국방환경에서 모바일 앱 관리체계 구축방안 제시
- 국방 앱스토어 및 검증시스템 중심으로 -

이갑진* · 고승철**

A Guidelines for Establishing Mobile App Management System in Military Environment
- focus on military App store and verification system -

Gab-jin Lee* · Sung-cheol Goh**

요 약

최근 빠르게 대중화된 스마트폰은 이제 생활 필수요소로서 우리의 삶 속 깊숙이 자리 잡고 있으며, 다양한 기능을 제공하는 애플리케이션(앱)은 쇼핑, 뱅킹, SNS, 게임 등 풍부한 서비스는 물론 효율적인 업무 수행을 위한 스마트워크 모바일 오피스 등의 영역으로 확산되고 있다. 그러나 이러한 스마트폰 앱은 앱스토어라 불리는 애플리케이션 마켓에서 쉽게 다운로드가 가능한 반면 개발자들 또한 쉽게 업로드 할 수 있어 많은 보안 위협이 존재하고 있다. 따라서 작전용 앱은 민간 앱과 동일하게 인터넷 기반의 상용 앱스토어를 통해 배포할 경우 각종 보안위협에 노출될 수밖에 없다. 이러한 현실을 극복하기 위해, 본 연구에서는 군내 스마트기기에서 사용할 군용 앱 개발 배포 시 보안점검 및 각종 위해 요인의 사전 차단이 통합적으로 수행 가능한, 군전용 밀리터리 앱스토어와 앱 보안성 검증시스템의 구축 방안을 제시하고자 한다.

ABSTRACT

Recently. smartphones have been popularized rapidly and now located deep in our daily life, providing a variety of services from banking, SNS (Social Network Service), and entertainment to smart-work mobile office through apps. Such smartphone apps can be easily downloaded from what is known as app store which, however, bears many security issues as software developers can just as easily upload to it. Military apps will be exposed to a myriad of security threats if distributed through internet-basis commercial app store. In order to mitigate such security concerns, this paper suggests a security guidelines for establishing a military-excusive app store and security verification system which prevent the security hazards that can occur during the process of development and distribution of military-use mobile apps.

키워드

앱스토어, MDM(모바일 단말기 관리체제), 모바일 보안 위협, 보안성 검증시스템

Key word

Appstore, MDM(Mobile Device Management), Mobile Security Threats, Security Verification System

* 정회원 : 수원대학교 (leegabjin0226@yahoo.co.kr)
** 정회원 : 수원대학교 (교신저자)

접수일자 : 2013. 02. 01
심사완료일자 : 2013. 02. 17

Open Access http://dx.doi.org/10.6109/jkiice.2013.17.3.525

Ⅰ. 서 론

최근 스마트폰이 대중화되면서, 다양한 정보사용이 가능한 모바일 애플리케이션(이하 '앱(App)')이 크게 주목받고 있다. 스마트폰 사용자들은 시간・공간적으로 제한을 받지 않고 금융・교통・취미활동 등을 하기 위해 모바일 앱을 이용하고 있으며, 정부 및 기업들은 다양한 기능의 모바일 앱을 개발하여 언제 어디서도 업무결재가 가능한 '모바일 오피스' 시스템을 도입하는 등 다양한 업무용 앱 개발이 확산되고 있다[1].

이러한 스마트폰과 앱스토어의 대중화로, 모바일 앱의 군사적 활용 또한 재평가되고 있으며 미국을 비롯한 각국에서 군용 스마트폰과 앱 개발 등 군사적 활용 분야에 대한 도전이 활발히 진행되고 있다.

한편 모바일 앱・앱스토어의 비약적인 발전과 함께 새로운 보안 위협들이 등장하였고 그 규모와 피해 또한 급속도로 증가하고 있다. 오픈마켓의 개방성을 악용한 악성 앱은 사용자들의 개인정보를 빼내거나 모바일 기기를 임의 통제하는 등 모바일시대의 심각한 보안위협 요소가 되었으며 실제로 구글 안드로이드 OS를 타깃으로 하는 악성코드의 수가 2012년도 3/4분기에만 5만개를 넘어선 것으로 분석되었고 그에 따른 피해사례들도 그 규모와 빈도에서 급증세를 보이고 있다[2].

이와 같은 피해를 예방하고 최소화하기 위해, 국내에서도 모바일 단말기 기반 전자 행정의 안전성을 강화할 목적으로, 전자정부 모바일 앱 보안성 검증센터를 구축 및 시범 운영하고 있다[3].

