화이트리스트를 이용한 안드로이드 앱 관리 방안

지경배*, 임형민*, 김필중*, 전문석*
*숭실대학교 컴퓨터학과
e-mail:znj1211@gmail.com

The Method for Managing Apps of Android Systems Using White List.

Gyeong-Bae Jee*, Hyung-Min Lim*, Pill-Jung Kim*, Mun-Suk Jyun*
*Dept of Computer Science, Soong-Sil University

요 약

많은 사용자 들이 스마트폰을 사용하고 있으며 다양한 앱을 국.내외 앱 스토어를 통해 다운로드하여 사용하고 있다. 앱 스토어를 이용하여 배포되는 앱들은 개별 앱 스토어의 검증 체계를 통해 검증을 받고 있으나, 그 방법이 공통적이지 않다. 심지어 앱 스토어가 아닌 다른 방법을 통하여 앱을 설치·사용하고 있어, 다양한 악성 앱으로 인한 위협에 노출되어 있다. 본 논문에서는 검증된 앱을 화이트리스트에 등록, 관리하여 사용자들에게 검증된 앱을 설치·사용하게 하기 위한 방법을 제시한다.

1. 서론

최근 스마트폰 시장이 빠르게 확산되고 있다. 정부와 기업에서는 업무 효율을 향상시키기 위해 스마트폰을 이용하여 업무를 처리할 수 있도록 많은 앱을 만들고 활용하고 있다. 그러나 스마트폰에 기업의 비밀문서와 개인정보가 저장 및 이용되고 있으며, 안전하지 않은 앱으로 인해 많은 위험에 노출되어 있다. 특히 안드로이드의 경우 검증된 앱 스토어가 아닌 다른 경로를 통해 apk파일만 다운로드 하면 설치가 가능하며, 각 앱이 고유의 저장 공간이 아닌 같은 저장 공간을 사용함으로써 악성 앱에 대한 위험성이 크다고 할 수 있다.

PC 상에서의 백신은 악성 코드나 프로그램을 패턴에 따라 분류하여 검색, 치료를 제공함으로써 악성코드로 인한 피해를 방지하고 있으나, 모바일 백신 프로그램은 스마트폰 OS의 특성상 모든 악성 앱을 실시간으로 검색하여 삭제하는 기능을 제공하지 못하고 있다. 따라서, 스마트폰에서의 안전한 앱을 사전에 검증하여 이를 관리함으로써 안전한 앱만을 설치하도록 유도하는 방법 및 절차가 필요한 시점이다.

본 논문의 2장에서는 악성 앱의 위험과 국내 앱 스토어의 동향에 대해 설명하고, 3장에서는 본 논문에서 제안하는 방안을 설명한다. 그리고 4장에서는 결론과 향후 연구 과제에 대한 설명으로 구성하였다.

2. 관련동향

본 장에서는 악성 앱의 위험성과 국내 앱 스토어의 동향에 대해 설명한다.

2.1. 악성 앱 관련 연구

많은 사용자들이 스마트폰에 개인정보를 저장하고 있으며, 또한 사용하고 있다. 그리고 기업의 경우 업무를 처리함에 있어 사용되는 정보들을 스마트폰이 가지고 있게 된다. 결국 악성 앱이 설치되어 스마트폰 안에 있는 개인정보 및 기업의 정보가 노출 될 수 있는 위험이 존재한다.

그리고 스마트폰의 경우 일반 PC가 악성코드에 감염되어 좀비 PC가 되는 것과 같이 악성 앱에 의해 좀비폰이 되어 의도하지 않게 서버 공격에 이용될 수도 있다.

현재 국내 사용자가 많이 사용하는 앱스토어인 구글 플레이, T스토어, Olleh 마켓, U+앱마켓, 삼성앱스 등에서 모바일 앱을 다운로드 받아 설치·사용하고 있다. 이런 앱 스토어에선 자체적인 검증 체계가 존재하여, 검증된 앱만을 배포하고 있으나, 각각의 앱 스토어별로 다른 검증체계를 가지고 있으며, 검증을 거친 앱 중에서도 악성코드가 포함되기도 한다. 특히 안드로이드 OS를 설치한 단말의 앱 설치는 앱 스토어를 이용하지 않고, apk파일만 있으면 쉽게 가능하다. 많은 사용자들이 검증되지 않은 apk파일을 인터넷을 통해 다운받아 사용하고 있는 문제점이 존재하며, 이를 통해 많은 악성 앱이 전파되고 있다.

