情 報 保 護 學 會 誌
第23卷 第1號, 2013. 2

스마트폰 뱅킹 앱 무결성 검증을 위한 보호기술 동향

최 지 선*, 김 태 희**, 민 상 식***, 성 재 모****

요 약

최근 스마트폰 이용자의 급증에 따라 고객의 편의성을 고려한 스마트폰 전자금융서비스가 다량 출시되고 해마다 그 이용자수가 급증하고 있다. 한편, 스마트폰에서의 보안위협이 언론에 대두되면서 금융당국은 2010년부터 꾸준히 스마트폰 전자금융서비스를 보호하기위한 대책마련을 추진하고 있는 실정이다. 본 논문은 최근 스마트폰 뱅킹 서비스 보안에서 이슈가 되고 있는 뱅킹 앱 위·변조 위협요소를 정리하고 이에 대응할 수 있는 보안기술 동향에 대해 살펴보고자 한다.

Ⅰ. 서 론

스마트폰의 출시와 더불어 태블릿 PC 등 다양한 스마트 기기의 출현으로 금융회사에서는 다양한 전자금융서비스를 제공하고 있다. 특히 장소에 구애 받지 않는 편의성 때문에 스마트폰을 사용한 전자금융서비스 이용자 수는 급속도로 증가하고 있다. 한국은행 보도 자료에 따르면 2012년 3분기 하루 평균 모바일뱅킹 이용건수와 금액은 전 분기 대비 각각 9.9%와 7.1% 증가한 1,330만 건과 9,734억 원으로 집계되었고 이 중 스마트폰 기반 모바일뱅킹서비스 이용건수와 금액은 1,325만 건과 8,913억 원으로 전체 모바일뱅킹 이용실적의 대부분(99.7%와 91.6%)을 차지한다[1].

한편, 전자금융거래는 양방향의 거래주체를 확인할 수 없고 거래 내역에 대한 외부 유출이나 변경의 가능성이 높아 거래 사실에 대한 증빙이 어렵기 때문에 컴퓨터 보안의 3요소(기밀성, 무결성, 가용성)뿐만 아니라 인증 및 부인방지까지도 보안 요소로 고려되어야 한다[4].

특히 스마트폰을 이용한 전자금융거래는 기존 전자금융거래의 보안위협 뿐만 아니라 스마트폰 자체의 보안 취약점까지도 그대로 반영되기 때문에 스마트폰 뱅킹 프로그램(APP 등)에 대한 무결성 검증 부분을 간과해서는 안 된다. 이에 금융당국은 스마트폰 전자금융서비스 보호 관련하여 2010년 1월과 2011년 2월 각각 ‘스마트폰 전자금융서비스 안전대책’, ‘스마트폰 금융거래 10계명’을 발표했다. 2012년 3월에는 전자금융거래 프로그램의 위·변조 여부 검증을 위한 ‘새로운 보안위협에 대한 대응 능력을 강화’ 할 것을 요청하여 금융회사에 스마트폰 어플리케이션(이하 : 앱) 위·변조 대책 마련을 마련하도록 하였다[3].

2011년 12월 실시한 한국 저작권위원회 실태조사에 의하면, 스마트폰 이용자수의 8.3%가 운영체제를 변조한 경험이 있고 그 중 대부분이 이 환경을 유지하는 것으로 나타났다[9]. 이러한 운영체제 변조는 성능 향상 및 유료 앱의 무료 사용 등의 목적으로 기존 운영체제의 원래 기능을 변경하기 때문에 스마트폰 전자금융서비스 보안에서도 그 위협이 함께 증대시키고 있는 실정이다. 이에 대해 금융회사는 상기 조치의 일환으로 정상적인 운영체제에서만 뱅킹 앱이 동작하도록 하고 있다. 하지만 일부은행의 스마트폰 금융 앱 접속 현황에 따르면 변조된 운영체제에서 서비스가 가능하도록 위·변조된 앱으로 뱅킹 시스템에 접속하는 시도는 하루 평균 700건에 달한다[2].

본 논문은 스마트폰 뱅킹 앱 무결성 검증을 위해 위와 같은 환경에서 발생할 수 있는 스마트폰 앱 위·변조

* 금융보안연구원 보안기술팀 (jschoi@fsa.or.kr)
** 금융보안연구원 보안기술팀 (thkim@fsa.or.kr)
*** 금융보안연구원 보안기술팀 (ssmin@fsa.or.kr)
**** 금융보안연구원 정보보안본부 (sitcom@fsa.or.kr)

위협을 정리하고 이에 대한 대응을 위한 앱 무결성 검증 보호기술을 분석하고자 한다.

