스마트폰 어플리케이션 오픈마켓의 새로운 검증모델 제안

이기홍*, 민재원*, 조신영**, 박민우**, 정태명*
*성균관대학교 컴퓨터공학과
**성균관대학교 전자전기컴퓨터공학과
e-mail : wlcraze@hanmail.net, jaewonm@live.co.kr,
{sycho, tmchung}@imtl.skku.ac.kr, tmchung@ece.skku.ac.kr

A New Model for Verifying Smartphone Applications in the Open Market

Ki-hong Lee*, Jae-won Min*, Shin-Young Cho**, Min-Woo Park**, Tai-Myoung Chung*
*Dept. of Computer Engineering, Sung-kyun-kwan University
**School of Information Communication Engineering, Sungkyunkwan Univ.

요 약

스마트폰 어플리케이션 오픈마켓은 누구나 자유롭게 어플리케이션을 개발하여 등록하고, 사용자가 원하는 어플리케이션을 구매하여 사용할 수 있다. 이러한 시스템은 어플리케이션 시장을 활성화시킨 반면 많은 보안상의 위협을 야기한다. 이러한 문제점을 해결하기 위해 여러 방안이 제시되고 있는데, 본 논문에서는 어플리케이션을 등록할 때의 검증절차를 보다 효율적으로 개선하기 위한 보안등급 세분화를 연구하였다. 개발자가 어플리케이션을 마켓에 등록 시 적절한 검증 등급을 설정하여 검증시스템의 효율을 높이고, 마켓에서 등록된 어플리케이션에 검증된 보안 등급 정보를 제공함으로써 사용자에게 구매할 어플리케이션의 안정성을 판단할 근거를 제공해 준다.

1. 서론

최근 스마트폰 사용자가 급속도로 증가하고 있다. 국내에서는 2009 년 11 월 KT 의 아이폰 보급을 시작으로 스마트폰의 경쟁이 심화되었으며, SKT 과 통합 LGT 도 안드로이드가 탑재된 스마트폰을 속속히 출시하고 있다. SKT 는 스마트폰 가입자가 200 만명을 넘어섰으며[6], KT 의 경우 아이폰 가입자가 100 만명을 돌파했다고 보도한 바 있다[3]. 스마트폰이 주목을 받는 가장 대표적인 이유는 오픈마켓에서 제공하는 방대한 양의 어플리케이션 때문이다. 사용자는 오픈마켓이라는 사이버 공간을 통하여 필요한 어플리케이션을 구매하고, 때로는 다른 사용자가 필요로 하는 어플리케이션을 직접 개발하여 판매하기도 한다. 현재 애플의 앱스토어에는 약 25 만개, 구글의 안드로이드 마켓은 12 만개 이상의 어플리케이션이 등록되어 있다. 하지만 방대한 양으로 쏟아져 나오는 어플리케이션 중에는 문제를 야기시키는 어플리케이션 또한 상당 수 존재하며, 이러한 어플리케이션들이 사용자들에게 확산되면서 개인정보가 유출되는 등의 보안상 문제가 끊임없이 발생하고 있다. 애플은 이러한 보안 위협을 사전에 막기 위해 강력한 검증 시스템을 통해 앱스토어를 폐쇄적으로 운영하고 있으며 특정 어플리케이션은 등록을 거부하는 정책을 취하고 있다. 반면 구글의 안드로이드 마켓은 개발자에게 전자서명과 해당 어플리케이션이 사용하는 자원의 목록을 명시하기를 요구하고, 이후에 발생하는 문제점에 대한 책임은 사용자에게 떠넘기고 있다. 이러한 각각의 방식에는 장단점이 존재하므로 이를 적절히 절충하여 개선한다면 보다 나은 검증 시스템을 구축할 수 있을 것이다. 본 논문에서는 기존의 획일적인 검증 방식과 대조되는 세분화된 검증 등급을 도입하여 보다 유연하고 효율적인 어플리케이션 검증 모델을 제안하고자 한다.

