스마트폰 운영체제의 보안 취약성과 대책

신민호, 권호열[1)]
강원대학교 컴퓨터정보통신공학과
e-mail : nautes86@nate.com, hykwon@kangwon.ac.kr

Security vulnerabilities and their Countermeasures of the Operating Systems for Smart Phones

M. H. Shin, H.Y. Kwon
Department of Computer and Communications Engineering,
Kangwon National University

요 약

최근 애플의 아이폰과 안드로이드폰이 국내에 출시됨에 따라 스마트폰에 관심이 크게 증가하고 있다. 이에 따라오는 인터넷 서비스등도 같이 크게 활성화되고 있다. 본 논문에서는 스마트폰의 보안위협에 대해서 각각의 운영체제에 따른 보안 기술을 파악하고, 서로의 보안 취약성을 비교 분석함에 따라 향후 보안 강화를 위한 방안 연구 방향을 제시하였다.

1. 서론

최근 스마트폰 시장에서는 대표적 두가지 진영이 서로 대립하고 있다. 애플의 iOS와 구글의 안드로이드 환경이다. 최근 발표한 보고서[1]에 따르면, 지난 4분기 스마트폰 성장세에 힘입어 전 세계 휴대폰 시장 규모가 5분기만에 플러스 성장한 것으로 조사되며, 2009년 4분기 전 세계 스마트폰 출하대수는 전년대비 30% 성장한 5300만대로 이에 힘입어 2009년 연간 규모는 1억7380만대로 확대되었다고 한다(IDC). 또한 국내 스마트폰 사용이 증가됨에 따라 보안 위협에 대한 관심이 더 집중되고 있다.

그중에 먼저 구글 안드로이드 환경이 보안에 취약하다는 지적이 제기되고 있다. 안드로이드에 대한 보안문제는 비교적 보안에 강한 현재 PC환경과는 크게 다르고 안드로이드 개발 시에 사용되는 Java언어로 만들어진 프로그램이 악성코드의 위협으로부터 자유롭지 못하다는 것에 있다. 그에 비하면 애플의 iOS 환경은 조금 낫다고 볼 수 있다. 그러나 그렇다고 완벽한 것은 아니다. 탈옥이라 불리우는 해킹의 경우에는 안전성이 급격히 떨어진다. 앱스토어에 허가되지 않은 어플을 다운받을 경우에는 그 위험성은 더욱더 커진다.[1, 2]

본 논문에서는 스마트폰 보안이슈에 대해 알아보고 OS별 비교분석 및 보안 대응방안 등을 통해 향후 스마트폰에서의 보안 강화를 위한 방향을 제시하였다.

2. 스마트폰 OS의 보안 취약성

스마트폰 마다 전용 운영체제를 가지고 있기 때문에 버그와 같은 여러 위협이 존재하게 된다. 이러한 버그가 기기의 고장을 유발하는 것이 됨과 동시에 저장된 데이터를 삭제시키기도 한다. 또한 데이터의 암호화가 존재하지 않으면 그 정보는 누구에게나 노출이 되게 된다. 이러한 데이터는 여러 경로를 통해서 제 3자에게 접근을 허용시키게 된다. 이로 인해 개인정보 또는 기업정보의 노출까지 여러 심각한 문제를 발생시키게 된다.

그 뿐만 아니라 스마트폰은 무선네트워크 외에 3G 네트워크를 활용하기 때문에 언제 어디서든 때와 장소를 가리지 않고 정보 유출 및 악성코드에 감염되는 위협이 발생되게 된다. 이러한 악성코드에 감염된 스마트폰은 다른 PC 및 스마트폰에게 유포하게 됨으로 더욱더 문제를 일으키게 된다.

2.1 안드로이드

현재까지 Java의 다양한 취약사항이 발견되어왔고 개선되었지만 아직까지 보안취약점은 존재하고 있다. 그 중 외부 시스템에서 생성된 프로그램이 내부에서 실행되는 것인데 그중 웹브라우저에서 Local과 Remote 환경으로 실행되는 Java Applet 프로그램ㄹ은 각종 Game, Utility 들로 널리 이용되고 있다.

Java의 가상머신인 JVM과 유사한 리눅스 커널 기반에서 동작하는 Dalvik 가상머신을 사용하는 안드로이드는 휴대성 등의 특성으로 인하여 보안에 취약할 수밖에 없다. 안드로이드가 보안에 약한 이유를 더 자세히 살펴보면 애플리케이션에 대한 검증 절차가 없다는 것과 멀티태스킹이 가능한 환경을 악용한 악성코드 삽입 등 안드로이드는 현재까지 보안에 많이 취약한 상태이다.

