전자정부 모바일 앱 보안성 검증체계

정회원 방 지 호*, 하 란*, 강 필 용**, 김 홍 근**

Security Verification Framework for e-GOV Mobile App

Jiho Bang*, Rhan Ha*, Pilyong Kang**, Honggeun Kim** ***Regular Members***

요 약

최근 스마트폰의 보급이 빠르게 확산되고, 국내·외 앱스토어를 통해 다양한 모바일 앱이 개발·배포됨에 따라 많은 사용자들이 필요에 따라 자유롭게 앱들을 설치·삭제하고 있다. 앱스토어에서 배포되는 앱들은 각각의 앱스토어 검증체계에 따라 검증되고 있으나, 보안성에 대한 부분이 미흡하며, 최근 개인정보 등 중요정보의 임의 유출로 인한 피해가 증가하면서 모바일 앱에 대한 보안성 검증 필요성이 증가하고 있다. 보다 높은 보안성을 요구하는 전자정부의 모바일 서비스 앱에 대해 보안성을 검증하기 위해서는 별도의 검증정책이 필요하다. 따라서, 본 논문은 전자정부 모바일 앱의 안전·신뢰성을 제고할 수 있는 보안성 검증체계를 제안한다. 제안된 검증체계의 효과를 분석하기 위해 시범검증을 수행하고 해당 결과를 제시한다.

Key Words : Mobile App, App Store, Security Verification, Vulnerability

ABSTRACT

Recently smart phones have been proliferating widely and quickly. Since the number of mobile apps that are being developed and deployed to domestic/international app stores is rising, more apps are being installed and deleted by users without any difficulty. The deployed apps are each attested through distinct verification framework of specific app stores. However, such verification frameworks are insufficient in checking security concerns. Unfortunately, the security verification framework is necessary since the incidents of leaking privacy and confidential information are being increased in lately. The aim of this paper is to provide the security verification framework that assures security and reliability of the e-government mobile apps. In order to verify proposed verification framework, a few apps were selected and inspected through proposed framework and these inspection results are included in this paper.

Ⅰ. 서 론

최근 스마트폰의 하드웨어 사양이 PC에 버금갈 정도로 높아지고, 국내·외 앱스토어를 통해 다양한 모바일 앱(App, Application의 약자)이 개발·배포되면서 스마트폰 보급율 및 이용율이 빠르게 증가하고 있다. 또한, 게임, 음악·영화감상 등 개인용도에서부터 시간과 장소에 구애받지 않고 원격업무를 수행할 수 있는 스마트워크, 즉 회사업무용도에 이르기까지 스마트폰의 활용처가 다양해 졌다. 이처럼 스마트폰 기반의 다양한 모바일 서비스가 확산됨에 따라 그에 따른 모바일 앱에 대한 개발 수요도 증가되고 있다.

* 홍익대학교 컴퓨터공학과 실시간시스템 연구실(jhbang@kisa.or.kr, rhanha@cs.hongik.ac.kr)
** 한국인터넷진흥원(kangpy@kisa.or.kr, hgkim@kisa.or.kr)
논문번호 : KICS2011-07-307, 접수일자 : 2011년 7월 18일, 최종논문접수일자 : 2012년 2월 13일

한편, 모바일 앱의 기능이 다양해지고 복잡해짐에 따라 PC기반 어플리케이션에서 발생했던 보안위협들이 모바일 앱에서도 그대로 발생하게 되었으며, PC 환경에서는 고려되지 않던 개인위치정보와 같은 일부 보안위협들이 모바일 환경의 특수성으로 이슈가 되고 있다. 모바일 앱을 통한 개인위치정보의 무단 수집·활용의 대표적인 예는 애플 아이폰의 개인위치정보 축적, 광고모듈에 탑재된 위치정보 수집기능으로 인한 80만명 위치정보 유출[1] 등이 있다. 최근 기사(2011.5.11 서울경제, 애플리케이션 장터 악성코드 '득시글')에서 볼 수 있듯이, 안드로이드 단말기에 대한 악성코드 공격이 지난 1년여 동안 5배나 늘어 악성코드의 유통도 활발해 졌다.

스마트폰 기반의 모바일 앱과 관련된 주요 보안취약점은 다음의 표 1과 같다. 같은 보안취약점이라도 개인·업무용도 앱보다 정부시책 및 기밀을 다루는 전자정부 앱에 더 위협적이라고 할 수 있기 때문에 전자정부 앱에 대한 보안취약점 검증을 강화할 필요가 있다.

표 1. 모바일 앱 관련 주요 보안위협
Table 1. The main security threats related to mobile apps

유형	주요내용
정보유출	· 개인정보(SMS, 주소록, 통화목록 등) · 위치정보(현재위치, 누적된 이동경로 등) · 금융정보(계좌번호, 카드번호 등) · 인증정보(패스워드, 인증서 등) · 업무정보(결재문서, 내부보고자료 등)
부적절한 관리	· 인증정보(패스워드, 인증서 등) · 암호키
악성코드	· 구현된 목적이외의 기능 동작(대량메시지 발송, 무단 정보 유출 등)

한편, 국내·외 앱스토어는 개발자에게 개발에 필요한 가이드 및 개발지원 도구를 제공하고 있으나, 보안취약점에 대응할 수 있는 개발보안 관련 지침 및 가이드 개발·제공 노력은 미흡하다. 또한, 앱스토어는 자체 검증체계를 통해 모바일 앱을 검증하지만 품질위주의 점검만 수행하기 때문에 모바일 앱에 잔존하는 보안취약점을 사전에 제거하는데 한계가 있다.

앱스토어별 서로 상이한 검증체계에도 불구하고 모바일 앱의 품질 및 보안성에 영향을 미치는 앱스토어 검증체계에 대한 연구 및 표준화 활동은 미흡한 반면, 플랫폼과 모바일 사업자에 상관없이 어떤 단말로도 앱스토어를 이용할 수 있는 개방형 앱스토어에 대한 연구 및 표준화 활동[2]은 활발히 진행되고 있다.

모바일 앱은 모바일기기 소프트웨어로 정보시스템 소프트웨어와 규모의 차이는 있으나 개발언어, 개발과정 등 동일한 환경을 가지고 있기 때문에 정보시스템 소프트웨어 관련 연구 및 표준화 활동을 참고할 수 있다. 정보시스템 소프트웨어 발주·관리 표준프로세스[3]의 경우, 정보시스템 소프트웨어 개발단계별 발주자 및 개발자가 준수해야하는 절차를 표준화한 문서로 보안측면이 배제되어 있다. 그러나, 정보보호제품을 평가·인증하기 위해 국내에서 적용하고 있는 공통평가기준[4]은 보안관점의 소프트웨어 개발방법론을 제시하고 있기 때문에 모바일 앱 검증체계의 좋은 모델이라고 할 수 있다.

