情 報 保 護 學 會 誌
第21卷 第3號, 2011. 5

스마트워크 보안 위협과 대책

이 형 찬*, 이 정 현**, 손 기 욱***

요 약

이동통신기술의 발달과 스마트기기 이용의 확산은 업무 환경에 큰 변화를 가져왔다. 고성능 연산장치와 기억장치가 내장된 스마트폰, 태블릿을 활용함으로써, 과거 사무실 안, 원격근무지 안 등으로 한정되어 있던 업무공간의 제한이 없어지고 언제 어디서나 효율적으로 업무를 처리하는 스마트워크가 가능해졌다. 최근 국내에서 스마트워크에 대한 관심이 증대되고 있으며, 서서히 스마트워크 시스템을 구축하고 있다. 하지만, 업무의 효율성을 높여주는 스마트워크 시스템에도 보안 위협이 존재하며, 그에 대한 체계적인 분석과 대책이 현재까지 부족한 실정이다. 이에 본 논문에서는 스마트워크 환경의 보안 위협 요소와 보안 요구사항에 대해 고찰해보고, 그에 대한 대책을 논하여 본다.

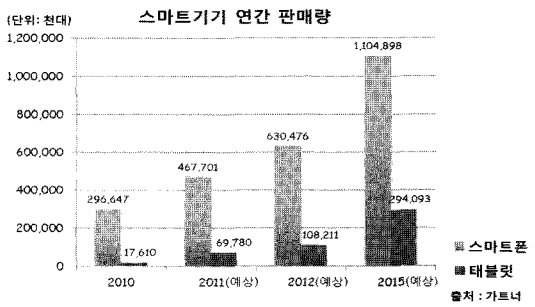
Ⅰ. 서 론

최근 휴대폰은 단순통화기능으로 출발하여 PDA기능, 모바일 결제(mCommerce), MP3, 카메라, DMB, 인터넷 및 E-mail 접속기능에 이르기까지 매우 빠른 속도로 진화하고 있다. 그 중에서도 기존 휴대폰의 통화 기능에 PC 환경에서 제공되던 다양한 인터넷 서비스 기능까지 하나의 단말기로 융복합화된 것이 스마트폰이다. 이와 같은 휴대단말 기능의 융/복합화 및 인터넷연동의 가속화 추세는 제2세대(2G)에서 제3세대(3G)에 이어 3.5G, 4G의 흐름으로 진화중인 무선 이동통신 기술의 발전에 의해 더욱 촉진되고 있다.

스마트폰, 태블릿과 같은 스마트기기들은 점점 보편화되어가는 추세이며, 그 수요가 점점 증가하고 있다. 2011년 4월 가트너에서 공개한 [그림 1]의 자료에 따르면, 2010년 한해간 2조 9천만대 이상 스마트폰이 판매되었으며, 2015년에는 11조대 이상 판매될 것으로 예측되었다 [1,2].

이처럼 스마트기기는 급속도로 현대인에 생활에 전파되어 영향력을 끼치고 있다. 진보된 스마트 기기를 통해 무선 인터넷에 접속하고, PC 수준의 연산능력을 활용하여 필요한 정보를 공간에 구애받지 않고 획득, 가공, 공유할 수 있게 됨으로, 최근 국내에서 이를 활용하여 업무의 효율을 높이는 스마트워크에 대한 관심이 증대되고 있다 [3].

스마트워크는 유·무선 네트워크를 활용하여 언제 어디서나 사무실과 같이 구성원 협력하여 효율적으로 업무를 처리하는 방식 및 환경으로 볼 수 있다. 스마트워크와 원격근무의 차이점은 기존 원격 근무의 경우, 회사



〔그림 1〕 스마트기기 연간 판매량

이 논문은 2010년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업(No. 20100011057)과 ETRI 부설연구소의 연구비 지원에 의해 수행되었습니다.

* 숭실대학교 대학원 컴퓨터학과 석사과정(lee.hyeongchan@ssu.ac.kr)
** 숭실대학교 컴퓨터학부 교수 (jhyi@ssu.ac.kr)
*** ETRI 부설연구소 (kiwook@ensec.re.kr)

사무실의 공간제약을 벗어나, 원격지 예를 들어 자택에서 근무를 할 수 있으나, 여전히 특정 공간에 국한된다. 하지만, 스마트워크의 경우 보편화된 스마트 기기와 무선통신망을 활용하여 이동 중에도 업무가 가능하다. 즉, 스마트워크는 원격근무와 달리 공간의 제약을 완벽히 극복한다 [4].

스마트워크는 이동통신기술을 적극 활용함으로 업무 처리시 공간의 제약을 받지 않는 반면에, 스마트기기의 보안 위협이 스마트워크의 보안 위협으로 직결되는 문제를 안고 있다. 뿐만 아니라, 업무용 PC에서 발생할 수 있는 보안 위협, 예를 들어 업무 관련 데이터 보호, 사용자 인증, 데이터 접근 관리 등의 보안 위협 역시 스마트워크의 보안 위협이라 볼 수 있다. 이러한 보안 위협들이 실제 보안 사고로 이어진다면, 기업은 산업정보 및 기술 유출 등의 심각한 금전적 손실에 직면할 수 있다.