2. 기존 앱 검증 시스템

2.1. 애플 앱스토어

애플 앱스토어는 폐쇄적인 오픈마켓의 모델로 대표될 수 있는데, 40 명 이상의 reviewer 를 구성하여 최소 2 명 이상에게 어플리케이션을 학습시켜서 모두 승인을 해야 등록이 이루어진다. 또한, 앱스토어 책임자들은 매주 1 회 Executive Review Board 를 열어 검증 절차와 정책에 관한 토의가 이루어진다.

앱스토어의 등록 절차는 <그림 1>에 도식화 하였다. 승인 기준은 매우 까다로운 편에 속하는데 개인정보를 침해하거나 결함이 있으면 안되며, 승인 받지 않은 프로토콜, API 의 사용은 금지된다. 특히 UI 가이드에 엄격한 기준을 적용하고 있으며, 기술적인 면뿐만

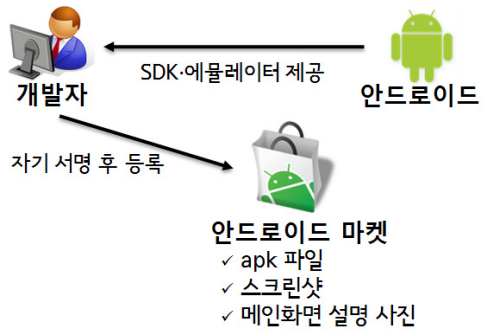
아니라 어플리케이션의 내용(contents)도 검증 대상이 되어 성인물, 폭력물 등 회사 정책과 맞지 않는 어플리케이션은 승인이 거부된다. 이러한 과정을 통과해야만 앱스토어에 등록될 수 있기 때문에 다른 오픈마켓보다 보안상 안전하다고 할 수 있다.

등록은 대략 14 일 이내에 처리되는데, 일관되지 않은 검증 기준을 적용하여 비난을 받는 사례가 종종 발생하고 있다. 폐쇄성과 일관되지 않은 앱 등록으로 인한 마찰은 Adobe 사의 Flash 지원 사례와 국내에서 벅스, 소리바다, 엠넷 등 음원서비스업체의 모바일 어플리케이션 삭제 사례 등이 있다.

<그림 1> 애플 앱스토어의 어플리케이션 등록 절차

2.2. 안드로이드 마켓

안드로이드 마켓의 경우 개발자의 서명과 어플리케이션이 사용하는 자원의 접근 권한만을 확인하고 보안과 관련된 검증은 추가적으로 거치지 않고 있으며, 어플리케이션의 구입과 설치에 대한 책임은 전적으로 사용자에게 있다. 설치 시에 어플리케이션 메니저가 디바이스 특정 자원의 사용에 대한 권한 허가를 요청하고, 사용자는 이를 모두 허용을 하거나 설치를 거부할 수 있다. 설치 이후에는 권한 허용을 취소할 수 있는 방법이 없기 때문에 이러한 시스템은 사용자의 행동방식에 따라 심각한 보안상 문제가 발생할 소지가 있다[4]. 또한 공식 마켓을 제외한 제 3 의 오픈마켓에서도 구매가 가능하기 때문에 잠재적인 위험성은 훨씬 크다. <그림 2>는 구글 안드로이드 마켓의 등록 절차를 도식화한 것이다.



<그림 2> 안드로이드 마켓의 어플리케이션 등록 절차

<표 1>은 현재 가장 많은 양의 어플리케이션이 등록되어 있는 두 오픈 마켓의 장· 단점을 비교한 것이다.