행정안전부와 한국인터넷진흥원(KISA)은 2009년부터 정부부처 정보시스템 소프트웨어의 안전·신뢰성을 제고하기 위해 소프트웨어 개발보안에 대한 연구를 수행하고 있으며, 전자정부지원사업으로 구축되는 정보시스템 소프트웨어에 대해 소스코드 수준의 보안취약점을 시범적으로 진단하고 있다. 또한, 담당공무원 및 개발자를 대상으로 소프트웨어 개발보안 교육을 제공하고 있으며, 최근 안전한 정보시스템 소프트웨어 개발을 위한 소프트웨어 개발보안 가이드[5]를 제작·배포하였다. 해당 가이드는 JAVA 및 C 언어에 대한 시큐어코딩 가이드 이외에 구글 안드로이드에 대한 시큐어코딩 가이드를 포함하고 있다. 구현언어 관점으로 작성되었기 때문에 모바일 앱의 기능 및 모바일 플랫폼별 메커니즘에 대한 부분은 아직 미흡하며, 애플 iOS는 아직 포함되지 않았다.

본 논문은 앱 검증기술 및 체계 관련 연구, 민간 앱스토어 검증체계, 평가 관련 표준화 등 관련 연구 및 동향을 분석하여 모바일 환경에서 안전한 전자정부 서비스를 제공할 수 있는 보안성 검증기준·절차 등 전자정부 모바일 앱 보안성 검증체계를 제안한다. 제안하는 검증체계 모델은 민간 앱스토어 검증체계의 보안성을 향상시킬 수 있도록 동일하게 적용할 수 있다.

본 논문은 2장에서는 모바일 앱 검증관련 국내·외 동향을 설명하고, 3장에서는 본 논문에서 제안하는 전자정부 모바일 앱에 대한 보안성 검증체계를 설명한다. 그리고, 4장에서는 본 논문에서 제안하는 검증체계을 시범 적용한 사례 및 효과를 분석하고, 5장에서는 결론을 맺는다.

표 2. 국내·외 앱스토어별 주요 검증항목(각 앱스토어별 제공 가이드 참고)
Table 2. Key verification items of domestic and foreign app store

유형		국내			국외
		KT Olleh 마켓	LGU+ OZ스토어	SKT T스토어	애플 앱스토어
검증시기		사전·사후	사전·사후	사전·사후	사전·사후
주요 검증 항목	유해성	· 이용등급 분류 적절성 · 콘텐츠 유해성	· 성인아이콘 등 컨텐츠	· 대용량 서비스 제공 · 반국가/반사회적인 내용 등 불건전 주제 포함 · 선정적 등 유해물	· 성인물 및 거부감, 폭력성, 명예훼손 등의 컨텐츠
	단말동작	· 상품등록정보 · 기능 정상 동작 · 과금 검증	· 기능 정상 동작 · 개발자 자체 적용 결과(소스코드 검증 및 기능 커버리지 분석도구 제공)	· 기능 정상 동작 · ARM 정상 적용 · 유료화 API 관련 과금 및 고지	· 기능 정상 동작 · 미공개 API 사용 · 기본목적에 맞지 않은 백그라운드 서비스
	보안성	· 악성코드 및 바이러스, 해킹, 개인정보 유출 및 어플 설치 시 불필요한 정보요청 등	· 위치기반서비스 제공 적합(사업자 등록)	· 개인정보 및 위치정보 수집·활용에 대한 고지·동의메뉴 구현 · 바이러스·악성코드 포함	· 개인정보 및 위치정보의 무단 수집·활용 · 바이러스·악성코드 포함

Ⅱ. 관련 동향

본 장에서는 앱 검증기술 및 체계 관련 연구, 민간 앱스토어 검증체계, 평가 관련 표준화에 대해 설명한다.

2.1. 앱 검증기술 및 체계 관련 연구

초기에는 모바일 환경에서의 악성코드 탐지[6]를 중심으로 연구가 진행되었으나, 최근 구글 안드로이드 플랫폼의 인기가 높아지면서 모바일 플랫폼의 보안기술[7-9] 연구가 활발히 진행되고 있다. 또한, 개인정보 및 위치정보 등 중요정보 유출사고가 빈번해 짐에 따라 개인정보 및 위치정보 유출 관련 연구[10,11] 또한 활발하게 진행되고 있으며, 모바일 앱 보안성 검증방법 및 체계[12,13]에 대한 연구도 진행되고 있다.

모바일 플랫폼 관점의 보안기능 점검시 관련 연구결과들을 활용할 수 있으며, 개인정보 및 위치정보 유출과 관련된 함수 및 필요한 권한 정보를 이용하여 모바일 앱 구현시 적용여부를 점검할 수 있다. 그러나, 기존 연구 활동은 모바일 플랫폼 관점에서 출발하여 비정상동작에 초점이 맞추어 있기 때문에 모바일 앱·서버의 인증기능에 따른 인증정보 안전한 저장 및 전송, 외부 입력값에 대한 유효성 점검 등과 같은 모바일 앱 구현기능 관점의 보안취약점이 간과되고 있다.

따라서, 모바일 앱 보안성 검증시, 모바일 플랫폼 보안메커니즘과 개인정보 및 위치정보 유출에 사용될 수 있는 함수 및 사용권한에 대한 기존 연구결과물을 활용하고, 모바일 앱의 보호자산 대비 보안위협을 식별하여 기능구현 관점의 보안 요구사항을 도출해야 한다. 도출된 보안 요구사항을 기반으로 기능관점 보안취약점을 점검하고, 언어 기반 보안취약점을 연구하여 소스코드 정적분석을 수행하는 것이 필요하다.

2.2. 민간 앱스토어 검증체계

일반적으로 개인 또는 법인 개발자는 앱을 개발·배포하기 위해 배포채널을 선택하여 개발을 수행하며, 국내·외 앱스토어는 개발자에게 개발에 필요한 가이드 및 개발지원도구 등 개발환경을 제공한다. 개발자가 개발한 앱은 앱스토어를 통해 배포되기 전에 각 앱스토어별로 마련된 자체 검증체계(그림 1)에 따라 앱을 검증한 후 각 앱스토어를 통해 등록·배포된다.

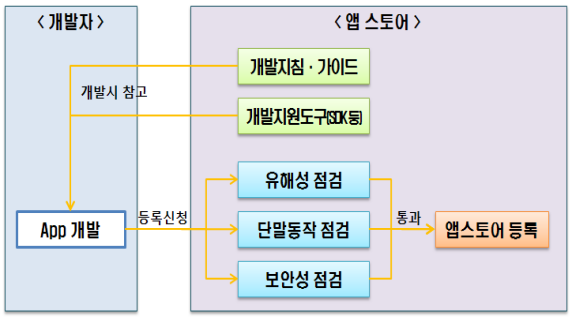

그림 1. 일반적인 앱스토어 검증절차
Fig. 1. Typical verification process of app store

국내·외 주요 앱스토어별로 살펴봤을 때, KT Olleh마켓은 셀러지원센터[14]를 통해 개발에 필요한 가이드 및 개발지원 도구를 제공하고 있으며,

LGU+는 OZ스토어 개발자센터[15]를 통해 개발에 필요한 가이드 및 개발지원도구를 제공하고 있다. OZ스토어는 다른 앱스토어와는 달리 명확한 검증가이드를 제공하고 있지 않지만, 개발가이드 및 공지사항을 통해 검증항목에 대한 정보를 간접적으로 제공하고 있다. T스토어 개발자센터[16]를 통해 개발에 필요한 가이드 및 개발지원도구를 제공하고 있다. 애플 앱스토어는 iOS 개발센터[17]를 통해 개발에 필요한 가이드, 개발지원도구, 앱스토어 리뷰가이드 등을 제공하고 있다. 구글 안드로이드마켓[18]은 안드로이드 개발자 사이트를 통해 개발관련 가이드를 제공하고 있다.