때문에 본 고에서는 스마트워크 보안 위협을 살펴보고 이에 대한 보안대책을 논하여 본다.

Ⅱ. 스마트워크 보안 위협 요소

스마트폰 자체가 가지는 보안위협 요소는 크게 스마트폰의 도난·분실, 스마트폰을 통한 중요자료의 외부유출과 같은 물리적인 보안 위협과 악성코드 감염과 같은 소프트웨어적 보안 위협으로 구분할 수 있다. 그밖에 스마트워크 환경에서 업무서버와 단말 사이 데이터 송·수신으로 인해 네트워크 보안 위협과 모바일 센터 보안 위협이 존재한다.

2.1 물리적 보안 위협

스마트폰은 휴대하기 편리하고, 대용량 메모리 및 통신 기능이 있기 때문에 스마트워크 환경에서 업무용, 영업용으로 활용이 가능하다. 뿐만 아니라, 사용자는 스마트폰을 항상 휴대하며 언제 어디서나 스마트폰을 이용해 회사 내부 시스템에 접속하여 업무 처리를 할 수 있는 장점이 있다.

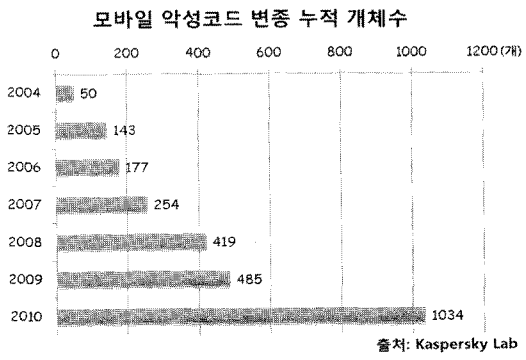
하지만 스마트폰은 개인 휴대기기의 특성상 이용자의 부주의로 인해 기기 및 메모리카드 등을 도난·분실할 위험성이 존재한다. 특히 스마트폰에는 일반적으로 통화내역, 수신메시지, 전화번호부, 일정, 위치정보, 금융거래정보 등과 같은 다량의 개인정보가 저장된다. 업무용 혹은 영업용으로 사용되는 경우 회사 기밀정보 및 업무정보 또한 스마트폰에 저장되기 때문에 스마트폰이 도난·분실될 경우에 스마트폰에 저장되어 있는 개인정보 및 업무정보가 외부로 유출될 가능성이 존재하며, 이로 인해 개인 및 기업에 피해가 발생할 가능성이 존재한다. 뿐만 아니라, 악의적인 사용자가 도난·분실된 스마트폰을 습득하는 경우, 이를 통해 업무용 서버에 불법 접속하여 업무 정보를 유출하거나 위·변조가 가능한 문제가 존재한다.

또한 스마트폰은 그 자체가 대용량의 이동식 저장매체로써 내부자에 의해 회사 기밀정보가 외부로 유출되는 수단으로 사용될 수 있는 문제점이 있다.

2.2 소프트웨어 보안 위협

스마트워크 환경에서 사용되는 모바일 단말기인 스마트폰은, 단순한 핸드폰이 아닌 다양한 네트워크 인터페이스를 가진 컴퓨터로 현재 인터넷 환경에서 발생할 수 있는 모든 보안 위협이 스마트폰 환경에서 동일하게 적용된다. 또한 오픈된 개발 환경의 제공으로 자유로운 프로그램 개발 및 설치가 가능하다는 점은 다양한 어플리케이션의 제작이 가능하다는 점에서는 환영할 일이지만, 반대로 악성코드와 같은 어플리케이션의 제작이 가능하여 보안 문제가 발생할 가능성이 높다. 또한 이렇게 제작된 어플리케이션을 오픈마켓을 통해 손쉽게 유통이 가능하기 때문에, 악성코드 어플리케이션이 제작되어 배포될 경우 PC에 비해 더 큰 파급력을 가지게 된다.

실제 2004년 카비르(Cabir)라는 웜(Worm)이 최초 발견된 이후, [그림 2]와 같이 현재까지 약 1000여종의



〔그림 2〕 모바일 악성코드 변종 누적 개체수

악성코드가 스마트폰에서 발견되었다[5,6,7]. 이들 대부분은 스마트폰에 탑재되는 운영체제의 취약점을 이용하여 동작하는 것으로, 이러한 모바일 악성코드는 정상 동작 방해, 원격 제어, 개인 정보 유출, 과금 유도, 유해 사이트 접속과 같은 공격을 수행하는 것들이 대부분이었다.

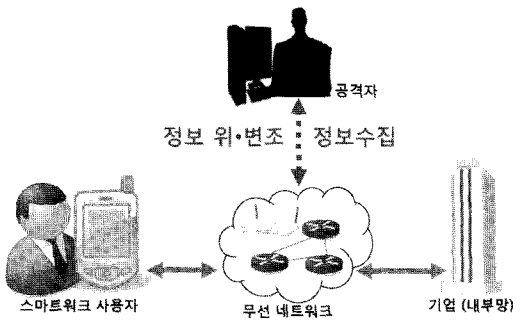
스마트폰 환경에서는 원격제어 가능하다. 정상코드 내에 삽입된 악성코드는 마켓, SMS, 노트북과 같은 다양한 경로를 통하여 스마트폰에 설치되며, 설치된 후 스마트폰 내부의 정보를 무선랜, 블루투스와 같은 통신 매체를 이용하여 공격자에게로 전송하는 것이 가능하다. 특히 스마트워크 환경에서 사용되는 스마트폰의 경우 회사 기밀 정보를 담고 있다는 점에서 악성코드를 통한 정보 유출과 같은 문제가 발생할 경우 그 피해는 매우 클 것으로 예상된다.