이러한 현실을 고려 시, 보안성이 중요한 군사용 앱을 민간 앱과 동일하게 인터넷 기반의 상용 앱스토어를 통해 배포할 경우 각종 보안위협에 노출될 수밖에 없다.

따라서 본 연구에서는 군사용 앱 개발 및 배포 시, 보안점검 및 각종 위해 요인의 사전 차단이 통합적으로 수행 가능한 국방 앱스토어와 앱 보안성 검증시스템의 구축 방안을 제시하고자 한다.

Ⅱ. 국내・외 국방 앱 활용 동향 및 보안과제 도출

스마트폰의 급속한 보급과 다양한 앱 활용은 민간분야를 넘어 국방 분야에까지 확산되어, 현재 우리나라를 비롯한 많은 국가들이 전장 환경에서도 활용 가능한 앱들을 개발하고 있다.

2.1. 국외 군사용 앱 활용 현황

미군에서는 전용 비화스마트폰(SME-PED)을 개발, 영관급 이상 주요 직위자에게 보급하여 상용망을 이용한 모바일오피스를 활용하고 있다[4].

또한 군사작전 전용 단말기(GD300)도 개발하여 미 육군 전술지휘통제체계에 연동, 활용성을 시험평가 완료하였으며 군사용 앱을 탑재해 피아위치식별, 표적 영상정보 획득, 지도확인, 목표까지의 이동정보를 표시할 수 있다[5].

이러한 정부주도의 앱 이외에도 민간 군수업체에서 제작하여 사용되는 작전용 앱도 활용 중에 있는데, 'V 커뮤니케이터'는 타국에서 작전을 수행하는 장병들을 위한 통역 앱으로 현재 국제적 작전지역을 담당하고 있는 미군에서 현지 언어 소통을 위해 사용하고 있다[1].

이와 유사한 앱으로 미국의 DARPA(Defense Advanced Research Projects Agency)에서 개발 중인 언어 번역 앱인 'TRANSTAC'은 아랍어와 중국어로 표현된 비공식 대화, 이메일, 텍스트, 방언 등을 영어로 실시간 쌍방향 번역 기능을 갖추고 있다.

'ARMAR'은 미 해병대에서 사용하는 군사용 앱으로 증강현실 기술을 이용하여 장비 유지보수 및 고장수리에 활용되고 있는데 스마트폰 화면에서 장비에 관한 말풍선 형태의 설명과 정비 절차에 대한 내용을 볼 수 있어 기계에 대해 잘 모르는 사용자라도 장비의 유지보수 및 고장조치가 가능하다[6].

레이시온사에서 개발한 'One Force Tracker'는 3G 네트워크, GPS, 전자나침반을 이용하여 현재 자신의 위치, 아군의 위치, 적의 위치를 전술상황 화면에 표시해 주는 기능을 갖고 있다. 이 앱은 미군 여단급 이하 지휘통제체계의 전술 네트워크 장비에서 볼 수 있는 높은 수준의 전술적 기능들을 구현하고 있어 이를 통해 연대에서 분대

1) 2011년 3월 15일 국방일보

차량으로 직접 상황전파가 가능하다.

스마트폰과 앱을 군사적 용도로 활용하려는 노력은 미국뿐만 아니라 여러 강대국들로 확산되고 있다. 영국은 이미 2010년 아프가니스탄에 파병될 병사들을 훈련하는데 아이패드 앱을 사용했다. 이 앱은 작전 환경에 필요한 사전지식을 습득하고 작전상황시 목표물의 위치를 전송하거나 보충인원을 요청하는 등의 실질적인 보고절차 등을 숙달하는데 활용되었다[7].

독일군 또한 국민과의 소통과 대국민 홍보를 위해 스마트폰 앱을 활용하고 있으며 군 관련 뉴스, 동영상, 이미지 및 모병 관련 소식 등을 실시간으로 제공하고 있다. 중국 또한 이와 유사한 군 전용 앱을 개발해 인민군의 최신 소식을 제공하고 있다.

2.2. 국내 군사용 앱 활용 현황

우리 군에서도 이러한 스마트폰 앱의 유용성을 인식하여 다양한 대민서비스용 앱을 제작・운용 중에 있으며 일부 작전용 앱도 제작하여 시험평가 중에 있는 것으로 확인되었다.

대민서비스용 앱의 경우 2011년 7월 이후 현재까지 20여개에 이르는 앱을 개발하여 운용 중에 있으며 대부분 복지시설 예약 또는 훈련소 정보제공 및 자군 홍보 앱이다.

