논문 12-37C-10-14

한국통신학회논문지 '12-10 Vol.37C No.10
http://dx.doi.org/10.7840/kics.2012.37C.10.986

사이버 국방을 위한 스마트 단말 보안기술

손 익 재◆, 김 일 호*, 양 종 휴**, 이 남 용°

Smart Device Security Technology for Cyber Defense

Iek-jae Son◆, Il-ho Kim*, Jong-hyu Yang**, Nam-young Lee°

요 약

스마트폰과 같은 스마트 모바일 단말의 활용이 급증하면서 군에서도 스마트 단말을 이용하여 전투를 지휘하고 전장에서 활용하고자 하는 움직임이 있다. 이에 따라 미래전은 각종 정보통신기술이 융합된 스마트 모바일 단말이 군의 지휘통제체계를 포함한 각종 무기체계에 접목되면서 전쟁양상의 일대 변화를 일으킬 가능성이 존재하며, 합동 전투지휘를 위한 스마트폰 기반의 실시간 정보기술은 감시정찰, 지휘통제체계에 융합되어 국방-IT 융합에 대표적인 사례가 될 것이다. 더 나아가서 이동망과 무선망 환경에 최적화된 모바일 단말 보안기술은 무인화체계인 국방로봇에 적용이 가능할 것이다. 이 논문에서는 전투지휘체계를 지원하거나 군사용으로 쓰이는 스마트 단말 동향을 살펴보고 보안 위협요소와 함께 이들 위협에 대응하기 위한 군사용 모바일 단말 보안기술 동향을 소개하고자 한다.

Key Words : Smart Device Security, Cyber Defence, Battle Command, Mobile wireless network environment, Military robots, 스마트 단말보안, 사이버국방, 전투지휘, 모바일 무선네트워크 환경, 국방로봇

ABSTRACT

As the utilization of smart mobile devices such as smartphones increases, the desire to utilize such devices to control and monitor combat situations also arises. As smart mobile devices with various ICT get integrated with various weaponry system, a new phase of future warfare can be introduced. Moreover, smartphone-based real-time information technology for joint battle command system will be converged with surveillance control to become a leading example of convergence of cyber defense and information technology. Furthermore, mobile device security technology ideal for mobile wireless network environments can be applied to military robots. The following paper will give an overview of smart mobile device usage used for military purposes in battle command system, various security threats and the mobile device security technology to correspond to such security threats.

Ⅰ. 서 론

현재 3세대 이동통신의 발달과 이를 활용한 풍부한 모바일 애플리케이션을 제공하고 있는 스마트폰의 성장으로 인해 모바일 서비스 이용률이 급증하고 있다. 모바일 서비스를 지원하는 모바일 단말의 진화 과정을 살펴보면 1세대에 아날로그방식의 음성 통화를 목적으로 한 기본적인 폰 기능에서 2세대에 디지털방식으로 전환되면서 음성 통화 및 SMS와 같은 소량의 데이터 전송이 가능한 데이터 서비스를 지원하였다.

◆ 주저자 : 국방부, ahson2@naver.com, 정회원
° 교신저자 : 숭실대학교 일반대학원 IT정책경영학과 주임교수, nylee@ssu.ac.kr, 정회원
* 국방부, navyking@hanmail.net, 정회원
** 해군군수사령부, yjhhyu@hanmail.net
논문번호 : KICS2012-08-360, 접수일자 : 2012년 8월 17일, 최종논문접수일자 : 2012년 10월 16일

현재 지원하고 있는 3세대 이동 통신은 음성, 데이터 및 영상 등을 고속으로 주고받을 수 있는 멀티미디어 통신 서비스를 지원하고 있다. 3세대 이동통신 기술을 지원하는 모바일 단말은 주로 스마트폰으로, 스마트폰에 따라 모바일 서비스를 지원하는 범용 OS 및 모바일 애플리케이션을 포함하는 소프트웨어 플랫폼은 다양하다.