<표 1> 안드로이드마켓과 앱스토어의 장단점 비교

	안드로이드 마켓	앱스토어
장점	짧은 등록대기 기간	신뢰성 있는 검증
단점	보안 검증 절차 미비	검증과정 지연

3. 새로운 검증 모델

스마트폰과 오픈마켓의 이용자 수가 급격히 늘어가고 있는 현재 상황에서, 마켓에 올라오는 어플리케이션이 문제가 있을 경우 그 피해의 파급효과는 심각할 수 있다. 하지만 일반 스마트폰 사용자의 경우 보안 관련지식이 부족하고 보안 의식이 낮은 경우가 많으므로, 적절한 검증절차 없이 등록된 어플리케이션이 악성코드를 포함하고 있는 경우 개인정보 유출과 같은 사회적으로 심각한 문제가 발생하게 된다. 또 다른 문제점으로는 앞으로 오픈마켓에 대한 관심과 수요가 늘어남에 따라 더 많은 양의 어플리케이션들이 쏟아져 나올 것이며, 따라서 현재 검증 시스템으로는 일정한 검증 기간을 보장하기가 어렵다.

앞으로의 바람직한 오픈마켓 모델은 문제의 소지가 있는 어플리케이션의 등록을 최대한 억제하여 안정성을 보장하고, 수많은 등록 요청을 효율적으로 처리할 수 있는 검증 시스템이 도입되어야 한다.

3.1. 보안 등급 세분화

본 논문에서 제안하는 보안검증 모델은 3 단계의 보안등급을 적용하여 어플리케이션의 보안 상태를 <표 2>와 같이 Unstable, Secure, Stable 로 구분한다.

<표 2> 보안등급별 적용 검증 절차

등급 명칭	보안 상태	적용 검증 절차
Unstable	하	개발자 서명 값 확인 static binary analysis static source analysis
Stable	중	(이전 검증절차 포함) dynamic binary analysis dynamic source analysis
Secure	상	(이전 검증 절차 포함) Program monitoring 암호화 기능 검사 컨텐츠 검사

3.1.1. Unstable 등급

Unstable 등급 검증 과정에서는 개발자의 서명을 확인한 후 정적(static) 분석을 수행한다. 정적 분석은 소스 코드(source code) 또는 머신 코드(machine code)를 실행하지 않고 프로그램 코드 상에서 분석하는 방법이다. 컴파일러가 문법을 검사하거나 코드를 최적화하는 것이 정적 분석의 한 예가 된다. 소스 코드(source code) 레벨에서는 함수, 변수 등을 검사하고 바이너리 코드(binary code) 레벨에서는 목적코드(object code) 나 실행 코드(executable code)로 저장되어있는 머신 코드를 분석한다. 가상 머신에서 실행되는 중간 코드인 바이트 코드(byte code)를 분석하는 것이 binary analysis 에 해당한다. 이러한 분석법으로 메모리 주소, 레지스터, 명령어 등을 분석하여 문제점을 찾아낼 수 있다[5].

3.1.2. Stable 등급

Stable 등급 검증 과정에서는 Unstable 등급 과정의 검증과정을 포함하여 코드를 동적(dynamic)으로 검사한다. 동적 분석은 어플리케이션을 실행하면서 분석하는 방법으로 실행 도중에 사용되는 실제 데이터를 분석하기 때문에 정적 분석 방법보다 정확한 검증을 할 수 있다. 검증 절차는 동적 분석 도구로 분석 코드(analysis code)를 어플리케이션에 삽입하여 어플리케이션의 일부분으로 실행되면서 성능을 분석하거나 버그를 찾는다. 분석 코드는 분석을 수행하면서 상태에 대한 정보를 로그파일에 저장하고 유지하는 역할을 한다[5].

