안드로이드 어플리케이션 신뢰성 검증을 위한 무결성 인증 방식

최진성, 최옥경, 예홍진
아주대학교 대학원 지식정보보안학과
e-mail : popsae@ajou.ac.kr, okchoi@ajou.ac.kr, hjyeh@ajou.ac.kr

Authentication Method of Integrity for trust of Android Application

Jinsung Choi, Okkyung Choi, Hongjin Yeh
Dept. of Knowledge Information Security, Graduate School of Ajou University

요 약

현재 전 세계의 스마트폰 시장은 아이폰과 안드로이드폰의 구도로 되어 있다고 해도 과언이 아니다. 아이폰의 앱 스토어에 어플리케이션을 올리기 위해서는 애플의 검증을 거쳐야 가능하지만, 안드로이드의 안드로이드마켓은 구글의 검증 없이 누구나 자유롭게 올릴 수 있다. 그렇기 때문에 스마트폰의 보안문제가 대두되고 있는 요즘, 안드로이드마켓에서 내려 받는 어플리케이션에 대한 신뢰성이 떨어지는 것이 사실이다. 본 논문에서는 이러한 안드로이드 어플리케이션의 신뢰성 검증을 위한 인증 어플리케이션을 제안함으로써 사용자가 악의적으로 변조된 어플리케이션에 대한 대응이 가능하도록 하고자 한다. 마지막으로 테스트를 통하여 본 연구의 효율성 및 타당성을 입증하였다.

1. 서론

스마트폰은 주머니 속의 휴대용 컴퓨터라고 할 수 있을 만큼 언제 어디서나 인터넷에 접근이 가능하며, 각종 어플리케이션을 이용하여 다양한 서비스를 제공받을 수 있다. 그러나 지난 해 모바일 악성코드가 전년인 2010 년에 비해 155% 증가하였으며 또 운영체제 중에선 안드로이드가 악성코드 공격에 가장 취약했던 것으로 드러났다. 이와 같이 기존 PC 에서 악성코드나 바이러스 등을 심어 공격하는 방식이 최근에는 스마트폰의 어플리케이션에 악의적인 코드를 삽입하여 스마트폰을 공격하거나 폰에 저장되어 있는 개인정보 등을 침해하는 방식으로 전환되고 있다.

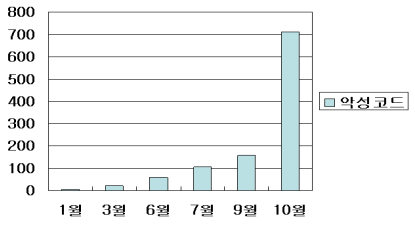
현재 애플에서는 아이폰에서 구동하는 어플리케이션을 안전하게 소비자들에게 제공하기 위해 앱 스토어에 등록하기 전에 모든 어플리케이션을 검사한다. 이와 반대로 안드로이드 어플리케이션을 거래하는 안드로이드마켓은 개방형 마켓으로써 누구나 자유롭게 어플리케이션을 올릴 수 있다. 그렇기 때문에 제대로 검증이 이루어지지 않은 어플리케이션도 다수 마켓에 존재하는 것이 현실이다. 지난해 전체 악성코드 중 46.7%가 안드로이드 운영체제에서 발견된 것을 보면 그 심각성은 날로 커져가고 있는 것을 볼 수 있다.

이에 본 논문에서는 본 논문에서는 이러한 안드로이드 어플리케이션의 신뢰성 검증을 위한 인증 어플리케이션을 제안함으로써 사용자가 악의적으로 변조된 어플리케이션에 대한 대응이 가능하도록 하고자 한다. 제안방식은 해쉬 함수를 이용한 무결성 검증방법으로써 일방향 함수의 특성상 같은 해쉬 값을 가진 다른 어플리케이션을 작성하는 것이 어렵기 때문에 어플리케이션에 악의적인 코드가 삽입되었다면 순수한 어플리케이션의 해쉬 값과 다르게 나온다는 점을 이용하였다.

