앱스토어 보안정책 동향

배정민[*] · 배유미[**] · 정성재[**] · 장래영[*] · 소우영[*]

[*]한남대학교 · [**](주)스컴씨엔에스

App Store security policy trends

Jung-Min Bae[*] · Yu-Mi Bae[**] · Sung-Jae Jung[**] · Rea-Young Jang[*] · Woo-Young Soh[*]

[*]Hannam University, [**]Sky Computing C&S

E-mail : bjmin86@nate.com, yumidw@hanmail.net, posein@naver.com, rene402@hnu.kr, wsoh@hnu.kr

요 약

스마트기기의 보급이 증가함에 따라 앱스토어 시장이 거대하게 형성되었고, 지금 이 시점에도 하루가 다르게 그 규모가 증가하고 있다. 이에 따라 기업 및 개인의 이익을 위해 스마트기기의 보안을 위협하는 악성앱들이 앱스토어에 심심치 않게 등장하고 있다. 단말기 보안은 국가와 기업, 그리고 많은 대학에서 연구를 통해 다양한 솔루션을 내놓고 있다. 하지만 악성앱이 앱스토어에 등록되지 않도록 어플리케이션 등록단계에서 차단하는 정책적인 접근에 대한 연구와 솔루션에 대해서는 앱스토어를 운영하는 기업에 전적으로 일임하고 있으며, 그 기준도 미흡하여 다양한 문제가 발생하고 있다. 본 연구에서는 현재 앱스토어의 보안정책의 문제점을 분석한 뒤 한계점을 제시한다.

ABSTRACT

Spread of smart devices increases, the App Store market is formed so huge, even at this point, every day the scale is increasing now. As a result, for the benefit of companies and private individuals, malicious apps that threaten the security of smart devices, have appeared occasionally in the App Store. Security of the terminal, has issued various solutions through research at many universities and companies, and country. However, solutions for research and policy approaches that are blocking the procedure to register the application malicious app, so that it is not registered in the App Store, Only company that operates the app store is doing it. And the reference is also insufficient, various problems have occurred. In this study, after analyzing the problem of the security policy of the current App Store, presenting the breaking point.

키워드

앱스토어, 앱스토어 보안, App Store security, App registered security, Security policies

Ⅰ. 서 론

최근 몇 년간 PC에서 스마트기기로의 문화이동은 큰 변화를 가져왔다. 이제는 영화, 음원, 뉴스, 게임, 금융 등의 수많은 분야를 사용자가 이용하기까지 스마트기기를 거치지 않은 것이 없다. 변화에 맞추어 스마트폰, 테블릿PC 등의 스마트기기의 사용자가 급격히 늘면서 어플리케이션의 수요과 공급이 하루가 다르게 치솟고 있다. 이에 따라 앱스토어 시장도 마찬가지로 방대하게 형성되고 있다. 하지만 어플리케이션 및 앱시장의 보안문제점에 대한 해결책은 앱시장의 확장속도를 따라가기 어려운 것으로 보인다.

본 논문에서는 현재 전세계 앱스토어 시장에 대하여 알아보고, 모바일 앱 환경을 위협하는 현황과 원인에 대하여 알아본 뒤, 앱스토어의 어플

리케이션 등록 단계별 문제점을 알아본다. 마지막으로 앞으로의 동향에 대해 분석하고 결론을 맺는다.

II. 모바일 어플리케이션 시장 현황

본 장에서는 앱스토어 시장의 보안 위협을 논하기 전에 전 세계적으로 모바일 앱 시장의 현주소를 먼저 파악하여 위협의 규모를 살펴보고자 한다.