최근 스마트폰의 등장과 성장에 따라 모바일 소프트웨어 플랫폼에 대한 관심이 증가하고 있다. 또한, 아이폰과 앱스토어의 성공은 스마트폰에서 사용될 애플리케이션에 대한 관심을 한층 끌어올리고 있다. 하지만 범용 OS를 채택하고 있는 개방성, 개인별로 가지고 다닌다는 휴대성, 앱스토어를 통한 소프트웨어 유통성, CPU 속도와 메모리 크기 등 저사양에 저성능 특징으로 인하여 모바일 단말은 모바일 악성코드의 제작을 용이하게 만들고, 분실, 도난 또는 비인가된 사용자의 접근에 의한 개인 및 그룹 정보 유출 가능성이 높기 때문에 모바일 공격의 피해가 증가할 것으로 예상된다[1].

최근 들어, 스마트폰과 같은 모바일 단말의 활용이 급증하면서 군에서도 스마트 단말을 이용하여 전투를 지휘하고 전장에서 활용하고자 하는 움직임이 일고 있다. 따라서 이러한 스마트 단말을 군에 적용할 때 더욱 지능화되고 다양한 형태로 변형될 수 있는 악의적 행위에 의한 정보 유출, 부정사용 등과 같은 보안 위협으로부터 보호하는 높은 수준의 스마트 단말 보안 기술 개발이 요구된다. 이 논문에서는 군에서 사용하는 스마트 단말의 동향을 살펴보고 이를 안전하게 사용하기 위한 스마트 단말의 보안 위협 요소를 분석하고 이들 위협에 대응하기 위한 군사용 모바일 단말 보안 기술을 소개하고자 한다.

Ⅱ. 사이버 국방 스마트 단말 동향과 보안 위협

2.1. 사이버 국방 스마트 단말

2.1.1. MONAX

미국 록히드마틴사에서 개발 중인 3G(3rd Generation) 무선통신 단말기인 MONAX는 아이폰 기반의 미군 통신시스템으로 가격은 약 $1,000 정도 예상된다. 전장에서 부대위치 및 전투상황을 파악하고 무인항공기까지 조종할 수 있는 어플들이 탑재되어 있다. 이 아이폰은 내구성이 강한 플라스틱 재질의 케이스로 구성되어 지상이나 비행체에 탑재 가능하며, 워키토키 기능을 비롯하여 음성과 데이터를 암호화하여 전송하는 기능을 제공한다. 아프가니스탄 같은 험난한 지역에서도 기지국 하나가 MONAX 모바일 단말과 20마일(약 32Km) 이상 통신이 가능하다. 이 제품은 이라크에서 군 통신망이 아닌 휴대폰 망으로 명령을 수행하고, 서로 통신하는 모습에서 착안하여 만들기 시작하였다. 전쟁이 나면 휴대폰 망이 파괴되겠지만, 파괴되기 전 까지는 유용하게 사용할 수 있는 군 통신 백업 망이기도 하다. 앞으로 군용 어플로서 무인정찰기, 부비트랩, 교전수칙 및 부상병이 생겼을 때 응급조치나 간단한 총기 조립법 등 다양한 어플들이 나올 수 있을 것이다.

2.1.2. GD 300

미국 제너럴 다이너믹스(General Dynamics)사가 개발한 GD 300은 안드로이드 기반의 군용 스마트 단말로 가격은 약 $1,200 정도이다. GPS와 군사용 무전기 인터페이스가 탑재되어 있으며, 팔과 가슴에 장착할 수 있다. 특히, 실시간 위치 정보를 제공하고 전장의 통신시스템과의 연결을 목적으로 개발된 군 규격의 내구성 시험을 통과한 안드로이드 기반의 플랫폼이다. 단말 규격은 600Mhz ARM Cortex A8 프로세서, 256MB 메모리, 8GB 저장장치로 구성되어 있으며, 군전용 앱인 저격수용 탄도계산 프로그램인 Bullet Flight, 안드로이드 전술 시스템인 RATS(Raytheon Android Tractical System), 그리고 전투와 관련된 정보를 전달하는 One Force Tracker 등을 탑재하여 활용한다.