다음은 현재까지 개발되어 활용되고 있는 대민서비스용 앱 현황이다.

표 1. 국방 분야 대민서비스용 앱 현황[8]
Table. 1 Military apps for civilian service

국방부 및 국직	국방웹툰, 국방부 예비군 앱
육군	육군훈련소, 육군부사관학교, 3사관학교 홍보앱, 입대장정 길라잡이, 육군모집, 육군 헌병
해군	해군사관학교, 해군교육사 홈페이지, 해군 체력단련장, 해군교육사 아이폰, 항공용어사전
공군	공군 모바일 앱, 공군 모바일 호텔콘도, 공군 모바일 체력단련장, 공군 아이폰, 군 기상 앱, 인터넷 차단 앱, 범죄신고센터

또한 지난 2012년에는 국방 정보보호 컨퍼런스 일환으로 개최된 “국방 보안 앱 개발 경진대회‘를 통해 국직부대 및 각 군에서 보안을 목적으로 모바일 앱을 개발하는 등 점차 국방업무에도 모바일 앱의 필요성을 인식하고 활용성이 증가하고 있다.

2.3. 국방 앱과 앱스토어 보안과제 도출

현재 국방에서 운용되고 있는 앱은 대부분 홍보, 부대소개 등 대민서비스용으로 구글 플레이스토어나 애플 앱스토어에 탑재되어 배포・활용됨에 따라 상용 앱・앱스토어를 대상으로 한 보안위협에 동일하게 노출되어 있다고 할 수 있다.

특히 군 위상제고 관점에서 주요이슈로 취급하는 것은 정보유출과 악성코드 유포지로 활용되는 것이라 할 수 있다.

정보유출 위협의 경우, 대민서비스용 앱 사용자들이 본인확인간 사용하는 주민등록번호나 비밀번호가 암호화되지 않고 평문으로 전송될 경우, 개인정보 노출로 인한 2차 피해 우려는 물론 개인정보보호법 위반사항[2]으로 간주될 수 있기 때문에 민감한 사항이다[9].

또한, 앱 개발간 미흡한 오류처리나 주석문에 포함된 시스템 주요 정보 등은 악의적인 공격을 위한 프로그램 구조 파악에 유용한 정보로서 악의적 공격자가 활용시 해당 앱을 감염시키거나 앱 서버를 악성코드 유포지로 전용 가능하기 때문에 더욱 주의를 요하고 있는 보안성 검증 항목이라 할 수 있다

만약 이러한 취약점으로 인해 대민 서비스용 앱으로 위・변조된 악성 앱이 미흡한 보안성 검증절차로 인하여 앱스토어에 게시되고 배포된다면 보안을 중요시하는 군이 개인정보를 노출하거나 DDoS와 같은 악의적인 공격 행위자로 오인될 수도 있으며, 특히 대민서비스용 앱들과 달리 현재 시범사업으로 진행 중인 군사작전 초동조치용 및 미래 작전용 앱을 상용 앱스토어에 게시・배포할 경우에는 내부 서버 자료 탈취 및 업무마비 등 광범위한 공격으로 막대한 피해를 초래할 수 있어 더욱 철저한 대비가 요구된다.

즉, 모바일 앱 자체의 보안이슈도 중요하지만 해당 앱에 정보를 제공하는 서버・네트워크 단에서의 보안대책은 모바일을 활용한 군사작전의 승패를 결정지을 정

2) 개인정보보호법 제24조(고유식별정보의 처리 제한)

도로 중요한 요소라고 할 수 있다.

따라서 군사정보와 사진, 군사지도를 활용하게 될 작전용 앱은 단말기에서 정보를 처리하지 않고 서버군에서 모두 처리한 뒤 보안대책이 강구된 네트워크를 통해 스트리밍 방식으로 제공되도록 구현되어야 하며, 작전에 필요한 각종 정보공유와 결심체계 등이 송・수신 될 수 있도록 서버・네트워크 단에서 보안대책을 강구하고 단말기상에서의 H/W암호화를 구현하는 등 체계 구성요소별로 강화된 보안대책이 마련되어야 할 것이다.

이러한 국방 환경과 전시 운용이라는 특수성을 고려시, 상용 앱스토어를 통해서 대민서비스/업무용 앱을 배포한다면 군에서 요구하는 강화된 보안수준을 적용할 수 없을 것이며, 특히 미래 전장 환경에서 사용될 작전용 앱은 인터넷망을 활용할 수 없기 때문에 전술통신망 내에 별도의 앱 관리 체계가 필요하다는 근본적인 제한사항이 도출된다.

