금보원 2010-08

금융부문 스마트폰 보안 가이드

2010. 12

금융보안연구원

본 가이드의 내용 중 오류가 발견되었거나, 내용에 대한 의견이 있을 경우 금융보안연구원 신기술분석센터(newtech@fsa.or.kr)로 해당 내용을 보내주시기 바랍니다.

머 리 말

최근 국내 스마트폰 활성화에 따라 모바일 오피스, SNS(소셜 네트워크 서비스), 포털 등 매우 다양한 서비스들이 스마트폰을 통해 제공되고 있으며 스마트폰의 편의성, 휴대성과 결합된 새로운 형태의 서비스들이 등장할 것으로 전망되고 있습니다. 이와 함께 금융부문 역시 스마트폰 기반의 다양한 전자금융서비스들을 출시하고 있으며 스마트폰의 장점을 활용한 편리하고 효율적인 서비스들을 제공하고 있습니다. 우리나라 스마트폰 전자금융서비스 이용자 수는 2010년 3/4분기 기준으로 130만 명을 돌파하여 2009년 대비 약 105배 증가하였으며 일평균 스마트폰 전자금융 거래 건수는 104만 8000건으로 2009년에 비해 약 55배 증가하는 등 빠른 속도로 발전하고 있습니다.

하지만 이러한 발전과 함께 스마트폰 보안에 대한 위협과 우려도 매우 급속히 증가하고 있습니다. 특히 스마트폰 전자금융서비스에 대한 보안은 금융기관과 금융서비스 이용자의 자산에 직접적인 영향을 미칠 수 있으므로 더욱 큰 관심과 주의가 요구됩니다. 따라서 스마트폰 전자금융서비스에서 발생 가능한 위협과 대응방안, 신규 취약성 등 보안에 대한 연구가 필요한 상황입니다.

이에 금융보안연구원은『금융부문 스마트폰 보안 가이드』를 개발하게 되었습니다. 이 가이드가 안전한 전자금융서비스 환경을 구현하고 제공하는 데 많은 도움이 되길 바라며 본 가이드를 작성하는데 도움을 주신 전문가 분들과 우리원 직원들에게 감사를 드립니다.

2010년 12월
금융보안연구원
원장 곽 창 규

차례

금융부문 스마트폰 보안 가이드

그림

금융부문 스마트폰 보안 가이드

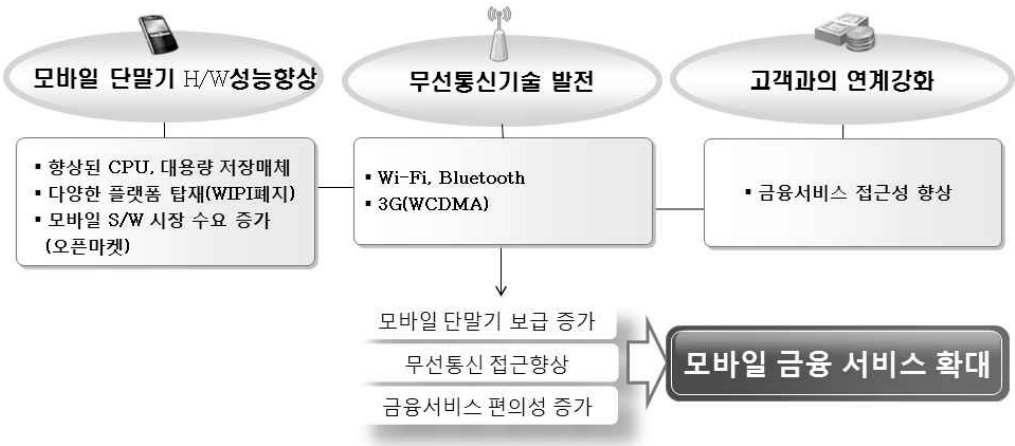
표

금융부문 스마트폰 보안 가이드

제1장 개 요

제 1 절 배 경

한국형 표준 모바일 플랫폼인 위피(WIPI - Wireless Internet Platform for Interoperability) 탑재 의무화가 폐지(2009.04월)된 이후 윈도우 모바일(MS社), 안드로이드(Google社), 아이폰(Apple社)과 같은 스마트폰 플랫폼의 보급이 확산되고 이용자 수가 급속히 증가하고 있다.



스마트폰을 이용한 모바일 금융서비스는 시간적, 공간적 제약 없이 금융거래를 이용할 수 있어 그 수요가 증대되고 있으며 금융사에는 단순히 이용자 편의성을 위한 서비스 차원을 넘어 비즈니스 기회를 확대할 수 있는 기회 수단으로 인식되고 있기 때문에 다양한 스마트폰 금융서비스들이 도입되고 있는 상황이다.

제 2 절 목 적

스마트폰 전자금융서비스의 확산에 따라 이러한 환경에서 발생 가능한 보안 위협 및 보안 고려사항의 연구가 요구되고 있다. 이를 위해 스마트폰 플랫폼별 특징, 국내 전자금융서비스의 구성, 스마트폰 전자금융서비스 보안 기준 등에 대해서 분석하고 이를 통해 발생 가능한 보안위협과 그 대응방안을 제시하고자 한다.

본 가이드에서는 스마트폰 플랫폼별 특징을 분석하여 스마트폰 전반에 대한 위협을 형태별로 구분하고 이에 대한 대응방안 및 스마트폰 금융서비스 도입과 운영 간에 고려해야 할 보안 고려사항을 기술한다.

제 3 절 범 위

본 가이드는 현재 금융권에서 운영 중인 스마트폰 전자금융서비스 구성과 방식을 대상으로 작성되었으며 연구범위는 서비스 구성 및 특징 분석, 위협 도출, 대응방안 및 고려사항 제시를 포함하고 있다. 대응방안 및 주요 보안 고려사항은 스마트폰 전자금융서비스 제공자들을 대상으로 한다.

제2장 스마트폰 전자금융서비스 현황

제 1 절 모바일 뱅킹 동향

1. 해외 모바일 뱅킹 시장 현황

해외 모바일 뱅킹 시장은 단말기 기술발전과 함께 지속적으로 이용자가 증가하고 있으며 서비스가 다양해지고 신뢰도가 증가하면서 시장규모 역시 매우 빠르게 성장할 것으로 전망되고 있다. 영국의 시장조사 기관인 Juniper Research의 조사 결과에 따르면, 전 세계 모바일 금융 시장은 2009년 이후 시장 규모가 급격히 성장할 것으로 보인다고 발표했다.

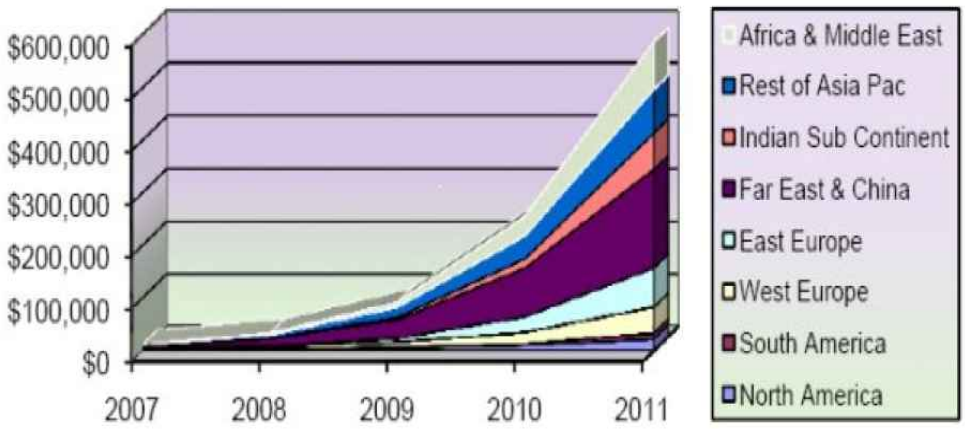


그림 1 전 세계 모바일 금융서비스 시장 전망 (거래규모기준, 단위 : 백만 달러)

출처 : Juniper Research, 2007-2011, 2008. 1

또한 2011년 전 세계 모바일금융 이용자가 6억 1200만 명에 이르고, 거래 금액은 총 5,890억 달러에 이를 것으로 전망하였다. 모바일 결제 서비스 시장도 2011년에 2억 400만 명의 이용자와 220억 달러의 거래규모를 가질 것으로 전망하고 있다.

2. 국내 모바일 뱅킹 시장 현황

국내 모바일 뱅킹 시장은 WAP 뱅킹, VM 뱅킹, 스마트카드 뱅킹 등 다양한 서비스들이 출시되면서 지속적으로 증가해 왔다. 특히 2010년 1/4 분기를 기점으로 스마트폰을 이용한 다양한 금융서비스들이 출시되면서 이용 고객수와 거래량이 급격히 증가하였으며 그 증가세가 더욱 가속화되고 있다. 한국은행 조사 자료에 따르면 모바일 뱅킹 등록 고객 수는 2010년 3/4분기 기준 1,432만 명이며 이 중 스마트폰 기반 모바일 뱅킹의 고객수가 137만 명을 넘은 것으로 집계되고 있다. 스마트폰 기반 모바일 뱅킹 이용건수는 일평균 105만 건이며 거래 금액은 483억 원으로 전 분기(2/4)대비 각각 368.6%, 297.5% 증가한 것으로 나타났다.

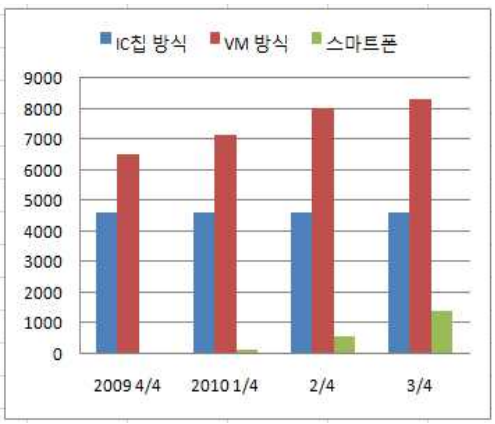


그림 2 모바일 뱅킹 등록고객 수 (단위: 천명)

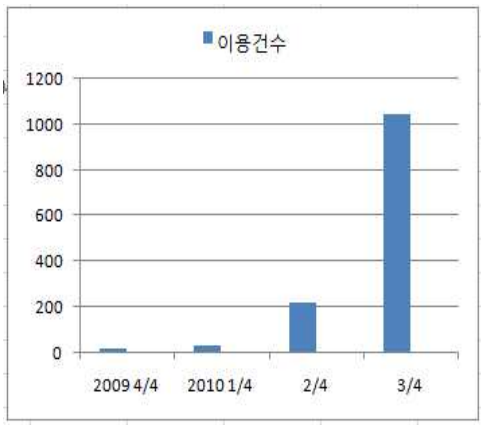


그림 3 스마트폰기반 이용 건수 (일일, 천건)

국내 스마트폰 보급은 2010년을 기점으로 높은 성장세를 지속할 것으로 전망되고 있으며 스마트폰 확산과 함께 스마트폰기반 금융서비스 이용자가 지속적으로 증가할 것으로 예상되고 있다. 이러한 이용자 증가에 따라 국내 금융기관들이 스마트폰기반의 서비스를 신규 출시하고 있으며 전자금융서비스 뿐만 아니라 각종 편의 정보제공, 증강현실 기술과 결합하는 등 다양한 형태의 서비스들을 제공할 예정이다.

제 2 절 모바일 전자금융서비스 발전 과정

국내 모바일 뱅킹 서비스는 단말기의 발전과 다양한 통신기술의 등장으로 WAP(Wireless Application Protocol) 방식, 스마트카드(Smart Card)를 이용한 방식, 그리고 VM(Virtual Machine) 방식을 거쳐 현재의 스마트폰 전자금융서비스까지 지속적으로 변화해 왔다.

1. WAP 방식 모바일 뱅킹

WAP(Wireless Application Protocol)방식은 모바일 금융서비스 초기 구현방식으로 휴대폰의 무선 인터넷서비스를 통해 이동통신사가 제공하는 서비스에 접속하여 각종 금융서비스를 이용하는 방식이다. 이는 한미은행과 SKT에 의해 시작되어 1999년 이후 이동통신 3사가 문자 메시지 서비스를 이용해 계좌정보, 주식 등의 조회서비스만 가능한 서비스를 출시하고 본격화함에 따라 2000년부터 국내은행들과 제휴하여 모바일 뱅킹 서비스가 활성화되었다. 그러나 접속시간이 길고 처리속도가 느리며 이용절차가 복잡하다는 단점을 가지고 있다.

2. VM 방식 모바일 뱅킹

VM(Virtual Machine)방식은 기존 무선인터넷서비스 이용방식에서 탈피하여 은행별로 제공되는 금융서비스를 위한 WIPI기반 전용프로그램을 고객이 소유한 휴대폰으로 다운받은 후, 해당 프로그램을 실행시켜 해당 은행 사이트에 접속한 뒤 계좌조회 및 이체 서비스 등을 이용할 수 있는 방식을 말한다. [그림 4]와 같이 다양한 서비스가 제공가능해지면서 모바일 전자금융서비스가 보편화하는데 큰 역할을 해왔다.

그림 4 VM 방식의 모바일 금융서비스

3. 스마트카드 방식 모바일 뱅킹

스마트카드(Smart Card)방식은 IC & USIM칩 뱅킹이라고도 하며 은행에서 고객정보를 저장하여 발행한 IC칩을 고객의 휴대폰에 탑재하여 사용하는 방식으로 기존 방식보다 사용의 편의성과 보안성을 향상시켰다는 평을 받고 있다. 이는 2003년 9월 LGT의 Bank-On 서비스에 의해 시작되었으며, 현재는 3G 단말기의 보급과 함께 USIM(Universal Subscriber Identification Module)을 이용하는 방식이 대세를 이루고 있다.

스마트카드 방식의 모바일 금융서비스는 3G 방식 단말기 보급이 확대됨에 따라 기존의 CDMA와는 달리 이동통신 가입자의 인식/인증이 가능해지면서 보다 다양한 서비스를 지원할 수 있어 앞으로 USIM을 이용한 모바일 금융서비스가 크게 발전할 것으로 보인다.

