서는 금융회사가 제공하고 있는 스마트폰 앱(안드로이드 운영체제)에 대한 정보획득 권한 즉, 개인정보 수집/활용 실태 관련 조사를 통해 모바일 서비스에 안전성 여부를 점검하고 취약한 부분에 대해 개선방안을 제시하고자 한다.

II. 관련 이론 및 선행학습

1. 스마트폰 서비스 보안위협 현황

스마트폰 앱의 전반적인 보안위협은 ‘운영체제 변조 위협’, ‘로컬 보안 취약성’, ‘원격 보안 취약성’, ‘잠재 취약성’으로 구분할 수 있다. 금융거래를 목적으로 하는 전자금융 모바일 서비스의 경우에는 전자거래 프로그램 위. 변조 위협과 스마트폰 자체의 취약점을 이용한 입력정보와 거래전문에 대한 보안위협을 예방하기 위한 보안 프로그램을 이용자에게 제공하고 있다. 이러한 위협은 보안기능의 무력화, 결제 시스템의 우회, 악성코드 삽입 후 배포 등의 위협을 증가 시킬 수 있어 개인정보 유출이나 금전적인 피해를 가져올 수 있다[6].

2. 스마트폰 전자금융서비스 안전대책

금융회사가 서비스하는 스마트폰 앱의 안전성 검증을 위해 금감원은 지난 2013년 스마트폰 안전대책을 제정하였다. 스마트폰 안전대책 가이드에서는 금융안전대책, 앱 위변조 방지대책, 기타 등으로 13가지 항목의 스마트폰 앱 보안준수사항을 제시하고 있다[7].

표 1. 스마트폰 전자금융 보안가이드
Table 1. Smartphone financial transaction safety measure

영역	내용
스마트폰 금융 안전대책	1.백신 프로그램 적용 - 앱 실행시 백신프로그램 구동 - 백신프로그램 업데이트
	2. 입력정보 보호대책 적용
	3. 금융정보 종단간 암호화 적용 여부
	4. 거래전문 무결성 검증 기법
앱 위변조 방지대책	5. 폰 임의개조 탐지 및 차단
	6. 중요 파일 무결성 검증기술 적용
	7. 코드/모듈 보호 - 코드보호 기술 적용 - 네이티브 라이브러리 구현 - 코드/모듈 업데이트
기타	8. 앱 취약점 점검
	9. 위·변조 앱 모니터링
	10. 앱 위·변조 로그 기록
	11.멀티로그인 금지
	12. 스마트폰에 금융정보 저장 금지
	13. 금융거래기록 보관

또한 금융보안연구원에서는 "전자금융 스마트폰 보안 가이드"에서는 프로그램 개발 시 필요한 절차에 대한 보안 통제방안을 제시하고 있다.

그림 1. 금융보안 연구원, 전자금융보안 서비스 보안 가이드, 2014.07
Fig 1. Financial Security
Agency, Smartphone security of electronic financial services guide, 2014.07

상기 Fig.1의 가이드에서는 스마트폰 전자금융서비스 "설계/개발" 단계에서 원칙 5가지 ①안전한 앱 구현 ②보안기능 적용③앱 보안성 확인 ④안전한 앱 배포 ⑤앱 업데이트 관리 등 제시하고 있다. 이 논문은 스마트폰 앱 권한에 대한 개인정보보호 정책에 대한 추가적인 규제사항 및 기업 내부통제에 대한 범위를 연구대상으로 자세한 기술적 내용은 금융보안연구원 홈페이지 자료실을 참조하면 된다.

3. 해외 모바일앱 보안 정책 동향

유럽 네트워크 및 정보보호 위원회(ENISA, European Network and Information Security Agency)에서 제안하고 있는 스마트폰 보안 가이드라인에 따르면 사용자의 금융 정보에 접근할 수 있는 NFC 결제 모듈, SMS 등 접근이 가능한 권한을 앱을 개발 할 때 제3자 노출 및 악용되지 않도록 개발해야 한다고 규정하고 있다[8].

미국은 연방거래위원회(FTC, Federal Trade Commission)에서 모바일 앱 개발자들이 프라이버시 및 보안문제를 피하기 위한 가이드라인을 규정하고 있다[9]. 이 가이드라인에서는 스마트폰 사용자로부터 얻는 모든 정보들은 사용자가 통제하고 명시적인 사용자 동의를 받도록 하는 등 모바일 개인정보수집에 대해 엄격히 다루고 있다.