구글은 앱에 개발자 서명이 되어있는지 여부만 점검하고 다른 앱스토어와는 달리 품질 및 보안성에 대한 사전검증을 수행하지 않는다. 대신 평판제도를 통해 사후대응을 하고 있다. 그 이외 앱스토어에서는 사전·사후 검증을 수행하면서 표 2의 검증항목처럼 모바일 앱의 품질 및 성능 중심의 검증항목으로 구성되어 있으며, 보안성에 대해서는 개인정보·위치정보 수집·활용, 바이러스 검출 등에 대해 점검을 하고 있다.

2.3. 평가 관련 표준화

현재, 모바일 앱 보안성 검증에 대한 표준화 활동은 없으나, IT제품 및 소프트웨어에 대한 보안성 보증 관련 표준화 활동은 활발히 진행되고 있다. 특히, 미국 DHS가 주도하고 있는 SwA(SW Assurance) 프로그램[19]을 통해 소프트웨어 보안성 개발생명주기, 평가 및 방법론 등에 대한 표준화(ISO/IEC 152207, ISO/IEC 15026 등)를 주도하고 있다. 행정안전부와 KISA는 전자정부 소프트웨어의 개발단계부터 보안취약점을 사전 진단·제거하기 위해 개발보안 생명주기 및 취약점 진단기준·방법론을 개발하고 있으며, 모바일 소프트웨어로 그 대상을 확대하고 있다.

소프트웨어 품질 요구사항 및 평가 관련 표준(ISO/IEC 25051, ISO/IEC 9126, ISO/IEC 14598 등)을 평가기준으로 삼고 있는 국내 GS(Good SW) 인증은 소프트웨어의 기능성, 사용성, 이식성, 유지보수성, 효율성, 신뢰성에 대해 평가를 하기 때문에 모바일 앱의 보안성을 검증하기 위한 기준으로 준용하기에 어려움이 있다.

정보보호제품에 대한 보안성 평가·인증 기준인 공통평가기준(Common Criteria, CC)[4]은 국제표준(ISO/IEC 15408)으로 국가간 평가결과를 상호인정하기 위해 미국, 유럽 등 기존의 여러 평가기준을 참조하여 단일화된 평가기준으로 개발되었다. 평가대상 제품의 기능 및 설계 대한 문서적 보증을 중시하는 CC는 평가대상 제품의 평가보증등급(EAL, Evaulation Assuarance Level)은 다음 표 3과 같이 7단계로 구분하고 있다. 개발기간이 짧고 IT 기능이 중심인 모바일 앱에 대한 보안성을 검증하기 위해, 문서적 보증이 강화된 정보보호제품 평가기준인 CC를 그대로 적용하기보다 보안취약점 평가부분만 참고를 하는 것이 필요하다.

표 3. 평가보증등급(EAL)
Table 3. Evaluation Assurance Level

등급	내용
EAL1	· **기능동작 위주**의 기초적 수준의 보증 · 잘 알려진 취약점 점검
EAL2	· 설계에 대한 보증 추가 · **외부 인터페이스에 대한 취약점 점검**
EAL3	· 개발환경에 대한 보증 추가 · 서브시스템 설계 및 구조 관점의 취약점 점검
EAL4	· 구현 및 개발도구에 대한 보증 추가 · 샘플링한 **소스코드에 대한 취약점 점검**
EAL5~7	· 보안정책 및 모듈화에 대한 보증 추가 · 전체 소스코드 등 다각적인 취약점 점검

Ⅲ. 전자정부 모바일 앱 보안성 검증체계

대부분의 앱스토어는 앱의 품질 및 유해성 관점에서 검증을 수행하고 있기 때문에 전자정부 모바일 앱을 검증하기 위해 기존 앱스토어의 검증체계를 그대로 적용하기에는 한계가 있으며, GS 및 CC와 같은 규모가 있는 소프트웨어에 대한 평가기준을 그대로 적용하기 역시 어렵다. 따라서, 본 논문은 전자정부 모바일 앱의 보안성을 검증하는데 효율적인 검증체계를 제안하며, 본 장에서는 앱에 대한 보안성 검증기준 및 절차 등에 대해 설명하고자 한다.

3.1. 절차

정책기관 및 검증기관은 사전에 개발보안가이드 및 검증가이드를 배포하고, 개발자를 대상으로 개발보안 교육을 실시한다. 전자정부 모바일 서비스 앱 개발자는 개발보안 교육을 이수하고, 기 배포된 개발보안가이드를 참고하여 안전하게 모바일 앱을 개발한다.

개발기관은 모바일 앱 보안성 검증을 받기 위해

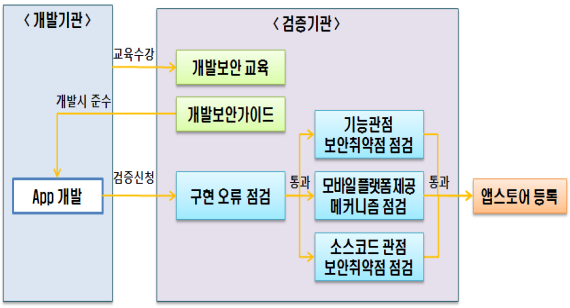

그림 2. 전자정부 모바일 앱 보안성 검증절차
Fig. 2. Security verification procedures of e-Gov mobile app

모바일 앱의 보안속성·구현기능·기능정상동작 여부를 명세한 보안명세서, 컴파일 가능한 형태의 소스코드, 실행 가능한 상태의 실행코드 등의 제출물을 제출한다.

검기관은 검증신청된 모바일 앱에 대해 제출물을기반으로 보안취약점이 잔존하는지 여부를 검증하고 안전한 앱만 배포되어 사용될 수 있도록 한다. 기능오류 및 보안취약점이 식별되면 개발기관에 보완 요청한 후, 보완된 모바일 앱에 대해 보완조치사항을 확인하고 보안취약점 잔존여부를 재확인하여야 한다.

세부검증 단계는 앱 기능의 정상동작 유무를 확인하는 사전검증 단계와 기능 및 소스코드 관점의 보안취약점을 검증하는 상세검증 단계로 구분(그림 2)되며, 각 단계별 검증기준 및 항목은 다음절에서 설명하도록 한다.

3.2. 검증기준

모바일 앱에 대한 보안성을 검증하기 위해 기능오류, 기능관점 보안취약점, 모바일 플랫폼 보안메커니즘, 소스코드 관점 보안취약점 등 4가지 항목에 대한 세부검증을 수행하여야 한다.

3.2.1. 기능 오류

모바일 앱에 대한 보안취약점을 점검하기 위해 기본적으로 모바일 앱은 정상적으로 설치 및 삭제되어야 하며, UI 기반 기능이 정상적으로 동작해야 한다. 따라서, 앱에 구현된 기능을 명확하게 파악해야 하며, 파악된 기능과 UI를 비교하고, 다양한 입력값 기반 반복시험을 통해 정상동작 여부를 점검해야 한다.