제 3 절 스마트폰 전자금융서비스

1. 서비스 현황

스마트폰을 이용하는 전자금융서비스는 2009년 국내 스마트폰의 확산에 따라 시작되어 2010년 1/4분기를 기점으로 은행, 증권, 카드 등 고객을 대상으로 금융서비스를 제공하는 다수의 금융기관들이 서비스를 확대하고 있다.

표 1 스마트폰 전자금융서비스 제공 현황(2010.10.25 기준)

금융사	은 행	증권·선물	카 드	보 험
서비스 현황	18개사	28개사	5개사	4개사

※ 금융보안연구원 회원사 대상

스마트폰 전자금융서비스는 기존에 PC기반으로 웹사이트를 통해 이용하던 전자금융서비스를 대부분 유사한 형태로 제공하고 있으며 이용자들은 스마트폰을 통해 다음과 같은 금융서비스를 이용할 수 있다.

○ 뱅킹(계좌 조회, 이체, 대출 서비스 등) 서비스
○ HTS(주식 시세조회, 주식 매매 등) 서비스
○ 카드결제금액 조회, 현금서비스
○ 보험계약 조회, 사고조회, 긴급출동 요청
○ 카드결제 서비스, 소액결제 서비스 등

국내에서 사용 가능한 스마트폰은 아이폰, 안드로이드, 윈도우 모바일, 블랙베리 등이 있으며 현재 이들 중 아이폰, 안드로이드, 윈도우 모바일에 대해서 전자금융서비스가 제공되고 있다.

표 2 스마트폰 별 국내 전자금융서비스 제공 여부

스마트폰	제조사	전자금융 지원	비 고
아이폰	Apple	O	단일 제조사
안드로이드	Google	O	OS개방으로 다양한 제조사 지원
윈도우 모바일	MS	O	2010년 말 윈도우 모바일 7 출시 예정
블랙베리	RIM	X	낮은 국내 점유율
심비안	NOKIA	X	

2. 서비스 이용 절차 및 인증방식

스마트폰 기반의 전자금융서비스 이용을 위해 이용자는 먼저 전자금융 어플리케이션을 스마트폰에 설치하게 된다. 이용자는 설치된 어플리케이션을 실행하여 3G망 또는 WiFi망을 통해 금융기관 서버에 접속하게 되고, 로그인 정보(아이디/패스워드/공인인증서)를 통해 인증절차를 거치게 된다. 인증 후에는 조회 및 거래 서비스를 이용하고 이체, 주식매매 등의 서비스에서는 보안카드, OTP와 같은 추가적인 인증수단을 이용하여 거래를 진행한다.

스마트폰 전자금융서비스는 스마트폰으로 플랫폼이 변화하였지만, 인증방식은 기존의 PC 기반의 인터넷 뱅킹과 동일한 형태와 수준의 인증방식을 채택하여 사용하고 있다.

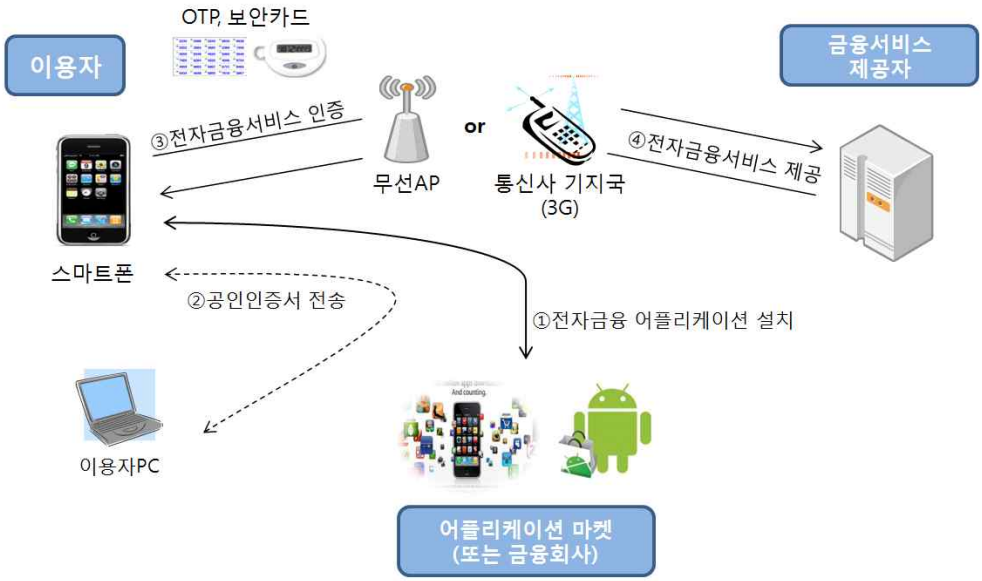


그림 5 스마트폰 전자금융서비스 이용 절차

표 3 스마트폰 전자금융거래 인증 수단

분류	접속 및 조회	이체 및 거래 서비스	공인인증서 이동 및 복사
뱅킹	공인인증서, (아이디/패스워드)	계좌비밀번호, 보안카드(또는 OTP), 공인인증서	PC에 저장된 공인인증서를 스마트폰으로 전송 (Wi-Fi / 3G)
주식거래			
보험		-	
카드		공인인증서, 카드정보(카드번호, 유효기간, CVC 등)	

※ 금융사에 따라 인증방법이 일부 추가될 수 있음

이용자가 접근하는 서비스의 종류에 따라 요구하는 인증의 수준이나 방식이 차이가 발생할 수 있으며 공인인증서를 이용할 경우에는 이용자의 PC에 저장된 인증서를 스마트폰으로 전송하여 이용하고 있다.

금융감독원이 2010년 1월 7일 발표한 “스마트폰 전자금융 안전대책”에 포함된 이용자 가입 및 인증절차는 다음과 같다.

{금융감독원 스마트폰 전자금융 안전대책}

2. 안전대책

가. 전자금융거래 부문

1 다단계 가입자확인*을 통해 전자금융서비스 가입절차를 강화

* 1단계 확인(ID·비밀번호 등) → 2단계 확인(일회용비밀번호 등) → 3단계 확인(공인인증서 등)

2 스마트폰 전자금융서비스 가입시 이용자 유의사항 안내 후 가입허용

3 로그인시 공인인증서를 사용하거나, ID·비밀번호 외에 일회용비밀번호(보안카드 포함)를 추가로 적용*하는 등 사용자 인증강화

* 이중요소 인증 (two-factor authentication) 적용

4 PC 인터넷뱅킹의 전자자금이체시 적용되는 거래인증방법(계좌비밀번호, 일회용비밀번호, 전자서명)과 보안등급별 자금이체한도를 적용

3. 서비스 구성

스마트폰을 이용한 서비스 구성방식은 크게 웹 방식, 어플리케이션 방식, 웹·어플리케이션 혼용방식으로 구분된다. 웹 방식은 스마트폰에 탑재된 웹 브라우저를 통해 서비스를 제공하는 방식이며 어플리케이션 방식은 서비스 전용 어플리케이션을 통해 서비스를 제공하는 방식이다. 혼용방식은 서비스 요청과 같은 트랜잭션은 웹 프로토콜을 이용해 처리하고 이용자 화면 구성(UI)등의 일부 기능을 어플리케이션으로 구성하는 방식이다. 국내 금융기관에서

제공하는 스마트폰 기반 전자금융서비스는 대부분 어플리케이션 방식이나 웹·어플리케이션 혼용방식으로 서비스를 제공하고 있다.(일부 카드결제 서비스의 경우 웹 브라우저를 통해 서비스 제공)

웹 브라우저 기반 서비스는 암호화 적용시 대부분 SSL을 적용하고 별도의 보안 모듈을 이용하지 않지만 어플리케이션 기반 전자금융서비스는 어플리케이션 내에 자체적인 데이터 암/복호화, 전자서명/인증 모듈을 포함하고 있으며 가상키보드와 같은 보안 모듈이 추가적으로 포함되는 형태로 구현되어 있다.

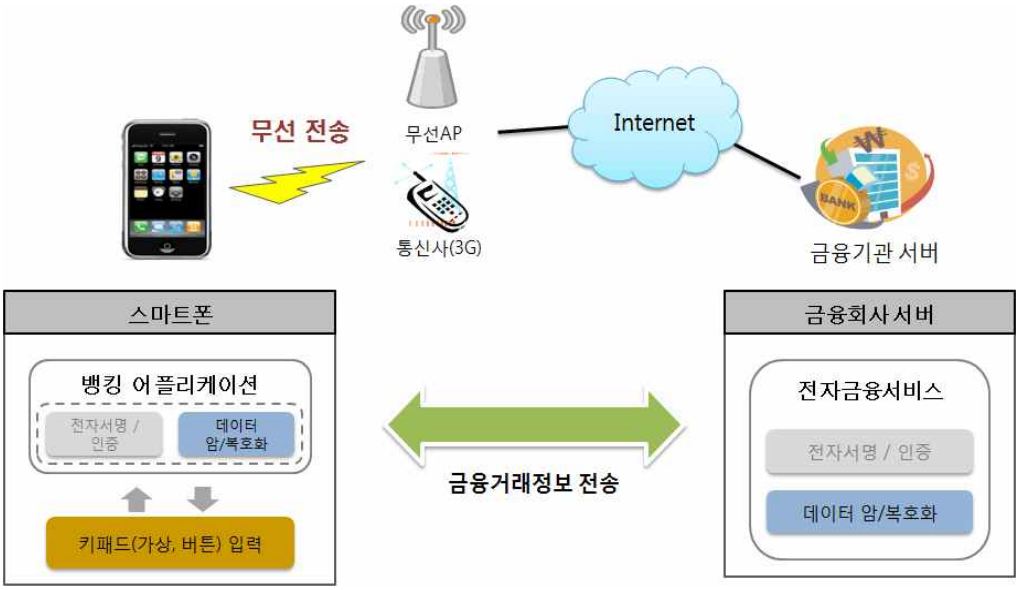


그림 6 어플리케이션 기반 전자금융서비스 구성

웹·어플리케이션 혼용방식은 금융거래정보의 전송과 데이터 처리는 웹 방식을 이용하며 스마트폰 어플리케이션에서는 어플리케이션방식과 동일하게 각종 보안 모듈들이 연동되어 동작한다. 혼용방식으로 서비스를 구성할 경우 스마트폰에는 뷰어로 동작하는 어플리케이션이 설치되기 때문에 클라이언트 프로그램 자체의 기능변경이나 업데이트를 최소화 시킬 수 있다.

제3장 스마트폰 플랫폼별 특징

제 1 절 윈도우 모바일(Windows Mobile)

1. 윈도우 모바일 개요

윈도우 모바일은 Microsoft社가 개발한 모바일용 운영체제로 초창기에는 포켓PC(PocketPC)라는 이름으로 알려지다가 2003년부터 윈도우 모바일이라는 이름으로 배포되기 시작했다. 윈도우 모바일은 Core OS인 윈도우 CE를 기반으로 제작되었다. 2010년 기준 6.5 버전이 주로 배포되고 있으며 2010년 말에 윈도우 모바일 7 버전이 스마트폰에 탑재되어 일반에 판매될 예정이다. 윈도우 모바일은 다음과 같은 구조로 되어 있다.

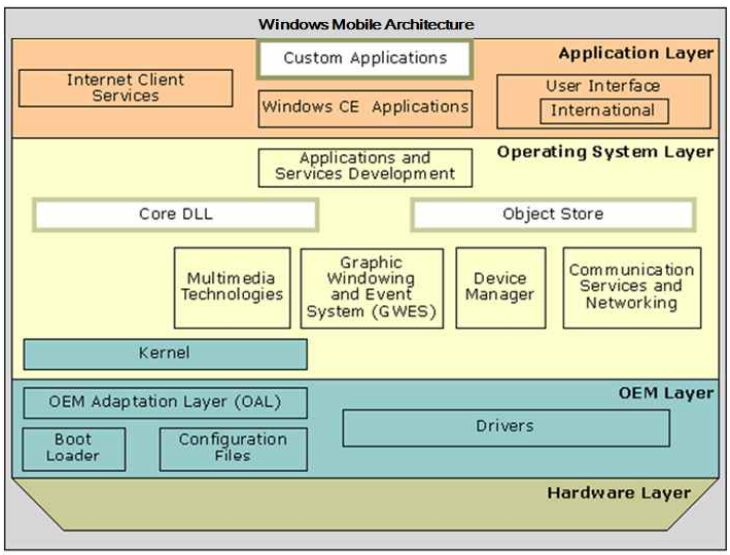


그림 7 윈도우 모바일 플랫폼 구조

○ **Hardware Layer** : 스마트폰의 물리적 장치영역으로서 CPU, 입력포트, 메모리 카드, ROM, Timer 등으로 구성

○ **OEM Layer** : 하드웨어 드라이버, 부트로더 등 하드웨어와 OS 커널의 중간에 존재하여 OS와 소프트웨어의 중간매개 역할을 수행

○ **OS Layer** : 운영체제 영역(커널)에 해당하며 파일시스템관리, 응용프로그램의 이벤트, 메시지처리, 서비스관리를 비롯하여 응용프로그램에서 사용하는 시스템 라이브러리를 제공

○ **Application Layer** : 응용프로그램 영역으로서 사용자 화면(UI)을 구성하고 각종 어플리케이션이 사용자와 상호작용 하는 역할을 수행하는 영역

2. 윈도우 모바일 어플리케이션 배포방식

윈도우 모바일의 어플리케이션 유통은 파일형태로 온라인(홈페이지)으로 배포되거나 통신사 마켓(SKT T스토어, KT 쇼앱스토어 등)을 통해 배포된다. 어플리케이션 검증은 개발이나 등록과 관련된 별도의 검증절차가 없으며 어플리케이션 설치시 설치 여부를 이용자에게 확인하는 검증절차만이 존재한다.