2.2. 앱스토어 검증체계

국내 앱스토어인 T스토어, Olleh 마켓, U+앱마켓, 삼성앱스는 모바일 앱 등록 시 검증을 수행하나, 구글 플레이의 경우 사후 검증을 통해 앱을 검증한다.

국내 앱 스토어를 이용하여 앱 배포 시 <표 1>의 검증기준과 <표 2>에 따른 사전 검증을 거친 후 앱스토어를 통해 배포된다.

<표 1> 국내 앱스토어 검증기준

마켓명	검증기준
T스토어	유해성, 단말동작 등 5가지 대 분류 검증
Olleh 마켓	바이러스, 유해 코드 등 7가지 대 분류 검증
U+ 마켓	기능, 정책 등 4가지 대 분류 검증
삼성 앱스	기능, 바이러스, 정책 등 9가지 대 분류 검증

<표 2> 국내 앱스토어 검증체계

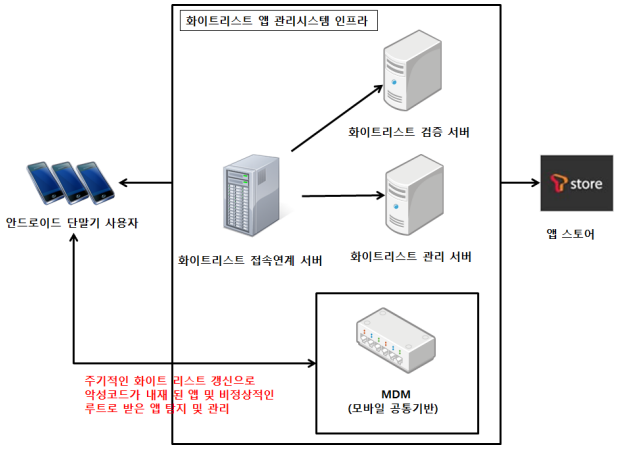
마켓명	검증항목
T스토어	①소스코드 검사와 커버리지 검사 수행 ②SKT 정책 위반 확인 ③단말기 호환 테스트 ④기능 수동 검사 ⑤운영 관리자 최종 판단
Olleh 마켓	①정책/유해성 검증 ②기능 검증 ③UI 검증 ④네트워크 검증 ⑤보안 검증 ⑥과금 검증
U+ 마켓	①개발자가 코드 검증 툴을 이용하여 소스 검증/테스트 커버리지 검증 ②리포트 결과 파일 등록 ③리포트 파일을 이용하여 심사
삼성 앱스	①악의적인 기능 확인 ②내용 심사 ③기능 및 호환성 검사 ④승인 여부 최종 결정

3. 제안내용

악성 앱의 설치 및 실행을 방지하기 위하여 이미 앱 스토어에서 검증된 앱이라도 공통적인 검증 체계를 거쳐서 그 결과를 화이트리스트로 저장 및 관리하여 사용자로 하여금 화이트리스트에 있는 앱만 설치되게 한다. 그리고 위변조 및 비정상적인 경로로 받은 앱의 경우 실행 시 화이트리스트에 있는지 여부를 확인하여 실행이 되지 않도록 관리한다.

3.1. 제안하는 시스템의 전체 구성

제안하는 시스템은 (그림 1)과 같이 구성된다. 제안시스템은 화이트리스트 접속연계 서버와 화이트리스트 관리 서버 등으로 구성되며 아래 <표 3>과 같은 기능을 수행한다. 추가적으로 MDM(Mobile Device Management)은 해시비교를 통해 등록된 앱과 사용자의 안드로이드 시스템에서 설치 및 사용하고 있는 앱이 일치하는지 확인하며, 만약 일치하지 않는 경우, 앱의 삭제를 사용자에게 권고하는 역할을 수행한다.



