안드로이드 앱 스토어 보안 기법 비교 분석

한재민*, 송주석*
*연세대학교 컴퓨터과학과
e-mail:{jaemin.han, jssong2526}@yonsei.ac.kr

An analysis on Security Schemes for Android App store

Jae-Min Han*, Joo-Seok Song*
*Dept of Computer Science, Yonsei University

요 약

전 세계에서 안드로이드는 가장 인기 있는 운영체제이다. 이에 따라 구글 스토어 뿐 만아니라 네이버 앱 스토어와 같은 서드 파티가 점차 다양해지고, 사용자가 앱을 다운로드 받을 수 있는 경로가 보다 많아졌다. 악의적 목적을 가진 사용자는 이러한 점을 악용하고 있다. 앱 스토어에 악성 앱을 유포하고 마치 정상적인 앱처럼 나타내어 사용자를 속이는 등 여러 피해를 주고 있다. 본 논문에서는 앱 스토어에 관한 최근 연구들을 기능 별로 분류하고 서술한다. 그리고 각 기능 별 향후 방향에 대해 제시한다.

1. 서론

전 세계적으로 모바일을 사용하는 사용자의 수가 많아지고 있다. Ericsson[1]에 따르면 2019년도에 모바일 사용자 수는 60억 명을 넘을 것이라고 예측했다. 특히나 데스크탑의 사용자 점유율과 비교했을 때, 모바일과의 격차는 매년 커지고 있다. 이렇듯 모바일이 주류를 이루고 있는 시대에 맞춰 여러 기업에서는 안드로이드, iOS, 윈도우, 블랙베리 등의 운영체제를 탑재한 모바일 기기를 출시하고 있다. 이들 운영체제는 서로 각기 다른 특성을 가지고 있는 가운데 안드로이드가 약 85%로 세계 시장[2]을 점유 하고 있다. 개발자 및 일반 사용자들이 안드로이드를 선택하는 이유는 크게 2 가지로 안드로이드의 공개 아키텍처와 보다 쉬운 앱 제작을 들 수 있다[3]. 공개 아키텍처를 통해 개발자들은 안드로이드를 직접 수정 하는 것이 가능해졌고, 커뮤니티의 활성화와 안드로이드 API 및 Java를 통해 쉽게 앱을 제작하여 배포할 수 있기 때문에, 앱 스토어에 큰 영향을 주었다. 앱 스토어에 많은 앱이 등록되고, 일반 사용자들은 다양한 앱을 접하면서 점차 앱 스토어에 접근하는 일반 사용자의 수가 늘고 새로운 앱 스토어가 많이 등장[4]해 앱 생태계가 활발해졌다.

하지만 심한 부작용 또한 발생했다. 다양한 앱 스토어들이 등장하면서 앱 배포가 보다 쉬워지고 앱 스토어 자체적인 보안 프로세스가 약하기 때문에 여러 악성 사용자들의 표적으로 전락했다. 이러한 상황으로 인해 일반 사용자들의 피해는 점차 늘어나고 있다.

본 논문에서는 앱 스토어를 중점으로 한 2012년부터의 연구들을 기능 별로 분류하고 서술한다. 그리고 각 기능 별 향후 방향에 대해 제시한다.

2. 앱 스토어 관련 연구 분류

본 논문에서는 앱 스토어에서의 관련 연구를 주요 기능에 따라 크게 4 가지 주제로 분류하였다. 물론 기존의 여러 연구들은 앱 생태계에 따라 탐지 기법, 프로토콜 등 다양한 기준으로 분류 하였지만, 본 논문은 앱 스토어의 관점으로 최근 연구에서 제시하는 주요 기능을 기준으로 아래와 같이 분류하였다.

(1) 앱 탐지 도구 사용 : 악성 사용자로부터 배포된 앱이 앱 스토어에 등록하는 과정 또는 등록된 앱을 찾기 위해 내부적으로 설계 된 도구를 사용하여 검사한다.
(2) 앱 검증 : 앱 스토어에 저장된 앱을 일반 사용자이 다운로드 할 때, 앱 스토어와 일반 사용자 간의 프로토콜 상 정상적인 앱이라는 것을 검증하기 위해 새로운 프로코콜을 설계한다.
(3) 앱 업데이트 : 일반 사용자들이 앱 스토어에 등록된 새로운 버전의 앱을 쉽게 다운로드 하지 않는 이유를 분석하고 새로운 모델을 제시한다.
(4) 앱 정보 분석 : 앱 스토어에 저장되어 있는 앱의 평점, 리뷰, 가격 등 일반적인 정보를 바탕으로 분석하여 새로운 모델을 제시한다.