2.1.3. SME-PED

미국 국토안보부와 국방부에서 보안 또는 비보안 통신을 위해 활용하는 SME-PED(Secure Mobile Environment- Portable Electronic Device) 단말은 미국 국가안전보장국(NSA)의 SME-PED 프로젝트에 의해 개발된 블랙베리(Black Berry) 운영체제 기반의 스마트 단말이다. 이 단말은 미국 오바마 대통령 전용 휴대폰으로, 실시간 뉴스 문자 전송, 위성 위치추적, 각종 무선 데이터를 연동하는데 사용하며, 음성 및 데이터 비화통신에 활용한다. 또한, 정찰 및 지휘 통제(C2) 기능을 지속적으로 활용하는 무선 이동 통신용 국방 서비스에도 활용된다. 이러한 서비스는 통합무선 전자메일, 웹 브라우징 및 문서보기 기능을 사용할 때 다단계 음성보안 및 데이터 암호화를 제공한다.

2.1.4. JBC-Platform

최근 미국 육군은 병사들에게 지급하는 군용 스마

트폰 운영체제로 구글의 안드로이드를 채택했다. JBC-Platform(Joint Battle Command-Platform) 단말은 미국의 비영리기관인 MITRE사에서 안드로이드를 기반으로 개발하였으며, 미군에서 이미 프로토타입을 시험 중이다. 이 단말에는 미국 연방정부가 소유하고 있는 안드로이드 기반의 'Mobile/Handheld Computing Environment'로 작성한 어플들이 탑재되어 있다. 이 단말 기능은 적의 위치 정보를 GPS와 지도를 이용해 우군에게 제공하거나, 중요한 메시지를 안전하게 송수신할 수 있는 기능, 의료헬기 및 긴급구조 요청 등 긴급호출 기능 이외에도 오피스 문서 뷰 등 일반 스마트폰의 기능도 갖추고 있다.

2.2. 사이버 국방 스마트 단말 활용 사례

2.2.1. 미국

미국에서는 국방용으로 스마트 단말을 MP3, GPS 용도로 주로 사용하며, 그 이외에도 탄도계산기, 소형 무인기 조종 등에 사용한다. 먼저 미군이 현지어 통역을 위해 사용하는 MP3 모델은 아이팟나노이며, 아프간에 파병한 미군(제10산악사단)들이 현지 주민과 대화를 하기 위해 아이팟이나 아이팟나노에 스피커를 부착한 모델을 구매하여 사용하였다. GPS는 미군이 사용하는 블랙베리 또는 아이폰 등 스마트폰을 활용하여 군용 GPS로 활용한다. 구글 맵을 사용하면, 위성사진과 함께 GPS 정보가 정확히 입력된 지도가 가능하므로 군용 GPS로 사용한다. 구형 모델은 큰 크기에 좌표밖에 표시를 못하였는데, 스마트 단말을 활용하여 정확한 GPS 정보를 활용할 수 있다.

또한, 미군이 사용하는 아이팟터치와 아이폰으로 저격도 가능한 탄도계산기로 활용할 수 있다. 미군에 저격 총을 납품하는 회사가 아이팟터치와 아이폰에 탄도계산 프로그램 "Bullet Flight"를 설치한 모델을 제공한다. 마지막으로 미군이 사용하는 스마트폰을 활용하여 영상을 보는 앱을 통해 소형 무인기를 조종하는 용도로 활용한다.