표 4 윈도우 모바일 어플리케이션(APP) 배포 방식

항 목	내 용
APP 유통	▪ 사용자 간 배포(개발자 ↔ 사용자) ▪ 기업(금융기관 등) 및 오픈마켓 ↔ 개인
APP 설치	▪ PC연결 및 Web 다운로드를 통한 설치 ▪ 설치파일: CAB 확장자
APP 검증	▪ APP 설치 시, 설치 여부 확인 ※ 개발, 등록관련 검증절차 없음

그림 8 어플리케이션 설치여부 확인

3. 윈도우 모바일 보안

윈도우 모바일은 현재 국내에서는 6.5 버전까지 제공되고 있으며 2010년 말에 윈도우 모바일 7을 탑재한 스마트폰을 출시예정이므로 6.5 버전을 기준으로 특징 및 보안장치에 대해 알아본다.

윈도우 모바일의 특징은 멀티태스킹을 지원하고 시스템에 대한 개방성으로 자원접근에 대한 제약이 없으며 어플리케이션 설치와 배포가 자유롭다는 점을 들 수 있다.

표 5 윈도우 모바일 플랫폼 특징

분 류	멀티태스킹	자원(파일, 메모리 등)접근	어플리케이션 검증	
			설치, 실행 검증	배포 검증
윈도우 모바일	지원	제약없음	설치여부만 검증	없음

이러한 특징과 함께 윈도우 모바일은 자체적으로 몇 가지 보안 기능을 제공하고 있다. 윈도우 모바일은 사용자가 설정한 패스워드를 이용해 장치 전체에 대한 잠금 기능을 설정할 수 있도록 장치 잠금(Device Lock)을 제공함으로써 장치의 안전성을 보장한다. 또한, 장치 초기화(Device Wipe), 데이터 암호화(Data Encryption), 그리고 인증서 지원(Certificate Support) 기능을 제공한다. 사용자들은 기기 진단, 수리 또는 기기를 도난당하거나 분실했을 때 잠금(Lock)장치를 걸거나 데이터를 지워버림으로써 자신의 정보를 관리할 수 있다.

○ **장치 잠금(Device Lock) :** 장치 잠금이란 사용자가 패스워드를 설정해 장치 전체에 대한 잠금 설정을 할 수 있는 기능이다. 장치 잠금 기능은 장치 잠금을 설정하는 패스워드 혹은 PIN에 대한 관리를 주 기능으로 하는데 패스워드/PIN 만료 기한(Expiration) 관리 기능, 히스토리 관리 기능을 제공하며, 번호 설정 방식에 제한을 두어 쉽게 알아낼 수 없도록 강한 PINs(Personal Identification Numbers)를 사용한다. 만료 기한 관리 기능은 사용자의 패스워드 혹은 PIN이 주기적으로 변경되도록 관리하는 기능이다.

○ **데이터 암호화(Data Encryption) :** 윈도우 모바일은 로컬 데이터에 대한 암호화는 지원하지 않는다. 따라서 로컬 데이터에 대한 암호화가 필요한 경우에는 별도의 소프트웨어를 활용해야 한다. 대신 모바일 기기에 장착하는 메모리 카드에 대한 암호화 기능을 제공하는데, AES 혹은 RC4를 이용해 암호화를 하도록 설정되어 있다.

○ **인증서 지원(Certificate Support) :** 윈도우 모바일은 인증서 다운로드 및 등록, 관리할 수 있도록 지원하나 국내의 PKI 시스템과는 연동이 되지 않아 별도의 기술을 필요로 한다.

○ **장치 초기화(Device Wipe) :** 장치 초기화란 장치의 데이터에 대한 부적절한 접근을 막기 위한 방법으로 장치의 메모리를 지우는 것이며 윈도우

모바일은 로컬 장치 초기화(Local Device Wipe)와 원격 장치 초기화(Remote Device Wipe) 기능을 제공한다. 로컬 장치 초기화는 장치 잠금 해제를 위한 패스워드 또는 PIN을 입력할 때 연속적으로 입력을 실패하는 경우 로컬 메모리를 모두 지우는 방법이다. 그리고 원격 장치 초기화는 기기를 분실 또는 도난 되거나 기기를 직접 초기화하기 어려운 상황일 때 장치를 초기화 하는 방법으로 SecureWipeAllVolumes Api를 사용해 원격에서 모바일 기기에 접속해 데이터를 삭제하는 기능을 제공한다.

그림 9 로컬 장치 초기화

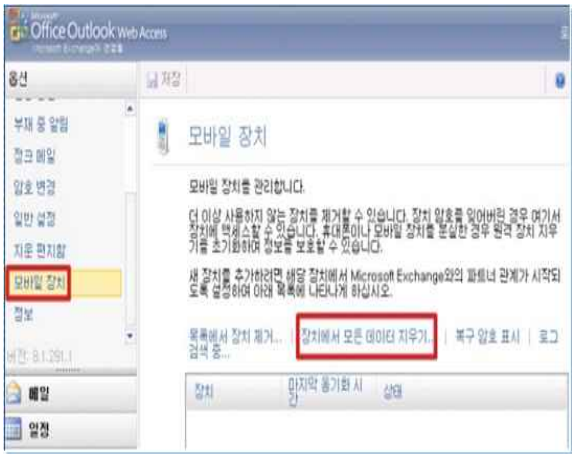


그림 10 원격 장치 초기화

윈도우 모바일은 기본적으로 PC의 윈도우와 유사한 시스템운영방식을 채택하고 있다. OS관리에 있어서 이벤트를 이용한 메시지 처리, 멀티 프로세스, 시스템 권한관리 등이 유사하기 때문에 기존에 PC에서 나타났던 메시지 후킹, 키로깅, 악성코드 등 대부분의 위협들이 윈도우 모바일에서 동일하게 적용될 수 있다.

제 2 절 아이폰(iPhone OS)

1. 아이폰 개요

아이폰 OS는 2007년 Apple社가 Mac OS X를 기반으로 개발한 OS로 아이폰 및 아이팟터치(iPod Touch)에 탑재되는 하는 모바일 플랫폼이다. 윈도우 모바일과 안드로이드가 플랫폼과 하드웨어 단말기 제조사가 다르게 유통되는 것과 달리 하드웨어 단말기도 Apple에서 통합 생산하고 있다.

2008년 6월에 아이폰 OS 상에서 소프트웨어를 개발할 수 있는 도구인 SDK가 공개되면서, 2.0 버전부터는 Apple의 앱스토어를 통해 자유롭게 사용자 어플리케이션을 공개하고 판매하는 것이 가능해졌다. Apple은 이미 아이팟과 아이튠스(iTunes)를 중심으로 다수 이용자와 개발자를 확보하고 있었으며 이로 인해 스마트폰 플랫폼 중 가장 많은 어플리케이션을 보유하고 있다.

아이폰 OS는 다음과 같은 기술 레이어로 구현되었다.

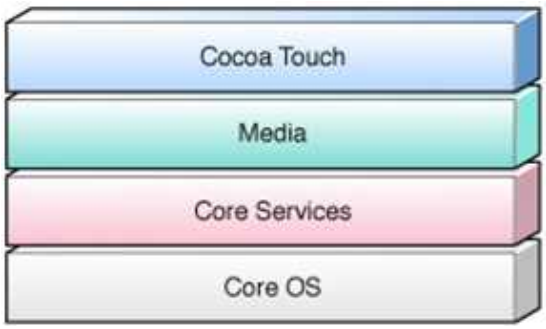


그림 11 iOS technology layers

○ **Cocoa Touch Layer :** 최상위 레이어로서 어플리케이션에 필요한 프레임 워크를 제공하고 있으며 각종 UI, 통지, 맵, 이벤트, 그래픽의 인터페이스(Object-C)를 제공한다.

○ **Media Layer** : 그래픽, 오디오, 비디오에 관련된 기술 프레임워크를 제공

○ **Core services Layer** : 주소록접근, 어플리케이션 데이터관리, GPS, Cell, Wi-Fi와 데이터베이스(SQLite) 및 앱스토어 관련 서비스를 제공

○ **Core OS** : 네트워크 프로토콜, 외부장치 통신, 어플리케이션 데이터보안 서비스를 제공하고 있으며 궁극적으로 시스템 커널과 관련된 기능(프로세스, 메모리, IO, 파일시스템 관리)을 제공

※ 아이폰 OS Kernel: Mach Kernel의 변형된 구조로서 BSD기반 유닉스를 모티브로 하고 있음

2. 아이폰 어플리케이션 배포방식

아이폰의 어플리케이션 배포는 Apple 앱스토어로 일원화 되어 있으며 다른 배포방식은 허용하고 있지 않다.(해킹된 어플리케이션 제외) 어플리케이션을 이용자들에게 배포하기 위해서는 앱스토어의 검증을 거쳐야 하며 이러한 검증과정에서 비정상 API를 이용하거나 제공되는 콘텐츠에 문제가 있는 경우 등록을 허용하지 않고 있다.

표 6 아이폰 어플리케이션(APP) 배포 방식

항 목	내 용
APP 유통	▪ 개발자→Apple 심사(검증)→앱스토어 등록→사용자
APP 설치	▪ 앱스토어 및 아이튠즈를 이용한 설치 ▪ 설치파일: IPA 확장자
APP 검증	▪ 코드서명된 APP만 설치 및 실행가능

3. 아이폰 보안

아이폰은 다른 스마트폰 플랫폼에 비해 상대적으로 폐쇄적인 운영정책을 가지고 있으며 일원화된 어플리케이션 배포, 멀티태스킹 미지원(제한적 지원), 시스템 자원 접근 금지와 같은 특징을 가지고 있다.

표 7 아이폰 플랫폼 특징

분 류	멀티태스킹	자원접근	어플리케이션 검증	
			설치, 실행 검증	배포 검증
아이폰	제한적 지원[1]	접근불가	앱스토어를 통한 설치만 가능	앱스토어 검증

이러한 폐쇄적인 정책으로 아이폰과 관련된 보안 이슈는 주로 플랫폼 변조(Jail Break)와 관련된 것이 주를 이뤘다. 아이폰이 출시되고 얼마 지나지 않은 2007년 7월, 아이폰에 대한 변조 방법이 처음으로 알려지면서 Apple에서 공급하는 유료 어플리케이션을 불법으로 무료 사용하는 것이 가능해졌다. 이후 2008년, Apple은 이를 보완한 새로운 버전의 아이폰 OS 버전 2.0을 발표하였으나 이 역시 변조 도구가 배포 되었으며, 최근 발표된 최신 4.1 버전 역시 출시된 지 한 달여 만에 변조 도구가 발표되었다.

과거 아이폰의 특징에 따라 상대적으로 다른 플랫폼에 비해 안전한 것으로 알려졌으나 최근 알려지지 않은 PDF 열람 취약점을 이용하여 플랫폼 변조를 진행하는 툴이 배포되는 등 보안에 대한 이슈가 제기되고 있다.

1) OS 4.0이후 지원되기 시작하였으나 실행되는 어플리케이션에서 멀티태스킹을 지원하도록 개발해주어야 하는 등 제약사항이 존재함

그림 12 PDF 취약점을 이용한 플랫폼 변조 기법

아이폰은 보안을 위해 취약점 발생시 OS 업데이트를 통해 취약성을 해결하고 배포되는 어플리케이션의 안전성 확보를 위해 코드 서명 기법을 이용하고 있다.

○ **취약점 패치 :** 아이폰은 Core OS 위에 Core Service 단계가 있고 그 위에서 어플리케이션이 실행된다. 아이폰은 보안을 위해 Core Service 단계에서 Security API를 제공하는데 각 Security API는 Core OS 단계의 서비스에 기반을 두고 있고 OS 업데이트를 통해 플랫폼 취약성을 해결하고 있다.

○ **코드 서명(Code Sign) :** 아이폰은 개발 도구들이 배포되어 사용자들이 직접 어플리케이션을 개발할 수 있으므로 개발된 어플리케이션의 안전성과 보안성에 대한 점검이 반드시 필요하다. 이를 위해 코드 서명 방법을 주로 사용하는데 코드 서명이란 실행 파일이 정당한 개발자에 의해 제작되어 위변조 되지 않았음을 확인하기 위해 파일 코드를 개발자가 서명 하는 것을 말한다. 아이폰은 코드 서명을 통해 부적절한 개발자가 어플리케이션을 조작하여 바이러스나 악성 소프트웨어를 실행시키는 것을 방지하며 불법 복제를 차단할 수 있다.

제 3 절 안드로이드(Android)

1. 안드로이드 개요

안드로이드는 Google社에 의해 개발된 모바일 전용 플랫폼으로 2007년 11월 초 OHA(Open Handset Alliance)에서 발표되었고 곧바로 안드로이드 SDK가 공개 배포되었다. 2008년 9월 말에는 Ver 1.0 SDK Release 1이 배포되었으며, 2008년 10월에는 안드로이드 전체 소스가 공개되었다.

Google이 발표한 안드로이드 플랫폼은 다음 그림과 같은 구조를 가지고 있다.

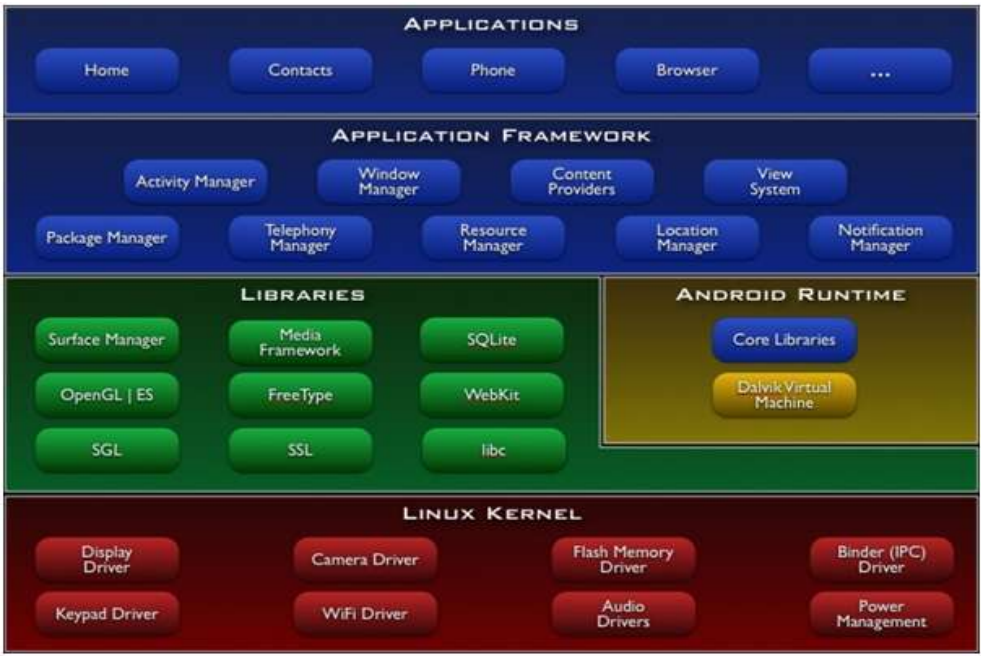


그림 13 안드로이드 플랫폼 구조

안드로이드에서 필수 응용프로그램들은 어플리케이션 계층에 기본적으로 탑재되어 있고, 모든 응용프로그램은 Java 코드로 작성되어 Dalvik VM(구글이

자체 개발한 가상머신)상에서 동작한다.