일본은 스마트폰 프라이버시 및 보안 연합회(SPSC, Smartphone Privacy and Security Council)를 통해 스마트폰 애플리케이션 개인정보보호 정책에서 모바일 앱 제공자는 모바일 개인정보보호정책을 수립하여 앱 권한과 취득되는 정보를 열거하여 사용자에게 알려주도록 규정하고 있다[10].

4. 선행학습 및 기타

스마트폰 앱의 보안관련 이론이나 논문들은 많으나 금융 앱 관련 권한 오남용에 대해 직접적으로 관련된 논문은 많지 않았다. 그 중 본 논제와 유사한 형태의 논문이라면 모바일 앱 권한이 아니라 스마트폰 보안 영역 전반에 대해서 문제점을 제기하고 개선방안을 제시한 연구사례는 있었다[11]. 이 논문의 경우 앱권한에 대해서는 다루지 않았지만 스마트폰의 앱에 대한 보안과 개발에 있어 전반적으로 고려해야 하는 사항을 중심으로 다루었다. 따라서 본 연구는 금융 앱을 대상하고 iOS 대비 보안에 취약한 안드로이드 운영체제를 중심으로 연구범위로 지정했으며, 앱 자체의 기술적 취약성 보다는 개인정보 수집/이용에 대한 정책 및 권한이 적정한지 여부와 정보 노출에 따른 리스크를 중심으로 연구하도록 하겠다.

Ⅲ. 관련 이론 및 선행학습

1. 스마트폰 서비스 보안위협 현황

본 연구의 앱 권한 점검기준은 구글 개발자사이트에서 제공하는 앱 권한 항목 총 146개를 활용하여 점검하였다[12]. 각 금융 업종별로 스마트폰 앱에서 요구하는 권한 현황을 살펴보면 증권이 가장 많은 21개의 권한을 요구하는 것으로 나타났고, 뱅킹이 19개, 카드 17.5개 순이었다.

표 2. 금융 모바일앱 권한 요구 현황
Table 2. Financial status smartphone app needs permission

구분	뱅킹	증권	카드
권한 갯수	19	21	17.5

뱅킹 스마트폰 앱에서는 요구하지 않는 권한을 증권과 카드 앱에서는 많이 요구하고 있는데, 신용카드사 앱

의 경우 "google 서비스 구성 읽기", "화면 잠금 사용중기", "바로가기 설치", "바로가기 제거", "다른 앱위에 그리기, "앱 디버깅 사용", "실행중인 앱 순서 재지정" 등을 요구하고 있다.

증권사 스마트폰 앱의 경우에는 뱅킹, 카드 스마트폰 앱에서는 요구하지 않는 "앱 직접 설치", "앱 삭제", "기기 전원 켜고 끄기", "기기 강제 재부팅"과 같은 권한을 요구하고 있다. 이러한 권한은 증권 서비스와는 무관한 것으로 보인다.

2. 스마트폰 서비스 보안위협 현황

3.1~3.3 은행, 증권, 신용카드사 현황에서 보는 바와 같이 각 회사별로 다른 앱 권한을 요구하고 있다. 또한 조사를 통해 확인된 일부 금융회사의 스마트폰 앱의 경우 금융회사가 제공하는 서비스와 무관한 "주소록 수정", "내 문자메시지 수정", "앱 삭제" 등 이용자 스마트폰에 접근하여 데이터의 변경(삭제 등) 행위 까지도 할 수 있다.

본 논문에서 조사된 18개의 전자금융 모바일 앱에서는 총 57개의 설치권한이 요구되는 것으로 나타났다. 이 권한들 중에 직/간접적으로 전자금융 서비스에 연관된 권한은 16개로 공인인증서, 인증 메시지 수신, 백신 가동 등에서 필요한 것으로 나타났다. 하지만 전자금융 서비스와 무관한 사진찍기, 녹음, 주소록 읽기/수정 등의 권한이 41개 이다.

연관 권한	무관 권한
•휴대전화 상태 및 ID 읽기 •USB 저장소의 컨텐츠 수정 또는 삭제 •WIFI 연결 보기 •실행중인 앱 검색 •네트워크 연결보기 •진동제어 •인터넷에서 데이터 받기 등	•사진과 동영상 찍기 •SMS 메시지 읽기, 보내기 •주소록 읽기/수정 •오디오 녹음 •앱 삭제 •통화 기록 쓰기 •기기 전원 켜고 끄기 •강제 재부팅 등
16개	41개

그림 2. 모바일앱 보안 가이드 실태
Fig. 2. 〈Mobile app security guide improvements〉

이는 개인정보보호법의 취지인 개인정보 수집/이용 최소화와는 상반된 결과이다. 금융 소비자가 앱을 사용하기 위해 설치 시 이용자의 의지와 무관하게 개인정보 수집 및 이용에 대한 포괄적인 권한을 요구하는 것이 현재의 가장 큰 문제이다.