2.2.2. 한국

한국에서는 국방용으로 스마트 단말을 활용하는 것은 현재 거의 초기 수준이다. 기존 2D 폰에 보안장치를 탑재하여 음성통화만을 하는 형태로 일부 운영하고 있고, 최근 상용 스마트폰을 활용하여 군사용으로 사용할 수 있는지 여부 판단을 위해 테스트베드 형태로 구축하여 전투력을 높이기 위한 다양한 시도를 하고 있는 것으로 알려져 있다. 특히, 이 단말은 데이터 송수신시 암호화 기능을 갖춘 IPSec 암호화 통신 기술을 기반으로 보안성을 높인 것이 특징이다. 하지만, 일반 휴대폰망의 특성상 보안 위협요소가 매우 많으므로 군사 분야에 적용하기 위해서는, 어떤 기술을 개발하고 어떻게 극복할 것인가 등 다각적인 연구와 도전이 있어야만 현 수준을 뛰어 넘을 수 있을 것으로 본다.

2.3. 스마트 단말 보안 취약점

모바일 단말이 일반폰에서 스마트 단말로 발전되어감에 따라 이러한 스마트 단말이 군에도 더욱 활용될 양상을 보이고 있다. 그러나 군에서 사용되는 스마트 단말은 보안 문제가 해결되지 않는다면 사실 활용이 어려울 것이다. 특히 스마트 단말은 기본적으로 일반폰 보다 성능이 우수하고, 개방형 환경에 따라 자체적으로 애플리케이션을 개발하는 폐쇄형 구조에서 모든 개발자에게 표준화된 개발환경을 제공하는 공개형 구조로 발전하고 있다.

안드로이드와 같은 개방형 플랫폼을 탑재한 단말의 등장은 제조사들에게 플랫폼의 단말 적용 편의성을 제공하지만 플랫폼 소스 공개에 따른 보안 취약점 노출 위협이 증대될 수 있다. 또한, 앱스토어를 통한 애플리케이션 유통은 구매자와 개발자간에 애플리케이션 유통 편의성을 제공하지만 악성코드가 포함된 애플리케이션을 보안성 검증 절차가 미비한 앱스토어에 올려 악의적인 바이러스 제작 및 유포 기회가 확대될 수 있다. 다양한 네트워크 접속환경 지원은 네트워크를 활용한 다양한 서비스를 제공할 수 있지만 스마트폰의 다양한 네트워크(Wi-Fi, Bluetooth, HSDPA) 등을 통한 감염 경로의 다양성을 제공할 수 있다.

이동 편의성 및 모바일 오피스 지원은 언제 어디서나 단말 사용자에게 모바일 서비스를 제공받을 수 있지만 휴대성에 따른 분실, 도난 및 모바일 오피스 지원에 따른 스마트폰 수요가 증가되어 개인 및 그룹 정보 유출 위협이 증대될 수 있다. 이러한 4가지 위협요소는 일반적으로 악성코드 감염, 개인 및 그룹정보 유출, 서비스 거부 공격과 금융사고 등의 피해를 유발시킬 수 있다.

2.4. 스마트 단말 OS별 악성코드

2011년 3월 방통위 자료에 따르면, 2010년 9월에 안드로이드가 아이폰을 앞질러 1위로 되면서, 11년 1월에는 거의 60%에 육박할 정도에 이르렀다.

모바일 악성코드는 스마트 단말을 포함한 모바일 단말을 대상으로 정보 유출, 단말 파괴, 불법 과금 등

의 악의적인 행위를 수행하기 위한 악성 프로그램으로 정의할 수 있다. 모바일 악성코드는 모바일 단말의 성장과 더불어 규모면에서 빠르게 증가하고 있고, 위협요인도 다양화되고 있다. 모바일 악성코드가 증가하는 원인은 악의적인 목적을 가진 악성코드의 제작 및 유통이 가능한 개방형 단말기의 증가와 함께 블루투스, Wi-Fi와 USB 등 외부 접속의 다양화가 원인이라고 할 수 있다. 모바일 악성코드는 초기에 단순히 전파를 목적으로 하거나 단말의 기능적 동작을 마비시키는 형태에서 개인정보의 유출 및 금전적 이득을 목적으로 하는 형태로 변화되고 있다. 최근 스마트폰 이용 확산에 따라 시간과 장소에 구애 받지 않고 무선 인터넷을 활용한 모바일 서비스가 활성화되면서 스마트 단말의 보안 위협이 더욱 증대되고 있다.