○ **Applications** : email, SMS, calender, map, browser, contacts를 포함한 각종 응용프로그램을 포함

○ **Application Framework** : 공유자원, 응용프로그램의 라이프 사이클 및 접근, 사용자 통지(Notification), 응용프로그램 활성(Activity) 관리 지원

○ **Libraries** : C/C++ 기반 라이브러리, 멀티미디어 라이브러리, SQLite 데이터베이스엔진 등 어플리케이션에 필요한 라이브러리를 제공

○ **Android Runtime** : 안드로이드 어플리케이션의 각각의 프로세스는 Dalvik 가상머신 상에서 동작하며 JAVA 언어의 핵심라이브러리를 포함

○ **Linux Kernel** : Linux 2.6버전을 기반으로 보안, 메모리, 프로세스, 네트워크 및 각종드라이버를 포함

2. 안드로이드 어플리케이션 배포방식

안드로이드의 어플리케이션 배포는 마켓을 통한 배포와 설치 파일을 온라인(웹사이트, 개인)으로 배포하는 방식을 지원한다. 현재 안드로이드 마켓에서는 소스코드에 대한 특별한 검증 절차가 진행되지 않고 있으나 어플리케이션 설치시 코드 사인이 되지 않은 어플리케이션을 설치되지 않도록 제한하고 있다.

표 8 안드로이드 어플리케이션(APP) 배포 방식

항 목	내 용
APP 유통	▪ 개발자↔사용자 ▪ 개발자↔오픈 마켓↔사용자
APP 설치	▪ 안드로이드 마켓 ▪ 설치파일: APK 확장자
APP 검증	▪ 설치 APP의 접근 영역 및 권한을 사용자에게 통지하여 사용자가 승인한 경우 설치가능

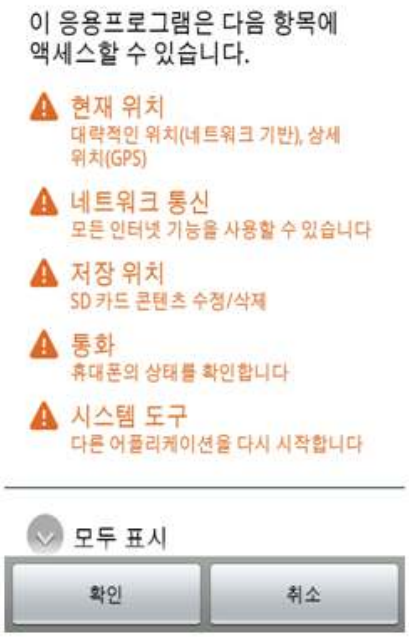


그림 14 어플리케이션의 접근 영역 및 권한 통지

3. 안드로이드 보안

표 9 안드로이드 플랫폼 특징

분 류	멀티태스킹	자원접근	어플리케이션 검증	
			설치, 실행 검증	배포 검증
안드로이드	지원	접근불가 (샌드박스)	등록 및 설치시 코드사인 검증	

안드로이드는 보안을 위한 도구로 허가(Permission)를 기반으로 하는 샌드박스(Secure Sandbox)시스템을 채택, 사용하고 있다. 시스템 커널은 Linux 계열을 사용하기 때문에 안드로이드 응용프로그램의 권한 및 접근 영역이 분리되어 운영된다. 안드로이드 상의 어플리케이션은 허가된 영역 외에 악의적인 결과를

일으킬 수 있는 어떠한 행위에 대해서 기본적으로 허용하지 않는다. 따라서 어플리케이션은 허가를 얻기 전까지 이용자의 개인 정보(전화번호부, 이메일 등)에 대한 읽기/쓰기를 비롯하여 플랫폼에 구동중인 다른 어플리케이션 파일에 대해서도 읽기/쓰기가 거부되며, 네트워크 접근, 장치 작동 등의 어떠한 작업도 수행할 수 없다.

추가적인 보안 기능으로 악성코드, 변조된 어플리케이션의 배포와 설치를 방지하기 위해 코드 사인을 통한 검증절차를 가지고 있다. 하지만, 이러한 검증절차가 개발자 식별을 주목적으로 하며 실제 악성코드나 변조된 어플리케이션 여부를 확인하지 않고 등록하고 있기 때문에 출처 확인 수준의 검증이라고 볼 수 있다. 또한, 어플리케이션의 코드 사인을 다른 사인으로 교체하여 배포할 수 있는 셀프사인(Self Sign) 취약점이 알려져 있으므로 출처 확인 절차의 우회가 가능하기 때문에 이에 대한 보안 문제가 제기되고 있다.

제4장 스마트폰 전자금융서비스 보안위협

제 1 절 개 요

스마트폰 전자금융에 대한 보안 위협은 공격 유형에 따라 다양한 형태로 분류될 수 있다. 본 연구에서는 위협이 발생되는 근원적인 시점에 따라 공격 모델을 정의하여 크게 스마트폰 시스템 위협, 이용자 중요정보 위협, 악성코드 및 피싱 위협, 네트워크 전송구간 위협 및 물리적 위협으로 정의하였다. 각 위협은 아래와 같이 구체적인 위협형태로 세분화 할 수 있다.

그림 15 스마트폰 전자금융 보안 위협 분류

스마트폰 기반 전자금융서비스는 어플리케이션 마켓이나 금융기관에서 전자금융 어플리케이션을 배포/설치, 스마트폰에서 전자금융어플리케이션 실행, 금융기관 서버와 통신을 통해 서비스를 이용하는 구간으로 구분할 수 있다. 각 구간에 대해 위에서 나열한 세부 위협들을 적용시키면 구간별로 발생 가능한 위협들을 확인할 수 있다.

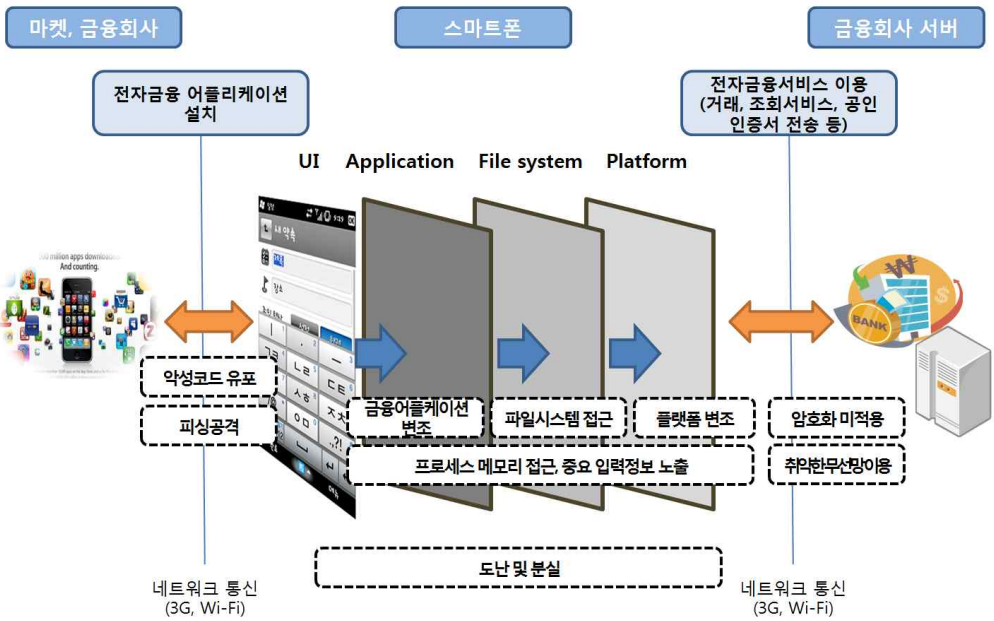


그림 16 각 구간별 발생가능 위협

위 위협들 중 대부분 PC와 유사한 위협들이 발생되는 것을 알 수 있다. 현재 스마트폰 전자금융서비스 방식이 기존 PC 기반 금융서비스와 유사하며 제공되는 인증 및 보안 수단들이 동일한 방식을 이용하기 때문에 비슷한 형태의 위협들이 발생 가능하다.

제 2 절 스마트폰 시스템 위협

1. 변조된 플랫폼 이용

스마트폰 플랫폼은 응용프로그램 관리, 사용자 인터페이스, 보안정책 등 스마트폰 시스템 운영에 필요한 기능을 수행한다. 스마트폰 제조사에서 제공하는 정상적인 플랫폼에는 관리자 권한 차단 등의 보안장치가 마련되어 있지만, 사용자 환경변경, 성능향상 등의 목적으로 변조된 플랫폼을 이용할 수 있는 방법들이 배포되고 있어 이로 인한 보안 문제가 발생할 수 있다.

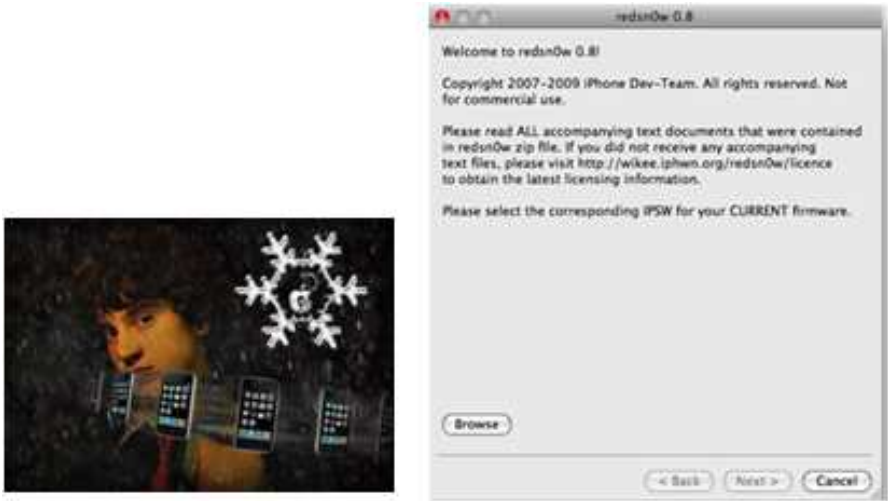


그림 17 아이폰 플랫폼 변조(Jail Break) 기법

아이폰과 안드로이드는 플랫폼 자체적으로 타 응용프로그램과 시스템에 대한 자원(파일, 프로세스 등) 접근을 차단하고 있으나 관리자 권한(Root)을 획득할 수 있는 플랫폼 변조기술이 존재하고 있으며 OS 버전 업데이트에 따라 지속적으로 개발되고 있다.(윈도우 모바일은 플랫폼 자원에 대한 접근이 제한되지 않기 때문에 별도의 플랫폼 변조가 불필요함)

표 10 플랫폼별 변조기법

플랫폼	아이폰	안드로이드	윈도우 모바일
변조기법	Jail Break	Rooting	-
	최신버전(4.1) OS 변조툴 배포중	제조사별로 기법 상이(대부분 가능)	-

○ 플랫폼 변조에 따른 발생위협

- 플랫폼 변조시 발생되는 주요 보안 변동사항에 따라 타 어플리케이션 프로세스 및 메모리 접근, 악성코드 설치, 중요 파일 노출 등의 다양한 위협에 노출될 수 있다.

- 악성코드 설치 : 플랫폼에서 제어하는 인증된 응용프로그램 이외의 악성코드 설치 및 실행이 가능

그림 18 검증되지 않은 어플리케이션 설치 가능

- 이용자가 인지하지 못한 상태에서 과도한 권한을 가진 악성코드가 설치되어 스마트폰 내에 저장된 정보 유출 가능
  - · 휴대폰 정보(기기정보), 시스템 정보
  - · 이용자 개인정보(SMS, MMS 데이터)
  - · 전화기록 및 위치 정보 등

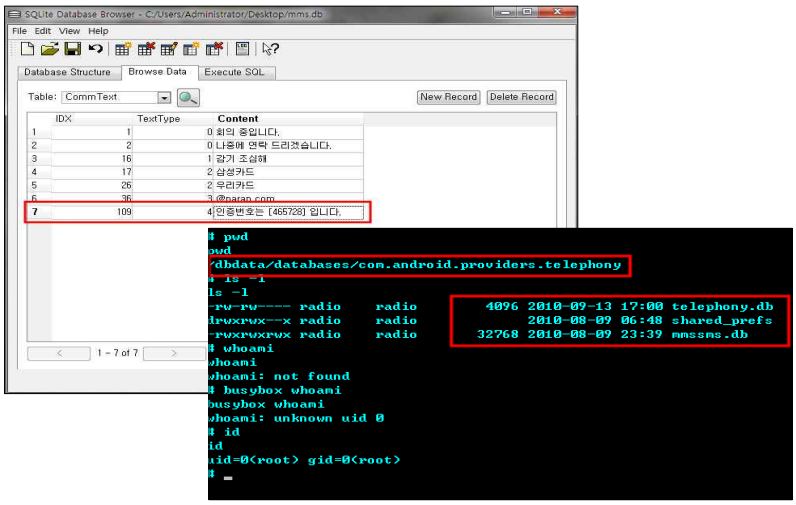


그림 19 안드로이드 SMS 저장 경로 및 내용 추출

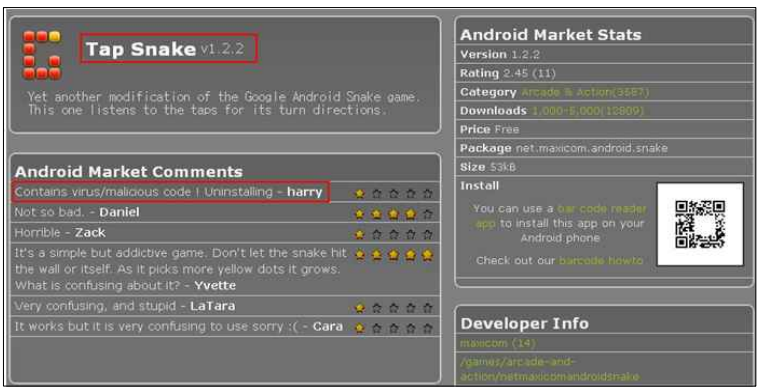


그림 20 스마트폰 위치추적이 가능한 AndroidOS.Tapsnake 악성코드

2. 금융 어플리케이션 변조

변조된 스마트폰 플랫폼으로 전자금융서비스를 이용할 경우 각종 보안 위협에 노출될 수 있으므로 대부분의 금융기관들이 아이폰 Jail Break 및 안드로이드 Rooting 상태에서 전자금융서비스의 이용을 제한하고 있다. 하지만, 역공학 분석(Reverse Engineering)을 통해 플랫폼이 변조된 스마트폰에서도 전자금융 어플리케이션이 변조검증을 우회하여 동작하도록 하는 기법들이 알려지고 있으며 이렇게 변조된 어플리케이션이 스마트폰에 설치 가능한 형태로 배포되고 있다.