Ⅳ. 개선방안 및 기대효과

1. 스마트폰 서비스 보안위협 현황

금융회사는 스마트폰 앱을 개발하는 단계에서 부터 불필요한 정보접근 권한 기능은 사용하지 않도록 금융보안연구원의 전자금융 모바일앱 보안 가이드의 설계/개발 단계에서 다음의 3가지 사항이 프로그램 개발절차에 반영되어야 한다.

(1) 모바일 서비스 관련 부서는 모바일 앱 기획 단계에서 요구되는 개인정보의 범위를 명확화 하고,
(2) 모바일 서비스 내부통제 부서는 개인정보 정책이나 법규 위배 사항 여부를 확인 하고,
(3) 모바일 개발 부서는 정보접근 권한에 대한 소스코드 정책을 사전에 수립, 개발 매뉴얼에 반영하고 이를 기반으로 개발 및 검수과정에 "앱 권한 최소화" 원칙을 추가하여 서비스에 반드시 필요한 개인정보 수집 권한이 반영되도록 해야 한다.

앱 설계 및 개발 시 보안 (기존)	개인정보 수집 최소화 (신규)	안전한 서비스 제공 (기존)	시스템 및 보안관리 (기존)
.안전한 앱 구현(기존) .보안기능 적용(기존) .앱 보안성 확인(기존) .안전한 앱 배포(기존) .앱 업데이트 관리(기존) .정보 수집 항목 정의(신규) .내부통제 검토(신규) .권한 개발검토(신규)	.모바일앱 권한 최소화(신규) .필요한 권한에 한정(신규)	.설치/실행 환경 관리 (기존) .앱 무결성 검증(기존) .이용자 확인 강화(기존) .안전한 통신(기존) .이용자 교육(기존)	.시스템 보안(기존) .보안관리(기존)
설계/개발 단계(기존)	권한 검토 단계(신규)	설치/이용 단계(기존)	시스템/관리 단계(기존)

그림 3. 모바일앱 보안가이드 비교
Fig. 3. 〈Mobile app security guide improvements〉

또한, 권한 검토 단계를 신규로 추가하여 보안 관련 부서에서는 설계/개발 단계에서 이뤄진 전자금융 모바일 앱에서의 개인정보 수집/처리에 대한 권한의 적정성을 검토해야 한다. 이렇게 한다면 불필요한 고객정보를 수집하는 취약성은 지금보다 크게 개선될 것이다.

2. 사용자 선택권 부여

현재 설치 스마트폰에 설치된 앱은 기본적으로 설치 시에 설치 동의를 구하게 되어 있다. 이것은 앱 개발사에

의해서가 아니라 OS 차원에서 수행되기 때문에 우리나라의 개인정보보호법 등이 반영되어 설치 시 확인하는 것이 아니다. 따라서 현재 개인정보 유출에 문제가 되고 있는 금융 앱의 경우 금융회사에서 개발 시 앱의 권한을 환경설정 등에서 사용자에게 알려주고 사용자는 이 중 본인에게 필요한 서비스에 한정하여 선택(삭제 등)할 수 있도록 구현해야 한다. 이렇게 한다면 금융소비자 입장에서 본인의 개인정보에 대한 올바른 판단을 통해 보다 안전한 금융 앱을 선택하여 사용할 수 있을 것이다.

3. 개인정보취급/처리방침 개정

개인정보보호법 제30조(개인정보 처리방침의 수립 및 공개)에 따라 공개하고 있는 개인정보취급방침 및 개인정보처리방침에 명시하고 있는 개인정보 수집 범위 이외에 스마트폰의 특수성을 감안한 항목을 추가적으로 반영해야 한다[13]. 즉, 본 연구에서 제안한 금융소비자의 스마트폰에서 수집, 처리되는 정보(전화번호, 휴대폰 문자, 주소록, e-mail 접근, 기기 재부팅 등)를 구체적으로 명시하여 각 금융회사가 이를 준수하도록 해야 한다. 그리고 명문화된 법규에 근거하여 소비자가 스마트폰 앱을 사용할 수 있도록 관련 사항을 충분히 고지하도록 하여 무분별하게 남용되어온 스마트폰 금융 앱 권한을 제거할 수 있도록 해야 한다.