따라서 안전한 스마트폰 서비스 환경을 보장하고 향후 발생 가능한 보안위협에 대해 선제적 방어체계를 구축하기 위해서는 앱에 대한 사전 철저한 보안성 검증 및 절차를 갖춘 국방 앱스토어가 필요하다.

Ⅲ. 안전한 국방 앱스토어 구축방안

3.1. 국방 앱스토어 기본 보안정책

국방에서 대민서비스용 앱과 내부업무용 및 작전용이라는 다양한 목적과 운용망이 존재하는 특수성을 고려, 운용망에 따라 대민서비스/업무용 앱스토어와 작전용 앱스토어로 구분하는 이원화된 형태가 요구된다.

이원화된 망에 동일 목적의 체계를 구축하는 특성상 보안정책은 상호간 비슷하겠지만 작전용은 추가적인 보안대책이 강구되어야 할 것이다.

먼저 대민서비스/업무용 앱스토어와 작전용 앱스토어에 공통적으로 적용될 보안정책을 살펴보면 다음과 같다.

첫째, 스마트폰 단말기에 MDM(Mobile Device Management, 모바일 단말기 관리체제)이 설치되어 앱스토어에서 강제적으로 보안정책을 적용할 수 있어야 한다. MDM을 통해 카메라와 녹음기능 통제는 물론 특정 폴더 저장자료 임의 복제방지, 허용된 앱만 설치 등 각종 보안기능이 보장될 것이다.

둘째, 앱 서버측과 연동을 위한 네트워크는 VPN (Virtual Private Network, 가상사설망)등을 이용해 안전성이 확보되어야 한다. 네트워크상에서의 터널링 확보만으로는 도청이나 MiTM(Man in the Middle Attack, 중간자 공격) 등에 안전하다 할 수 없지만 다른 보안대책과 연동을 통해 악의적 공격 성공률을 현저히 낮출 수 있다.

셋째, 앱스토어 운용모듈에 접근하려면 반드시 사용자인증 및 기기인증을 통해 명확히 식별 후 접근권한을 부여한다. 사용자인증을 통한 권한설정은 과도한 권한부여를 견제함과 동시에 침해대응 및 감사차원의 로그정보 분석 효율성을 높여줄 것이며, 기기 인증의 경우 공격 시도 확률을 크게 낮춰줄 수 있는 제한조건으로 작용될 것이다.

넷째, 앞선 보안기능들의 안정적 구현을 위해서는 단말기가 사전요구기능탑재 (Pre-Load) 가능한 플랫폼이어야 한다. 사전요구기능탑재가 가능하다는 것은 해당 플랫폼에 대한 완벽한 보안기능 설계・적용이 가능하여 우회나 무력화 시도가 원천적으로 차단될 수 있다는 것을 의미한다.

다섯째, 단말과 연동되는 보안기능과 앱은 물론 앱 게시・배포・관리의 핵심이 되는 앱스토어 기능 구현에 있어 보안개발 가이드라인을 준수한 가운데 개발단계부터 운용직전까지 보안대책검토와 보안측정을 통해 사전 보안취약점 제거 및 운용환경에서의 보안기능 신뢰성이 검증되어야 한다. 앞선 보안정책은 기술적인 보안에 대해 설명하였다면 이러한 기술적 보안대책이 제대로 구현되었는지 확인하고 검사하는 검증활동으로서 기존 수행해오던 보안대책검토와 보안측정은 여전히 효과적인 보안지원이라 할 수 있다.

여섯째, 보안성이 검증된 앱만을 게시・배포하기 위해서는 별도의 검증 시스템이 마련되어야 한다.

앱스토어 기능에 모바일 앱 보안성 검증절차를 강화하여 하나의 시스템으로 운영할 수도 있으나, 정보통신체계 특성상 해킹・악성코드 공격에 취약할 수밖에 없으며, 동시에 권한탈취시 악성코드 유포지로 활용 또는 업무마비가 우려된다.

따라서 해킹・악성코드 공격이 가능한 접점의 최소화 차원에서 별도의 보안정책과 보안기술을 적용한 검증센터를 앱스토어와 이원화하여 구축한다면 국방환경에서 원활한 업무분장과 효율성을 기대할 수 있을 것이다.

3.2. 대민서비스/업무용 앱스토어 구축방안

대민서비스/업무용 앱스토어는 인터넷 상용망에서 안전한 대민서비스와 장병들의 일반 업무용 앱이 동시에 관리될 수 있도록, 가상화 기술과 사용자 및 기기 인증 기술을 통해 보다 강화된 접근통제 대책이 적용되어야 할 것이며 개념도는 다음과 같다.