어플리케이션의 변조는 다음과 같은 방식으로 이루어진다.

○ 플랫폼 변조를 통해 관리자 권한을 획득하면 스마트폰에 설치된 응용 프로그램의 추출 가능

○ 어플리케이션의 동작할 때의 메모리상에서의 루틴을 해석하여 해당 어플리케이션의 변조 여부를 탐지하는 함수 등을 검색한 후 추출된 바이너리를 수정 및 변경함으로써 탐지 루틴을 우회

※ GDB와 같은 디버거(분석툴)를 이용하여 메모리를 검색하면 다음과 같이 어플리케이션을 처리루틴을 확인할 수 있으며 검증절차를 처리하지 않고 우회하도록 루틴을 변경할 수 있음

```
(gdb) x/8i 0xbf6ca
0xbf6ca:    ldr    r1, [pc, #84]  (0xbf720)
0xbf6cc:    adds   r4, r0, #0
0xbf6ce:    ldr    r1, [r1, #0]
0xbf6d0:    blx    0x16cf98 <dyld_stub_objc_msgSend>
0xbf6d4:    sxtb   r0, r0
0xbf6d6:    cmp    r0, #1
0xbf6d8:    bne.n  0xbf71c
0xbf6da:    ldr    r1, [pc, #72]  (0xbf724)
```

그림 21 GDB를 이용한 어플리케이션 코드 분석

그림 22 변조된 어플리케이션을 통해 전자금융서비스 이용

이렇게 변조된 스마트폰에서 전자금융서비스를 이용하는 경우 이용자의 전자금융 중요정보(로그인 비밀번호, 계좌 비밀번호, 공인인증서 비밀번호 등)가 수집되어 외부로 전송되거나 악성코드 감염으로 인한 스마트폰 비정상 동작(통화 과금 발생 등)을 발생시킬 수 있다. 또한, 악성코드가 삽입된 전자금융 어플리케이션이 배포될 경우 정상적인 어플리케이션으로 위장하여 이용자가 인지하지 못하는 상태로 위협에 노출될 수 있다.

3. 인가되지 않은 파일시스템 접근

스마트폰(아이폰, 안드로이드)은 플래시메모리에 PC의 하드디스크처럼 시스템과 응용프로그램에서 필요한 파일을 저장하고 있으며 계정에 따른 권한설정으로 인하여 허가되지 않은 사용자(어플리케이션)의 접근이 불가능하도록 설계되어 있다. (윈도우 모바일은 별도의 권한 없이 시스템의 모든 파일에 접근가능)

하지만, 플랫폼이 변조되어 관리자권한을 획득한 사용자 및 어플리케이션은

플랫폼에서 권한별로 분리된 파일정보 접근이 가능하므로 공인인증서 파일 추출, 응용프로그램 파일 추출 등이 가능하다.

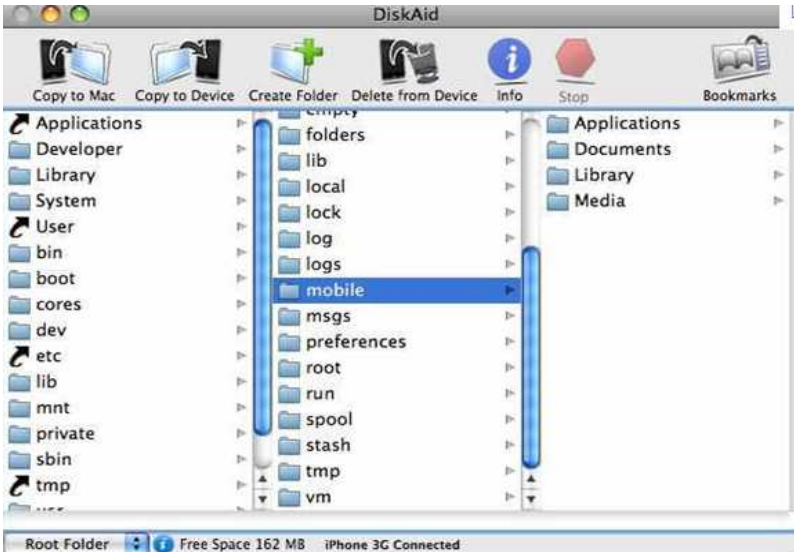


그림 23 아이폰 파일시스템 정보(변조 된 경우)

※ 윈도우 모바일, 안드로이드에 사용되는 공인인증서는 파일형태로 모바일 단말기 파일시스템과 SD 카드영역에 각각 보관한다. 아이폰의 경우 플랫폼에서 제공하는 보안영역(Key Chain)에 DB의 레코드 형태로 현재 저장

특히 금융 어플리케이션이 이용자의 아이디, 비밀번호와 같은 중요정보를 저장할 경우 이로 인한 위협이 더욱 가중될 수 있다. 해외에서는 일부 은행의 스마트폰 전자금융 어플리케이션이 전자금융 아이디, 계좌번호, 비밀번호를 저장하는 것이 확인되어 보안 문제가 제기된 바 있다.([그림 24] 참고)

그림 24 해외 전자금융 어플리케이션의 중요정보 저장

전자금융서비스 어플리케이션에 의한 중요정보 저장뿐만 아니라 전자금융 이용자가 편의를 위해 비밀번호, 보안카드 등을 메모나 사진으로 저장하고 이러한 기능을 제공하는 어플리케이션을 이용하는 것도 보안 위협을 발생시킬 수 있다. 중요정보들이 저장되고 열람되는 과정에 대한 암호화 적용이나 열람 권한 설정과 같은 보안 수준이 확인되지 않았으므로 이로 인해 발생되는 취약성을 통해 중요정보가 수집되거나 노출될 수 있다.

그림 25 보안카드관리 어플리케이션

제 3 절 이용자 중요정보 위협

1. 메모리 중요정보 추출

윈도우 모바일기반 스마트폰과 플랫폼이 변조된 아이폰, 안드로이드폰은 타 프로세스에 대한 접근(파일, 메모리, 프로세스)이 가능하다. 프로세스 메모리상에서는 일시적으로 중요정보가 평문으로 존재할 수 있으며 응용프로그램 개발자가 평문으로 사용한 변수 및 버퍼의 데이터를 초기화 또는 삭제하지 않을 경우 금융거래에 사용한 중요정보가 메모리상에 프로세스 활성화 동안 유지될 수 있다.

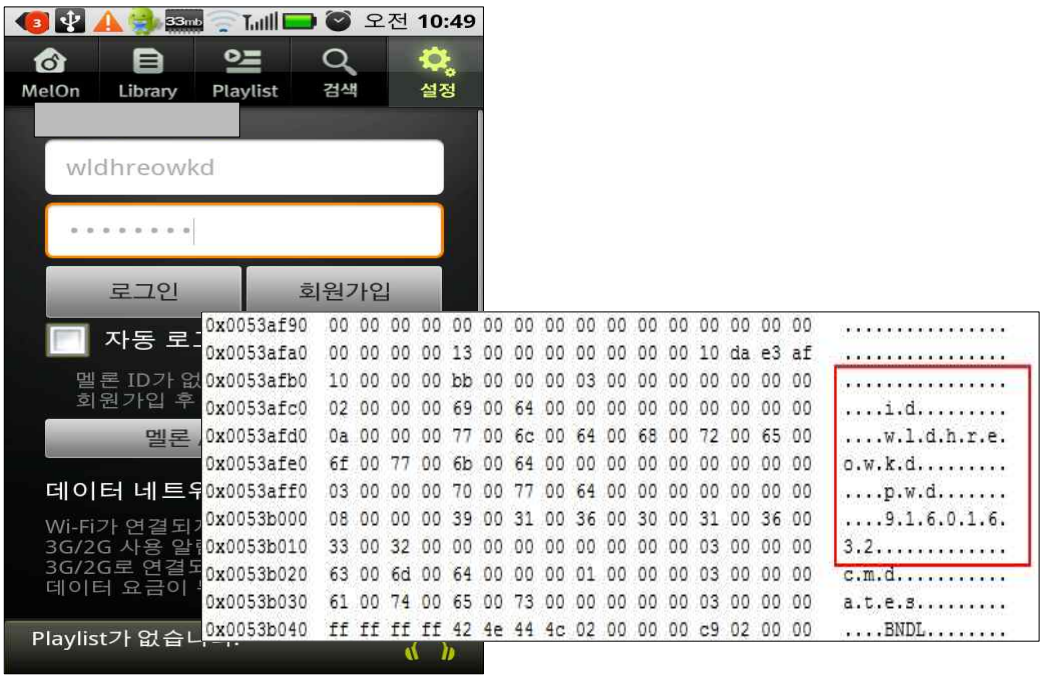


그림 26 루팅된 안드로이드의 프로세스 메모리 접근(ID/PW 노출)

메모리 덤프는 실시간으로 동작하고 있는 메모리를 추출하는 작업이기

때문에 추출 시점 및 스마트폰의 상태에 따라 그 결과가 다를 수 있으며 특정 지점, 패턴을 분석하여 정보를 수집해야하므로 여러 가지 제약사항이 발생할 수 있다. 하지만, 대부분의 중요정보가 메모리를 통해 처리되기 때문에 메모리 추출 위협에 대한 주의가 요구된다.

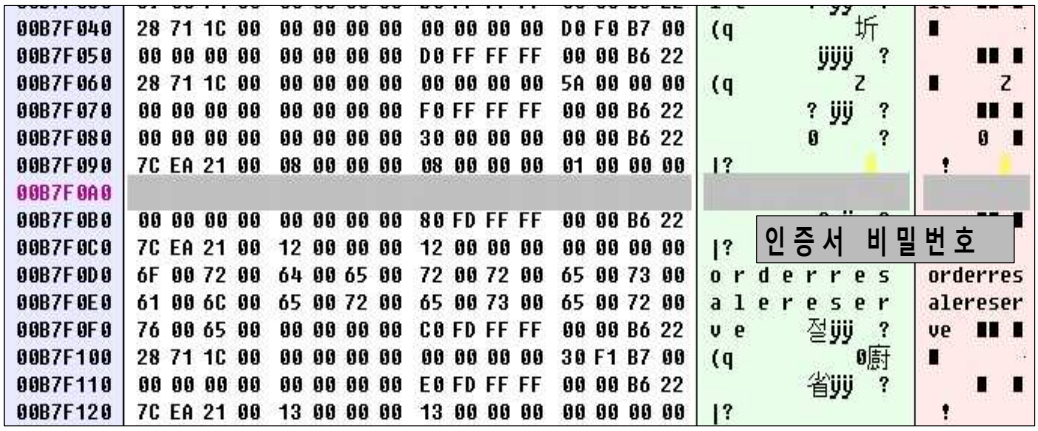


그림 27 윈도우 모바일에서 프로세스 메모리 접근(인증서 비밀번호)

2. 이용자 입력정보 노출

스마트폰에서 각종 비밀번호, 인증정보와 같은 중요정보입력은 터치스크린 또는 키패드를 이용하여 이루어진다. 이러한 스마트폰 입력장치는 PC의 키보드와 유사하기 때문에 기존에 키보드에서 발견되던 입력정보 노출 위협이 동일하게 발생될 수 있다.

입력되는 정보를 수집하기 위해서는 OS나 어플리케이션 레벨에서 키 입력 이벤트나 키 입력 정보를 후킹(Hooking)하는 방식으로 전송되는 입력정보를 가로챌 수 있다. 입력장치에 의한 수집뿐만 아니라 키 입력이 전달되는 입력창의 속성이나 텍스트 정보를 수집하는 기법을 통한 입력정보 수집도 가능하다.

이렇게 수집된 정보는 네트워크를 통해 전송되거나 스마트폰 기기 내에 저장되고 입력 기록을 열람될 수 있게 된다.