Ⅱ. 스마트폰 위협현황

스마트폰의 전반적인 위협은 표 1과 같이 '운영체제 변조 위협', '로컬 보안 위협', '원격 보안 위협', '잠재 위협' 으로 구분할 수 있다.

〔표 1〕 스마트폰 위협

구 분	위 협
운영체제 변조 위협	커스텀 롬 위협, 어플리케이션 권한 획득 등
로컬 보안 위협	커널 권한 획득, 어플리케이션 권한 획득 등
원격 보안 위협	Heap Spraying 위협, Drive-By-Download 위협
잠재 위협	이용자 수, 앱 스토어 관리, OS패치 수준, 관리자 권한 획득 등

한편, 국내 스마트폰에 사용되고 있는 운영체제 중 가장 일반적으로 사용되는 운영체제인 안드로이드(이하 : Android)와 아이오에스(이하 : iOS)의 공식적으로 파악된 취약점 수는 표 2와 같다.

〔표 2〕 스마트폰 Exploit

모바일 운영체제별 Exploit	취약점 수(개)
Android Local Exploit	8
Android Remote Exploit	5
iOS Local Exploit	0
iOS Remote Exploit	21

Android의 취약점은 총 13개(원격 취약점 5개 포함), iOS의 취약점은 총 21개로 현재까지 iOS가 Android에 비해 다소 많은 취약점이 발견되었으나[6] 최근들어 Android 기반의 취약점과 악성코드가 많이 증가하고 있는 실정이다.

2.1. 운영체제 변조에 의한 스마트폰 위협현황

스마트폰 전자금융서비스 앱을 변조하여 이용하는 주된 이유는 변조된 운영체제(일명 루팅 또는 탈옥, 이하 : OS변조)폰에서 전자금융서비스를 이용하기 위함이다. 하지만 운영체제를 변조하면 일반 사용자가 접근할 수 없었던 시스템 파일 등에 대한 접근 및 변경권한이 가능해지고, 이에 따라 보안수준이 낮아지므로 보안 프로그램의 무력화 및 결제시스템 우회 등이 가능해지면서 더 많은 보안위협에 노출된다. 변조되지 않은 운영체제(이하 : 일반 OS)와 변조된 운영체제의 주요 위협은 표 3에 나타내었다.