(그림 1) 제안 시스템 구성도

<표 3> 구성 요소 기능

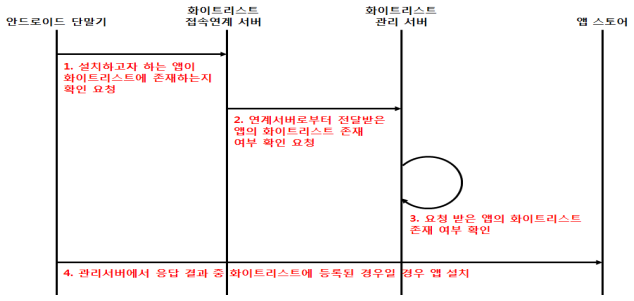
항 목	기 능
화이트리스트 접속연계 서버	화이트리스트 운영을 위해 관련기관 연계 기능을 제공하는 서버
화이트리스트 관리 서버	화이트리스트 관리 및 등록, 앱 정보 저장을 위한 서버
화이트리스트 검증 서버	화이트리스트 검증 및 악성코드 검출을 위한 서버

3.2. 제안하는 시스템의 기능 별 프로세스

제안하는 시스템은 앱의 설치와 등록 그리고 관리의 총 세 가지 기능을 가지고 있다. 아래에서 각각의 프로세스를 보다 자세하게 설명한다.

3.2.1. 앱 설치 프로세스

앱 설치 프로세스는 앱 설치 시 설치 될 앱이 화이트리스트에 존재하는지 확인을 하는 프로세스이다.



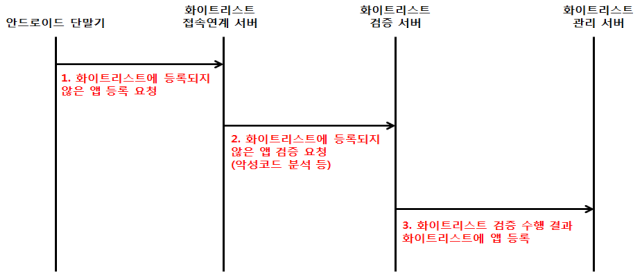
(그림 2) 앱 설치 프로세스

(그림 2)에서 보듯이 화이트리스트에 존재할 경우에만 앱이 설치되도록 한다. 그렇지 않은 경우는 아래 3.2.2의 앱 등록 프로세스를 완료하여야 앱을 설치 할 수 있다.

3.2.2. 앱 등록 프로세스

앱 등록 프로세스는 앱을 화이트리스트에 등록하는 프로세스를 말한다. (그림 3)에서는 보다 명확한 프로세스를

볼 수 있다. 만약 앱이 화이트리스트에 등록되어 있지 않다면, 사용자는 화이트리스트에 등록요청을 할 수 있다. 이 경우 서버에서는 요청을 받아들여 미리 정해진 규칙에 따라 충분한 안전 검증을 수행하여 화이트리스트에 그 내용을 추가한다.

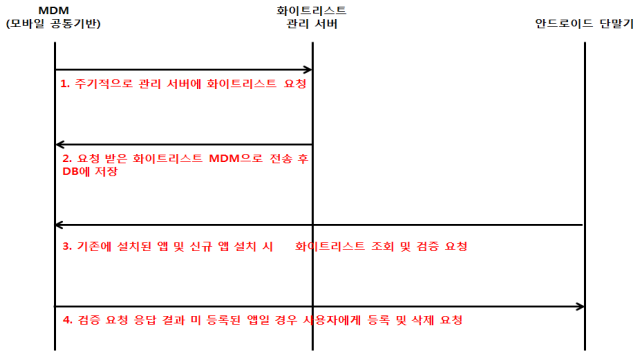


(그림 3) 앱 등록 프로세스

3.2.3. 앱 관리 프로세스

앱 관리 프로세스는 화이트리스트에 등록된 앱과 사용자의 안드로이드 시스템에 설치된 앱이 일치하는 지를 주기적으로 검증하는 프로세스를 말한다.