2.1 세계 모바일앱 이용자 수

스마트 기술 환경이 확산되고 이를 기반으로 하는 콘텐츠시장이 확장되면서, 모바일 분야는 이제 세계적으로 큰 흐름으로 자리잡고 있다. 이러한 모바일 중심의 트렌드는 이전의 온라인화에 비해 그 변화 및 확산 속도 측면에서 매우 빠르게 진행되고 있다. 해외 조사기관 Portio Research에서는 올해 상반기에 발간한 'Mobile Application Futures 2013-2017'을 통해, 모바일 어플리케이션 시장에서 나타나는 변화 양상을 소개하고 있다. Portio Research에 따르면 세계 모바일 어플리케이션 이용자 수는 2010년 4억 7백만 명에서 2011년 7억 4천만 명, 2012년 약 12억 명으로 증가하였고 이후에도 연평균 20~60%의 성장률로 지속적인 증가 추세를 보일 것으로 전망했다.[1]

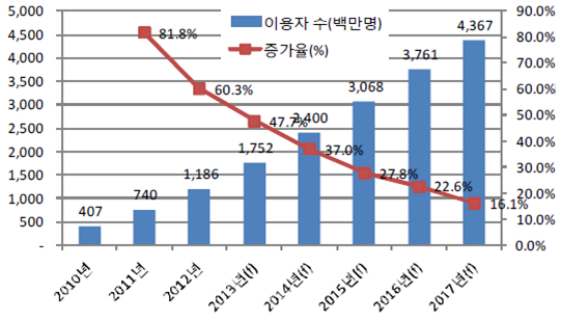

그림 1. 세계 모바일앱 이용자 수

2.2 마켓 시장별 점유율

세계 모바일 어플리케이션(이하 앱) 시장이 꾸준히 성장하고 있다. 글로벌 앱 시장 조사 업체인 DISTIMO가 지난 20일(한국시간) 발표한 보고서에 따르면, 2013년 3월부터 8월까지 6개월 동안 세계 앱 시장은 애플 앱스토어와 구글 플레이 스토어를 통틀어 약 17%의 성장을 보였다(바다OS 등 마이너 시장은 제외). 시장의 전체적인 규모가 커진 가운데, 구글 플레이 스토어의 성장이 눈에 띈다. 지난 2013년 3월부터 8월까지 61% 성장한 매출 규모에 힘입어 매출 점유율도 3월 25%에서 8월 35%로 10% 상승했다.

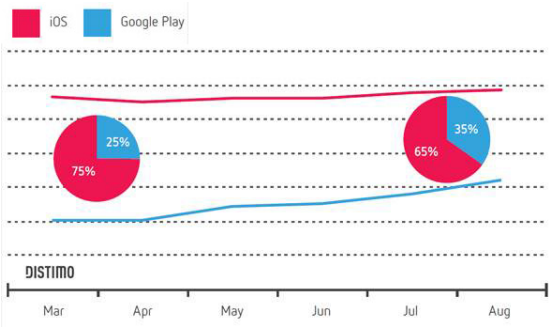

그림 2. 마켓 시장별 점유율 추이

2.3 세계앱 시장 규모순위

2013년 3월~8월간 DISTIMO의 전 세계 앱스토어 분석 보고서 발표에 따르면 미국, 한국, 일본 시장이 마켓 성장에 기여하는 정도가 절대적이라는 점은 기존과 변하지 않았다. 8월 한국의 앱 시장 규모는 미국과 일본에 이어 3위를 차지했다. 이어 영국, 중국, 호주가 각각 4위, 5위, 6위를 차지했다. 한국과 일본을 제외한 국가 대부분에서는 애플 앱스토어의 매출 점유율이 70% 이상을 차지하고 있어 2013년 전체적인 세계 시장 추이는 변하지 않고 있다.[3]

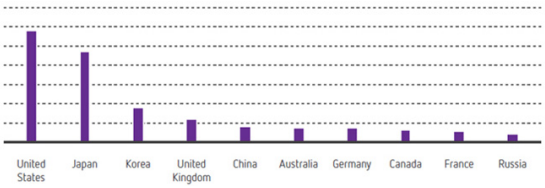

그림 3. 세계앱 시장 규모순위

III. 모바일 앱 시장 보안 위협

이번 장에서는 앞장에서 살펴보았듯이 현재 세계적으로 모바일 어플리케이션 및 앱스토어 이용자가 급상승하는 상황에서 앱스토어 및 스마트폰을 위협하는 현황과 유형이 무엇인지 알아보도록 한다.