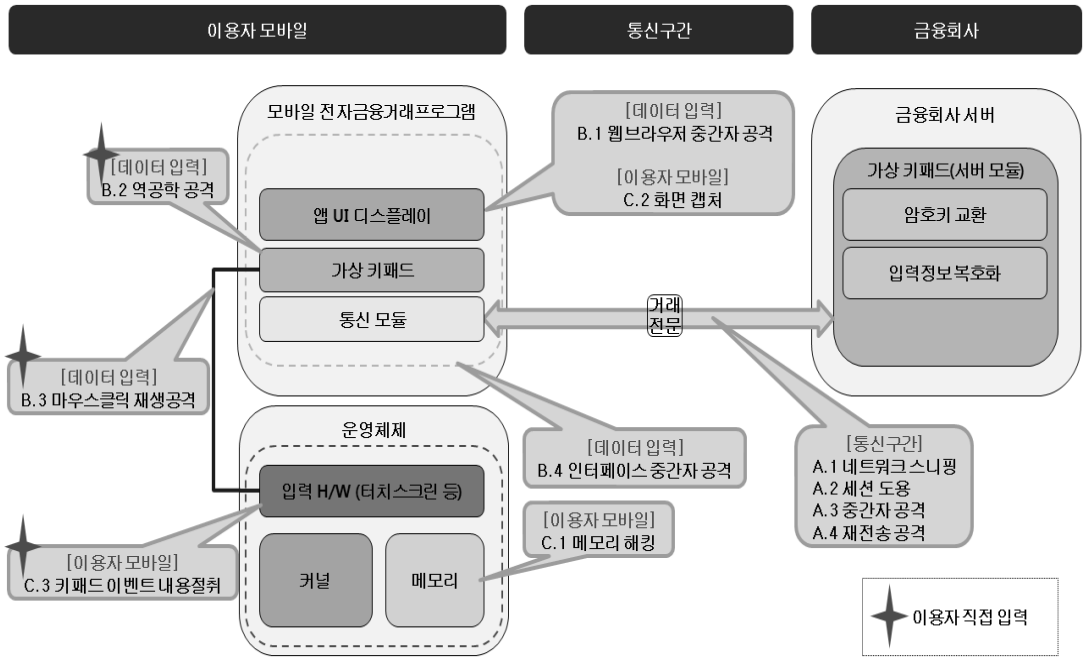
〔표 3〕 스마트폰 위협 구분

일반 OS 위협	OS변조 위협
악성 앱 설치 (정보 유출, 키로깅)	권한 상승 (시스템파일접근, 커스텀 롬 이미지설치 등)
정상 앱 변조 (악성기능추가, 보호기능 해제)	커널레벨 악성코드 (악성코드 동작, 변조 탐지 기능 우회)
이용환경 위협 (웹브라우저 이용 등)	'일반 OS 위협'
화면캡처	

일반 OS에서는 역공학 기술을 이용한 앱 기능 분석, 악성 앱 설치, 웹브라우저를 통한 악성코드 감염 등으로 관리자 권한 획득, 정보 유출, 키로깅, DDOS 공격 등이 이루어 질 수 있다.

OS변조의 경우 커널수준에서의 화면캡처, 키로깅 등 루트킷 수준의 악성코드 동작이 가능하고 앱 기반의 OS변조 탐지 기능, 메모리 변조 탐지 기능 등 특정 영역 변조여부를 탐지하는 기능자체에 대한 우회가 가능하여 일반 OS에서 발생할 수 있는 위협과 더불어 추가적인 보안위협에 노출된다.

한편, 이러한 위협을 가져오는 악성코드 유입경로는 앱 배포 프로세스와도 관련이 있다. Android의 경우 마켓 또는 온라인 등 다양한 경로를 통해 앱 설치가 가능하며, 마켓에서 소스코드의 검증절차를 수행하지 않기 때문에 일반 OS에서 코드사인의 절차를 수행하더라도 코드 사인을 다른 사인으로 교체하면 출처 확인 절차를 우회하는 셀프사인 취약점이 있고 iOS의 경우, 앱 코드 사인이 구매자 인증 정보 시스템을 통해 개발자와 구매자를 확인하고 앱 자체를 검열하는 앱스토어 심사제도를 운영하여 검증된 앱만을 설치하도록 하고 있다. 하지만, 보안이 항상 완벽할 수 없듯 이러한 프로세스 상에서도 아이폰의 보안 취약점을 이용해 앱스토어에 비승인 코드를 구동하고 원격으로 아이폰을 제어할 수 있는 악성 앱 등록관련 공격 시도가 꾸준히 진행·발표되고 있다[7].



〔그림 1〕 입력정보 및 거래전문 보안위협

2.2. 스마트폰 전자금융 서비스 위협현황

금융사에서는 이용자가 안전한 전자금융거래를 이용할 수 있도록 각종 보안프로그램을 제공하고 보안프로그램이 설치·동작하는 상태에서 금융거래가 가능하도록 해야 한다. 인터넷뱅킹 및 스마트폰 뱅킹에서 제공하는 보안프로그램 기능은 거의 유사하며 차이가 있다면, 인터넷뱅킹의 경우 주로 마이크로소프트社에서 제공하는 인터넷익스플로러(Internet Explorer : 이하 IE)등의 브라우저(Browser) 기반이고 스마트폰뱅킹의 경우 금융사에서 제공하는 별도의 거래 프로그램(APP) 기반이라는 점이다. 표 4는 PC에서 인터넷 뱅킹을 수행할 때 이용자 단말PC에 설치되는 프로그램의 종류와 예시이다.

〔표 4〕 이용자 PC에 설치되는 보안프로그램

프로그램 종류	예 시
이용자 입력 값 보호	키보드해킹방지프로그램, 가상키보드 등
이용자 본인 확인	공인인증서 관리 프로그램 등
금융거래 데이터 암호화	SSL, 웹 암·복호화 프로그램 등
악성코드 해킹 방지	개인방화벽 및 안티바이러스 프로그램 등

상기 거론한 주요 보안프로그램 중, '악성코드 해킹 방지 프로그램'을 제외한 나머지 보안프로그램이 금융거래의 안전성 및 신뢰성을 유지와 직접적인 연관성이 있으며, 특히 국내 인터넷뱅킹의 경우 IE 브라우저를 기반을 중심으로 거래가 이루어지도록 되어 있어, 이에 대한 추가적인 보완 기술이 필요한 실정이다[5].