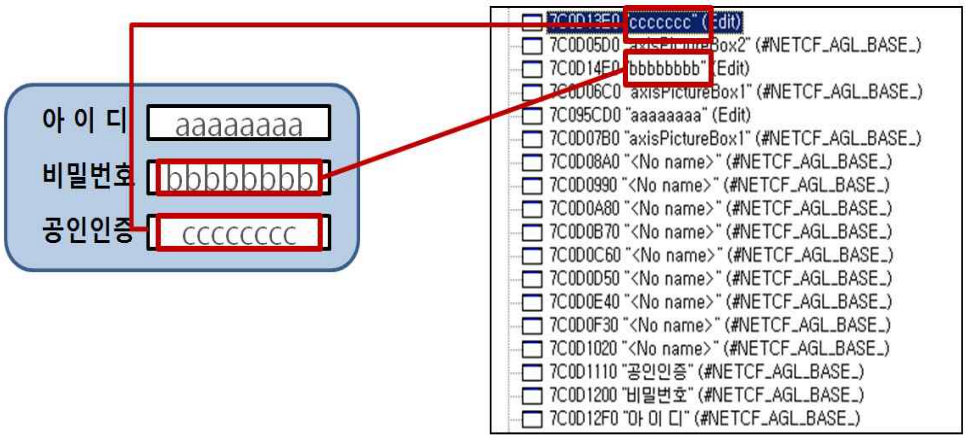


그림 28 입력창 속성을 통한 입력정보 노출

입력정보 노출은 상용화된 키로거나 개발 툴 등으로도 통해 이루어질 수 있으며 키 입력을 수집하기 위해 다양한 기법들이 이용될 수 있기 때문에 이로 인한 위협이 가중 될 수 있다.

그림 29 이용자의 화면 터치를 기록하는 키로거

제 4 절 악성코드 및 피싱 위협

1. 악성코드 유포

스마트폰 악성코드는 PC기반의 악성코드보다 미약한 수준이였지만 최근에는 유포와 활동이 증가하고 있으며 그 형태도 다양화되고 있다.

표 11 스마트폰에서 발견된 주요 악성코드

플 랫 폼	악성코드명	악 성 행 위
안드로이드	Android -Spyware/SMSReplicator	문자메시지를 사용자 몰래 실시간으로 특정 사용자에게 유출
	Android-Trojan/SmsSend	문자메시지를 통한 과금 발생 유도 다수의 변종이 출현
	Android-Spyware/Snake	사용자의 GPS 정보를 특정 서버로 전송. 유료 어플인 GPS Spy로 TapSnake가 설치된 스마트폰의 위치 확인 가능
	Android-Spyware/Ewalls	스마트폰 내의 개인 및 단말기 정보를 수집하여 특정 서버로 전송 다수의 유사 프로그램 발견
윈도우 모바일	WinCE/TredDial	주기적으로 국제전화를 무단 발신하여 원치 않는 과금 발생
	WinCE/Duts	Windows Mobile 최초의 바이러스 실행파일감염, 개념증명바이러스
아이폰	Ike worm	배경화면 변경, 아이폰 최초의 악성코드 (탈옥된 기기에서 동작)

출처 : 안철수연구소

악성코드의 유입경로는 OS 또는 어플리케이션의 취약점을 이용하는 방법, 외부로부터 파일을 전송받는 PC연결, E-Mail, 설치경로가 포함된 SMS 등을 통한 방법이 가능할 수 있다. 또한, 마켓의 관리가 허술한 플랫폼은 악성코드가 포함된 어플리케이션이 마켓에 등록되어 일반 이용자들이 정상 어플리케이션으로 인지하고 설치할 수도 있다.

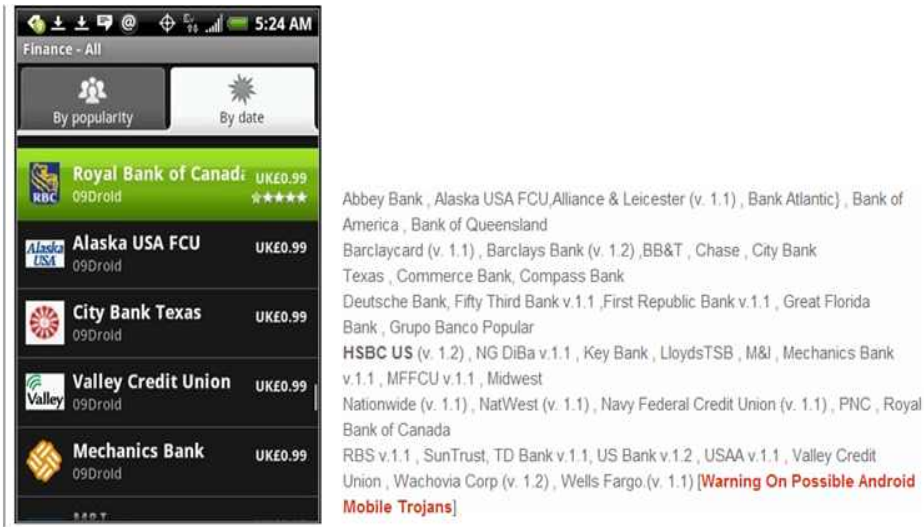


그림 30 마켓에 등록된 금융어플리케이션을 가장한 악성코드

악성코드의 유입경로는 더욱 다양해질 수 있으며 앞으로 발생되는 플랫폼 및 응용프로그램의 취약성을 이용하여 시스템 관리자 권한이 획득하는 등 PC와 유사한 형태의 악성코드들이 유포될 수 있을 것으로 예상된다.

그림 31 악성코드 유입 경로

2. 피싱 공격

스마트폰 이용자는 어플리케이션 마켓, P2P, 웹사이트를 통해 스마트폰 어플리케이션을 다운로드하거나 웹사이트 접속을 통해 서비스를 이용하지만 해당 어플리케이션이나 웹사이트가 정상적인 서비스인지 여부를 사용자가 확인하기에는 어려움이 있다.

피싱 공격은 정상적으로 보이는 서비스이지만 사용자의 입력정보, 개인정보, 금융거래에 필요한 정보 등을 탈취하기 위해 금융, 게임 등의 정상적인 서비스를 가장하는 다양한 형태로 사용자에게 유포될 수 있다.

피싱 공격은 악성코드와 마찬가지로 E-Mail, SMS, 어플리케이션 등 매우 다양한 형태로 시도될 수 있으며 대부분의 스마트폰 서비스들이 단순함을 표방하기 때문에 이러한 서비스들을 모방하는 것이 더욱 간단해지고 있는 상황이다. 또한, 스마트폰의 특성상 여러 가지 서비스를 연계하거나 몇 번의 클릭으로 다른 서비스를 실행, 접속 할 수 있으므로 피싱 공격에 더욱 쉽게

노출될 수 있다.

다음과 같이 SMS등을 이용하여 어플리케이션의 설치경로를 전송하는 방식으로 악성 어플리케이션을 배포하거나 서비스 접속을 유도할 수 있으며 일부 플랫폼에서는 이를 클릭할 경우 바로 링크로 접속되어 실행되므로 피싱 공격에 대한 주의가 필요하다.

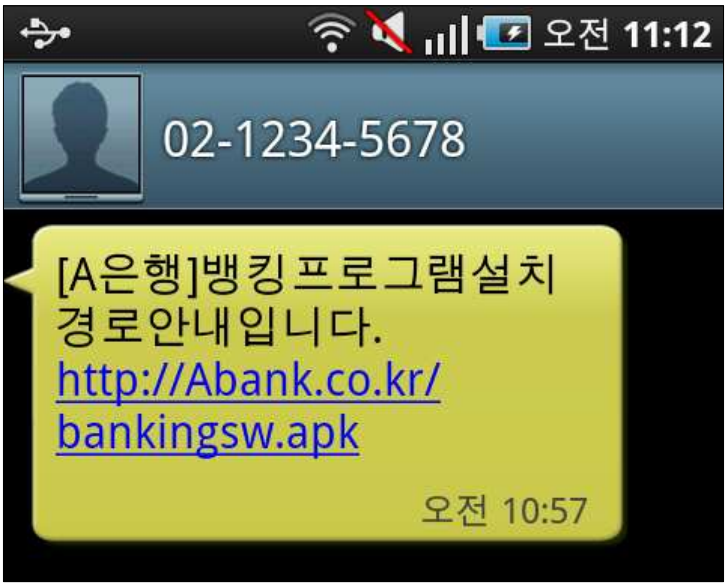


그림 32 SMS를 이용한 피싱 어플리케이션 배포

제 5 절 네트워크 전송구간 위협

1. 중요 전송정보 노출

스마트폰 이용시 이용자가 서비스를 이용하며 데이터를 전송할 때 공격자가 무선 네트워크 구간에 접근이 가능할 경우 전송되는 정보를 습득할 수 있다. 만약 이들 중요정보가 평문으로 전송되거나 적절한 수준의 암호화가 적용되지 않으면 전송되는 정보들이 네트워크 스니핑 툴(Network Sniffing Tool)을 통해 수집될 수 있으며 이렇게 수집된 정보에서 이용자의 개인정보나 중요정보를 추출할 수 있다.

특히 전자금융 어플리케이션이 금융거래정보(계좌 비밀번호, 인증서 비밀번호, 카드 유효기간 등)를 전송할 때 이를 평문으로 전송하게 되면 수집된 패킷을 분석하여 이들 정보를 획득할 수 있다.

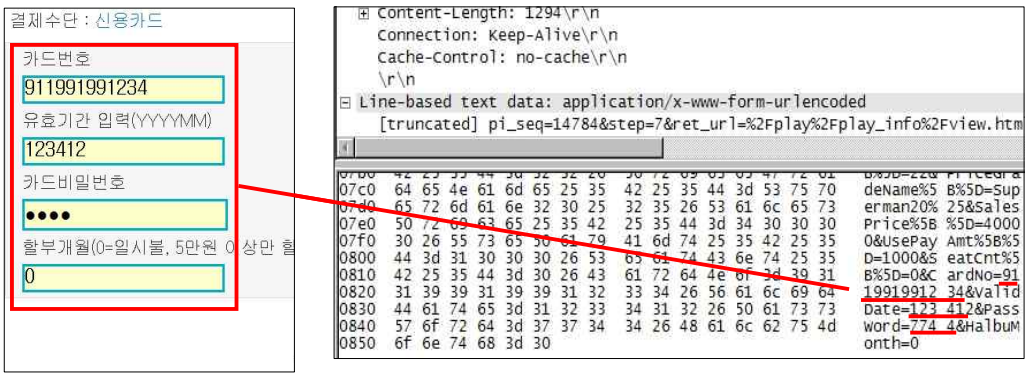


그림 33 카드결제 정보(유효기간, 비밀번호) 노출

대부분의 전자금융 어플리케이션들이 중요정보에 대한 암호화를 적용하고 있으나 이러한 암호화가 정상적으로 적용되지 않거나 중요정보의 암호화가 일부 누락되는 경우에는 이러한 위협에 노출될 수 있다.

특히 무선(Wi-Fi)을 통해 데이터를 전송하는 스마트폰의 특성 때문에 네트워크에 직접 접속하지 않고 스마트폰 주변에서 전송되는 무선데이터를 수집하는 것만으로도 이러한 정보 획득이 가능하다.

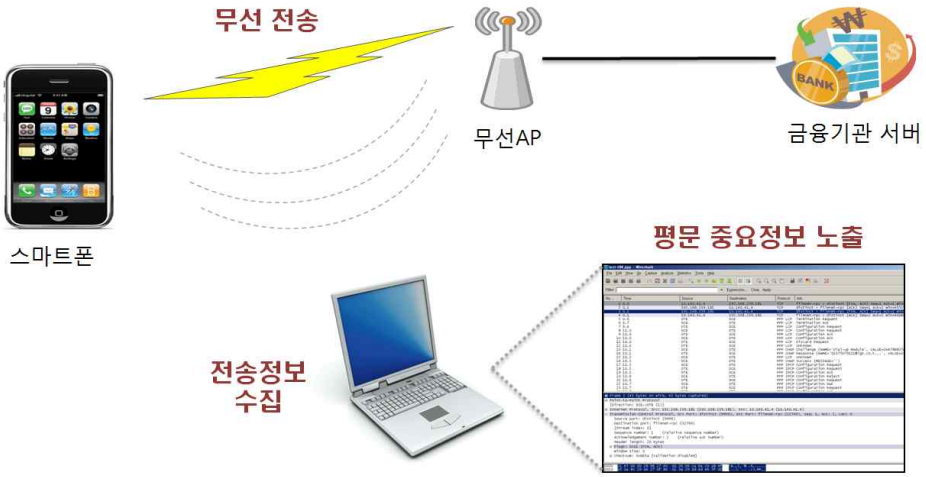


그림 34 무선을 통한 네트워크 전송정보 수집 방법

2. 취약한 무선망 이용

스마트폰은 Wi-Fi 및 3G 통신을 지원하고 있으며 Wi-Fi는 무선공유기(Access Point)를 통해 네트워크에 접속할 수 있다. 최근 Wi-Fi 인프라의 보급에 따라 다양한 공공장소에 무선공유기가 설치되고 있어 스마트폰을 이용한 무선랜 접속이 활성화되고 있는 추세이다.

일반적으로 3G망을 통해 데이터 통신을 이용하면 데이터 요금이 과금되기 때문에 스마트폰 이용자들은 주변에 공개된 무선공유기가 확인되면 이를 이용하여 데이터 통신을 하는 경우가 많다. 하지만, 보안이 취약한 무선공유기를 공격자가 점령하거나 공격자가 설치한 무선공유기(Rogue AP)를 이용하는 경우

무선공유기에 접속한 사용자의 통신데이터가 공격자에 의해 수집될 수 있다.