3.1 악성앱 증가현황 및 원인

시만텍(www.symantec.co.kr)이 14일 발표한 '모바일 애드웨어 및 악성코드 분석 보고서'에 따르면 구글 플레이에 정식 등재된 모바일 앱의 23%가 보안위협이 높은 '매드웨어(Madware)'인 것으로 나타났고 계속적으로 안드로이드 기반 어플리케이션에서 보안위협이 지속적으로 증가하고 있는 것으로 나타났다. 전년대비 8% 상승 하였고 지난해 중반과 2013년 2분기에 악성앱 파일(APK)이 급격하게 증가했으며, 써드파티 앱스토어에 비해 보안 위협에 대한 노출이 낮았던 구글 플레이에서도 매드웨어의 비율이 전체 앱의 23%로 늘었다. 모바일 악성코드는 전년 대비 4배 증가했으며, 게임 및 엔터테인먼트 카테고리 비율이 높고,

구글 플레이 외의 안드로이드 앱스토어에서 위협이 높았다. 지난해 6월부터 2013년 6월까지 1년간 확인된 악성코드가 69%까지 크게 증가했으며, 알려진 악성코드 샘플은 총 27만5000건으로 전년대비 4배 증가했다. 써드파티 앱스토어에서 가장 위험성이 높은 카테고리는 게임/아케이드&액션이며, 그 다음이 사진 카테고리, 구글 플레이에서는 멀티미디어 앱 순이었다.[4]

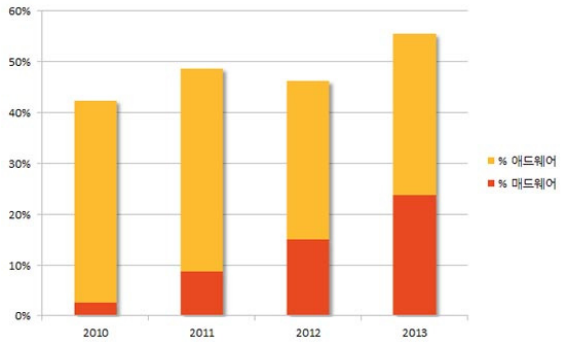

그림 4. 구글 플레이에서의 매드웨어 증가

또 핀란드 보안업체 F-Secure는 매 분기별로 모바일 위협 보고서(Mobile Threat Report)를 발표하고 있는데, 보고서 내용에 따르면 새로 발견되는 모바일 악성코드 유형은 해마다 그 수가 증가하고 있으며, 이들 중 대부분은 안드로이드 플랫폼 대상 악성코드이다.

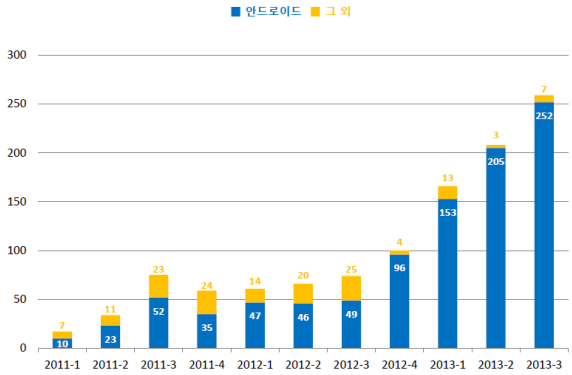

그림 5. 분기별 신종 모바일 악성코트 유형 및 변종 발견수(F-Secure 모바일 위협 보고서)