본 연구는 지식경제부 및 한국인터넷진흥원의 “고용계약형 지식정보보안 석사과정 지원사업”의 연구결과로 수행되었음.

2. 관련 연구

2011 년 중반까지 발견된 악성코드의 유형으로는 1)위치 정보나 단말기 정보 등 개인정보를 유출하는 악성코드, 2)원격 조종 기능과 이를 이용한 통화 SMS 발송으로 무단 과금하는 기능, 3)사용자 동의 없이 root 권한을 강제로 얻는 기능 등이 복합돼 있는 것으로 드러났다. 악성코드를 퍼뜨리는 방법도 단순히 어플리케이션 안에 악성코드를 숨겨놓는 방법뿐만 아니라 pc 에서 발견되는 dropper 처럼 정상적으로 작동하는 어플리케이션으로 보이나 실행되면 내부에서 악성코드를 설치하는 방법으로도 진화했으며, Wi-Fi 나 무선랜, 또는 QR 코드를 통한 유포 등, 악성코드 유포 방법이 점점 지능화되고 있다[1].

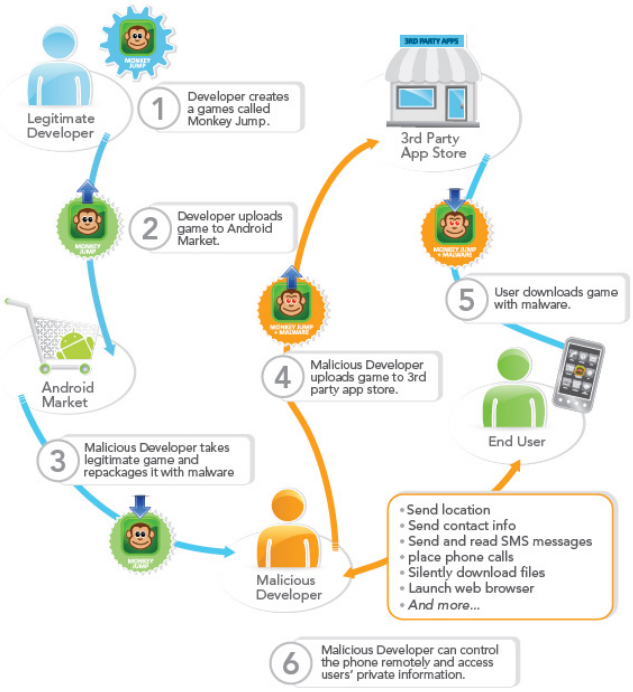


[그림 1] 안드로이드 악성코드 증가 추세

안철수 연구소와 Juniper Network 보고서에 따르면 안드로이드 악성코드가 기하급수적으로 증가하는 추세이며, Lookout Security 는 전 세계 안드로이드폰의 약 30%가 이미 감염됐을 수 있다고 분석하였다[2,3].

현재 안드로이드의 보안 취약점에 대응하기 위해 악성코드의 존재나 활동을 감지하는 서명식별방법(Signature-based detection)을 이용한 '알약 안드로이드', 'Kaspersky Mobile security', 'Norton Security for Android' 어플리케이션들이 있으며, 서명식별방법과 더불어 안드로이드 플랫폼의 특성에 맞춘 행위기반탐지를 모두 지원하는 'V3 Mobile' 어플리케이션이 배포 중이다. 하지만, 급격하게 증가하고 지능화되는 악성코드들을 모두 찾아내어 업데이트하기 어려울 것이다[4].

앞에서 살펴본 바와 같이 현재 배포되고 있는 보안 솔루션은 행위 기반이나 시그니처 기반으로 악성코드의 존재를 또는 활동을 감지하고 있다. 보안 솔루션을 가장하여 리패키징(repackaging)된 악성 어플리케이션도 종종 발견되는데 이 기법은 사용자들에게 이미 잘 알려진 어플리케이션에 악성코드를 담아서 배포하는 방법이다. 사용자들은 기존의 어플리케이션과의 차이점을 거의 느낄 수가 없기 때문에 속수무책으로 감염되고 있는 실정이다[5].