Ⅲ. 스마트 단말 보안기술

안전한 모바일 서비스 환경을 보장하고 향후 발생 가능한 보안 위협에 대해 선제적 방어 체계를 구축하기 위해서는 악성코드 실행 방지를 위한 플랫폼 보안 기술과 모바일 소프트웨어 보안성 검증 및 안전한 어플리케이션 사용을 위한 서비스 보안 기술, 단말 데이터보호 및 원격보안 관리를 위한 데이터 관리 기술, 악성코드 확산을 방지하는 네트워크 보안기술을 통해 국내외적으로 기술 초기단계에 있는 스마트 단말 보안기술 개발이 요구된다.

3.1. 플랫폼 보안 기술 - MTM, 가상화 보안

하드웨어 기반의 플랫폼 보안 기술 중 대표적인 것이 MTM(Mobile Trusted Module) 기술이다. 스마트 단말 사용자가 부주의로 단말장비를 분실 또는 도난을 당했을 때, 단말 복제, 도청, 악성코드 삽입 등 심각한 보안위협이 존재하는데 이에 대한 해결책이 없으면 사실 군에서는 사용하기 곤란하다.

일반적으로 소프트웨어는 하드웨어에 비해 쉽게 조작될 수 있기 때문에 물리적 보안 기술인 MTM 기술을 이용하여 스마트폰 단말의 데이터, 키, 인증서 등을 안전하게 보호하고, 단말 플랫폼의 무결성을 검증하는 등 더욱 향상된 보안기능을 제공할 수 있다[6]. MTM 무결성 측정 및 검증 기능과 보호된 저장장치를 통해 스마트폰 단말 보안기능을 강화하고 원격검증 및 MTM이 장착된 플랫폼간의 보증을 통해 보다 안전하고 신뢰할 수 있는 무선 네트워크 환경을 구축할 수 있을 것이다.

가상화 기반의 보안기술은 크게 하드웨어 기반 가상화와 소프트웨어 기반 가상화로 나눌 수 있다. ARM사의 TrustZone 기술은 물리적으로 하나의 코어를 두 개의 가상 Core로 분리하여 사용할 수 있도록 하드웨어적인 기능을 제공하고 있다. 즉, 통상의 응용프로그램이 실행되는 일반영역과 보안이 필요한 기능만을 실행하는 보안영역으로 분리할 수 있다. 이 두 개의 영역은 감시모드(monitor mode)를 이용하여 영역 전환이 가능하다. 일반영역의 가상 프로세서는 단지 일반영역의 시스템 자원만을 접근할 수 있다.

그러나 보안영역의 가상 프로세서는 시스템의 모든 자원을 접근할 수 있다. TrustZone은 보안을 위한 하나의 독립적이고 완전한 해결방법이라기 보다는 일종의 하드웨어적인 보안환경을 제공하는 것이라고 할 수 있다[5,7]. 하이퍼바이저(Hypervisor)를 이용한 소프트웨어 가상화도 모바일 단말 보안을 위한 하나의 방법이 될 수 있다. 소프트웨어 가상화는 하이퍼바이저 내에 보안정책을 위한 기능을 구현함으로써 MMU(Memory Management Unit)를 가지고 있는 모든 프로세서에 구현이 가능하고, 다른 추가적인 하드웨어의 요구사항이 없으며, 보안에 민감한 어플리케이션은 안전영역 환경에서 수행이 가능하다는 장점이 있다.

ARM사의 TrustZone 또는 하이퍼바이저를 이용한 가상화 방법은 모바일 실행환경을 일반도메인과 안전도메인으로 분리함으로써 단말의 보안성을 보다 향상시킬 수 있다. 이와 같은 단말 실행환경의 가상화 방법은 중요한 기능 및 데이터를 안전 도메인 내에 둠으로써 군사용 서비스를 안전하게 보호할 수 있으므로 향후 군사용 모바일 단말의 실행환경으로 각광받을 것으로 예측된다.