3.2..2. 기능 관점 보안취약점

모바일 앱에 구현되는 일반적인 기능 유형과 해당 유형에 따라 고려해야 하는 주요 보안속성은 표

표 4. 기능유형 및 보안속성
Table 4. Feature types and security attributes

유형	유형설명	보안속성
사용자 로그인	서비스를 이용하기 위한 사용자 식별 및 인증	패스워드
상호인증 (서버, 단말)	서비스를 이용·제공하기 위한 상호인증	인증정보
개인위치정보	특화된 서비스 제공을 위한 개인위치정보 생성·저장·전송	위치정보
개인정보	서비스 이용 등을 위한 개인정보(이름, 주민등록번호, 카드번호 등) 생성·저장·전송	개인정보
업무정보	업무데이터 등 중요정보의 생성·저장·전송	중요정보
암호화	중요정보의 외부유출을 방지하기 위한 암호화	암호알고리즘 암호화키

4와 같이 분류할 수 있다.

유형별 기능을 구현하기 위해서는 표 4에서 식별한 보안속성의 안전·신뢰성을 보장해야 한다. 따라서, 각각의 보안속성이 내부 단말에 안전하게 저장 및 관리되는지, 외부 서버로 안전하게 전송되는지 등을 점검해야 하며, 관련 법령[20,21]에 위배되지 않는지 점검해야 한다.

3.3.3. 모바일 플랫폼 제공 메커니즘

구글 안드로이드, 애플 iOS 등 각각의 플랫폼을 기반으로 모바일 앱을 개발할 때, 각 플랫폼에서 제공하는 보안기능을 최대한 활용하여 안전하게 개발할 수 있다. 예를 들어 애플 iOS 플랫폼은 비밀번호와 키 같이 기밀성이 요구되는 정보를 암호화하여 안전하게 보관해 주는 저장 공간인 키체인(Keychain) 메커니즘[17]을 제공하기 때문에 개발자는 인증서나 암호화키를 키체인 메커니즘을 통해 안전하게 관리할 수 있다.

오픈소스라고 할 수 있는 구글 안드로이드 플랫폼은 폐쇄적인 애플 iOS 플랫폼에 비해 보안메커니즘이 상대적으로 부족하며, 리눅스 기반의 플랫폼이라는 특성 때문에 구글 안드로이드 플랫폼 기반 개발자는 안전한 모바일 앱을 개발하기 위해 조금 더 주의를 기울여야 한다.

안드로이드 플랫폼은 앱이 SMS 메시지를 읽거나 위치정보를 얻을 수 있는 권한 등을 앱 설치시 사용자가 필요한 권한인지 여부를 판단할 수 있도록 AndroidManifest파일(.xml)에 관련 권한들을 정의할 수 있는 기능을 제공한다. 그러나, 안드로이드 플랫폼에서 정의된 권한들(표 5) 이외에도 개발자는 별

표 5. 안드로이드 플랫폼에서 정의한 주요 권한
Table 5. The main authority on the Android platform

주요 권한	설명
ACCESS_FINE_LOCATION	정밀한 위치정보를 얻을 수 있는 권한
BLUETOOTH	연결되어 있는 블루투스 장치를 사용할 수 있는 권한
INTERNET	네트워크 소켓을 열 수 있는 권한
READ_CONTACTS	연락처 정보를 읽을 수 있는 권한
READ_SMS	SMS 메시지를 읽을 수 있는 권한

도 권한을 정의할 수 있다. 예를 들어 사용자 위치 정보에 접근해서 SMS 메시지로 보낼 수 있는 권한을 'SEND_LOCATION_MESSAGE'로 정의할 수가 있다. 따라서, 모바일 플랫폼 측면의 보안취약점을 점검할 때 불필요한 권한이 개발자에 의해 정의되었는지 반드시 확인해야 한다.

또한, 안드로이드 플랫폼의 인텐트(Intents), 액티비티(Activities), 브로드캐스트(Broadcasts), 서비스(Services), 컨텐츠 프로바이더(ContentProviders)를 안전하게 사용하기 위한 다양한 방법들이 연구[7-9] 되었으므로 모바일 앱 검증시 안전하게 사용되었는지 확인해야 한다.

표 6[18,22], 표 7[17]과 같이 개인위치정보 등 중요정보에 접근하기 위해 사용되는 API들을 모바일 앱 검증시 확인하여 중요정보가 임의로 접근·전송되는지 등의 여부를 확인해야 한다.

애플 iOS 플랫폼은 중요정보에 대한 안전한 저장공간인 키체인, 안전한 난수를 생성할 수 있는 난수화 서비스(Randomization Services), 암호화에 사용하는 키 생성 및 암호화 등의 기능을 제공하는

표 6. 정보접근 관련 주요 안드로이드 API
Table 6. The main Android API which accesses information

구분	주요 API
파일접근	OpenFileOutput
	OpenFileInput
와이파이상태	isWifiEnabled
위치정보	getLatitude, getLongitude
콘텐츠 접근	getContentResolver
네트워크 접근	openConnection
	setRequestMethod

표 7. 정보접근 관련 주요 애플 API
Table 7. The main Apple API which accesses information

구분	주요 API
위치정보	CLLocationManager
	CLLocationDegrees
	CLLocatonDistance
주소록	ABRecordCopyValue
	ABPersonGetTypeOfProperty
	ABAddressBookCopyArrayOfAllPeople
	ABPersonCopyImageData
네트워크 상태확인	kSCNetworkReachablilityFlagsIsWWAN
	kSCNetworkReachablilityFlagsISDirect

표 8. 주요 소스코드 보안취약점
Table 8. The main security vulnerabilities in source code

구분	보안취약점
API 악용	함수 결과 검사 부재
보안기능	하드코드된 사용자 계정
	주석문 안에 포함된 패스워드
	전역적으로 접근 가능한 파일
	역산이 가능한 단방향 해쉬함수
시간 및 상태	경쟁조건 : 검사시점과 사용시점
	심볼릭명이 정확한 대상에 매핑되어 있지 않음
에러처리	오류 메시지 등을 통한 정보노출
	액션 없는 오류 조건 탐지
	포괄적 예외를 사용한 catch, throws 선언
입력데이터 검증 및 표현	XML 유효성 미검사
캡슐화	민감한 데이터를 가진 내부 클래스 사용
	공용메서드로부터 리턴된 private 배열-유형 필드
	시스템 데이터 정보 누출
코드품질	널포인터 역참조
	메모리 누수
	사용되지 않는 변수 및 필드
	항상 참 또는 거짓인 논리식

인증서·키·신뢰서비스(Certificate, Key, Trust Services) 등의 보안메커니즘을 제공한다. 따라서, 모바일 앱 검증시 플랫폼에서 제공하는 보안메커니즘을 사용하였는지 여부를 확인해야 한다.

3.2.4. 소스코드 관점 보안취약점

구글 안드로이드 기반 모바일 앱은 JAVA 기반의 Android JAVA로 구현하기 때문에 Android

표 9. 민간 앱스토어와 검증체계 비교
Table 9. Comparison of private app stores verification system

항목	민간 앱스토어 검증체계	앱 보안성 검증체계
개발 지원	· 개발가이드 · 개발지원도구(SDK 등)	· 개발보안가이드 · 개발보안교육
제출물	· 개발자 점검사항 · 실행코드(앱)	· 보안명세서 · 실행코드(앱) · 소스코드
보안성 점검	· 개인정보 · 위치정보 무단수집 · 활용여부 · 바이러스 · 악성코드 포함	· 구현오류 · 기능취약점 · 플랫폼 메커니즘 · 소스코드 취약점

JAVA 소스코드 보안취약점은 JAVA와 관련된 소스코드 보안취약점을 상속받는다고 할 수 있다.