2.3 네트워크 보안 위협

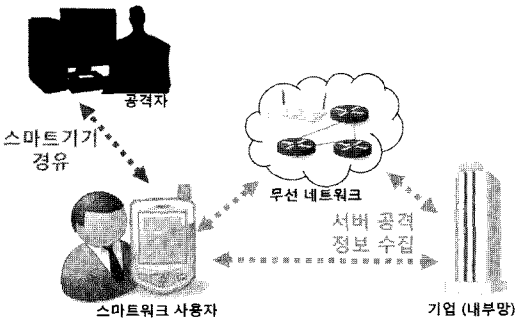
일반적으로 기업들은 기업 내부의 자료를 보호하기 위해 업무용 전산망을 사설망으로 구성하여 관리한다. 하지만 스마트워크 환경에서는 스마트기기를 통해 외부의 무선 네트워크에서 사내 사설망에 접속하여 업무를 보기 때문에, 일반적인 인터넷망에서 발생할 수 있는 네트워크 보안위협이 동일하게 적용되게 된다. 예를 들어, [그림 3]과 같이 업무 내용에 대한 도·감청이 가능하게 되며, 이를 악용하여 기업의 비밀정보를 수집하거나, 잘못된 정보를 보내 업무상 혼란을 발생시킬 수 있다.

2.4 모바일 센터 보안 위협

스마트워크 환경에서는 스마트폰이 사내 사설망 혹



[그림 3] 네트워크 보안위협



[그림 4] 스마트기기 경유 내부망 공격

은 사내 서버 공격의 경유지로 활용될 수 있는 보안위협이 존재한다. 사내 사설망으로 운용되는 일반적인 기업의 업무용 전산망에 비인가된 장비 혹은 비인가된 사용자는 외부에서 접근이 불가능하다.

하지만 [그림 4]에서 보는 바와 같이, 스마트폰 자체의 취약점을 이용해 스마트폰을 악성코드로 감염시키게 되면, 공격자는 외부 네트워크에서 3G 망을 통해 감염된 스마트폰으로 접속할 수 있게 되고, 다시 감염된 스마트폰에서 Wi-Fi를 통해 사내 내부망에 직접 접근하거나 혹은 외부 무선망을 통해 간접적으로 사내 사설망으로의 접근이 가능하게 된다.

이와 같은 방법으로 공격자가 사내 사설망에 접근하게 되면, 사내 사설망에서 전송되는 정보들을 수집하거나, 사내 주요서버를 공격하는 등의 보안위협이 발생할 수 있다.

Ⅲ. 스마트워크 보안 요구사항

스마트워크의 기술적 보안대상은 스마트폰 단말기, 네트워크, 센터(모바일 플랫폼 등) 영역으로 구분할 수 있으며, 본 장에서는 각 영역별 보안 대책을 분석한다. 단말 영역은 스마트폰 단말기 상에서 일어날 수 있는 침해사고에 대한 기술적 보안 대책을 지칭하며, 네트워크 영역은 네트워크상에서 발생할 수 있는 침해사고 보안대책을 의미한다. 모바일 센터 영역은 모바일 센터 및 사내 인트라넷의 침해사고 보안대책(모바일 PKI 인증, 모바일 방화벽)에 일컫는다.

3.1 단말 보안 요구사항

스마트워크 단말 보안 영역은 스마트폰 단말기 상에

서 일어날 수 있는 침해사고 대응 및 대비를 위한 영역이다. 단말 보안 영역은 악성코드 대응, 사용자 인증, 모바일 OS 보호, 자원관리, SW관리, 데이터 보호 범주로 나누어진다. 각각의 범주별 보안요구사항을 분석하여 [표 1]과 같이 구성한다.

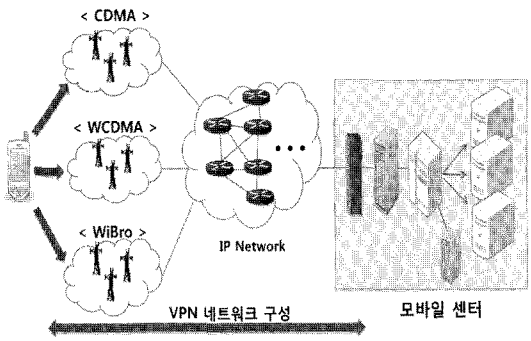
3.2 네트워크 보안 요구사항

네트워크 영역을 물리적 계층과 네트워크 계층으로 구분하여 각각의 보안 요구사항을 [그림 5]와 같이 분석한다. 물리적 계층에서는 악의적인 공격자가 내부망 근처에서 무선랜이나 기타연결 방식을 통하여 사내망에 접근할 위협이 있어, 무선랜 운용 및 기타 연결방식에 대하여 보안 요구사항을 분석한다, 공개된 망을 통한 데이터 송수신을 허용하는 네트워크 계층에서는 근본적으로 많은 보안 취약점을 가지고 있다. 때문에 네트워크 계층은 모바일 기기와 모바일 센터간 데이터 송수신에 참여하는 모든 네트워크 영역의 취약점을 분석하고 대처 할 수 있도록 침입차단, VPN, 보안관제 등을 고려한다.