이외에도 NFC, USIM, Secure Memory Card 기반의 플랫폼 보안 기술 등이 있는데 단말 제조업체나 이동통신사업자 그리고 단말보안 솔루션 업체들을 중심으로 각자의 이익을 추구하는 방식으로 개발을 진행중이나 군과 같은 높은 보안 수준이 요구되는 곳에서는 이러한 MTM 기반 플랫폼 보안기술이 반드시 필요할 것이다.

3.2. 서비스 보안 - 앱스토어 보안 기술

서비스 보안기술 중 대표적 기술인 앱스토어 보안기술은 앱스토어에 애플리케이션을 등록하고, 배포 시 애플리케이션의 안전성을 확보하는 기술로 모바일 애플리케이션의 유통인증 기술과 앱스토어에 등록된 애플리케이션에 대한 보안검증 기술의 적용이 요구된다.

모바일 애플리케이션의 유통인증 기술은 애플리케

Table 1. Coverage and Measure for Improvement of mobile device security technology

Category	Platform Security	Service Security	Data Management	Network Security
Security technology for mobile device	- MTM hardware technology - Virtualization based security technology	- Security for app store	- Remote control of mobile device - Data encryption technology	- Connection control technology for compromised device - Wireless IPS technology
Characteristics	- H/W-based mobile platform solution against security threats of device loss, device cloning, eavesdropping, insertion of malicious code, etc. - Applicable to military mobile devices by using virtualization based security technology, protecting important functionalities and persistent data in the secure storage	- Guarantees application's integrity and authenticity during its life cycle - application registration, distribution, and installation - for verifying application in the app store	- provides remote control and management functions over mobile devices using device management protocol - Protects persistent data stored in the device's storage through data encryption even when device is lost or stolen	- Increase trustworthiness of network by allowing only verified devices to connect into the network - provides malicious code detection and realtime monitoring functionalities to solve the security vulnerabilities in high-speed wireless network
Application area	- not in use	- limited use of application authentication	- provided as a MDM function, but not complied with standard protocol - SW-based data encryption is applied	- limited application for connection control of jailbreaked or rooted devices
Measure for improvement	- indispensable for military device	- needs more systematic security measures for verifying application authenticity and its integrity in the app store	- needs standard-compliant MDM solution as well as HW-based data encryption technology	- needs malicious code detection, connection control by integrity check, and location tracing technologies for the compromised device

이션이 앱스토어에 등록되어 이용자에게 전달되기까지의 유통자 증명을 위해 코드 사이닝(Code Signing) 기술을 적용하고 있다. 개발자는 애플리케이션의 신원증명을 위해 인증서로 코드 사이닝하여 앱스토어에 등록하고, 앱스토어에서는 애플리케이션의 신원증명을 확인 후 개발자 확인절차를 수행한다.

그러나 현재 일부 앱스토어에서는 공인인증서를 통한 코드 사이닝을 적용하고 있지만, 대부분은 자가 서명(Self Signing)이나 코드 사이닝을 적용하지 않아 개발자 신원증명 부재에 따른 악성코드 유포자의 확인이 불가능한 사례가 발생되고 있다. 개발자의 신원증명을 위해서는 공인인증서를 이용한 애플리케이션 코드 사이닝 기법을 적용하여 개발자 신원증명 절차가 필요하다. 모바일 애플리케이션 보안검증 기술은 앱스토어에 등록된 애플리케이션에 대해서 등록 전에 검증센터에서 보안성 검사를 통해 애플리케이션의 안전성 여부를 확인해야 한다.