스마트폰 뱅킹은 전자거래 프로그램 위·변조 위협뿐 아니라 그림 1과 같이 스마트폰 자체의 취약점을 이용한 입력정보와 거래전문에 대한 보안 위협이 발생할 수 있다[8]. 각 위협에 대한 상세 정의 및 설명은 표 5에 나타내었다.

대표적인 스마트폰 전자금융서비스 위협으로는 메모리 영역에 대한 위협, 키패드 이벤트 내용 절취, 화면 캡처 등의 위협이 있으며, 이용자가 데이터 입력 시 역공학 기술을 이용한 데이터 위·변조, 입력 좌표 값 절취 로그인(또는 인증 우회), 모듈과 상호 연동된 인터페이스 절취, 웹 앱의 경우 웹 브라우저로 전송된 웹 페이지 위·변조 등이 있다. 또 데이터를 서버로 전달하는 통신구간에 대한 위협도 존재하는 데 송·수신되는 데이터 트래픽을 도청하거나 사용자와 서버 간 연결된 세션 도용, 네트워크상의 중간자 공격, 인증관련 정보를 획득하여

〔표 5〕 입력정보 및 거래전문 보안위협 상세

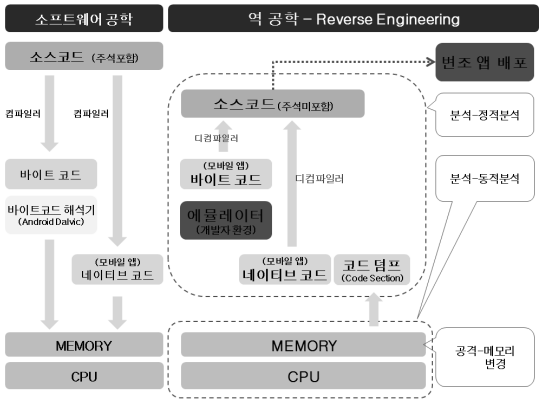
구분	위 협	정 의
A. 통신구간	1. 네트워크 스니핑	네트워크에서 송·수신되는 데이터 트래픽을 도청
	2. 세션 도용	사용자와 서버 간 연결된 세션 정보를 이용하여 권한 획득
	3. 중간자 공격	네트워크상에서 전송되는 데이터 위·변조
	4. 재전송 공격	인증 관련 정보를 획득하여 재사용
B. 데이터입력	1. 웹 브라우저 중간자 공격 (웹앱의 경우)	웹 브라우저로 전송된 웹 페이지를 위·변조
	2. 역공학 공격	가상 키패드에서 특정 지식을 추출하여 데이터 추출, 위·변조
	3. 마우스 클릭 재생 공격	가상 키패드 이미지와 클릭된 마우스 X·Y 좌표값을 절취한 후 서로 다른 세션 또는 로그인 시 기존 저장된 좌표 값을 재생하여 인증 우회
	4. 인터페이스 중간자 공격	모듈과 상호 연동되는 인터페이스를 후킹(Hooking)하여 전송되는 데이터 열람 또는 위·변조
C. 이용자 모바일	1. 메모리 해킹	애플리케이션 동작에 필요한 메모리 영역 열람 또는 위·변조
	2. 화면 캡처	키패드 화면 내용 절취
	3. 키패드 이벤트 내용 절취	운영체제에 발생하는 키보드 이벤트를 통해 키패드 이용자 입력 정보 절취

재사용하는 공격 등 입력 정보 및 거래전문에 대한 많은 위협이 존재한다.

특히 그림 2와 같은 역공학 분석을 통한 공격이 이루어 질 경우, 위·변조 대상 스마트폰 뱅킹 앱의 구조분석이 더 용이하여 디컴파일러 등의 도구를 사용한 정적 분석 기반 코드 변조 혹은 동적 분석을 통한 코드 실행 흐름 파악 후 중요 로직 변경, 메모리상 중요 로직 변경 등 데이터를 입력하는 시점에서의 데이터 변조 공격에 대한 위협이 증가할 것으로 보인다.