네트워크 영역의 세부적인 보안 요구 사항은 다음 [표 2]과 같다.

〔표 1〕 단말 보안 요구사항 분석

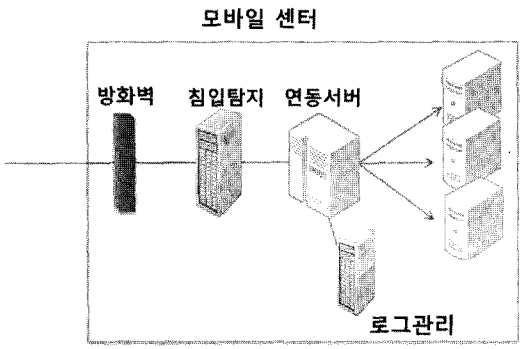
분 류		세부 요구 사항
사용자 인증	수행 시점	구동시 사용자 인증 수행 일정시간 미사용시, 자동 잠금 잠김 해제시 사용자 인증 수행
	인증 방법	추측하기 어려운 8자리 이상의 비밀번호 사용 비밀번호 평문 저장 금지
	인증실패 조치	일정횟수 이상 인증 실패시 보안 담당자만 해제 가능
악성코드 대응	안티 바이러스	안티바이러스 SW 설치 최신 엔진 상태 유지 실시간 감시 수행
		기술적 통제된 정기적인 검사 수행
	안전한 인터넷 이용	의심스러운 파일 다운로드 금지 다운로드 파일 검사 후 실행
모바일 OS 보호	모바일 OS 보안패치	모바일 OS 보안패치 최신상태 유지
	모바일 OS 변조방지	기술적 통제된 주기적 모바일 OS의 무결성을 검사하여 변조 방지
자원 관리	H/W지원 접근통제	마이크, GPS, 카메라 등 HW에 대한 인가된 프로그램만 접근허용
SW 관리	SW 배포 및 설치	기업에서 서명 또는 허가한 SW만 설치하도록 기술적 통제 수행
데이터 보호	저장매체 접속통제	스마트폰↔업무PC 접속 및 데이터 전송 통제 담당자에게 허가받은 저장매체만 스마트폰에 사용
	데이터 저장여부	기업 기밀 및 기술 콘텐츠는 자료저장을 통제 ※ 휘발성 메모리 저장만 가능. 불가피한 경우 파일은 암호화하여 임시 저장 후 삭제
	화면 캡처 방지	기업 기밀 및 기술 콘텐츠는 화면 캡처 방지
	분실 및 도난 대책	분실 및 도난 스마트폰에 대한 원격 삭제 기능 제공



〔그림 5〕 네트워크 보안 요구사항

〔표 2〕 네트워크 보안 요구사항

분 류		세부 요구 사항
물리적 계층	무선랜	인가된 내부 무선 AP만 운용 및 접속 허용 - 접속시 스마트폰 사용자 인증 및 암호화 통신 사용 - AP의 SSID Broadcast 통제
	기타	허가 받지 않은 장치를 통한 인터넷 연결 금지(예: 테더링 기능 사용금지)
네트워크 계층	무선 침입방지 시스템	사내 무선랜 운용시 비인가 무선 단말·AP 탐지 등을 위한 무선 침입방지시스템 운영
	VPN	스마트폰에서 모바일 센터영역까지 VPN 적용
		VPN 클라이언트는 보안담당자의 통제를 받아 배포
		VPN이 동작하는 동안 他프로세스들의 통신은 모두 차단
	보안관제	해킹, 웜·바이러스 감염 대응을 위한 보안관제



〔그림 6〕 모바일 센터 보안 요구사항

3.3 모바일 센터 보안 요구사항

모바일 센터 보안 영역은 스마트워크 업무서버, 관제서버, 정책서버 등이 포함된 서버 운용을 위한 영역으로 안전한 모바일 센터 운용을 위해 [그림 6]와 같이 침입탐지, 보안관제, 로그 관리 등을 다룬다.

모바일 센터 보안을 위한 세부적인 요구 사항은 다음 [표 3]과 같다. 서버보안 영역의 보안 요구사항의 모든 주체는 서버관리자에 해당된다.

〔표 3〕 모바일 센터 보안 요구사항

분 류		세부 요구 사항
관리자 인증	계정관리	개발시 사용된 계정 및 비밀번호 폐기
		8자리 이상의 비밀번호 사용
		비밀번호 암호화 저장
	수행시점	각종 서버 접근시, 인증 수행
		일정기간 입력이 없을시, 자동으로 각종 서버와 접속 해제
	인증방법	비밀번호 혹은 전자서명 인증서를 이용한 인증 수행
		OTP, 보안카드, 바이오인식 등의 방법으로 추가 인증을 수행
로그 관리	사용자 행위 기록	스마트폰 사용자가 스마트워크 서비스 사용내역을 기록
		로그를 관리하기 위한 별도의 서버 운영
악성 코드 대응	불필요한 서비스 제거	불필요한 서비스와 포트를 차단
	호스트 방화벽	별도의 호스트 기반 방화벽 운영

Ⅳ. 스마트워크 보안 대책

4.1 단말 보안 대책

스마트폰 단말 보안 영역 상에서 일어날 수 있는 침해사고 대응 및 대비를 위한 보안요구사항을 악성코드 대응, 사용자 인증, 모바일 OS보호, 자원관리, SW관리, 데이터 보호 범주로 나누어 기술한다.