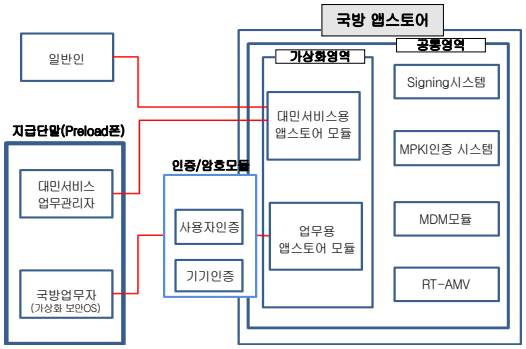

그림 1. 국방 대민서비스/업무용 앱스토어 개념도
Fig. 1 Military Appstore Concept for Civilian Service and Office Work

이러한 대민서비스/업무용 앱스토어의 구성요소별 기능과 특성은 다음과 같다.

첫째, 지급단말은 사전보안기능요구사항이 적용된 Pre-load폰이어야 한다. 자세한 보안기능은 MDM기능에서 다룰 것이며 단말과 앱스토어 연동간에 주요기능은 가상화기반의 보안OS가 탑재된 단말기로서, 해당 단말기로 대민서비스용 앱스토어 접속이 가능하며, 동일 단말기에 탑재된 가상화 보안OS상에서만 강화된 보안대책을 통해 업무용 앱스토어 모듈로 접근 가능하다.

둘째, 인증/암호모듈은 단말기와 앱스토어간 터널링 형성 및 접근통제를 구현하게 된다. 즉, 네트워크상에서 안전한 자료 송・수신을 위한 VPN기능 구현과 사용자(MPKI인증서)・기기(UUID, Unique User Identidfier, 고유식별자) 인증기능을 의미한다.

셋째, 공통영역은 앱스토어로서 제공해야 할 일부기능과 보안을 제공한다.

가) Signing시스템은 게시된 앱들에 해쉬값과 같은 특정길이의 유일한 식별값을 생성하여 배포・관리간 무결성 보장 용도로 사용하게 된다.

나) MPKI(Military Public Key Infrastructure, 국방 공개키 기반구조)인증모듈은 단말기에 탑재된 MPKI인증서와 운용 환경상 구현된 MPKI인증체계 중계역할로서 인증서를 이용한 사용자인증 및 권한부여에 관여한다.

다) MDM모듈은 단말기상에서 구현되어야 할 보안기능을 통제하고 관리하는 등 보안정책을 수립/배포할 수 있는 모듈로서 주요 보안기능은 다음과 같다.

표 2. MDM 기능[10]
Table. 2 MDM Functions

기 능	설 명
데이터암호화	내장 및 외장 메모리에 대한 암호화 제공 기능
원격 잠금 및 삭제	분실, 도난, 침해된 모바일 단말기에 대한 원격 잠금 또는 데이터 삭제 기능
매체 연결 통제	와이파이, 블루투스, IrDA 등의 네트워크 연결, USB 등 로컬 연결에 대한 통제 기능
네트워크 접근 통제	허가된 사내의 무선AP 또는 메일 서버에만 접근을 허용하는 기능
단말잠금	무차별대입형 로그인 시도 및 특정 시간 타임아웃 이후 잠금 기능
부팅시 패스워드	단말 부팅시 로컬 패스워드 인증 기능
로밍 통제	해외출장이 빈번한 경우, 로밍 통제를 통해 통신 비용을 관리하는 기능

라) RT-AMV(Real-Time Anti Mobile Virus, 실시간 모바일 백신)는 기존 스마트폰에 탑재되어 로컬상에서만 진단하는 모바일백신과 달리 앱스토어에 게시된 앱 대상 실시간으로 바이러스/악성코드 감염여부를 진단하는 모듈이다. 보안성 검증간 바이러스 진단과는 별도로 앱스토어 게시 이후 제로데이 공격[3] 등을 이용한 앱스토어 권한 탈취 및 위・변조 앱 게시로 인한 2차 피해와 악성코드 유포지로서 악용을 탐지・차단하는 보안성 강화 대책이다.

3.3. 작전용 앱스토어 구축방안

작전용 앱스토어의 경우 앱 게시, 배포, 폐기 등 상용 앱스토어의 기본기능을 수용하면서도, 전술통신망 환

3) 제로데이 공격(Zero-Day Attack): 컴퓨터 소프트웨어의 취약점을 공격하는 기술적 위협으로, 해당 취약점에 대한 패치가 나오지 않은 시점에서 이루어지는 공격

경에서 운용되는 특성상 다음과 같은 추가 보안대책을 통해 보안성이 강화되어야 할 것이다.