3.3. 데이터관리 기술 - 원격보안관리, 단말암호화

데이터 관리 기술 중 대표적인 것이 원격 보안관리 기술로 단말관리 프로토콜을 사용하여 모바일 단말의 보안기능을 원격에서 제어하고 관리한다. 이를 위해 모바일 서비스 표준화 단체인 OMA(Open Mobile Alliance)에서 정의한 DM(Device Management) 프로토콜을 사용할 수 있다. 이 DM 프로토콜은 두 통신상대가 장치관리 서비스를 제공하는 서버와 장치관리 서비스를 받아 처리하는 클라이언트 관계로서 장치관리 서버의 역할은 클라이언트에게 장치관리 명령을 수행하고, 클라이언트는 주어진 명령을 수행한다.

현재 OMA의 DM 보안기능에는 단말 잠금과 데이터 삭제 기능을 정의하고 있지만, 보안관리 측면에서 장치관리 서버는 스마트폰 보안관리 서버의 역할을 담당하고 클라이언트는 스마트폰에 설치하여 다양한 원격보안관리 서비스를 제공한다. OMA의 DM 프로토콜은 HTTP, Wireless Session Protocol, OBEX(Object Exchange) 등의 전송 프로토콜과 바인딩 규격들이 마련되어 있으므로 산업계 인터넷 표준인 Web, WAP(Wireless Application Protocol), 블루투스 환경에서 프로토콜 메시지 전송이 가능하다.

데이터 관리 기술 중 다른 하나는 단말 암호화 기술이다. 단말이 분실 또는 도난당했을 때 단말 저장장치 내 데이터 유출을 방지하기 위해 데이터를 암호화하

는 기술이다. 또한, 단말을 통한 음성통화와 데이터 통신 시 스니핑에 의한 데이터 유출을 방지해야 하므로 음성과 데이터 통신 시에 암호화하여 전송하는 기술이 필요하다. 이러한 음성 및 데이터 비화통신 기능이 군에서 사용하는 스마트 단말에 제공되어야 하는데 이를 위해서는 경량 초전력 암호 알고리즘 및 암호 칩셋기술 등이 제공될 수 있도록 해야 한다.

3.4. 네트워크 보안 기술 - 침해단말 접속제어, 무선 IPS

네트워크 보안 기술의 대표적인 것이 침해단말 접속제어 기술이다. 이것은 단말이 네트워크에 접속할 때 단말의 무결성을 검증하여 확인이 되면 네트워크에 접속하도록 하는 기술이다. 스마트 단말은 CPU 성능, 메모리 크기 등 성능 제약이 있어서 백신을 상시 실행시키기 어려우므로 네트워크에 접속할 때 단말에 악성코드가 묻어있는지를 확인하는 것이 효율적이다. 게다가 탈옥 아이폰이나 루팅된 안드로이드폰 같은 경우에는 단말을 통해 개인정보가 유출되거나 좀비 PC가 되게 하여 DDoS 공격을 할 수 있기 때문에 탈옥 단말이나 루팅 단말의 접속도 제어하도록 해야 한다.

네트워크 보안 기술 중 다른 하나는 무선 IPS(Intrusion Prevention System) 기술이다. 고속의 무선 LAN 환경에서 위장 AP 등 보안상의 많은 취약점들이 존재한다. 이를 해소하기 위해서는 무선 환경에서 들어오는 패킷을 분석하여 악성코드를 탐지하는 기술과 이를 통해 침해 단말의 위치를 추적하는 기술 등이 필요하다. 이를 위해 무선 취약점을 실시간으로 감시하여 탐지하고 관리하는 기술들이 자동으로 제공될 수 있도록 해야 한다.

이상과 같이 향후 발생 가능한 각종 보안 위협에 대처하고 모바일 서비스 환경을 보장하기 위한 스마트 단말 보안기술과 특징, 적용범위, 개선방향 및 대책에 대해 종합적으로 정리하면 <표 1>과 같다.