단말 보안 요구사항을 만족시키기 위한 기술적인 안전 대책을 사용자 인증 대책, 단말 인증대책, 앱 보안 대책, 악성코드 대책, 단말 분실·도난 대책, 플랫폼 보안 대책, 원격제어 대책, 콘텐츠 보안 대책, 하드웨어기반 보안 대책으로 범주를 나누어 [표 4]와 같이 기술한다.

4.1.1. 사용자 인증 대책

사용자 인증은 ID/패스워드(8자리 이상) 방식 또는 PKI 기반 인증서 방식을 우선 적용하도록 한다. 이때 PKI 인증서는 단말이 제공하는 안전한 공간에 저장하여야 한다. 패스워드 방식의 경우, 패스워드가 설정 되어 있지 않거나 일정회수 이상의 입력 오류시에는 사용이 차단되어야 하고, 패스워드 자동 잠금 기능의 설정 여부를 판단할 수 있어야 한다. 높은 보안성이 요구되는 서비스 운용시에는 PKI 인증서와 더불어, 추가적인 인증 솔루션(OTP등)을 적용하여야 한다.

4.1.2. 단말 인증 대책

단말 식별 및 인증을 위해서는 PKI 인증서 또는 기기 인증서 방식을 적용하도록 한다. 또한, 암호키 분배를 위해서도 인증서 기반 방식을 적용하도록 한다. 단말 인증을 위한 전자서명 생성 및 검증 알고리즘으로는 RSA(2,048비트), 해쉬 함수는 SHA-2(256비트) 보안 수준 이상의 알고리즘을 사용할 것을 권장한다.

4.1.3. 앱 보안 대책

스마트워크에 사용되는 클라이언트 앱에 대해서는 공인된 앱 검증기관으로부터 CC 수준의 보안성 검증을 받아야 하고, 검증된 앱은 앱 검증기관이 발급한 코드서명용 인증서에 기반한 코드서명 기술을 적용하여야

〔표 4〕 스마트워크 보안 대책

분류	세부 보안 대책
사용자 인증 대책	패스워드 미설정/일정회수 이상 입력 오류시 사용 차단
	패스워드 자동 잠금 설정 탐지
	PKI 인증서
	인증서와 동등한 보안성을 가지는 인증 솔루션 적용
단말 인증 대책	PKI 기반 단말 인증 및 키 분배
	기기인증서 기반 단말 인증 및 키 분배
앱 보안 대책	신뢰된 인증기관에 의한 코드서명 적용
	이동통신망만을 통한 업데이트
	패치관리시스템(PMS) 통한 버전 관리
	소프트웨어(코드서명) 기반 앱무결성 검증
	주요 H/W(카메라, GPS, 마이크)에 인가된 SW만 접근허용
악성 코드 대책	전용 백신 S/W 제공
	이동 저장매체 접속시 악성코드 자동탐지 및 삭제
	악성행위 탐지시 세션 강제 종료 및 로그 기록
단말 분실·도난 대책	원격 잠금, 원격삭제
	원격 단말 위치 추적
	Mission-critical 데이터 백업 및 복구
플랫폼 보안 대책	플랫폼 구조변경(탈옥, 루팅 등) 자동 탐지
	코드서명 기반 플랫폼 무결성 검증
	실행영역의 논리적 권한 분리 (Sandboxing)
	실행영역 메모리 무결성 검증
	멀티 태스킹 기능 차단
	멀티 태스킹 기능 선택적 제어 기능
	사용자 프로세스의 파일시스템 접근 권한 제한
원격 제어 대책	디바이스 설정값(configuration)의 변경 탐지 및 복구
	플랫폼 무결성 원격 검증 (Remote Attestation)
	앱 무결성 원격 검증 (Remote Attestation)
접속 관리 대책	P2P, 웹하드 접속 금지
	스마트폰-PC간 유무선 직접연결 차단
	스마트폰-PC간 테더링 연결 차단
콘텐츠 보안 대책	첨부파일을 이미지화하여 보기만 가능
	기업내부문서에 대한 화면캡처 방지
	송수신암호화
하드웨어 기반 보안 대책	하드웨어(TPM, USIM 등)기반 개인키 저장 관리
	하드웨어(TPM)기반 플랫폼 무결성 검증
	하드웨어(TPM)기반 앱 무결성 검증
	하드웨어(TPM)기반 플랫폼 무결성 원격 검증
	스마트워크하드웨어(TPM)기반 앱 무결성 원격 검증

한다. 스마트폰 제조사 또는 통신사의 사전 검증을 받지 않았거나, 개인 등 신뢰할 수 없는 자가 자체 서명한 앱은 설치할 수 없도록 기술적 통제 장치가 마련되어야 한다.