V. 결 론

지금까지 주요 은행, 증권, 신용카드사에서 배포한 전자금융거래용 스마트폰 앱 권한의 실태를 조사, 분석하고, 본인의 동의 없이 불필요하게 오/남용되어지고 있는 앱 권한으로 인해 개인정보 침해 및 유출 사고의 개연성이 있을 수 있음을 충분히 확인할 수 있었다. 우리나라 성인의 대다수가 사용하고 실생활과 밀접하게 연관되어 있는 스마트폰에서 사용자 개인정보에 대한 리스크가 크게 존재함에도 불구하고 지금 이 순간에도 스마폰 금융 앱을 사용하고 있는 현실이다. 특히 앱 권한 실태조사에서 본 바와 같이, 일부 금융회사가 아닌 대다수의 금융회사의 앱 서비스가 개인정보 오남용 또는 정보유출 사고의 근원지로 악용될 수 있을 개연성을 생각하면 심각한 문제가 아닐 수 없다. 지난 4월 개인정보보호위원회에서는 방송통신위원회로 스마트폰 앱의 과도한 권한 요구에 대해 개선안을 권고한바 있다. 이것은 정부차원에서도 개인정보에 대한 문제를 심각하게 바라보고 있는 상황이며, 특히 신뢰가 바탕이 되어야 하는 금융회사의 전자금융거래용 매체에서도 조사한 바와 같이 보안 취약성이 존재한다는 것은 우리사회의 보안에 대한 전향적인 인식 전환이 필요해 보인다.

본 연구를 위해 관련이론 및 선행학습을 하면서 “모바일 앱 권한”에 대한 보안관련 논문이나 자료가 의외로 많지 않음을 알 수 있었다. 이것은 현재 금융회사의 개인정보유출 사고가 계속 증가하는 상황에서는 향후 추가적인 연구가 계속 필요할 것으로 보인다. 또한 이 논문은 안드로이드를 기준으로 연구하였기에 앞으로 iOS나 기타 일반기업에서 제공하는 스마트폰 앱에 대해서도 권한남용 및 개인정보보호법에 위배되는 부분이 있는지 여부 등 다각적인 조사, 연구가 필요할 것으로 보인다.

References

[1] The Bank of Korea, “2013 year-round non-financial institution payment service usage Electronic Press”, 2014.06
[2] http://www.ciokorea.com/news/19234
[3] Korea Association for ICT Promotion "Perspective of the users and the smartphone Utilization Study analyzed after regulation", 2010.12.31.
[4] Noh-Hyung Park "A Study on Mobile Data Protection", 2011.12
[5] Seoul Metropolitan Police, "Telecommunications companies Personal Information Disclosure arrested case Press", 2012.03
[6] Sang-Sik Min "Protection technology trends smartphone banking app for integrity verification", 2013.02
[7] Financial Security Agency “Smartphone security of electronic financial services guide ”, 2014.06
[8] ENISA "Smartphone Secure Development Guidelines"
[9] http://business.ftc.gov/documents/bus81
[10] Japan MCF "スマートフォンのアプリケーション・プライバシーポリシーに關するガイドライン", 2012.11

[11] Tae-Han Song "Mobile apps development methodology in considering the functionality and security", 2014.02
[12] http://developer.android.com/reference/android/Manifest.permission.html
[13] http://www.law.go.kr/lsInfoP.do?lsiSeq=142563&efYd=20140807#0000
[14] Jang-Mook Kang, Woo-Jin LeetPrivacy 'The Study for Privacy Trust Zone of Smart Monitoring in Mobile Environment", 2010.04

저자 소개

임 종 인(정회원)

- 1986년 : 고려대학교 수학과 이학박사
- 現 고려대 정보보호대학원장,개인정보보호위원회위원,국방부정보화책임관자문위원 등

<관심분야 : 사이버국방, 정보법학, 디지털포렌식, 개인정보보호, 융합기술보안 등>

김 보(정회원)

- 2008년 : 고려대학교 정보경영공학과(석사)
- 2013년 : 고려대학교 정보보호대학원 박사과정
- 現 고려대학교 정보보호연구원 금융보안연구센터 수석연구원

<관심분야 : 금융보안, 전자결재보안, 보안정책, 융합보안 등>

조 용 현(정회원)

- 2007년 : 아주대학교 정보통신대학원 정보보호학과(석사)
- 現 정보안전포럼 책임연구원

<관심분야 : 디지털포렌식, 정보안전, 사이버범죄예방, 금융보안 등>