첫째, 단말기의 경우 작전용으로 별도 제작되어야 한다. 미래 전술통신망 TICN(Tactical Information Communication Network)환경에서 운용되어야 하는 특성상 해당 주파수 대역에서 작동할 수 있어야 함은 물론 변하지 않는 기기고유값을 이용한 기기인증과 접근통제가 구현되어야 할 것이다. 또한, 접근이 허락된 후에도 앱스토어 모듈별로 접근권한이 부여되어 최소한의 정보제공이라는 기밀성 원칙을 준수해야 할 것이다.

둘째, H/W 암호모듈을 이용한 사용자인증을 지원해야 한다. 기존 상용 앱스토어에서는 단말기 로컬상에 탑재된 인증서를 이용해 사용자 인증기능을 지원하였으나, 전술통신망에서는 이보다 보안성이 강화된 형태로서 H/W 암호모듈내 메모리와 CPU를 활용해 인증서를 탑재 및 암호키 생성・연산을 수행한다.

셋째, 작전용 앱스토어 모듈은 대민서비스/업무용 앱스토어 모듈과 물리적으로 분리된 형태여야 한다. 물리적으로는 국방부 산하 특정 센터 또는 부서에 전산시스템이 설치되어 통합 운영되겠지만, 운용환경(상용망, 전술통신망)이 상이함에 따라 각종 앱스토어 기능・보안모듈 또한 별도로 구축되어야 할 것이다.

그 외 구성요소는 대민서비스/업무용 앱스토어와 유사하며 개념도는 다음과 같다.

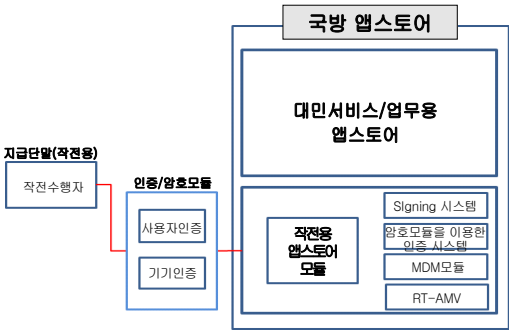

그림 2. 작전용 앱스토어 개념도
Fig. 2 Military Appstore Concept for Military Operation

이러한 앱스토어들의 운용방안은 국방 메가센터와 연계되어 고려되어야 할 것이며 전군대상 체계적인 전산지원을 관리할 수 있는 기관/부대에서 운용해야 할 것이다.

Ⅳ. 국방 모바일 앱 보안성 검증센터 구축

4.1. 기본방향

국방 모바일 앱 보안성 검증센터는 전군에서 개발・도입하는 모바일 앱의 보안취약성을 탐지, 해소하고 보안성 검증기능을 통해 전군 대상 적시적이고 효율적인 보안지원을 하는 데 목적이 있다.

해당 검증센터는 전술통신망 환경에 설치되어 작전용 앱스토어와는 실시간 연동하면서 검증신청, 결과통보 등 검증업무를 온라인상에서 수행하고, 대민서비스/업무용 앱스토어의 검증요청은 오프라인 형식으로 소스코드 등을 제공받아 수행하게 된다.

검증센터는 각 앱스토어로부터 제공받은 소스코드를 대상으로 정적분석을 수행함과 동시에 실제 앱을 설치하여 운용환경하 동작형태를 분석하는 동적분석을 병행하는 보안성 검증 활동을 전개할 수 있도록 구성한다. 이러한 보안성 검증 활동은 내・외부세력에 의한 도청, 개인정보 및 군사목적으로 개발한 앱에 대한 변조・악용을 방지하는 등 군사보안에 대한 위협요인을 사전 차단할 수 있으며 이러한 사고발생시 즉각적인 조치도 가능하다. 또한 작전용 앱 운용환경에서 백본(Back-Bone)망과 연계된 DPI(Deep Packet Inspection)를 통해 계획된 암호화 알고리즘 및 암호의 안정성이 적절하게 적용 및 운용되고 있는지 실시간으로 검증할 수 있도록 구축되어야 할 것이다.

4.2. 구성 요소별 기능 및 특징

전군 모바일 앱 보안성강화를 목적으로 구축되는 보안성 검증센터의 개념과 구성요소별 기능 및 특징은 다음과 같다.