애플 iOS는 가상 메모리 기술을 사용해서 당장 사용하지 않는 메모리의 일부분을 디스크에 저장해 두는 스와핑을 지원하지 않기 때문에 사용 가능한 메모리는 물리적인 메모리 공간으로 한정된다. 또한, 메모리가 부족한 경우 아이폰은 리부팅되기 때문에 애플 iOS 플랫폼에서 메모리 관리가 부적절할 경우 서비스거부공격(DoS, Denial of Service)이 유발될 수 있는 빌미를 제공하게 된다.

표 8[5]는 구글 안드로이드 및 애플 iOS 플랫폼 기반으로 구현된 모바일 앱과 관련된 주요 소스코드 취약점을 나타낸다. 따라서, 소스코드 정적분석을 통해 소스코드에 잔존하는 보안취약점을 제거해야 한다.

Ⅳ. 전자정부 모바일 앱 보안성 검증체계 분석 · 적용

제안한 모바일 앱 보안성 검증체계는 민간 앱스토어 검증체계와 비교(표 9)해서 보안명세서, 소스코드를 추가적으로 제출받아서 개인정보 · 위치정보의 무단수집 · 활용여부가 포함된 기능취약점, 구현오류, 모바일 플랫폼 보안메커니즘, 소스코드 취약점에 대해 검증을 수행한다. 또한, 발주기관 · 개발기관의 담당 공무원 및 개발자에게 개발보안교육 및 개발보안가이드를 제공하여 보다 안전한 전자정부 앱을 개발할 수 있는 환경을 제공한다.

기존 평가체계와 비교(표 10)해봤을 때, 모바일 앱은 IT제품 및 정보보호제품보다 규모가 매우 작기 때문에 요구하는 문서는 최소로 하면서 기능 중심의 보안성을 검증하기 때문에 보다 효율적으로 모바일 앱의 보안성을 검증할 수 있다.

제안한 모바일 앱 보안성 검증체계의 효과를 분석하기 위해 '11년 5월부터 8월까지 제안된 검증체계에 따라 시범검증을 진행하였다. 검증대상은 운영체계 유형, 위치정보 등 중요정보 활용 여부를 고려하여 구글 안드로이드 기반 앱 9종, 애플 iOS 기반 앱

표 10. 주요제출물 및 평가항목 기반 유사 제도 분석
Table 10. Analysis of similar systems based on the main submissions and assessment items

구분	GS	CC	모바일 앱
제출 문서	· 설명서	· 보안목표명세서 · 설계서 · 설명서 · 시험서	· 보안명세서
평가 항목	· 품질(기능성 등) · 업무적합성	· 문서보증사항 · 기능정상동작 · 보안취약점(기능, 소스코드)	· 기능정상동작 · 보안취약점(기능, 소스코드)

그림 3. 구현기능수(평균)
Fig. 3 The number of implemented features(Average)

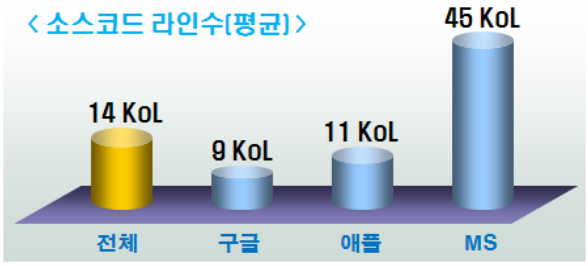

그림 4. 소스코드 라인수(평균)
Fig. 4 The number of lines in source code(Average)

그림 5. 보안취약점 건수(평균)
Fig. 5. The number of security vulnerabilities(Average)

9종, MS 윈도우모바일 6.5 기반 앱 2종 등 전체 20개 앱을 선정하였다. 선정된 앱의 평균 구현기능은 30개였으며, 평균 1.4만라인 이었다(그림 3, 그림 4).

시범 검증한 결과, 평균 2.5개의 기능오류가 존재하였으며, 패스워드 평문 전송 등 평균 1.25개의 보안기능 취약점을 발견하였다. 그리고, '매우낮음' 이상의 소스코드 취약점은 앱당 평균 77개(천라인당 5.6개) 였으며, '높음' 이상의 취약점만 고려할 경우 앱당 평균 16.6개 취약점(1,000라인 당 1.2개)이 존재하였다(그림 5).

시범검증을 통해 모바일 전자정부서비스 앱 관련 보호자산과 보안위협을 식별하였으며, 식별된 보안위협에 대응할 수 있는 기능 관점의 보안 요구사항을 도출하였다. 그리고, 보안취약점 세부 검증항목을 보완하였다. 식별된 보안위협 및 보안 요구사항은 <부록 1>에 기술하였으며, 세부 검증기준 및 항목은 <부록2>에 기술하였다. 보완된 세부 검증기준 및 항목을 기반으로 모바일 전자정부서비스 앱 검증신청기관을 위한 '모바일 앱 보안성 검증안내서[23]'를 발간('11년 8월)하고, '11년 9월부터 제안한 검증체계에 따라 모바일 앱 보안성 검증서비스를 제공하고 있다.

또한, '11년 9월에 구글 안드로이드 및 애플 iOS 플랫폼 기반 앱 개발자를 대상으로 기능관점 보안 고려사항, 플랫폼 보안메커니즘, Android JAVA 및 Objective C 언어 기반 소스코드 보안취약점에 대해 2회 교육을 실시하였다.

V. 결 론

본 논문에서는 모바일 앱 보안성 검증기술 관련 국내·외 연구동향, 국내외 민간 앱스토어의 검증체계, 소프트웨어 평가기준 및 체계 분석을 통해 모바일 앱 보안성 검증체계 및 수준을 정의할 수 있었다.

전자정부 모바일 앱의 보안성을 검증하기 위해 민간 앱스토어의 검증체계 및 소프트웨어 평가기준을 그대로 적용하기에는 제한사항이 있으므로 본 논문에서는 전자정부 모바일 앱의 안전·신뢰성을 보장할 수 있는 검증기준 및 절차 등 모바일 앱 보안성 검증체계를 제시하였다. 그리고, 모바일 앱 보안성 검증체계를 기반으로 시범 적용한 결과를 제시함으로써 본 논문에서 제안하는 검증체계의 실효성을 증명하였다.

또한, 본 논문에서 제시하는 검증기준 및 항목을 민간 앱스토어에서 자체 검증체계에 적합하게 수용하여 적용하면 보다 모바일 앱에 대한 보안성이 높아질 것으로 기대한다.

향후, 본 논문에서 제안한 검증체계를 기반으로 모바일 앱의 보안성 검증에 적용한 효과를 분석하고, 제안한 검증기준 및 항목을 자동화하여 검증할 수 있는 자동화 도구를 개발할 예정이다.