스마트워크 앱의 패치 및 정기 업데이트는 무선랜(WiFi)을 통해서는 할 수 없고, 이동통신망(CDMA, WCDMA, WiBro)을 통해서만 하여야 한다. 애플리케이션 공급 사이트(앱스토어, T스토어, 쇼스토어 등)를 통한 원격 패치 및 정기 업데이트는 허용하되, PC와의 연동 방식(PC Sync)은 PC 측면에서 사용자 인증 등 추가적인 보안 대책을 적용한 경우에만 허용하여야 한다. 또한, 설치된 소프트웨어 버전 등의 관리를 위하여 PMS(Patch Management System) 환경을 구축·운영하여야 한다.

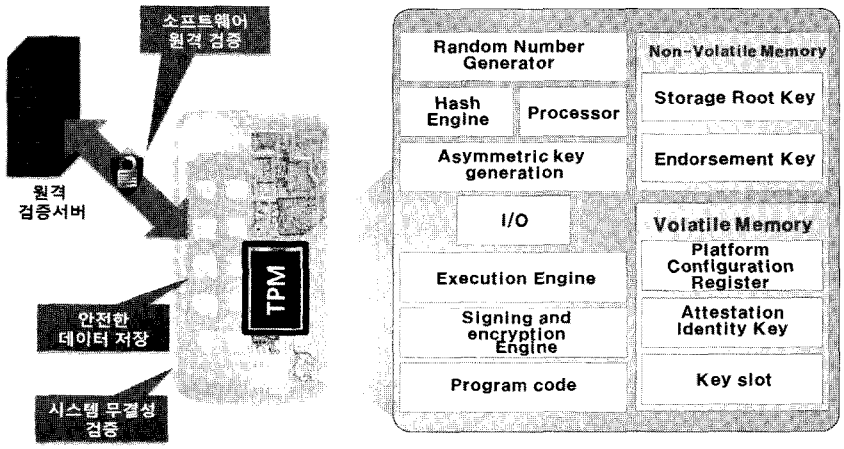
소프트웨어 구동 시 단말 프로세스 환경에서 해킹 여부를 필수로 검증하여 변조되지 않은 단말기 환경에서만 접속이 가능하도록 하여야 한다. 스마트워크에 사용되는 앱에 대한 안전성을 공인된 앱검증 기관의 인증서를 이용하여 앱의 코드서명 확인을 통해 무결성 여부를 판단한다. 또한, 스마트폰 H/W(카메라, GPS, 마이크 등)에 대한 임의접근을 허용하지 않아야 한다.

4.1.4. 악성코드 대책

Virus, Trojan, Worm 등 유해 프로그램을 통한 해킹 및 네트워크 공격 방지를 위해 전용 Anti-Virus 단말 솔루션을 제공하여야 한다. 스마트폰 단말에 대한 백신프로그램 설치를 의무화하고 자동 업데이트 기능을 지원하여야 한다. 스마트폰에 저장매체(SD 카드 등) 접속 시, 저장매체에 악성코드 설치 여부를 자동점검 및 삭제하는 기능을 제공하여야 한다. Jailbreaking, Rooting 등으로 인해 모바일 OS의 무결성이 보장되지 않을 경우 스마트워크 서비스 접속을 차단하여야 한다. 또한 비정상적인 접속 및 비정상적인 자료 송신 시에는 강제로 세션을 종료시키고, 세션에 대한 정보를 로그로 남겨야 한다.

4.1.5. 분실 및 도난 대책

단말의 수리 및 분실 시, 데이터 유출을 막기 위해 저장된 사용자 계정, 개인 정보 및 스마트워크 클라이언트



〔그림 7〕 TPM 단말 보안

앱 등을 원격 삭제할 수 있어야 한다. 분실된 단말기의 위치를 추적할 수 있어야 하고, 분실 대비 사전에 업무용 중요 데이터의 백업 기능과 단말기 회수 또는 교체 시 백업 데이터의 복구 이전 기능을 제공하여야 한다. 원격에서 이러한 기능 지원 및 관리하기 위한 MDM (Mobile Device Management) 시스템 구축, 운용하여야 한다.

4.1.6. 플랫폼 보안 대책

스마트폰 OS의 무결성을 검사하기 위해 탈옥(Jailbreaking), 루팅(Rooting) 등 플랫폼 구조변경 유무를 자동으로 탐지할 수 있어야 한다. 운영체제 커널 모듈, 보안 라이브러리 모듈 등에 대한 시스템 소프트웨어 실행 단계에서 코드서명에 기반한 무결성 검사를 실시하여야 한다. 샌드박스(Sandbox) 등에 기반한 앱 실행 영역이 논리적으로 분리되어야 한다. 프로세스 메모리 후킹 등 실행시 시스템 메모리 영역에서 코드의 변경 또는 조작을 시도하는 악성코드의 경우 정적 코드 무결성 검사에서 탐지되지 않기 때문에, 메모리에 로딩된 코드의 동적 무결성을 점검하는 기능을 제공하여야 한다. 또한, 코드 서명이 없는 앱이 설치되었더라도 커널에서 실행되지 못하도록 프로세스별 실행 권한(Privilege) 제어 기능을 제공하여야 한다.