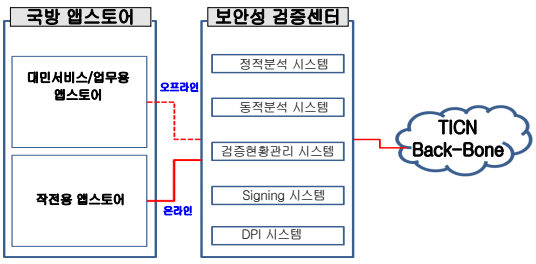

그림 3. 국방 모바일 앱 보안성 검증센터 개념도
Fig. 3 Military Mobile App Security Verification Center Concept

첫째, 정적분석 시스템은 앱 소스코드 대상 보안취약점을 진단할 수 있는 자동화 도구이다. 다양한 보안취약점 분류가 있으나, 기본적으로 전자정부 모바일 보안지원을 위해서 행정안전부에서 고시한 보안취약점 분류(7개분야, 41항목)를 준수한 가운데 특정 취약점 항목(CWE[4]) 또는 표준(NIST, CC 등) 보안기준 항목을 추가 반영하여 보안성을 강화해야 할 것이다[11].

둘째, 동적분석 시스템은 검증 대상 앱과 앱서버를 실 운용환경과 유사하게 테스트장비에 구성하여 상호간 송・수신 패킷, 단말기상 요구권한, 오작동 및 악성행위 유발 등 실제 운용간 발생하는 이벤트를 확인・검토토록 구성된 가상화 시스템이다.

셋째, 검증현황관리 시스템은 보안성검증센터에서 수행한 검증내역을 저장하고 분석 할 수 있는 웹환경 서비스이며, 불완전한 보안기능으로 인해 지속적인 수정・검증작업을 반복한 앱 소스코드 대상 형상관리 기능도 지원한다.

넷째, Signing시스템은 검증 완료된 앱 대상 무결성을 보장하기 위한 것이다. 단, 앱스토어에서 운용중인 Signing시스템과 별다른 시스템이 아닌 동일한 시스템으로서 앱스토어에 게시된 앱들의 무결성을 실시간으로 감시하기 위한 이중 보안대책으로 운용될 것이다.

다섯째, DPI시스템은 모바일환경에 계획된 암호 알고리즘과 암호에 대한 안전성을 실시간으로 확인하고 검증하기 위한 것이다. 전술통신망 환경에서는 다양한 암호장비가 운용됨에 따라 네트워크상에서의 상호연동성이 중요하며 또한 전시 운용성을 보장받기 위한 생존성차원에서 암호화패킷의 안전성과 신뢰성에 대한 실시간 감사활동은 반드시 필요할 것이다.

다만, 암호화패킷 안전성 차원의 암호장비 관련 감사활동은 통신비밀보호법에 의거 군내 통신제한조치가 가능하고 암호장비관련 업무를 취급하는 기관이나 부대에서 수행해야 한다는 제한사항이 있다.

4.3. 모바일 앱 검증 절차

위와 같은 구성요소별 기능과 특징을 바탕으로 제시된 전반적인 국방 모바일 앱 관리체계와 모바일 앱 검증절차는 다음과 같이 요약할 수 있다.

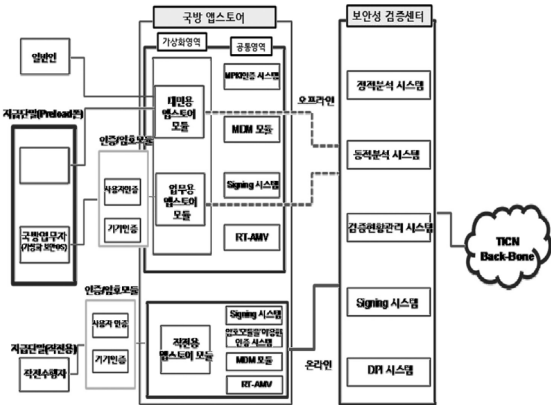

그림 4. 국방 앱스토어 및 검증센터 개념도
Fig. 4 Military Mobile Appstore and Verification System

1) 신청단계 - 신청부대/개인은 컴파일 가능한 소스코드 일체, 실행파일, 모바일 앱 요구사항 정의서, UI정의서, 앱의 보안속성, 구현기능, 시험항목 및 결과 등을 서술한 보안명세서 등을 포함한 '모바일 앱 보안성 검증신청서'를 앱스토어에 제출하면 앱스토어는 검증센터에 보안성 검증을 의뢰(오프라인 또는 온라인)하게 된다.