Ⅲ. 스마트폰 뱅킹 앱 위·변조 방지 보호기술

스마트폰 뱅킹에서는 앞 장에서 살펴본 스마트기기 위협요소가 추가되면서 위·변조된 앱의 설치·실행으로 인한 스마트폰 뱅킹 시 보안 기능의 무력화, 결제시스템



〔그림 2〕 역공학에 의한 스마트폰 앱 보안위협

우회, 악성코드 삽입·배포 등 거래 주요정보에 대한 위협으로 인한 개인정보 유출이나 금전적인 피해를 가져올 수 있다.

3.1. 스마트폰 뱅킹 앱 보호를 위한 기 적용 기술

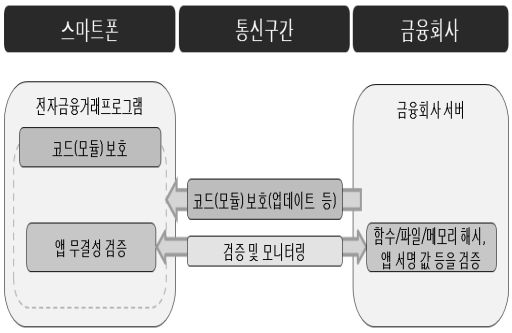
현재 금융회사에서는 스마트폰 뱅킹 앱 보안을 위해 앱에 대한 보호와 더불어 악성코드 탐지를 위한 백신프로그램, OS 변조 여부 확인을 위한 운영체제 변조 탐지, 입력 값 보호를 위한 가상키패드 등의 보안프로그램을 제공하고 있다. 또한 전자금융 거래 시 보안을 위한 인증용도로 공인인증서, 보안카드, OTP 등이 이용되고 있다.

3.2. 스마트폰 뱅킹 앱 위·변조 방지 기술

본 절에서는 스마트폰 뱅킹 앱의 위·변조와 방지 기술에 대해 위조와 변조 개념으로 나누어 설명하고자 한다.

먼저, 스마트폰 뱅킹 앱 위조에 대응하기 위해서 다양한 보호기술을 적용하기보다 스마트폰 뱅킹 앱과 비슷한 명칭 및 GUI(Graphical user interface)를 이용하는 앱을 주기적으로 검색하여 앱스토어 또는 홈페이지 등에서 삭제하도록 조치하는 것이 필요하다. 이는 기술적인 측면의 대응기법이라기보다 관리적인 측면에 가깝다고 볼 수 있지만 개방형 OS가 일반적인 시장 흐름이고 신뢰할 수 없는 앱 스토어 시장에서 위조된 앱의 배포를 방지하기위해서는 금융사의 꾸준한 조사·관심이 가장 주요한 핵심이다.

또, 금융사 내부 개발자의 보안의식 및 관리프로세스



〔그림 3〕 스마트폰 앱 변조 방지 기술

도 방심치 않고 살펴보아야 한다.

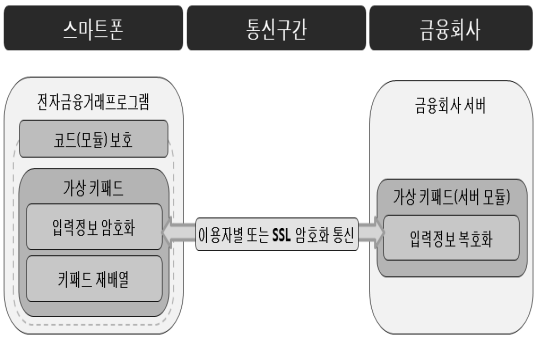
한편, 공격자들의 스마트폰 뱅킹 앱 변조를 방지하기 위해서는 스마트폰 앱 내부에서 이용하는 함수, 파일, 메모리 해시, 앱 서명값 등을 검증하여 해당 앱이 변조되었는지 여부를 기술적으로 판단하고 금융회사 서버측에서 앱 해시 값 및 버전 변경으로 인한 검증 및 모니터링이 필요하다.

더불어 스마트폰 뱅킹 앱의 해시를 검증하는 코드를 분석하여 해당 보호기술을 우회하는 공격을 방지하기 위해서, 검증 코드 또는 모듈에 대한 보호방안도 고려할 필요가 있다.