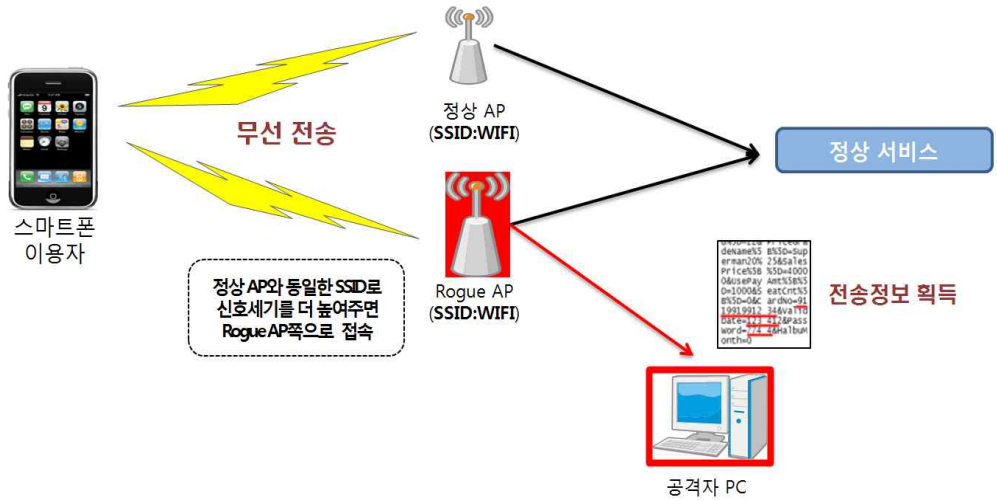


그림 35 공격자가 설치한 무선공유기(Rogue AP)로 인한 정보 노출

또한, 무선공유기 접속 이용자의 정상적인 서비스 접속 요청에 변조된 응답을 전송하여 피싱 공격을 시도할 수 있는 등 다양한 공격 유형이 존재하고 있다.

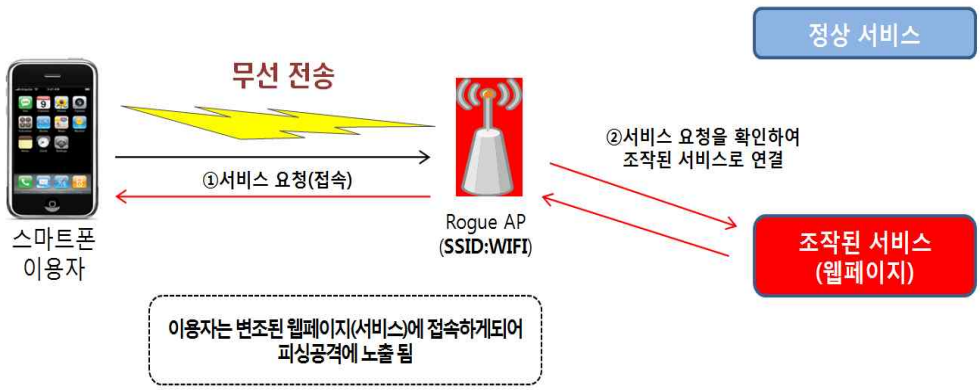


그림 36 변조된 서비스로 접속 유도

이렇게 공격자에 의해 설치된 무선공유기는 SSID를 정상적인 무선공유기와 동일하게 설정하는 경우가 많으며 특정 네트워크(개인, 기업)에 포함되어 있지 않은 경우에는 정상여부나 설치위치 등을 탐지해 내기가 쉽지 않다. 따라서 스마트폰 이용자들이 무선 공유기의 보안수준을 확인하기에는 어려움이 있으며 대부분의 이용자들이 무료로 공개되어 있는 무선공유기를 우선적으로 접속하기 때문에 이러한 위협에 노출될 가능성이 크다.

제 6 절 물리적 위협

1. 도난 및 분실

스마트폰은 이동성과 휴대성이 장점이지만 이러한 특성으로 인해 기존의 PC보다 타인의 접근이 쉽고 도난과 분실의 위험이 크기 때문에 물리적인 형태의 위협에 더욱 쉽게 노출될 수 있다.

도난 및 분실시에는 비인가자의 스마트폰 접근이 가능하며 특히 잠금장치나 중요 데이터의 암호화가 적용되어있지 않은 경우 스마트폰 내에 저장된 모든 정보에 대한 접근이 가능하다.

기본적으로 스마트폰 내에 금융관련 정보는 저장되지 않지만 어플리케이션의 결함 또는 이용자가 편의성을 위해 중요정보를 저장해 두는 경우 이들 정보의 유출로 인한 보안 문제가 발생할 수 있다.

제5장 스마트폰 보안 고려사항

앞서 스마트폰 전자금융서비스 환경에서 발생 가능한 보안 위협을 제시하였으며 본 장에서는 이러한 위협들에 대응하기 위한 방안과 주요 보안 고려사항을 알아보도록 한다. 대응방안과 보안 고려사항은 위협의 특성에 따라 '스마트폰 시스템 보호방안', '이용자 중요정보 보호방안', '악성코드 및 피싱 대응방안', '네트워크 전송구간 보호방안', '추가 고려사항'으로 구분하여 기술하였다.

제 1 절 스마트폰 시스템 보호방안

1. 플랫폼 변조여부 탐지

스마트폰 플랫폼 측면에서는 플랫폼의 변조에 따른 위협을 방지하기 위해 변조된 플랫폼을 탐지(차단)하는 기술 적용이 요구된다.

표 12 스마트폰 플랫폼 보호 고려사항

구 분	고 려 사 항
스마트폰 플랫폼	변조된 플랫폼의 서비스 접근 차단기술 적용
	어플리케이션 실행시, 중요거래 접속시 변조 탐지절차 수행
	신규 변조기법 배포시 차단기술 업데이트 가능

- 플랫폼 변조 위협을 방지하기 위해서는 전자금융서비스 이용시 이용자 스마트폰기기의 변조 여부를 확인하는 절차의 적용이 필요하다.
- 스마트폰 플랫폼 변조에 따라 다음과 같은 주요 변경사항들이 발생하며 이러한 변경사항들을 바탕으로 변조 확인 절차를 마련할 수 있다.

표 13 플랫폼 변조에 따른 주요 변경사항

분 류	플랫폼 변조	
	before	after
관리자(Root) 권한 획득	X	O
타 프로세스 및 메모리 접근	X	O
시스템 파일 및 타 어플리케이션 파일 접근	X	O
불법 어플리케이션 설치	X	O (안드로이드는 루팅 이전에도 가능)

- 이러한 확인 과정이 최초 서비스 접속시 뿐만 아니라 중요거래 이용시에도 재확인 절차를 적용하게 되면 서비스 이용 간 발생되는 플랫폼 변조에 추가적으로 대응 가능하다.
- 또한, 스마트폰 기기의 기종과 버전에 따라 플랫폼 변조 기술이 다양화되고 있으며 탐지기법을 우회하는 변조 기술이 유포되고 있으므로 신규 변조 기술의 탐지가 가능하도록 변조여부 확인절차의 지속적인 개선이 필요하다.

2. 어플리케이션 변조 방지

어플리케이션 측면에서는 역공학을 통한 어플리케이션 분석 및 변조에 따른 위협에 대응하기 위한 방안들이 요구된다.

표 14 어플리케이션 보호 주요 고려사항

구 분	고 려 사 항
어플리케이션	어플리케이션 소스코드 내 중요정보 제거
	변조된 어플리케이션 실행방지 방안 적용(파일 무결성 확인 등)
	어플리케이션 변조방지 방안 적용(디버깅 탐지 등 바이너리 보호 방안)

- 역공학을 통해 소스코드에 포함된 데이터들의 수집이 가능하므로 서버관련 중요 설정정보나 금융거래 관련 정보들이 소스코드에 포함되지 않도록 어플리케이션을 구현한다.
- 금융 어플리케이션의 변조를 방지하기 위해서는 어플리케이션 실행시 실행되는 어플리케이션의 무결성이 훼손되었는지를 확인하고 비정상적인 변동이 있을 경우 정상 어플리케이션을 다시 다운로드 받거나 서비스 접근을 차단할 수 있다.

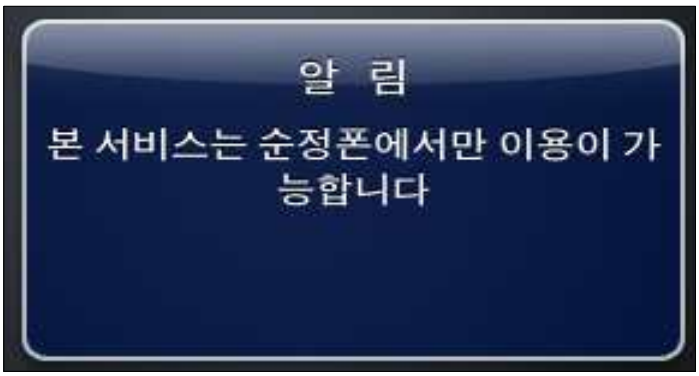


그림 37 변조된 플랫폼에서의 전자금융거래 접근 차단

- 또한, 역공학을 통한 바이너리 변조가 어렵도록 디버깅 방지코드 삽입이나 소스코드 난독화 기법 적용과 같은 바이너리 변조방지 방안들을 적용하여 변조된 어플리케이션의 배포가 이루어지지 않도록 조치가 필요하다.

○ **아이폰 디버깅 방지 코드**

※ 디버깅 상태를 알아내어 어플리케이션을 강제종료

```
#import <Cocoa/Cocoa.h>
#include <sys/ptrace.h>

int main(int argc, char *argv[])
{
    //Build settings -> Other C Flags: -DDEBUG
#ifdef DEBUG
    //do nothing
#else
    ptrace(PT_DENY_ATTACH, 0, 0, 0);
#endif
    return NSApplicationMain(argc,  (const char **)
argv);
}
```

[참고사이트] (1)http://iphonedevwiki.net/index.php/Crack_prevention
(2)http://www.seoxys.com/3-easy-tips-to-prevent-a-binary-crack

- 역공학 방지 기술 역시 역공학을 통한 분석 및 우회에 취약할 수 있으므로 여러 가지 기법을 혼용하거나 최신 기법을 적용하는 등의 지속적인 개선이 필요하다.

제 2 절 이용자 중요정보 보호방안

1. 중요 입력정보 보호

중요 입력정보의 보호를 위해서는 이용자에게 입력받은 중요정보(로그인 비밀번호, 계좌 비밀번호, 공인인증서 비밀번호, 일회용 비밀번호, 보안카드 번호 등)에 대해 입력정보가 노출되지 않도록 입력정보 보호기술을 적용하고 중요정보 입력지점에 대한 기술 적용이 누락되지 않도록 적용하는 것이 요구된다.

표 15 중요 입력정보 보호 고려사항

구 분	고 려 사 항
입력정보 보호	입력정보 보호방안 적용(터치패드/키패드)
	중요정보 입력지점에 대한 입력정보 보호방안 동등 적용
	입력정보 전달구간 내 중요정보 저장 및 노출 금지 (메모리, 모듈간 연동 지점, 입력정보 전달 및 출력 지점 등)

- 전자금융 어플리케이션 개발시 가상키보드, E2E(End To End)암호화 등 입력정보를 보호할 수 있는 기술을 적용하여 이용자의 중요 입력정보가 메모리나 키로거를 통해 유출되지 않도록 처리한다.
- 터치패드와 키패드를 혼용하는 스마트폰은 키패드를 통한 중요정보 입력 허용시 키패드 입력정보에 대한 보호기술의 추가 적용이 요구된다.
- 입력정보 보호가 필요한 입력지점(로그인 비밀번호, 계좌 비밀번호, 공인

인증서 비밀번호)을 사전에 정의하여 보안방안의 적용이 누락되지 않도록 확인하여 적용한다.

- 이들 기술 적용시 입력창과 보안 모듈을 연동하는 부분과 같이 입력정보가 전달되는 부분에 대해서 이미 처리된 입력정보들이 삭제되지 않는 등의 추가적인 취약요소가 없는지 확인하여 적용하는 것이 필요하다.
- 일부 스마트폰은 제조사에서 제공하는 정상적인 플랫폼에서의 메모리 덤프 기법이나 키로깅 기법이 아직 유포되고 있지 않지만 앞으로 새로운 공격 기법들이 개발되거나 이용자가 스마트폰 플랫폼을 변조(Jail Break, Rooting)하여 이용하는 경우를 대비하여 위 방안들을 적용하는 것이 필요하다.

2. 파일 시스템 내 금융정보 노출 방지

입력받은 중요정보나 거래 간 발생되는 거래정보, 인증정보들이 파일 시스템에 저장되지 않도록 처리하고 공인인증서의 저장 및 이용은 공인인증서 이용 기술규격을 준용하여 처리한다.

표 16 인증/거래정보 저장 고려사항

구 분	고 려 사 항
인증/거래정보 저장	거래 종료 후 인증/거래 정보의 기기 내 저장 금지
	거래 간 중요정보 인증/거래 정보의 기기 내 저장 금지
	공인인증서 저장 및 이용 기술규격 준수

- 전자금융 어플리케이션 개발시 금융거래정보, 이용자 중요정보가 파일형태로 저장되지 않도록 처리하고 어플리케이션 관련 중요정보가 불가피하게 파일로

저장될 경우에는 암호화하여 저장한다.

- 공인인증서의 이용 및 저장은 “무선단말기에서의 공인인증서 저장 및 이용 기술규격(KISA)”을 기준으로 구현한다. 기술규격 중 ‘저장매체’ 및 ‘저장 및 이용 방법’은 다음과 같다.

[무선단말기에서의 공인인증서 저장 및 이용 기술규격]

한국인터넷진흥원(2010.3)

1. 저장매체

<저장매체 별 공인인증서 저장위치 및 저장형식>

<table>
<tr><th rowspan="2">구분</th><th rowspan="2" colspan="2">비(非) 스마트폰</th><th colspan="3">스마트폰</th></tr>
<tr><th>iPhone OS</th><th>안드로이드</th><th>윈도우 모바일</th></tr>
<tr><td>내장형 메모리</td><td colspan="2">부록 2표준 인터페이스 함수(PKCS#11)</td><td>App ID</td><td colspan="2">부록 2의 표준 인터페이스 함수(PKCS#11)</td></tr>
<tr><td>외장형 메모리</td><td colspan="5">드라이브명:\NPKI\인증기관 식별자</td></tr>
<tr><td rowspan="2">USIM (또는 IC칩)</td><td>저장토큰</td><td colspan="4">{KCAC.TS.UI}의 부록 3. 스마트카드 파일구성도 및 메모리 맵 참조</td></tr>
<tr><td>보안토큰</td><td colspan="4">{KCAC.TS.HSMU}와 {KCAC.TS.HSMS} 준용</td></tr>
</table>

※ 최상위인증기관 인증서는 기본적으로 내장형 메모리에 저장하되, 외장형 메모리, USIM에 저장할 경우 해당 규격을 준용하여 저장해야 함

2. 저장 및 이용 방법

무선단말기 내 내장형 메모리, 외장형 메모리, USIM(저장토큰)에 전자서명생성키를 저장하는 경우, 전자서명생성키는 {PKCS#5}를 준용하여 암호화 하고, {PKCS#8} 저장형식을 준용한 후, 안전하게 저장되어야 한다.