앱의 동작시 플랫폼의 멀티태스킹 기능을 차단하거나, 앱의 특성에 따라 선택적으로 백그라운드 프로세스의 동작을 제어할 수 있어야 한다. 아울러, 파일 시스템에 대한 접근 권한을 제한하고 사용자 프로세스의 시스템 자원에 대한 접근을 방지하여야 한다.

4.1.7. 원격제어 대책

주요 디바이스의 설정값(configuration)을 임의로 변경할 수 없도록 하고, 이의 변경시 자동 탐지 및 복구 기능을 제공하여야 한다. 앱 및 플랫폼 구성정보와 실행 코드의 무결성을 원격에서 주기적으로 검증(Remote Attestation)할 수 있어야 한다. 이를 위해 모바일 센터에서는 원격 검증 서버(Remote Attester)를 운영하여야 한다.

4.1.8. 접속관리 대책

스마트폰을 이용한 P2P, 웹하드 접속을 단말에서 차단하는 기능을 제공하여야 한다. 스마트폰과 일반 PC간의 유무선 직접 연결을 통한 데이터 전송을 통제할 수 있어야 하고, 스마트폰과 PC간의 테더링(Tethering) 연결을 차단하여야 한다. 또한, 업무용 PC에는 스마트폰용 저장매체(USB, microSD 등)에 대한 접근을 통제할 수 있는 기능이 제공되어야 한다.

4.1.9. 콘텐츠 보안 대책

기업 내부 문서나 데이터는 단말에 저장되지 않도록 하며, 이미지 등 편집이 불가능한 형태로 변환하여 스트

리밍 방식으로 이용자 단말로 전송되어야 한다. 스트리밍 방식으로 첨부파일을 확인하는 뷰어 프로그램을 지원하되, 세션 타이머 기능을 적용하여 자동으로 종료되도록 조치하여야 하며, 프로그램 종료 시 임시 저장된 파일은 삭제하여야 한다.

모든 데이터는 송수신시 뿐만 아니라 스마트폰에 임시 저장 시에도 암호화 하고 메모리에 로딩 시에만 복호화 할 수 있어야 한다. 암호 알고리즘으로는 AES(128비트), ARIA(128비트) 또는 이상 수준의 알고리즘을 사용할 것을 권장한다.

4.1.10. 하드웨어(TPM) 기반 단말 보안 대책

단말 불법 복제, 도청 및 악용, 개인정보 보호 위협, 악성 코드 삽입 등 외부 공격으로부터 데이터, 키, 인증서 등을 하드웨어 적으로 안전하게 보호 하고, 비밀키를 하드웨어 외부로 유출하지 않으면서 암복호 및 서명 검증 기능 수행이 가능하도록 하는 하드웨어 칩형태의 보안 솔루션을 TPM(Trusted Platform Module)이라 부른다. TPM이 단말에 장착되면 [그림 7]과 같이 사용자 인증, 플랫폼 무결성 인증, 앱 무결성 인증, 원격 검증 등 다양한 범주에서 보다 안전하고 신뢰성 있는 보안 솔루션을 제공할 수 있다.

4.2 네트워크 보안 대책

네트워크 보안 요구사항을 만족시키기 위한 기술적인 보안 대책은 [표 5]와 같다.

4.2.1. 무선망 연결 대책

기업내 사내망의 접속은 이동통신망(CDMA, WCDMA, WiBro)을 통해서만 가능하도록 하고, 무선랜(WiFi)과 블루투스(Bluetooth)를 통한 접속은 자동으로 차단할 수 있어야 한다. 불법 AP, 애드혹 연결 차단, 단말기 피싱 공격 등 무선랜 보안 위협을 차단할 수 있어야 한다.

4.2.2. 통신망 암호화 대책

종단간 데이터 및 음성의 도·감청 방지를 위해 암호화(AES 128bit, ARIA 128bit)된 통신채널을 생성하여야 한다. VPN 인증 및 보안 채널 생성에 사용되는 인증서는 PKI기반 인증서를 적용하는 것을 원칙으로 한다.

4.3 모바일 센터 대응 방안

모바일 센터 보안 요구사항을 만족시키기 위한 기술적인 보안 대책은 [표 6]과 같다.

4.3.1. 침입 차단 및 방지 대책

해킹 및 비인가자의 접근 차단을 위해 이동통신망과 연동되는 구간에 침입차단시스템 구축·운영하고, 비정상 트래픽의 상시 모니터링을 위해 이동통신망과 연동되는 구간에 유해트래픽탐지시스템 구축·운영하여야 한다.

4.3.2. 보안 관제

위협관리대응 및 침해사고 대응시스템을 구축·운영하여, 24시간 보안관제를 실시한다. 침해사고 및 보안정보를 안내 및 공지를 통해서 각각의 서비스에 제공하고, 웹을 통한 침해사고 접수, 처리 및 결과통보하도록 한다.