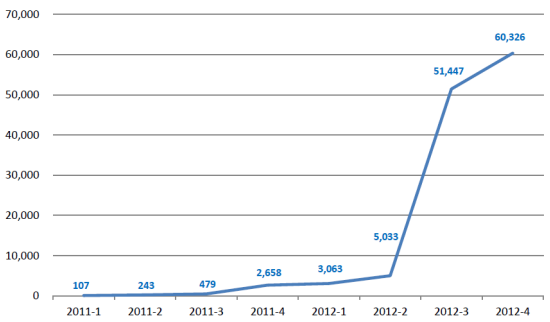

그림 6. 분기별 안드로이드 악성 APK 발견수

안드로이드 악성코드가 iOS를 비롯한 다른 모바일 운영체제보다 많은 이유는 높은 시장 점유율과 더불어 악성 어플리케이션의 제작 및 유포의 용이성 때문이다. 안드로이드는 오픈소스 운영체제로 모든 사람에게 커널 소스가 개방되어 있다. 또한, 각각의 어플리케이션이 APK파일 형태로 되어 있어서 PC를 이용하여 다운로드를 통해 스마트기기에 저장하여 실행하기만 하면 쉽게 해당 어플리케이션을 설치 할 수 있다. 무엇보다 안드로이드는 다양한 서드파티 앱스토어가 있는데 이러한 앱스토어의 상당수가 엄격한 어플리케이션 검증 절차 없이도 등록이 가능한 구조이다. 공식 앱스토어인 구글 플레이에서 아무리 보안정책을 강화하더라도, 그 외 앱스토어에는 영향을 주지 못하기 때문에 악성 어플리케이션 제작 및 유포가 다른 모바일 운영체제에 비해 쉽다는 문제점이 있다. 사용자는 이러한 앱스토어를 통해 어플리케이션 파일을 다운받아 스마트폰이나 태블릿 디바이스에 설치하게 된다. 각 서드파티 앱스토어를 통한 안드로이드 어플리케이션 다운로드 수는 구글 플레이의 것에 비하면 한참 못미치는 수치지만, 전체 앱스토어 개수와 업로드 된 어플리케이션 개수 당 다운로드 수를 고려한다면 서드파티 앱스토어가 미치는 영향력은 구글 플레이의 영향력보다 더 크다. 이처럼 서드파티 앱스토어가 사용자들에게 인기가 많은 이유는 무엇보다 무료나 저렴한 어플리케이션이 많고, 특정 사용자를 대상으로 하는 전용 앱스토어도 만들어져 있기 때문이다. 대표적인 서드파티 앱스토어로는 제조사 휴대폰 구매 시 기본적으로 깔린 통신사 앱스토어(olleh 마켓, T스토어, U+ 스토어)와 네이버 앱스토어, 삼성 앱스, AppZil 등이 있고, 전 세계적으로 많이 이용되고 있는 것으로는 아마존 앱스토어, SlideMe, F-Droid 등이 있으며 전체 약 30여 개가 넘는다.[5]

Ⅳ. 앱스토어 보안

4.1 모바일 어플리케이션의 Life Cycle

일반적으로 모바일 어플리케이션은 개발자에 의해 개발되고 앱스토어에 올라와 사용자가 이용되기까지 5가지 단계를 거친다. 개발, 등록, 검증, 배포, 이용 이 5가지인데 본 장에서는 각 단계별로 문제점을 살펴보고자 한다.

표 1. Life Cycle 단계별 문제점[6]

단계	문제점
개발	· 앱스토어 활성화를 위한 콘텐츠 확보에만 주력하여 오동작을 유발하는 악성앱 등록 개발자에 대한 이력 및 추적관리가 수행되지 않고 개발 부주의 및 기능테스트 미흡