참 고 문 헌

[1] 중앙일보, "스마트폰 앱 80만명 위치정보 빼가", Apr. 2011

[2] 허재두 등, "모바일 앱스토어 기술 동향", *전자통신동향분석*, 제25권 제3호, pp.52-61, 2010

[3] 정보통신부, "공공부문 SW사업 발주·관리 표준 프로세스", *한국정보통신표준(KICS.KO-09.0038)*, 2007

[4] ISO/IEC 15408:2009, "Common Criteria for Information Technology Security Evaluation Version 3.1"

[5] 행정안전부, "소프트웨어 개발보안 가이드", *발간등록번호(11-1311000-000330-10)*, 2011

[6] Adrienne Porter Felt, Matthew Finifter, Erika Chin, Steve Hanna, David Wagner, "A survey of mobile malware in the wild", *Proceedings of the 1st ACM workshop on Security and privacy in smartphones and mobile devices*, Oct. 2011

[7] J. Burns, "Developing Secure Mobile Applications for Android", *iSEC Partners*, 2008

[8] W. Enck, M. Machigar, and P. McDaniel, "Understanding Android Security", *IEEE Security & Privacy*, pp.50-57, 2009

[9] A. Shabtai, U. Kanonov, Y. Elovici, S. Dolev, and C. Glezer, "Google Android: A Comprehensive Security Assessment", *IEEE Security & Privacy*, pp.35-44, 2010

[10] David Wetherall, Ben Greenstein, Seungyeop Han, Peter Hornyack, Jaeyeon Jung, Stuart Schechter, Xiao Wang, David Choffnes, "Privacy Revelations for Web and Mobile Apps", *Proceedings of HotOS*, May 2011

[11] M. Egele, C. Kruegel, E. Kirda, and G. Vigna, "PiOS: Detecting Privacy Leaks in iOS Applications", *NDSS*, 2011

[12] Peter Gilbert, Byung-Gon Chun, Landon Cox, and Jaeyeon Jung, "Vision: Automated Security

Validation of Mobile Apps at App Markets", *Proceedings of Workshop on ACM Mobile Cloud Computing & Services*, June 2011
[13] William Enck, Machigar Ongtang, and, Patrick McDaniel, "On lightweight mobile phone application certification", *Proceedings of the 16th ACM conference on Computer and communications security*, Nov. 2009
[14] KT Olleh마켓, *http://seller.ollehmarket.com*
[15] LGU+ OZ스토어, *http://devpartner.lguplus.co.kr*
[16] SKT T스토어, *http://dev.tstore.co.kr*
[17] 애플 앱스토어, *http://developer.apple.com*
[18] 구글 안드로이드마켓, http://market.android.com
[19] BSI, http://buidsecurityin.us-cert.gov
[20] 방송통신위원회, "위치정보의 보호 및 이용 등에 관한 법률(시행 2010.9.23)", *법률 제10166호*, 2010
[21] 행정안전부, "개인정보 보호법(시행 2011.9.30)", *법률 제10465호*, 2011
[22] KISA, "모바일 운영체제 기반의 악성코드 대응 기법 연구", 2010
[23] 한국인터넷진흥원, "모바일 앱 보안성 검증 안내서", *행정안전부 · 한국인터넷진흥원*, Aug. 2011

방 지 호 (Jiho Bang) 정회원

1996년 2월 홍익대학교 컴퓨터공학과 졸업
2001년 8월 홍익대학교 컴퓨터공학과 석사
2004년 3월~현재 홍익대학교 컴퓨터공학과 박사과정
2001년 7월~2009년 7월 한국정보보호진흥원
2009년 7월~현재 한국인터넷진흥원 책임연구원
<관심분야> 모바일/SW보안, 모바일컴퓨팅, 실시간 시스템 등

하 란 (Rhan Ha) 정회원

1987년 2월 서울대학교 컴퓨터공학과 졸업
1989년 2월 서울대학교 컴퓨터공학과 석사
1995년 4월 University of Illinois at Uubana-Champaign 전산학 박사
1989년 3월~1990년 7월 한국통신 전임연구원
1995년 9월~현재 홍익대학교 컴퓨터공학과 교수
<관심분야> 모바일컴퓨팅, 실시간시스템, SW보안 등

강 필 용 (Pilyong Kang) 정회원

1996년 2월 숭실대학교 컴퓨터공학과 졸업
1998년 2월 숭실대학교 컴퓨터공학과 석사
2001년 8월 숭실대학교 컴퓨터공학과 박사
2001년 9월~2009년 7월 한국정보보호진흥원
2006년 5월~2006년 11월 카네기멜론대학교 방문연구원
2009년 7월~현재 한국인터넷진흥원 팀장
<관심분야> SW보안, 시스템/네트워크 보안, 전자서명 등

김 홍 근 (Honggeun Kang) 정회원

1985년 2월 서울대학교 컴퓨터공학과 졸업
1987년 2월 서울대학교 컴퓨터공학과 석사
1994년 2월 서울대학교 컴퓨터공학과 박사
1994년 5월~1996년 5월 한국전산원
1996년 5월~2009년 7월 한국정보보호진흥원
2009년 7월~현재 한국인터넷진흥원 단장
<관심분야> 병렬처리, 컴퓨터 보안, 소프트웨어 보안 등

〈부록 1〉 주요 보안위협 및 보안 요구사항

1. 보안위협

모바일 서비스를 제공하는 모바일 앱(또는 웹) 서버와 모바일 단말기에 설치·운영되는 모바일 앱으로 구성되는 모바일 소프트웨어의 안전·신뢰성 제고를 위해 개발단계에서 고려해야 하는 보안위협은 다음과 같이 분류할 수 있다.

〈 주요 보안위협 〉

보호자산	보안위협	주요보안고려사항
인증정보	사용자 패스워드 등 인증정보가 입력 및 전송단계 등에서 유출되거나 약한 수준의 패스워드 길이·조합규칙으로 쉽게 유추할 수 있어 인증정보가 도용·악용될 수 있는 보안위협	인증정보 보호
개인정보	서비스 이용 등을 위해 사용되는 개인정보(이름, 주민등록번호 등)가 임의 생성·수집되고 부적절하게 관리되어 유출되어 도용·악용될 수 있는 보안위협	저장·전송데이터 보호
개인위치정보	사용자의 위치가 임의 생성·수집되거나 부적절하게 관리되어 불법적으로 사용자 위치가 식별 및 추적될 수 있는 보안위협	저장·전송데이터 보호
업무정보	내부메일, 결재문서 등의 기관의 내부 업무정보가 모바일 단말기에 평문으로 저장 및 전송되어 외부에 유출될 수 있는 보안위협	저장·전송데이터 보호
금융정보	세금납부를 위한 금융정보(카드정보, 계좌정보 등)가 평문으로 저장·전송되어 유출·도용될 수 있는 보안위협	저장·전송데이터 보호
암호화정보	취약한 비밀성·무결성 알고리즘(DES, MD5 등)을 사용하거나 암호키(seed 값, 비밀키 등)가 평문으로 저장·전송되어 암호화된 정보 및 암호키가 외부에 유출될 수 있는 보안위협	암호알고리즘 및 암호키 안전성
앱구현기능	외부 입력값에 대한 유효성 검증 부재 또는 부적절한 유효성 검증으로 발생할 수 있는 인증정보 등 중요정보 유출, 예상치 못한 기능 동작을 발생시킬 수 있는 보안위협	외부 입력값 유효성 검증
시스템정보	구현된 기능오류, 예외처리 등으로 인한 오류정보 출력시 과도하게 시스템 정보가 노출되어 공격자에게 간접적인 공격정보를 제공하는 보안위협	과도한 시스템 정보노출 차단

2. 기능 관점 보안 요구사항

식별된 보안위협에 대응할 수 있는 모바일 전자정부 서비스 앱의 기능 관점 보안 요구사항은 다음과 같다.