3.1.3. Secure 등급

Secure 등급 검증 과정에서는 이전 등급 검증을 실시한 후, 추가적으로 일정 기간 동안 run-time program monitoring 을 한다. Program monitor 는 어플리케이션의 control flow 에 끼어들어 데이터를 분석하면서 만약 어플리케이션이 보안정책에 위배되는 행동이 있는지 관찰한다. 또한 암호화 기능을 검사하는 것도 매우 중요한데 개인정보를 암호화하여 통신하는 것은 가장 기본적인 보안행위라 할 수 있다. 여기서는 국제표준 암호화 알고리즘을 제대로 구현했는지를 검사한다. 마지막 과정으로는 콘텐츠에 대한 검사가 이루어지는데 어플리케이션 코드의 보안성 검사도 중요하지만, 가지고 있는 데이터의 내용도 중요하게 다루어져야 하기 때문에 국가의 비공개 정보를 포함하거나 폭력물, 성인물이 포함된 어플리케이션은 등록을 금지한다. 이를 위해서는 오픈 마켓을 운영하는 책임자들이 금지 항목에 대한 명확을 기준을 마련해야 한다[1][2][5].

3.2. 어플리케이션 검증 절차

보안등급이 세분화된 오픈마켓 모델의 어플리케이션 검증 절차는 <그림 3>과 같이 이루어 질 수 있다.

<그림 3> 어플리케이션 검증 절차

먼저 개발자는 어플리케이션 등록 시, 안정성 검증을 받을 보안등급을 선택하여 등록 인증을 요청한다. 오픈마켓의 검증 시스템은 요청된 어플리케이션의 보안등급을 확인하고 해당 검증 절차를 수행하여 승인을 완료하거나 거부한다.

승인이 완료되면 오픈마켓에 등록이 이루어지게 되고 사용자가 마켓에서 구매 시에는 검증 받은 보안등급도 같이 명시되기 때문에, 사용자는 어플리케이션의 종류와 보안 등급을 확인하여 적절한 판단을 내릴 수 있는 객관적 근거를 갖게 된다. <그림 4>는 스마트폰으로 오픈마켓에 접속하여 어플리케이션을 구매하는 화면을 나타낸 것으로 어플리케이션 정보와 함께 보안등급이 표시되어 있다.

반면, 인증이 실패하였을 경우 개발자에게 승인 거부 요인을 통보하고 요청된 어플리케이션을 오픈마켓에 등록하지 않는다.

<그림 4> 오픈마켓 상의 보안등급 확인 예시

3.3. 보안 재평가

오픈마켓에 어플리케이션이 등록된 이후에도, 사용자에 의해 문제점이 제기될 수 있는데, 이때 사용자는 프로그램 상의 문제가 있다고 판단될 경우 재검증을 요청할 수 있다. 어느 수준 이상으로 재검증 요구가 발생하면 오픈마켓의 검증 시스템은 보안상의 문제점이 있다고 판단하고, 한 단계 상위 등급으로 재평가를 실시하여 보다 정확한 진단을 수행한다. 문제점이 명확하게 밝혀지면 해당 어플리케이션에 대한 접근을 막고 개발자에게 통보하여 어플리케이션의 수정을 요구한다.

또한 개발자에 의해서도 재평가 요청이 이루어질 수 있는데, 어플리케이션 등록 이후에도 상위 등급으로 재검증을 요구할 경우 이를 실시한다. 상위 보안등급은 이전 등급의 검증 절차를 모두 포함하고 있으므로 추가적인 검증 절차만 수행하면 된다. 따라서 상위 등급 재검증은 시간이나 비용 면에서 큰 부담없이 보안등급을 재평가할 수 있다.

4. 보안 등급 세분화의 우수성

본 논문에서 제안한 검증모델은 기존의 획일적인 검증 방식과 달리 검증 등급을 세분화하여 절차에 유연성을 제공하므로, 기존 앱 스토어의 검증 절차와 비교해 검증 기간과 비용을 줄일 수 있다. 또한 개발된 어플리케이션의 보안 상태를 가장 잘 알고 있는 사람은 개발자 자신이므로, 개발자에게 보안 등급을 선택할 수 있는 기회를 주면 검증의 효율성을 높이게 되고, 상위 등급으로 인증 받기 위해 보안성을 고려하면서 개발에 임하다 보면 자연스럽게 개발자의 보안 의식을 높이는 효과를 얻을 수 있다.