1) 교신저자

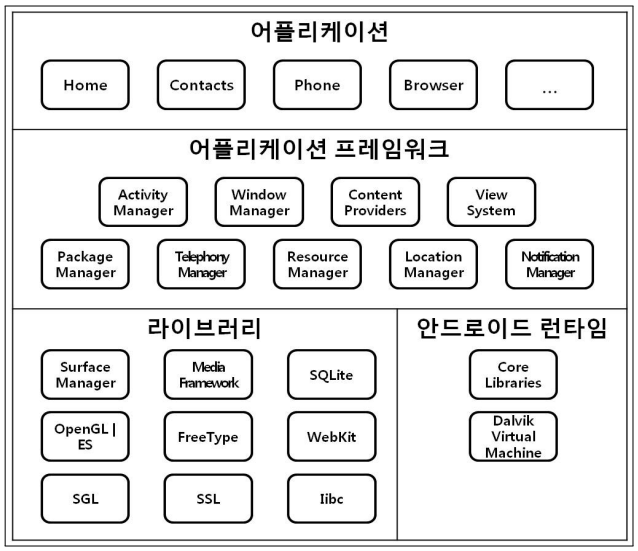

그림 1. 안드로이드 운영체제의 내부 구조

2.2 iOS

iOS 자체에 큰 취약사항은 현재 발견되어있지는 않다. 정상적인 루트에서는 앱스토어 자체에서도 어플리케이션을 검증을 한 후에 올리는 형식이기 때문에 어플리케이션의 문제가 생기는 경우는 지극히 낮다고 할 수 있다.[3]

문제는 JailBreak라는 해킹을 했을 때이다. iOS 내부데이터에 마음대로 접근할 수 있을뿐더러 검증되지 않은 어플리케이션을 사용자 마음대로 설치할 수 있기 때문에 이 경우는 안드로이드 경우보다 더욱 위험할 수 있다. 백신 또한 존재하지 않기 때문에 보안 분야에 있어서는 오히려 안드로이드보다 더 취약해질 수도 있다.

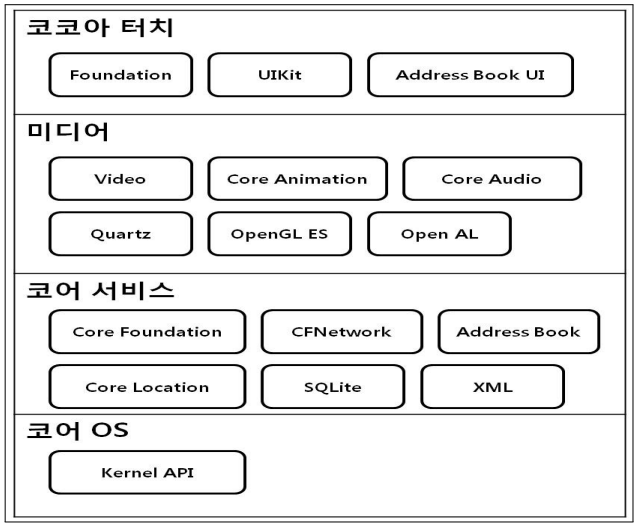

그림 2. iOS 운영체제의 내부 구조

3. 스마트폰 OS 보안 대책

3.1 안드로이드

o 보안 샌드박스 : 안드로이드 보안 구조 설계의 핵심 기술은 보안 샌드박스(Secure Sandbox)이며, 이는 외부로부터 들어온 프로그램이 보호된 영역에서 동작해 시스템이 부정하게 조작되는 것을 막는 보안 형태임, 이는 다른 어플리케이션, OS 또는 사용자에게 영향을 줄 수 있는 동작에 대해서 권한을 갖으며, 이는 Contacts, e-mail, Home Screen 등 각 어플리케이션의 Private date를 읽고 쓰거나, 네트워크에 접근하거나 폰을 깨어있는 상태로 유지하거나 또는 다른 어플리케이션 파일을 읽고 쓰는 것들을 포함함

o 모든 안드로이드 어플리케이션은 코드서명이 되며, 이것은 안드로이드 어플리케이션이 자가 서명된 인증서를 사용하는 것을 허용함, 인증서는 어플리케이션이 구축될 수 있는지를 통제하는 것이 아닌, 어플리케이션 사이의 신뢰 관계를 구축할 경우에만 사용되며 서명이 보안에 영향을 주는 가장 중요한 점은 누가 서명 기반의 허가에 접근할 수 있고 누가 사용자 ID를 공유할 수 있는지를 결정함

o 사용자 ID와 파일 접근 : 장치 상에 인스톨된 각 안드로이드 패키지 파s일에 유일한 리눅스 사용자 ID가 주어짐, 이 사용자 ID는 파일에 대해 샌드박스를 생성하고 다른 어플리케이션을 건드리는 것을 방지함