[그림 2] 리패키징되는 과정[5]

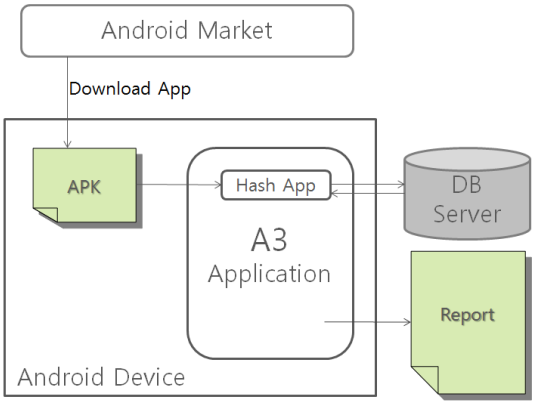
3. 설계 방안 및 구현

3.1 설계 방안

본 연구에서는 기존의 방식과 다른 방법으로 악성코드의 위협으로부터 벗어나고자 한다. 본 연구에서 제안하는 방법은 신뢰할 수 있는 어플리케이션 개발자로부터 원본 APK 파일을 받아 저장된 해쉬 값을 통해 APK 파일의 신뢰성을 검증하고 악성코드가 삽입되어 있거나 변조된 리패키징 어플리케이션을 걸러내고자 한다.

3.2 구현

해쉬를 이용한 어플리케이션 무결성 검증을 위하여 인증 어플리케이션을 설계하였다. AA(Application for Authentication)는 안드로이드 기기에 설치되어 있는 어플리케이션의 목록을 불러와 사용자가 검증을 원하는 어플리케이션을 목록에서 선택할 수 있도록 한다. 선택된 어플리케이션의 해쉬 과정으로 얻은 해쉬 값은 서버로 보내져 서버의 데이터베이스에 저장되어 있는 해쉬 값과 비교하여 사용자가 선택한 어플리케이션의 무결성을 검증하게 된다. 데이터베이스에는 신뢰할 수 있는 개발자로부터 등록 받은 순수한 어플리케이션의 해쉬 값이 미리 저장되어있다.



[그림 3] AA 시스템 구조

[그림 3]은 제안 방식의 시스템 구조로 똑같은 어플리케이션을 두 개를 만들어서 하나의 어플리케이션에만 임의의 코드를 삽입하였다. 단, 삽입하는 코드는 최소한으로 하되, 정상적인 어플리케이션처럼 동작하도록 하였다. 서버에는 정상적인 어플리케이션의 해쉬 값을 미리 저장해 놓고, 안드로이드 기기에는 변조된 어플리케이션을 설치하였다. 시나리오 대로 변조된 어플리케이션을 실행하기 전에 AA를 실행하여 변조된 어플리케이션 검사를 하였다. AA는 서버의 데이터베이스의 해쉬 값과 비교하여 변조되었음을 감지하였고, 선택된 어플리케이션이 무결성 측면에서 유효하지 않음을 검증하였다.

[그림 4] AA 구현 결과 화면

ETRI(Electronics and Telecommunications Research Institute)에서 발행한 전자통신동향분석에서도 개방형 어플리케이션 마켓의 보안 필요성에 대해 언급하면서 마켓에 어플리케이션을 등록하기 전에 검증 센터에서 보안성 검사가 필요하다고 하고 있다[6]. 하지만 이 방법은 마켓에 등록되는 어플리케이션을 검증할 뿐 마켓 이외에도 다양한 방법으로 어플리케이션을 설치하는 안드로이드 유저에게는 검증이 어렵다.