	등을 핑계로 악성 개발자에 제제방안 미흡 · 보안인식이 부족한 개발자에게 개발 가이드라인 제공 및 교육 등이 선행되지 않음 · 개발된 어플리케이션에 대한 후속 검증이 미흡한 상황에서 개발자 검증 및 테스팅 결과에 의존함에 따라 개발자 부주의 또는 고의로 악성앱 발생 우려
등록	· 일부 앱스토어의 경우 적절치 않은 신원확인 절차에 의해 개발자 아이디 도용이나 신원 위조를 통한 악성 어플리케이션 유포에 악용될 소지가 있음 · 어플리케이션 등록 시 제출해야 하는 바이너리 코드가 담긴 보고서를 거짓으로 제출 - 일부 앱스토어의 경우 유효성검증이 미흡하여 필터링 되지 않음
검증	· 앱스토어의 보안검증은 크게 코드검증과 사전심의를 포함한 동작검증으로 나누어 진행되고 있는데 코드검증의 경우 안드로이드, 윈도우모바일 기반 어플리케이션에 대한 검증이 개발자 키 사인 검토와 개발자가 제출한 1차 검증 및 테스팅 결과에 의존한 바이너리 유효성 검토만 수행하기 때문에 복합지능 다양화되고 있는 은닉형 악성코드에 대한 위험이 발생 · 단일플랫폼 기반의 스마트폰용 백신을 이용한 점검을 수행하고 있지만 크로스 플랫폼에서는 상대적으로 점검이 미흡 · 유해성, 폭력성, 선정성 등은 게임등급위원회와 KIBA의 사전 심의를 거치치만, 이외의 별도 테스트센터를 통해 수행되는 동작검증의 경우 다수의 어플리케이션을 수동으로 검증해야 하나 이를 위한 자동화된 검증방안이 부족하여 실제 보안관점의 검증이 아닌 기능오류, 스트레스 테스트 수준의 검증만 이루어지고 결과적으로 기능에는 충실하지만 악의적 행위가 내재된 어플리케이션이 유통
배포	· 공격 성공 가능성을 높이기 위한 자기 은폐형 악성코드 기술들은 빠르게 변화하고 있지만 현재 앱스토어 보안검증은 최초 배포전 사전검증에만 치중 · 과금 및 업데이트를 위한 개발자 키 검증 외에 현재 사용자에게 서비스 및 다운로드 되고 있는 어플리케이션의 위변조 여부에 대한 무결성 검증과 신규 악성코드 은닉 여부에 바이러스 검증 등이 수행되지 않음
이용	· 시간/공간 및 불특정 다수를 대상으로 유발하는 악성앱으로 보안사고가 발생할 경우 그 피해는 급속히 확산/악화될 수 있어, 앱스토어에 서비스 된 모든 앱에 대한 지속적인 모니터링 및 사후방안이 요구되지만, 현재는 다운로드 및 이용 활성화 차원에서 판매된 앱에 대해서만 사후관리에 치중하고 있음. 다수의 사용자가 이용하는 앱이 악의적으로 활용될 경우 사용자의 피해와 사회적 불신 증대는 불가치하며, 반대로 잘못된 사고접수로 인한 선의의 개발자가 발생되는 사례도 예상됨

Ⅴ. 결 론

모바일 앱스토어 및 스마트 기기의 보안을 강화한다는 것은 크게 두가지 유형으로 볼 수 있다. 앱스토어에서 악성앱 어플리케이션을 다운받았을 시 각종 보안업체의 백신 또는 백신과 유사한 솔루션을 통하여 기기자체에서 악성행위를 막는 유형과 Ⅲ장과 Ⅳ장에서 살펴본 문제점들을 해결하기 위해 어플리케이션이 앱스토어에 등록되는 단계에서 보안이 강화되는 정책을 수립하여 악성앱의 유입경로의 원천차단하는 유형이 있다. 현재 보안업체나 스마트기기 제조업체, 국가기관 등에서는 전자를 연구하고 개발하는 것이 대부분이다. 후자를 통한 앱스토어 보안강화는 앱스토어 운영사측의 금전적 문제와 사회적 반발 등의 리스크가 예상된다. 따라서 국가가 나서 앱스토어 운영사측과 원만한 협의를 통해 주도적으로 정책을 수립하지 않는다면 앱스토어의 보안을 강화하기에는 많은 어려움이 예상된다.

참고문헌

[1] 홍유진, 한국콘텐츠진흥원 KOCCA 통계브리핑 제13-15호(해외편)
[2] http://www.edaily.co.kr/news/NewsRead.edy?SCD=JC11&DCD=A00305&newsid=02833926602905352
[3] http://m.thisisgame.com/webzine/news/nboard/4/?page=115&n=49631
[4] http://www.datanet.co.kr/news/articleView.html?idxno=69412
[5] http://www.hacknsecurity.com, 안드로이드 악성코드 분석 현황
[6] 윤선중, 앱스토어 모바일 어플리케이션 보안검증 개선 방안에 관한 연구