3.3. 스마트폰 뱅킹 앱 거래전문 보호 기술

스마트폰 뱅킹 앱의 거래전문을 보호하기 위해서는 입력정보와 그 정보를 전송하는 통신구간의 보호가 필요하다.

먼저 이용자 측 스마트폰에서는 입력정보에 대한 무결성을 보장하는 암호화와 데이터 입력 시 해당 정보의



〔그림 4〕 스마트폰 뱅킹 앱 거래전문 보호 기술

유추를 어렵게 하는 키패드 재배열 기술이 적용된 가상 키패드 등을 통해 입력정보를 보호할 수 있다.

또 앱 내부 및 전송 단에서 거래전문의 무결성을 확보하기 위해 이용자별 암호화 통신구간 생성, SSL (Secure Sockets Layer, 이하 : SSL) 암호화 통신 등의 보호기술을 적용할 수 있는데 이 때 기본적으로 채택하는 SSL은 글로벌 표준 암호화 알고리즘이 적용되어 있고, 금융권에서 제공하는 이용자별 자체 암호화 통신구간 생성 및 전송으로 인해 네트워크 데이터 전송에서의 무결성 검증 방법이 따로 크게 부각되지 않고 있는 실정이다.

하지만 전체적으로 볼 때 거래전문 보호 기술에 대한 위협을 방지하기 위해서는 앱 해시 검증 기술과 마찬가지로 거래전문 검증 코드 또는 모듈에 대한 보호방안을 고려해야 한다.

3.4. 코드 및 모듈 보호 기술

무결성을 입증하는 수단이 될 수 있는 앱 해시 검증 등의 기술은 바이트 코드 또는 네이티브 코드로 개발이 가능하다. 공격자의 입장에서는 이러한 보호용 기술까지도 분석하여 무결성 검증을 우회하는 공격을 시도할 수 있다. 이에 대한 근본적인 방어로서 해당 코드 및 모듈을 보호하기 위해 아래와 같은 기술을 적용할 수 있다.

- 코드 난독화 기술 : 코드의 정적/동적 분석을 어렵게 하여 내부 구조 파악 및 변조를 어렵게 함
- 안티 디버깅 기술 : 공격자가 동적 분석을 위해 디버거 툴을 이용하는 경우 분석을 어렵게 할 수 있음
- 주기적 또는 실시간 업데이트 : 공격자의 모듈 또는 코드 분석에 의한 공격을 방어하기 위함

표 6~8은 상기 세 가지 코드 및 모듈 보호 기술에 대해 실제 앱 개발에 적용할 수 있는 기법으로 분류하였다.

〔표 6〕 Android - 코드 및 모듈 보호 기술

기 법	설 명
바이트 코드 구현	자바 또는 .NET등의 언어를 이용하여 개발하는 경우 컴파일 결과는 바이트 코드가 생성됨(비슷한 분석수준을 갖는 코드 포함)
바이트 코드 난독화	코드의 정적/동적 분석을 어렵게 하기 위하여 코드 난독화 기술을 이용할 수 있음
네이티브 모듈 업데이트	공격자의 모듈 분석에 의한 공격을 방어하기 위해 주요모듈을 주기적으로 교체

〔표 7〕 Android, iOS - 코드 및 모듈 보호 기술

기 법	설 명
네이티브 코드 구현	Android : JNI를 이용하여 네이티브 코드 호출가능 iOS : 기본적으로 네이티브 코드로 개발됨 (Objective C)
안티 디버깅	동적분석 위해 디버거 툴을 이용하는 경우 분석을 어렵게 할 수 있음
네이티브 코드 암호화	코드의 정적/동적 분석을 어렵게 하기 위하여 코드 암호화 기술을 이용할 수 있음
네이티브 코드 난독화	코드의 정적/동적 분석을 어렵게 하기 위하여 코드 난독화 기술을 이용할 수 있음
동적코드 업데이트	공격자의 코드분석에 의한 공격을 방어하기 위해 동적코드를 주기적 또는 실시간으로 교체

〔표 8〕 OS변조 - 코드 및 모듈 보호 기술

기 법	설 명
커널레벨 앱 보호	(관리자 권한이 획득이 가능한 경우) 시스템 수준에서의 OS변조 탐지 및 보호기능 수행 (강화된 OS변조탐지, 입력,메모리보호, 화면캡처방지 등 다양한 기능을 수행할 수 있음)