3.2 iOS

o 장치 통제 및 보호 : 인가된 사용자만이 아이폰에 저장된 데이터에 접근하도록 하는 패스코트 정책, 보안 정책 등을 포함하는 설정 프로파일을 제공하는 장치 설정을 제공함

o 데이터 보호 : 데이터 보호를 위해서 3GS는 장치내의 데이터를 보호하기 위한 AES를 활용하며, 아이폰 분실이나 도난을 고려해서 원격으로 데이터를 삭제하도록 지원, 장치는 패스코트 입력에 실패할 경우 로컬 내용을 삭제하는 등 로컬삭제 기능을 제공함

o 보안 네트워크 통신 : VPN, SSL/TLS, WPA/WPA2를 지원

o 보안 플랫폼 : 개발자를 위한 어플리케이션 데이터 저장을 암호화하는데 활용할 수 있는 공통 크립토 구조를 제공, 런타임 보호, 의무적인 코드서명, AES, RC4 또는 3DES, SHA-1 등을 지원하는 공통 암호구조 등을 제공함

3.3 보안 문제의 해결방안

위의 보안 대책에도 불구하고 발생하는 문제들이 있으며, 그것에 대한 해결방안이 필요하다.

첫째, 안드로이드는 오픈 소스방식으로서 보안의 취약할 수 밖에 없는 태생적인 한계가 있다. 그것을 방지하기 위해 샌드박스와 인증서 등이 있지만, 사용자가 악성코드 프로그램을 설치만 하게 되면 그것은 무용지물이 되며 하드웨어 및 개인정보 등에 접근이 가능하게 되어버린다. 악성 프로그램의 판단과 설치 후의 책임은 사용자의 몫이 되어버리는 것이다.

결국 이 문제는 공개된 안드로이드 마켓의 단점이 되게

된다. 그렇기 때문에 이에 대한 해결 방안이 필요하게 된다. 문제는 응용프로그램의 보안성 및 정당성을 검증하는 절차가 없는 것이다. 따라서, 두 가지 방법을 생각해 볼 수가 있는데, 검증된 인증기관이 별도로 존재하여 해당 기관에 인증을 받고 배포하는 방법과 알려진 악성코드를 수집해서 데이터베이스화 한 후에 악성코드 여부를 판단하여 차단하는 방법이다.

둘째, iOS는 폐쇄된 마켓시장을 사용함에 따라 어플리케이션의 안전성은 검증되어있다. 또한, 다양한 보안기술로 어느정도 대책을 마련해두었지만, 무선 인터넷 Wi-Fi가 취약하기 때문에 최근 발견된 몇 가지 보안 취약점이 분명히 존재한다. 좀비 프로그램 침투로 인한 개인정보 유출이나 분산서비스거부 공격에 취약한 점이 그것이다.

접근하긴 어렵지만 침입에 성공하기 시작하면, iOS는 백신이나 감지어플리케이션을 승인하지 않기 때문에 잠재적인 위험요소가 충분하다. 따라서 개인 스스로의 보안유지를 강요함으로 끝내는 것이 아니라, 이에 대응할 수 있는 어플리케이션을 허가하거나, 내부데이터의 접근 시에는 사용자의 의사를 물어보게 되는 일종의 인증서와 같은 시스템의 구축이 필요하다.

4. 결론

스마트폰의 활용이 높아짐에 따라 서비스 환경 또한 증가하고 있다. 따라서 이러한 보안 위협에 안전하게 대응하기 위해 정부 및 업체에서 대응책을 마련하고는 있지만, 보다 효율적으로 규격화된 보안기술과 대책을 마련하는 것이 필요하다. 뿐만 아니라 사용자 스스로의 보안 의식을 높임으로서 개인정보의 보관에 주의함으로써 정보의 접근을 보다 막을 수 있게 노력해야 한다.

참고문헌

[1] 박성준, “안드로이드 기반 자바 어플리케이션 보안 취약성 개선”, 한국정보처리학회 2010년 춘계 학술발표 논문집 vol.17, No.1, pp.812-815, 2010. 4

[2] 최은영, “스마트폰 보안 강화를 위한 방안 연구”, 한국인터넷정보학회 2010년 학술발표대회, pp. 781 -785, 2010. 6.

[3] Dave Mark, Jeff LaMarche, “시작하세요! 아이폰3프로그래밍”, 위키북스, 2009.