〔표 5〕 네트워크 보안 대책

분류	세부 보안 대책
무선망 연결 대책	비인가 장비로부터의 무선랜 접속 차단
	불법 AP, 애드혹 연결차단 및 탐지
	Wi-Fi, 3G 이외의 서비스 (예: 블루투스) 접속 방식 차단
	이동통신망(3W)만을 통한 서비스 연결
통신망 암호화 대책	안전한 암호화 통신채널 사용
	PKI 기반 VPN 인증 및 보안 채널 생성

〔표 6〕 모바일 센터 보안 대책

분류	세부 보안 대책
침입차단 및 방지 대책	방화벽, IDS 등 보안장비 구축 및 운영
	주기적인 로그 분석을 통한 비정상 접속 여부 점검
	앱 업데이트 서버 URL 검증 및 모니터링
보안 관제	24시간 보안관제
서버 보안	비밀번호 또는 PKI 인증서 적용
	이용자 로그 암호화 저장

4.3.3. 서버 보안

모든 서버는 호스트 기반의 방화벽 운용, 비밀번호 또는 인증서 적용, 로그관리, 불필요한 포트 차단 및 접근·권한 통제 등의 기능을 제공하여야 한다. 또한, 모바일 플랫폼에서 행정서비스 관련 자료는 저장하지 않으며, 이용자 로그 등에 대하여만 암호화하여 저장할 수 있다.

V. 결 론

스마트워크는 스마트 폰과 통신 인프라를 기반으로 하는 혁신적인 IT 서비스의 대표적인 기술이다. 스마트워크를 통해 기업은 생산성 향상과 편리성 증대를 위해 많은 비용과 노력을 투입하여 시범 사업을 수행하고 있다. 그러나 스마트 단말의 분실, 악성 앱의 설치, 기업 정보 및 기술의 무단 유출과 같은 보안 문제는 기존의 PC 기반 서비스에서는 경험하지 못했던 새로운 문제로 지적되고 있다. 이러한 보안 문제에 대한 개선 없이는 안전한 스마트워크 환경 구축을 할 수 없다.

스마트워크 환경의 보안 문제의 체계적인 분석을 위해 본 논문에서는 스마트워크를 구축하는 과정에서 예상되는 보안 문제를 스마트폰 단말기, 네트워크, 모바일 센터의 영역에서 보안 문제를 분석하였으며, 기술적 보안 대책을 논의하였다. 더불어 이러한 보안 문제를 완화시키는 보안 대책을 제시하였다.

본 논문의 대책을 활용하여 현재 구축된 스마트워크 환경 및 새롭게 구축될 스마트 워크 환경의 보안성 수준을 평가 및 검토 한 후 보완할 때, 더 안전한 스마트워크 환경을 구축할 수 있을 것으로 판단된다.

참고문헌

[1] "Gartner Says Android to Command Nearly Half of Worldwide Smartphone Operating System Market by Year-End 2012," http://www.gartner.com/it/page. jsp?id=1622614, Gartner, Apr. 2011.

[2] "Gartner Says Apple iOS to Dominate the Media Tablet Market Through 2015, Owning More Than Half of It for the Next Three Years," http://www.gartner.com/it/ page.jsp?id=1626414, Gartner, Apr. 2011.

[3] 이재성, 김흥식, "스마트워크 현황과 활성화 방안 연구", 한국지역정보화학회지, 13(4), pp. 75-96, Dec. 2011.

[4] 윤창근, "Telework의 고도화를 위한 미국의 동향과 시사점", 지역정보화지, 67, pp. 45-48, Mar. 2011.

[5] D. Maslennikov, "Mobile Malware Evolu- tion: An Overview, Part 4," http://www. secure-list.com/en/analysis?pubid=204792168, Kaspersky Lab, Mar. 2011.

[6] A. Gostev, "Mobile Malware Evolution: An Overview, Part 3," http://www.sec urelist.com/en/analysis?pubid=204792080, Kaspersky Lab, Sep. 2009.

[7] A. Gostev, "Mobile Malware Evolution: An Overview, Part 1," http://www.sec urelist.com/en/analysis?pubid=200119916, Kaspersky Lab, Sep. 2006.

〈著者紹介〉

이 형 찬 (Hyeong-chan Lee)
학생회원
2010년 2월 : 숭실대학교 컴퓨터학부 학사
2010년 3월 ~ 현재 : 숭실대학교 컴퓨터학과 석사과정
관심분야 : 모바일 보안, 소프트웨어 취약점 분석

이 정 현 (Jeong Hyun Yi)
종신회원
1993년 2월 : 숭실대학교 전자계산학과 학사
1995년 2월 : 숭실대학교 컴퓨터학과 석사
2005년 8월 : *University of California at Irvine*, Computer Science 박사
1995년 2월 ~ 2001년 8월 : 한국전자통신연구원 연구원
2000년 4월 ~ 2001년 3월 : 미국 표준기술연구원(NIST) 객원연구원
2005년 10월 ~ 2008년 8월 : 삼성종합기술원 수석연구원
2008년 9월 ~ 현재 : 숭실대학교 컴퓨터학부 조교수
관심분야 : 모바일 보안, 네트워크 보안

사 진

손 기 욱 (Ki Wook Sohn)
정회원
1990년 2월 : 성균관대학교 정보공학과 학사
1992년 2월 : 성균관대학교 정보공학과 석사
2002년 8월 : 성균관대학교 전기전자컴퓨터공학과 박사
1992년 1월 ~ 1999년 12월 : 한국전자통신연구원 선임연구원
2000년 1월 ~ 현재 : ETRI 부설연구소 책임연구원/실장
관심분야 : 소프트웨어 취약점 분석, 시스템 보안