Ⅳ. 결 론

지금까지 군에서 사용하는 스마트 단말 동향과 활용 사례, 보안 위협 요소 및 이에 대응하기 위한 모바일 보안 기술들을 살펴보았다. 미래전은 각종 IT 기술이 융합된 스마트 모바일 단말이 군의 지휘통제체계를 포함한 각종 무기체계에 접목되면서 군 작전 등 다양한 분야에 많은 변화를 일으킬 것이다. 따라서 군과 같은 다양한 전장 환경에서 향후 스마트폰 사용이 불가함으로 인한 전투지휘체계의 안전성과 효율성을 저하시키는 저해요인을 제거하기 위해 국내외적으로 기술 초기단계에 있는 군사용 스마트 단말 보안기술의 개발은 필수적이다. 우리 군에서도 전투력 상승 목적으로 스마트 단말 사용을 시도하고 있는데, 군에서 이러한 스마트 단말을 활용하려면 스마트 단말 보안 기술이 플랫폼 보안, 서비스 보안, 데이터 관리, 네트워크 보안 각 분야별로 체계적으로 개발되어 기반으로 구축되어야 한다. 특히, 이러한 스마트 단말 보안기술 확보는 경제적으로도 파급효과가 매우 커서 산업발전과 민간 보안기술 수준을 한 단계 끌어올리는 중요한 계기가 될 것으로 기대하므로 시급히 추진해야 할 것으로 본다.

References

[1] KISA, “Internet & Security issues”, 2010.03.

[2] Ki-young Kim, Dong-ho Kang, ″Smart phone security technology at open mobile environment″, *Korean Institute of Information Scientists and Engineers*, vol. 19, no. 5, 2009.12.

[3] Ji-eon Lyu, ″Key enabler of the smart phone: Software″, *SW Insight*, 2009.04.

[4] Gwang-ho Baek, ″Recent trends in research and technology of Secure Execution Environment″, *Electronics and Telecommunications Trends*, vol. 22, no. 5, 2007.10.

[5] ARM, “ARM Security Technology Building a Secure System using TrustZone Technology”, Apr. 2009. pp1-108.

[6] Trusted Computing Group, “TCG specification architecture overview. specification revision 1.4”, Aug. 2, 2007. pp1-54.

[7] Trusted Computing Group, “TCG mobile trusted module specification. Specification version 1.0, revision 6”, June 26, 2008. pp1-105.

[8] Trusted Computing Group, “TCG mobile reference architecture. Specification version 1.0, revision 1”, June 12, 2007. pp1-87.

[9] Reiner Sailer, “Xiaolan zhang, Trent faeger, Leendert van doorn: design and Implementation of a TCG-based integrity measurement architecture”, *13th Usenix Security Symposium*, June 27, 2004.

[10] Ji-ho Bang, Lan Ha, Pil-young Kang and Hong-geon Kim, "Security verification framework for e-GOV mobile App.", *Journal of the Korean Institute of Communications and Information Sciences*, vol.37, no.2, pp119-131, .2012.

손 익 재 (Iek-jae Son)

1992년 2월 인하대학교 전자계산학 석사
2011년 12월~현재 국방부 정보화 기획관실 정책기획담당
<관심분야> 정보보호, 사이버전, 소프트웨어 엔지니어링 등

김 일 호 (Il-ho Kim)

2001년 8월 아주대학교 정보통신대학원 석사
2011년 1월~현재 국군사이버사령부 예방팀장
<관심분야> 상호운용성, 정보보호, 사이버전 등

양 종 휴 (Jong-hyu Yang)

1992년 12월 FloridaTech 석사
2011년 12월~현재 해군정보통신전대 전대장
<관심분야> C4I, 사이버전, 정보보호, 네트워크중심전 등

이 남 용 (Nam-yong Lee)

1999년 9월~현재 숭실대학교 IT정책 경영학과 주임교수
2012년 8월~현재 SW특성화대학원 원장
1999년 9월~현재 (사)한국IT정책 경영학회 회장
<관심분야> 시스템엔지니어링, 엔지니어링, 경영정보시스템 등