2) 검증단계 - 검증기관은 신청 앱이 검증기준에 명시된 요구수준을 만족하는지 여부를 소스코드 대상 및 기능구현을 통해 검증한 결과를 종합하여 적합・부적합 판정을 앱스토어에 통보하면, 판정별로(적합-앱스토어 게시, 부적합-재검증) 보완이 필요한 경우 신청부대에 보완을 요청하여 보안성 검증 기준을 만족할 때까지 재수행한다.

3) 배포단계 - 적합 판정을 받은 앱의 경우 앱스토어에 게시 및 배포하게 되며 실시간으로 바이러스나악성코드 감염여부와 무결성을 모니터링 한다.

V. 결 론

본 논문에서는 IT 기술의 급격한 발달로 1년이 멀다하고 새로운 스마트폰이 출시되고 제조사별로 다양한 하드웨어 특성을 가진 스마트폰 운영체제에 적시적 보

4) Common Weakness Enumeration

안기술 적용이 제한되는 현 상황에서, 군사용 앱을 사용하기 위해 선결되어야 할 국방 앱스토어와 앱 보안성 검증센터 구축방안을 제시하여 앱에 대한 사전 보안성 검증 및 상시 보안조치·관리를 통해 모바일 환경에서의 보안성 강화방안을 고찰해 보고자 하였다.

즉, 사전 보안성이 검증된 앱만을 배포하고, 국방 앱스토어 접속시 다양한 인증기법으로 접근통제하여 악의적인 목적의 접속을 최소화하고, 사전보안요구기능이 탑재된 Preload폰과 중앙통제방식의 MDM을 구현하여 고질적 문제점으로 지적되던 무력화·우회방안을 사전차단 하였다.

또한 DPI시스템을 통해 전시환경에서의 암호화된 패킷 안전성을 상시 진단하는 등의 전략적 보안지원 활동으로 생존성 보장에도 기여토록 하였다.

하지만, 본 연구는 실제 국방 앱스토어와 앱 보안성 검증센터가 구축된 실증환경에서가 아닌 기술적 이론을 토대로 보안성이 확보될 수 있다는 것을 제안하고 있다는 것이 연구과정에서의 한계점이다. IT 환경에서는 여러 가지 변수가 존재하기에 본 연구에서 제안한 사항들의 실효성을 입증하기 위해서는 실제 테스트베드 환경에서의 연구가 필요한 것이 사실이다. 향후 국방차원에서 동 연구에서 제안한 방식들이 실제 구현되어 보안성이 확보된 안전한 모바일 앱 사용환경이 구축되길 기대해 본다.

참고문헌

[1] 삼성경제연구소(SERI 경영 노트 제373호), 이승환 수석연구원, '개화하는 정부 앱, 만발의 조건', 2012. 3.20

[2] F-Secure, "Mobile Threat Report Q3 2012", 2012.11

[3] 방지호, 하란, 강필용, 김홍근, "전자정부 모바일 앱 보안성 검증체계", 한국통신학회논문지 12-02, Vol. 37C, No.2, pp.119-127, 2012

[4] Secure Mobile Environment - Portable electrionic Device(SME-PED) Frequently Asked Questions(FAQs), 2012.05

[5] 손익재, 김일호, 양종휴, 이남용, "사이버 국방을 위한 스마트 단말 보안기술", 한국통신학회 논문지 12-10, Vol.37C, No.10. pp.986-992, 2012

[6] Steven Henderson and Steven Feiner, "Augmented Reality for Maintenance and Repair(ARMAR)", Technical Report AFRL-RH-WP-TR-2007-0112. United States Air Force Research Lab. Jul 2007.

[7] UK soldiers use iPad app to train for Afghan operations 2010.7.30. www.bbc.co.uk/newsbeat/10813964

[8] 육군이 개발한 다양한 스마트폰 어플리케이션, 취재기사, 2012.12.25. http://news1.kr/articles/946902 Popularity Comes at a Price", 2012.10.22.

[9] 장월수, 최중영, 임종인, "군 통합보안시스템 구축방안 연구", 정보보호학회논문지 제22권, 제3호, 2012. 6

[10] '11.5, Network Times, 윤상인, 스마트워크 시대 필수 솔루션 'MDM'

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

저자소개

이갑진(Gab-Jin Lee)

수원대학교 컴퓨터학과 박사과정
※관심분야 : 군보안정책, 정보보호관리체계, 사이버테러, RFID

고승철(Sung-cheol Goh)

수원대학교 정보보호학과 교수
※관심분야 : 정보보호, 알고리즘, Computational Complexity