1) 식별 및 인증

가. 사용자 유형별 기능제한

〈 주요 보안 요구사항 〉

가. 관리자는 모바일 단말기를 통한 원격접속은 제한되어야 하며, 로컬 네트워크 또는 시리얼통신을 통해 신뢰된 구간에서만 접속해야 한다.
단, 전송데이터 보호 및 단말보안을 위한 보안인프라가 제공되는 경우, 정책 변경을 제외한 정책 열람 등의 제한적인 기능만 구현 가능하다.
나. 내부직원은 해당기관 그룹웨어 또는 오프라인 방식을 통해 내부직원 등록과정을 수행해야 하여 旣 승인된 사용자만 내부행정업무 앱 사용이 가능해야 한다.
다. 내부직원은 아이디/패스워드 방식 이외에 GPKI 인증서로 인증하여야 한다.
라. 일반사용자는 아이디/패스워드 방식으로 식별 및 인증할 수 있으며, NPKI를 적용할 수 있다.

나. 식별 및 인증정보 입력·설정

〈 주요 보안 요구사항 〉

가. 아이디는 英대소문자, 숫자 등의 문자열을 조합할 수 있으며, 최소 6자리 이상의 길이를 가져야 한다.
나. 패스워드는 英대소문자, 숫자, 특수문자 등의 문자열을 조합할 수 있으며, 2가지 종류의 문자를 조합할 경우 10자리 이상, 3가지 종류의 문자를 조합하면 8자리 이상의 패스워드 길이를 가져야 한다.
다. 아이디 및 패스워드는 사전공격(Dictionary Attack)이 가능한 사전식 단어를 사용하지 않아야 한다.

다. 인증정보 입력·피드백 보호

〈 주요 보안 요구사항 〉

가. 모바일 단말자판 입력정보 유출로 인한 인증정보 입력 내용 유출을 방지하기 위해 인증정보를 식별할 수 없도록 표시되어야 한다(예, '*' 문자 등).
나. 패스워드 입력 실패에 대한 인증시도 횟수 제한하는 패스워드 관리방안을 수립하고 이를 구현해야 한다.
다. 키로거 등을 통해 입력정보가 유출되지 않도록 가상키보드 등과 같은 입력방식을 적용해야 한다.
라. 팝업 등의 형태로 사용자에게 인증실패의 원인 제공시, 인증정보 유추할 수 있거나 인증시도 노력을 줄여줄 수 있는 정보를 제공하지 않아야 한다.

라. 인증정보의 안전한 관리

〈 주요 보안 요구사항 〉

가. 패스워드는 모바일 단말기에 저장하지 않아야 하며, 별도 저장시 암호화하여 저장해야 한다. 단, 외장메모리(SD카드)에 저장하지 않아야 한다.
단, 저장위치는 일반 메모리 또는 SD카드
나. 패스워드는 전송시 암호화하여 전송해야 한다.
다. 인증서(GPKI, NPKI 등)는 안전하게 저장 및 관리되어야 한다.
라. 인증정보가 포함된 쿠키정보로 추가적인 사용자 인증을 대체하는 경우, 세션 종료후 쿠키정보를 삭제해야 하며, 임시 저장시 쿠키정보를 도용할 수 없도록 암호화해야 한다.

2) 저장・전송데이터 보호

가. 개인정보

〈 주요 보안 요구사항 〉

가. 모바일 단말기의 기본 앱(전화번호부, 메시지, 메모 등)에서 관리하는 개인정보에 사용자 동의 없이 임의로 접근하지 않아야 한다. 나. 앱에서 생성되거나 서버에서 전송된 개인정보를 모바일 단말기에 별도 저장시 암호화하여 저장해야 한다. 다. 생성되거나 저장된 개인정보를 앱(또는 웹) 서버로 전송시 암호화하여 전송해야 한다. 라. 모바일 앱(또는 웹) 서버로 전송된 개인정보 저장시, 암호화하여 안전하게 관리하여야 한다.

나. 개인위치정보

〈 주요 보안 요구사항 〉

가. 개인위치정보를 이용하기 위해 개인위치정보를 생성・저장・전송시, 생성・이용목적, 저장・보유기간 등을 명시하고 사용자 동의를 받아야 한다. 나. 개인위치정보 이용 목적에 부합하지 않는 기능은 삭제되어야 한다. 다. 개인위치정보를 모바일 단말기에 저장・전송시, 암호화하여 저장・전송해야 한다. 라. 모바일 앱(또는 웹) 서버로 전송된 개인위치정보 저장시, 암호화하여 안전하게 관리하여야 한다.

다. 업무정보

〈 주요 보안 요구사항 〉

가. 모바일 앱(또는 웹) 서버에서 전송된 업무정보는 모바일 단말기에 저장되지 않아야 하며, 필요시 서비스 종료시까지 암호화하여 임시 저장할 수 있다. 나. 모바일 앱에서 생성한 업무정보를 내부 앱(또는 웹) 서버로 전송시, 암호화하여 전송해야 한다.

라. 금융정보

〈 주요 보안 요구사항 〉

가. 금융정보는 모바일 단말기에 저장되지 않아야 한다. 나. 금융정보를 내부 앱(또는 웹) 서버로 전송시, 암호화하여 전송해야 한다.

3) 암호알고리즘 및 암호키 안전성

가. 비밀성・무결성 알고리즘

〈 주요 보안 요구사항 〉

가. 취약한 비밀성 알고리즘(예, DES 등) 및 무결성 알고리즘(예, MD5 등)을 사용하지 않아야 한다. 나. 국가정보원 국가사이버안전센터(NCSC)에서 검증된 암호모듈 사용을 권고한다.

나. 암호키

〈 주요 보안 요구사항 〉

가. 암호키 생성에 사용되는 초기(Seed) 값은 일정 수준의 복잡도(Entropy) 및 난수성을 보장해야 한다. 나. 초기(Seed) 값 및 암호키는 외부에 유출되지 않도록 평문으로 저장・전송하지 않아야 한다.

4) 외부 입력값 유효성 검증

가. 사용자 입력

〈 주요 보안 요구사항 〉

가. 사용자가 정수 입력시, 지정된 길이를 초과하지 않도록 정수값의 길이 및 부호를 점검해야 한다. 나. 사용자가 문자(열) 입력시, 지정된 길이를 초과하지 않도록 문자열의 길이를 점검해야 한다. 다. 사용자가 정수 또는 문자(열) 입력시, 부적절한 데이터 형변환이 발생하지 않도록 주의해야 한다. 라. 사용자가 정수 또는 문자(열) 입력시, 부적절한 데이터(예, SQL 인젝션, 경로조작 등)가 포함되지 않도록 정해진 데이터 값만 입력받을 수 있도록 입력값을 제한하는 것이 필요하다.