뿐만 아니라 사용자 입장에서도 어플리케이션의 종류와 승인된 보안등급을 비교· 확인하여 구매를 선택할 수 있으므로 제품의 안정성을 판단할 때 보다 명확하고 객관적인 근거를 제공하게 된다. 또한 어플리케이션이 오픈마켓에 등록되면 평가가 끝나는 것이 아니라 등록 후에도 꾸준히 재평가 되므로 보안 신뢰성이 강화된다.

보안등급이 낮을수록 어플리케이션 검증 절차가 간결해지고 검증 기간이 짧아지므로, 개발자는 개발하는 어플리케이션의 특성에 따라 보안 신뢰성과 검증 기간을 고려해 적절한 보안등급을 선정하여 검증을 요청할 수 있다. 또한 등록 이후 어플리케이션의 평가와 인기에 따라 재검증을 요청 할 수 있기 때문에 안정성에 대한 중요도가 비교적 낮은 베타버전에서는 하위 등급으로 인증을 받아 사용자의 반응을 살펴보고 이후에 정식버전 등록 시 안정된 등급을 요청하는 방식 등의 다차원적인 활용도 가능하다.

5. 결론

본 논문에서는 보안등급을 기반으로 한 스마트폰 어플리케이션 검증 모델을 제안하였다. 검증의 정확도에 따라 보안등급을 나누어, 개발자는 어플리케이션 등록 시 검증 받을 보안등급을 선택하고 검증 시스템은 요구받은 검증절차로 어플리케이션을 평가한다. 승인 후 어플리케이션이 마켓에 등록되면 사용자는 어플리케이션의 보안등급을 참고할 수 있다. 또한 등록 이후에도 개발자나 사용자의 요청에 의해 상위 등급으로 재평가가 이루어 질 수 있다.

기존 검증 절차가 '승인 또는 거부'의 일차원적인 방식인데 비해, 보안등급이 세분화된 검증 모델은 절차에 유연성을 제공하여 검증 기간을 단축하고 검증 효율을 높이며, 사용자에게 보안등급을 명시하여 안정성 평가에 있어 객관적 판단의 기준을 제공한다.

현재까지는 본 논문에서 제안한 검증 시스템이 이론상으로만 연구되어, 보안 등급 세분화에 의해 발생할 수 있는 문제점과 개발자와 사용자의 구체적 행동에 대한 연구가 부족하다. 향후에도 연구를 지속적으로 진행하여 보안등급 별 검증과정을 더욱 세부적으로 설계하고 사용자의 행동을 보다 면밀히 분석하여 현실에 적합한 검증 시스템으로 발전시킬 것이다.

참고문헌

[1] Bauer L., Ligatti J., and Walker D., "Composing Expressive Runtime Security Policies", ACM Transactions on Software Engineering and Methodology, Vol. 18, No.3, Article 9, May. 2009

[2] Desmet L., Joosen W., Massacci F., Naliuka K., Philippaerts P., Piessens F., and Vanoverberghe D., "A Flexible Security Architecture to Support Third-party Applications on Mobile Devices", CSAW'07, Nov. 2007

[3] KT, "아이폰 가입자 100 만, 한국 통신시장을 바꾸다", 홍보센터 보도자료, Sep. 2010

[4] Nauman M., Khan S., and Zhang X., "Apex: Extending Android Permission Model and Enforcement with User-defined Runtime Constraints", ASIACCS'10, Apr. 2010

[5] Nicholas Nethercote, "Dynamic binary analysis and instrumentation", UCAM-CL-TR-606 ISSN 1476-2986, Nov. 2004

[6] SK 텔레콤, "SK 텔레콤, 국내 통신사 최초 스마트폰 가입자 200 만 돌파", 미디어센터 보도자료, Sep. 2010

[7] WISEWIRES, "Apple App store 등록절차 및 검증현황", 와이즈와이어즈 뉴스레터, Sep. 2010