Ⅳ. 결론

스마트폰 전자금융서비스는 현재, 위·변조 앱 설치, 제로데이 취약점 등을 이용한 관리자 권한 획득, 중요정보 유출, 키로깅, DDOS 등 금융거래 보안을 위협하는 요소들이 다양화되고 있다. 그 중에서도 스마트폰 전자금융서비스의 위·변조된 앱은 보안 기능의 무력화, 결제시스템 우회, 악성코드 삽입 후 배포 등의 위협을 증가시킬 수 있어 향후 개인정보 유출이나 금전적인 피해를 가져올 수 있다.

따라서 금융사가 안전한 스마트폰 뱅킹서비스 환경을 구축하고 제공하기 위해 본 논문에서 기술한 보호기술(앱 해시 검증 기능, 입력정보 및 통신구간 암호화, 네이티브 코드구현, 코드분석 보호, 중요 모듈 주기적 업데이트)들의 보호 수준, 구현 난이도 등을 고려하여 여러 가지 보호기술을 적용해서 앱 위·변조에 따른 위협에 대응하여야 할 것이다.

특히나 실행 프로그램과 이용자 입력 정보에 대한 무결성은 단일 보안 기능에 의존하여 구현 될 경우, 다양한 보안 위협에 노출 될 수 있음으로, 계층별 다양한 보안 기능을 함께 고려해야하며, 아울러 소프트웨어적인 방법을 통한 파일 무결성 검증 방법은 소프트웨어의 태생적 한계로 인해 지속적인 보안 취약성이 발견될 수 있음으로 최신 업데이트를 통한 소프트웨어 유지관리 등 침해사고 및 신기술을 대응하기 위한 노력을 해야 한다,

참고문헌

[1] 한국은행, *'2012년 3/4분기 국내 인터넷뱅킹서비스 이용현황'*, 2012. 11. 13.

[2] http://news.donga.com/3/all/20120320/44892193/1

[3] 금융보안연구원, *'모바일 앱 위변조 대응을 위한 보안기술 분석보고서'*, 2012.08

[4] ISO/IEC 27001 : Information technology - security techniques - information security management systems requirements.

[5] 금융보안연구원, *'프로그램 무결성 검증 기술 분석 보고서 V2.0'*, 금융부문 보안기술 동향 및 보안성 연구보고서, pp.105-121 2012.12

[6] 유동훈, Android 스마트 플랫폼 취약점 분석과 보안 위협, NetsecKR2012

[7] http://www.itworld.co.kr/news/72610

[8] TTA, *'가상 키보드 보안 요구 사항'*, 2011. 12. 21.

[9] 한국저작권위원회, *'스마트 기기를 통한 저작권 침해실태조사 및 대응 방안 연구보고서'*, 2011,12

〈著者紹介〉

최 지 선 (Jisun Choi)
2009년 8월 : 국민대학교 수학과 졸업
2011년 8월 : 국민대학교 수학과 석사
2011년 7월~현재 : 금융보안연구원 보안기술팀 연구원
관심분야 : 정보보호, 부채널 분석, 금융보안 분야

김 태 희 (Taehee Kim)
2010년 2월 : 서울여자대학교 정보보호학과 졸업
2010년 9월~현재 : 금융보안연구원 보안기술팀 연구원
관심분야 : 정보보호, 모바일 보안, 금융보안 분야

민 상 식 (Sangshik Min)
2009년 8월~현재 : 금융보안연구원 보안기술팀 팀장
관심분야 : 가상화 및 클라우드 컴퓨팅, 대용량 데이터 분석, 모바일 보안, HTML5, 소셜 네트워크 보안, 오픈뱅킹 보안

성 재 모 (Jaemo Seung)
정회원
1993년 2월 : 스트븐스공과 대학교 전산학 석사
2011년 2월 : 전남대학교 정보보호 박사
1993년 8월~2003년 8월 : LG 데이콤 정보보호기술팀 팀장
2003년 8월~2006년 10월 : KISA 인터넷침해사고대응지원센터 해킹대응팀 팀장
2006년 10월~현재 : 금융보안연구원 정보보안본부 본부장
관심분야 : 컴플라이언스, 정보보호 관리체계, 포렌식, 컴퓨터와 네트워크, 모바일 보안, 금융보안 분야