나. 파일시스템 등을 통한 입력

〈 주요 보안 요구사항 〉

가. 파일을 통해 입력받은 데이터에 악성코드가 포함되어 있지 않은지 입력값에 대한 유효성을 점검해야 한다. 나. 입력값으로 사용되는 설정파일의 널값(NULL 또는 NIL) 여부를 점검해야 한다. 다. 입력값으로 사용되는 설정파일 등에 대한 파일에 주기적인 바이러스 검사가 권고된다.

5) 상세한 시스템 정보노출 차단

가. 디버깅 코드

〈 주요 보안 요구사항 〉

가. 앱 배포시, 디버깅 코드는 삭제해야 한다. 나. 예외 또는 오류처리 메시지 안에 디버깅 수준의 메시지가 출력되지 않도록 해야 한다.

나. 오류처리

〈 주요 보안 요구사항 〉

가. 오류메시지에 시스템 버전, 설치된 소프트웨어(웹서버, DB 등) 정보 등 시스템의 상세한 정보가 제공되지 않아야 한다. 나. 오류발생시, 사전에 정의된 오류메시지가 출력되도록 구현하는 것이 권고된다.

〈부록 2〉 검증기준 및 항목

1. 규제(법·지침 등) 준수 점검

다음과 같은 법·지침 등의 요구사항에 위배되지 않아야 한다.

1) 개인정보 보호 관련 법·지침

개인정보보호법, 정보통신망 이용촉진 및 정보보호에 관한 법률·시행령
☑ 개인정보 수집·저장·전송 등 보안 요구사항
- 개인정보 수집시, 법에서 언급된 불가피한 경우를 제외하고 정보주체 동의를 받아야 함
- 개인정보를 암호화하여 안전하게 저장 및 전송
- 개인정보 불필요시(보유기간 경과, 처리목적 달성 등) 복구·재생되지 않도록 파기해야 함
- 이용자의 개인정보 및 인증정보를 송·수신하는 경우 보안서버 구축 등의 조치를 취해야 함

2) 위치정보 보호 관련 법·지침

위치정보의 보호 및 이용 등에 관한 법률·시행령
☑ 위치정보 수집·저장·전송 등 보안 요구사항
- 개인정보 수집시, 긴급구조기관의 긴급구조 등을 제외하고 위치정보주체 동의를 받아야 함
- 개인위치정보의 수집·이용, 제공목적 달성시, 개인위치정보는 즉시 파기해야 함
- 위치정보의 누출·변조, 훼손 등을 방지해야 함

3) 개인정보 및 위치정보 이외 비밀번호 등 중요정보 보호 관련 법·지침

전자정부법 시행령, 정보통신망 이용촉진 및 정보보호에 관한 법률·시행령, 행정기관 정보시스템 접근권한 관리 규정, 정보시스템 구축·운영지침(안)
☑ 사용자 인증 및 계정관리 보안 요구사항
- 업무담당 및 시스템 관리자 인증은 행정전자서명 사용
- 민원인의 경우, 아이디/비밀번호를 사용하고 신분증명이 필요한 경우 공인인증서 사용
- 비밀번호 조합규칙(영문·숫자·특수문자 등 조합 9자리 이상 등) 및 일방향 암호화 저장

☑ 중요정보에 대한 보안 요구사항
- 주민등록번호 및 계좌정보 등 금융정보의 암호화 저장

4) 모바일 서비스 관련 보안가이드

SW 개발보안 가이드 등
☑ 모바일 전자정부서비스 앱 개발 대한 보안 요구사항
- 기능(식별 및 인증 등), 플랫폼, 소스코드에 대한 보안취약점이 잔존하지 않아야 함

2. 기본동작 점검

앱 보안취약점 검증을 위한 기본 전제조건으로 다음 사항을 만족해야 한다.

1) 앱 설치 및 삭제가 정상적으로 이루어져야 한다.

☑ 앱 설치 및 삭제시 오류 발생 여부

2) 구현된 기능이 정상적으로 동작해야 한다.

☑ 구현된 기능 동작시 오류 발생 여부

3. 보안취약점 점검

개발자 및 검증자에 의해 식별된 보안위협을 기반으로 다음 점검항목을 만족해야 한다.

1) 기능설명(예, 보안명세서, UI명 등) 내용과 실제 앱 기능이 일치해야 한다.

☑ 명세되지 않은 기능 존재 여부
☑ 악성행위(예, 불법 녹음, 임의 데이터 전송, 임의로 위치정보 수집·전송 등) 기능 존재 여부

2) 기능 동작에 필요한 최소 권한만 부여되어야 한다.

☑ 관리자 권한으로 동작되는 기능 존재 여부

3) 외부 입력정보를 기반으로 기능 동작시, 입력정보에 대한 유효성을 검증해야 한다.

☑ 외부 입력값의 유효성(예, 지정된 길이 초과, 악성코드 포함 등) 검증 기능 존재 여부

4) 중요정보(개인정보, 개인위치정보, 업무정보 등)는 안전하게 관리(저장, 전송 등)되어야 한다.

☑ 중요정보 저장·전송시 암호화 여부
☑ 필요시, 앱(또는 웹) 서버의 중요정보 관리기능 점검

5) 구현기능은 모바일 플랫폼의 보안모델에 위배되지 않아야 한다.

☑ 루팅, 탈옥 등과 같은 플랫폼 변조 기능 존재 여부
☑ 플랫폼에서 제공하는 보안기능 사용 여부

6) 구현언어 기반 소스코드 보안취약점(예, CWE, CWE/SANS Top25, 소프트웨어 개발보안 가이드 등)이 발견되지 않아야 한다.

☑ 입력데이터 검증 및 표현, API 악용, 보안특성, 시간 및 상태, 에러처리, 코드품질, 캡슐화 등 소스코드 취약점 분류에 따라 신청제품의 소스코드에 관련 취약점 존재 여부

7) 상용 또는 공개 모듈(소스코드 미제공)을 사용하여 기능 구현시, 해당 모듈에 대한 안전성은 보증되어야 한다.

☑ 상용 또는 공개모듈 사용 목적 및 기능의 적절성 여부
☑ 해당 모듈에 대한 개발업체의 안전성 확인 방법 및 결과의 적절성 여부

8) 안전한 모바일 전자정부서비스 제공을 위해 구축되는 공통인프라가 제공하는 보안기능이 검증제품에 필요한 경우, 공통인프라 기능을 사용하거나 그에 준하는 기능을 구현해야 한다.

☑ '('11년) 모바일 전자정부서비스를 위한 공통기반 구축 사업'에 따라 구축되는 보안인프라에서 제공하는 기능 사용 여부

9) 공개영역(예, 논문, 웹사이트 등) 등을 통해 잘 알려진 보안취약점이 발견되지 않아야 한다.

☑ 모바일 플랫폼(예, 안드로이드, iOS, 윈도우모바일 6.5/윈도우7 등), 개발언어(예, 안드로이드 자바, Objective C, C# 등) 등에 대한 알려진(및 신규) 취약점 존재 여부

10) 그 외(위 1~9번 항목), 검증대상 제품에 특화된 보안취약점이 발견되지 않아야 한다.

☑ 신청제품의 서비스 특성에 따른 추가적인 보안취약점 존재 여부