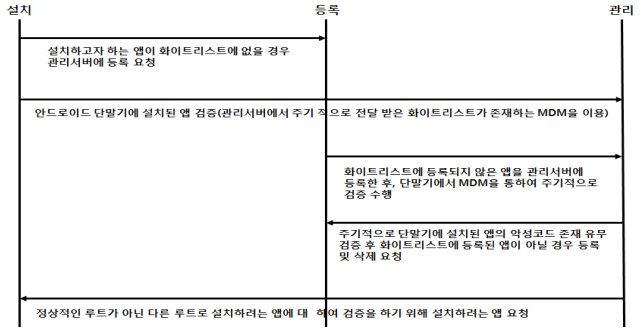
(그림 4)에서 보면 앱 관리 프로세스는 앱에 대한 주기적인 검증을 수행하며, 화이트리스트에 없는 앱인 경우 앱 등록 또는 삭제 요청을 사용자에게 제안한다.



(그림 4) 앱 관리 프로세스

3.3. 제안하는 시스템의 프로세스 흐름도

제안 하는 시스템의 앱 설치·등록·관리라는 세 기능별 흐름 및 운영 절차는 아래 (그림 5)와 같다.



(그림 5) 프로세스간 흐름도

4. 결론 및 향후 연구 과제

제안한 모바일 앱 화이트리스트 관리시스템을 사용하게 되면, 앱스토어 고유의 앱 검증 체계를 허용하면서 사후에 통합적인 검증을 수행하게 됨으로써 이중 검증 효과뿐만 아니라 기존에 일관적이지 못했던 검증 체계에 일관성을 부여 할 수 있게 된다. 그리고 화이트리스트 관리서버에 등록되지 않은 앱은 사용을 불허하기 때문에 악성 앱이 사용되는 것을 방지할 수 있으며, 앱의 설치부터 등록까지 위에서 제안한 절차대로 처리하기 때문에 악성 앱이 설치될 위협 자체를 원천적으로 방지할 수 있다.

<표 4> 제안시스템의 기능 비교

기능	기존 시스템	제안 시스템
앱 설치 및 사용	가능	가능
사용의 편의성	편리	보통
위·변조된 앱의 설치 가능성	부분 가능	불가능
설치된 앱의 위변조 가능성	가능	불가능
설치 및 사용 가능한 앱 관리 기능	불가능	가능

<표 4>에서 보듯이 기존의 앱 검증 시스템에서 제공되는 기능을 제안하는 시스템이 모두 포함하고 있으며 그 외에 위·변조된 앱의 설치 가능성을 보다 확실하게 방지하고 있으며, 설치된 앱의 위변조 가능성은 원천적으로 막고 있다. 뿐만 아니라 업무별로 설치 불가능한 앱을 지정하는 등의 관리까지 가능하다. 또한 제안하는 시스템은 서론에서 제기하였던 “위·변조된 앱 설치 가능성과” “설치 후 앱의 위·변조 가능성”의 보안을 위한 두 가지 문제점들을 모두 해결했음을 알 수 있다.

제안하는 시스템은 안드로이드 운영체제를 사용하는 스마트폰에만 우선 적용하였다. 향후에는 아이폰, 윈도우폰, 심미안, 바다 등 좀 더 다양한 운영체제에도 확대 적용할 수 있는 방안에 대한 연구가 필요하다.

참고문헌

[1] 방지호, 하란, 강필용, 김홍근 “전자정부 모바일 앱 보안성 검증체계” 한국통신학회논문지 ‘12-02 Vol.37C No.2

[2] Machigar Ongtang, stephen McLaughlin, William Enck, Patrick McDaniel “Semantically Rich Application-Centric Security in Android” ACSAC ’09 Proceedings of the 2009 Annual Computer Security Applications Conference

[3] Nikhilesh Reddy, Jinseong Jeon, Jeffrey A. Vaughan, Todd Millstein, Jeffrey S. Foster “Application-centric security policies in unmodified Android” UCLA Computer Science Department, Tech. Rep. 110017, Jul. 2011