무선단말기 내 응용프로그램에서 내장메모리에 저장된 전자서명생성키를 이용하여 전자서명 기능을 수행하고자 하는 경우에는 [부록 1. signText 함수] 또는 [부록 2. PKCS#11 함수]의 표준 인터페이스 함수를 준용하여야 한다. 특히, 무선 단말기 내 내장메모리 저장매체를 위한 객체 생성·복사·검색·삭제 등 관리 API는 공인인증서비스의 상호연동성 확보를 위해 [부록 2. PKCS#11 함수]에 따라 구현되어야 한다.

- 또한, 전자금융 이용자들이 개인의 중요정보(각종 비밀번호, 보안카드 등)를 스마트폰 어플리케이션이나 파일 형태로 저장하는 것을 방지하기 위해 이용자를 대상으로 금융정보 저장의 위험성과 유의사항을 안내한다.

제 3 절 악성코드 및 피싱 대응방안

1. 악성코드 예방

악성코드 예방을 위해서는 현재 백신이 적용 가능한 스마트폰 플랫폼(안드로이드, 윈도우 모바일)에서는 백신을 적용하고 지속적인 백신 업데이트를 통해 악성코드 유입을 방지할 수 있다.

표 17 악성코드 예방 주요 고려사항

구 분	고 려 사 항
악성코드 예방	전자금융서비스 이용시 백신 적용
	최신 업데이트 지원
	백신 업데이트 자동 적용

- 악성코드의 위협에 대비하기 위하여 대부분의 전자금융 어플리케이션들이 스마트폰용 백신프로그램을 탑재하고 있으며 스마트폰 제조사에서도 번들 형태로 백신프로그램을 제공하고 있다.
- 따라서 신규 악성코드가 출현한 경우 해당 악성코드를 탐지할 수 있도록 백신엔진의 빠른 업데이트를 지원하여 악성코드의 위협을 최소화한다.
- 백신엔진 업데이트 적용시 이용자가 수동으로 적용할 경우 적용률이 낮아 최신 악성코드 위협에 노출될 수 있으므로 업데이트 발생시 자동으로 업데이트가 실행 되도록 적용하는 것을 권고한다.
- 아이폰은 최신 운영체제에서 멀티태스킹을 지원하고 있으나 다른 플랫폼에 비해 제한적이기 때문에 백그라운드에서 악성코드나 백신이 동작하기 어려운

환경을 가지고 있다. 하지만 향후 새로운 취약성이나 악성도구가 등장하여 이에 대한 탐지나 차단이 필요할 경우 현재 구현되어 있는 플랫폼 변조여부 확인 절차와 연동하여 전자금융서비스 접속시 먼저 필요한 탐지절차를 수행하고 접속 여부를 허용하는 방안의 적용이 가능하다.

2. 피싱 예방

현재 스마트폰 플랫폼에서 피싱 공격을 막기 위한 별도의 보안장치를 제공하고 있지 않은 상황이다. 따라서 정상적인 전자금융 어플리케이션 배포 및 이용절차를 이용자들에게 알리고 피싱 공격을 구분할 수 있도록 비정상적인 어플리케이션 배포 방법, 이용자의 중요정보를 요구하는 피싱 기법 등의 주의사항을 안내하여 이러한 공격에 노출되지 않도록 한다.

또한, 마켓이나 온라인상에서 정상적인 전자금융서비스를 가장한 어플리케이션이나 서비스가 유포되고 있는지 주기적으로 확인하여 조치하는 것이 필요하다.

제 4 절 네트워크 통신구간 보호방안

1. 전송정보 암호화 적용

네트워크를 통해 전송되는 모든 중요정보(각종 비밀번호, 공인인증서 전송 등)는 암호화하여 전송하고 전송구간에서 평문으로 노출되지 않도록 처리한다.

네트워크 통신구간에 대한 안전한 암호기술 적용을 위해 금융권에서 현재 사용 중인 암호알고리즘을 기반으로 권장되는 암호알고리즘의 종류를 기술하였다.(아래 기술된 내용 이외에 국외 주요기관에서 안전성이 검증된 암호알고리즘의 적용도 가능)

○ 대칭키 암호알고리즘

<권장되는 대칭키 암호알고리즘>

용도	대칭키 암호 (키 길이)
암호화용	3-Key Triple-DES (168비트) AES (128비트)* SEED (128비트)** ARIA (128비트 이상)

* AES-192/256 경우 이론적으로 가능한 공격이 발표되어 추후 안전성에 대한 변화가 예상되므로 삭제함
** SEED-192/256이 발표된 상태이므로 안전성이 검증된 후 키길이 변화가 예상됨

○ 공개키 암호알고리즘

< 권장되는 공개키 암호알고리즘>

용도	공개키 암호 (안전성 파라미터)
전자서명	RSASSA-PSS (2,048비트 이상) RSASSA-PKCS#1(v1.5) (2,048비트 이상) ECDSA (224비트 이상) EC-KCDSA (224비트 이상)
키교환 및 암호화용	RSAES-OAEP (2,048비트 이상) ECDH (224비트 이상)

○ **해쉬함수**

해쉬함수의 경우 2010년 이후 HAS-160, SHA-1, SHA-224, SHA-256 등을 사용하되 SHA-1은 메시지 인증용으로만 사용을 권장한다.

○ **국내 외 권장 암호알고리즘**

이외에 국내 외에서 권장되는 암호알고리즘을 선택하여 암호 시스템을 구성하는 경우 다음과 같은 암호키 길이 및 보안강도를 유지하는 암호알고리즘으로 구성해야 한다.

<국내·외 권장 암호알고리즘 구성>

대칭키 암호 알고리즘 (보안강도)	해쉬함수 (보안강도)	공개키 암호알고리즘				암호 알고리즘 안전성 유지기간
		인수분해 (비트)	이산대수		타원곡선암호 (비트)	
			공개키 (비트)	개인키 (비트)		
112	112	2048	2048	224	224	2030년까지

※ 기술된 비트 및 보안강도 이상 유지

※ 추가내용은 『금융부문 암호기술 관리 가이드(금융보안연구원)』 참고

2. 확인되지 않은 무선(Wi-Fi)망 이용금지

중요정보에 대한 암호화를 적용하면 불법 무선공유기에 접속하더라도 암호화된 정보만 수집이 가능하기 때문에 이를 이용한 중요정보 수집이 불가능하다.

하지만 불법 무선공유기를 이용하여 비정상적인 서비스 접근을 유도하는 등의 위협이 발생할 수 있으므로 이용자가 확인되지 않은 무선공유기를 통해 전자금융서비스를 이용하지 않고 확인이 불가능한 경우에는 가급적 이동통신망(3G)을 이용하여 전자금융서비스를 이용하도록 안내한다.

제 5 절 추가 고려사항

1. 스마트폰 분실시 조치절차 마련

도난 및 분실과 같은 물리적 위협에 대한 대책으로 전자금융이용자의 스마트폰 분실사고 발생시 분실신고 절차 및 조치 절차 마련이 요구된다. 분실사고 발생시 먼저 이용자의 스마트폰의 전자금융서비스 접속을 차단하고 공인인증서 재발급 등의 후속조치 절차를 고객에게 안내하여 분실로 발생할 수 있는 사고를 방지할 수 있다.

분실 후 조치절차 마련뿐만 아니라 스마트폰 분실에 따른 전자금융서비스의 위험을 예방할 수 방안들이 함께 필요하다. 스마트폰의 도난 및 분실이 발생하더라도 스마트폰 기기 내에 금융거래를 위한 중요정보들이 저장되지 않는다면 유출된 정보로 인한 금융거래 위협을 방지할 수 있다. 따라서 인가되지 않은 파일시스템 접근 위협에 대한 대응방안과 마찬가지로 어플리케이션에서 처리되는 중요정보가 기기 내에 저장되지 않도록 구현하고 이용자가 중요정보를 저장하지 않도록 안내하는 방안이 필요하다.

2. 다중 로그인 허용기준 마련

PC, 스마트폰, PDA 등 전자금융서비스 이용 기기들이 다양화 되면서 동일기종 내에서 또는, 이기종 기기 간 다중 로그인 허용 여부에 대한 고려가 필요하다. 다중 로그인이 허용될 경우 피싱 공격이나 도난 및 분실사고 발생시 추가적인 위협에 노출될 수 있으므로 이를 허용하지 않는 것을 권고하며 이기종 기기 간 다중 로그인을 탐지할 수 있는 시스템 구축에 대한 고려가 요구된다.

제6장 맺음말

스마트폰 발전에 따라 전자금융서비스의 영역은 더욱 확대되고 있으며 기존에 제공되던 서비스 형태를 뛰어넘은 다양한 신규 서비스들이 개발되고 있다. 이렇게 서비스들이 개발되고 제공되는 과정에서 기존 위협들과 함께 새로운 취약성들이 등장하여 전자금융 전반을 위험에 노출시킬 수 있으므로 이에 대한 대비가 필수적이라 할 수 있겠다.

본 가이드에서는 현재 서비스되고 있는 전자금융서비스의 구성과 특징, 각 스마트폰 플랫폼별 보안 기술에 대해서 알아보고 이를 통해 전자금융서비스에서 등장 가능한 위협들을 분석하였다. 이러한 위협분석은 직접적인 형태의 위협뿐만 아니라 잠재적인 위협들에 대한 분석도 함께 진행하여 향후 발생 가능한 위협을 포함하고자 하였다. 이렇게 확인된 위협들에 대한 대응 방안은 실제 전자금융서비스 개발과 적용시 고려해야만 하는 방안들로 작성하여 현재 서비스를 제공하고 있거나 제공 예정인 금융기관들이 참고할 수 있도록 작성하였다.

본 가이드를 통해 검토한 내용 외에 향후 웹 기반의 스마트폰 전자금융서비스와 같이 새로운 형태의 서비스가 등장하거나 스마트폰 플랫폼에 대한 추가적인 취약성이 발견될 경우 위협에 대한 검토가 필요하며 바이너리 변조 방지 기술과 같이 위협을 최소화 할 수 있는 보안기술에 대한 지속적인 관심과 연구가 필요할 것으로 보인다.

이와 함께 전자금융서비스 이용자가 인지하고 준수해야할 안전수칙들을 홍보하고 안내하여 안전하고 편리한 전자금융서비스가 지속될 수 있도록 함께 노력해 나가야 할 것이다.

참고 문헌

[1] 금융감독원, 스마트폰 전자금융서비스 안전대책, 2010

[2] 삼성경제연구원, 스마트폰이 열어가는 미래, 2010

[3] 한국은행, 2010년 3.4분기 국내 인터넷뱅킹서비스 이용현황, 2010

[4] 한국인터넷진흥원, 무선단말기에서의 공인인증서 저장 및 이용 기술규격, 2010

[5] 금융보안연구원, 금융부문 암호기술 관리 가이드, 2010

[6] Microsoft Architectural Overview of Windows Mobile Infrastructure Components, 2008

[7] Ryan Selley, Swapnil Shinde, Michael Tanner, Madhura Tipnis, Colin Vinson, Vulnerability Study of the Android

[8] Nicolas Economou, Alfredo Ortega, Smartphone (in)security, 2009

[9] Mobile: Major Security Holes Found In Mobile Bank Apps on Friday, Slashdot, 2010

[10] 이정현, 스마트폰 금융서비스의 안전성 제고 방안, 2010

[11] 윤영삼, 모바일뱅킹 서비스 동향과 전망, 産銀調査月報 632호, p. 62-79, 2008. 7

[12] 탁승호, 모바일뱅킹 서비스의 최근 동향과 활성화 방안, 與信金融 제 17호, 2009. 3

[13] 김경숙, 손달호, 인터넷 뱅킹 활성화를 위한 결정요인, 經營經濟 제 41집 1호, p. 51-70, 2008. 2

[14] 백재영, 스마트폰 제품의 시장현황 및 개발 동향, 한국과학기술정보연구원, 2008. 12

[15] Microsoft, Windows Mobile, http://www.microsoft.com/korea/windowsmobile
[16] Apple, iPhone, http://www.apple.com/iphone/
[17] Google, Android, http://code.google.com/intl/ko/android/
[18] 배근태, 김기영, 모바일 단말 보안 운영체제 기술 동향, 전자통신동향분석, 2009. 8
[19] Nicolas Seriot, “iPhone Privacy”, 2010
[20] 조진만, 김수형, 문기영, 장종수, 손승원, 모바일지급결제의 시장 현황 및 표준화 동향, 전자통신동향분석 제20권 제1호, p. 33-41, 2005. 2
[21] 금융감독원, 전자금융감독규정, 2006
[22] 전길수, 스마트폰 보안이슈 및 대응방안, 한국인터넷진흥원, 2010. 3
[23] 와이즈인포, 스마트폰 시장/기술 및 연관산업(OS, App.Market) 동향 리포트, 2009. 3
[24] 권지인, 국내외 모바일 어플리케이션 마켓 현황, 방송통신정책 제 21권, 7호, p. 57-61, 2009. 4

이 가이드 작성을 위해 다음 분들께서 수고하셨습니다.

2010년 12월

총괄 책임자	금융보안연구원 사이버대응센터	센 터 장	성 재 모
참여 연구원	취약성분석팀	팀 장	장 재 환
		연 구 원	박 용 준
외부 전문가	쉬프트웍스	팀 장	홍 동 철
	안철수연구소	책 임	이 성 근
	NSHC	대 표	허 영 일

금융부문 스마트폰 보안 가이드

2010년 12월 인쇄
2010년 12월 발행
발행인 : 곽 창 규
발행처 : 금융보안연구원
서울시 영등포구 여의도동 36-1
키움파이낸스 스퀘어 빌딩 15층
Tel: (02) 6919-9114
인쇄처 : 일지사(TEL : 503-6971)

<비 매 품 >