따라서 본 연구에서는 악성코드가 삽입된 리패키징 어플리케이션을 걸러내는 어플리케이션을 구현하고 테스트하여 제안하는 방식의 효율성과 타당성을 입증하였다.

4. 결론 및 향후 연구

안드로이드 마켓과 제 3 의 마켓에서 유통되는 안드로이드 어플리케이션들이 검증되지 않은 채로 유통되고 있다. 급격히 늘어나는 리패키징 공격으로 2011 년 한해 동안 악성코드로 인해 감염된 안드로이드 기기는 30,000~120,000 대로, 안드로이드 사용자의 피해액은 백만 달러에 이를 것으로 추정하며, 앞으로의 악성코드 트랜드는 리패키징 공격이 될 것이라고 한다[7,8]. 현재 배포되고 있는 보안 어플리케이션들을 보완하기 위해 동적 분석 방법과 정적 분석 방법을 모두 이용한 악성코드 식별 연구가 있었다[9,10]. 하지만 이러한 방법들은 커널(kernel)을 수정해야만 하는 한계점이 있다. 그렇기 때문에 본 연구에서는 해쉬 함수를 이용한 간단한 방법으로 무결성을 검사하는 어플리케이션을 만들고 테스트하였다. 하지만 사용자가 어떻게 무결성 검사 어플리케이션에 대한 신뢰를 할 것이며, 서버 데이터베이스에 저장되는 원본 어플리케이션의 해쉬 값은 믿을 수 있는지에 대한 문제가 남아있다. 간단한 해쉬 값 비교를 통해 무결성을 검증할 수 있었지만, 누구나 신뢰할 수 있는 인증기관(CA)에서 어플리케이션을 검증하고 해쉬 값을 관리해 준다면 신뢰도 문제도 해결되리라 생각된다. 무결성을 검증하는 방법이 악성코드를 완전히 차단할 수는 없으나, 급격히 늘어나는 리패키징 공격에 상당히 효과적일 것이라고 기대한다.

참고문헌

[1] Timothy Vidas, Daniel Votipka, Nicolas Christin : “All Your Droid Are Belong To Us: A Survey of Current Android Attacks”, WOOT’11 5th USENIX Workshop on Offensive Technologies; San Francisco, California, August 8-9, (2011)

[2] Juniper Global Threat Center; “Mobile Malware Development Continues To Rise, Android Leads The Way”, November 15, (2011),

[3] Juniper Network; “Malicious Mobile Threats Report 2010/2011”, May, (2011)

[4] 박성현, “스마트 보안 솔루션”, ㈜ A3 Security, February 7, (2011)

[5] Lookout Mobile Security; “Lookout Mobile Threat Report”, August, (2011)

[6] 강동호, 한진희, 이윤경, 조영섭, 한승완, 김정녀, 조현숙, “스마트폰 보안 위협 및 대응 기술”, 전자통신동향분석 25 권 3 호, June, (2010)

[7] Lookout Mobile Security; “Lookout Unveils 2012 Mobile Threat Predictions : Mobile Pickpocketing, Botnets and Automated Repacking Will Be On the Rise”, December 12, (2011)

[8] Bernadette Caraig, Mark Balanza, Kervin Alintanahin, Oscar Abendan, Julius Dizon; “DoridDreamLight Lurks Behind Legitimate Android Apps”, Malicious and Unwanted Software9MALWARE), 2011 6th International Conference on, October, (2011)

[9] Thomas Blasing, Leonid Batyuk, Aubrey-Derrick Schmidt, Seyit Ahmet Camtepe, Sahin Albayrak : “An Android Application Sandbox System for Suspicious Software Detection”, Malicious and Unwanted Software (MALWARE), 2010 5th International Conference on; October, (2010)

[10] 심원태, 김종명, 류재철, 노봉남, “안드로이드 앱 악성행위 탐지를 위한 분석 기법 연구”, 情報保護學會論文誌, 第21卷 第1號, February, (2011)