위와 같이 4 가지의 주제를 통해 이후 과정에서는 앱 스토어에 관해 각기 어떤 연구가 이루어졌고, 향후 방향에 대해 제시하였다.

3. 앱 탐지 도구 사용

일반적으로 개발자가 만든 앱이 앱 스토어에 등록 될 때 앱 스토어 별로 내부 프로세스를 거치게 된다. 예를 들

어 구글 스토어는 평점 시스템을, 애플 스토어는 리뷰 시스템을 채택하였다. 하지만 악성 사용자들은 Stealth 기법과 같은 공격을 통해 앱 스토어 내부 프로세스를 피해 갈 수 있기 때문에 최근엔 여러 탐지 기법들이 연구 되었다. [5]는 DroidMoss를 통해 비슷한 앱을 비교 분석하여 악성 앱을 찾는 방법을 제시했다. [6]는 사용자 몰래 돈을 훔쳐가는 앱을 탐지하기 위해 휴리스틱 기법을 사용하는 MoneyGuard를 제시했다. [7]는 AndRadar로 여러 앱 스토어에 있는 유사한 앱들을 기존의 방법보다 더 빠르게 찾아 악성 앱을 보다 쉽게 판단 할 수 있는 방법을 제시했다. [8]는 앱 스토어에 등록되어 있는 앱들이 잠재적인 취약성이 있는지 검사하기 위해 Cassandra를 제시했다.

4. 앱 검증

악성 사용자로 인해 앱 스토어에 등록 된 모든 앱이 모두 안전하다고 말하기 힘들어졌다. 더욱이 보안성이 공식 앱 스토어보다 떨어지는 서드 파티 때문에 사용자는 다운 받는 앱이 안전한지 검증 할 필요가 있다. 그래서 최근 앱 검증과 관련된 연구는 사용자는 모든 앱 스토어에 등록 된 모든 앱과 모든 앱 스토어는 쉽게 신뢰 할 수 없다는 가정을 세워두고, 사용자와 앱 스토어 간의 프로토콜을 제시한다. [9] [10]는 사용자가 앱을 다운로드 할 때, 앱이 정상적이라고 검증하는 프로토콜을 제시했다. 때문에 사용자는 다운로드 받는 모든 앱은 정상적이라고 판단할 수 있다.

5. 앱 업데이트

사용자 모바일 기기에 설치되어 있는 앱은 일반적으로 시간이 지나면 앱 스토어에 새로운 버전의 앱이 등장한다. 하지만 새로 출시된 앱이 기존의 앱에 없는 취약성이 발견 될 수도 있고, 악의적 사용자에 의해 악성 앱이 될 수도 있다. 때문에 업데이트에 관해서 다음의 연구가 진행되었다. [11]는 기존 앱과 새로운 버전의 앱 간의 설치 및 다운로드 관계를 통해 사용자들이 생각보다 업데이트를 잘 하지 않는다는 연구를 진행했다. [12]는 새로운 구글 스토어의 자동 업데이트 정책에서 권한 상승 공격을 받을 수 있다는 연구를 보여주었다. [13]는 권한을 기반으로 한 앱 업데이트보다 실제 앱 사용자의 리뷰를 통한 업데이트가 보다 효율성 있다고 언급하였다.

6. 앱 정보 분석

앱이 앱 스토어에 등록이 되면 일반 사용자로부터 다운로드 될 수 있다. 하지만 사용자들이 앱 스토어에서 처음으로 출시된 앱을 인식하기까지는 광고나, 사용자의 입소문 등이 없으면 쉽지 않다. 때문에 정상적인 앱 뿐만 아니라 악의적인 앱은 여러 악의적인 수단을 통해 인기 있는 앱으로 둔갑시킨다. 이에 기존의 연구는 앱 스토어에서 얻을 수 있는 앱의 정보를 통해 다방면으로 분석을 하였다. [14]는 앱의 비즈니스 및 고객 정보 등을 분석하여 서로 간의 관계를 형성하였다. [15]는 앱 스토어의 유료 앱들을 판매 전략, 다운로드 패턴 등을 분석하여 모델링을 만들었다. 이 모델링을 통해 가격이 사용자에게 어떤 영향력을 끼치는지 확인했다. [16]는 앱의 사용자 리뷰 조작을 통해 인기 있는 앱으로 둔갑한 앱들을 조사했다. [17]는 WisCom 시스템을 통해 사용자의 평점 및 리뷰를 분석한다.

7. 결론

4 가지 주제를 바탕으로 각기 다양한 연구가 진행되고 있다. 하지만 고도로 진화하는 악성 사용자의 공격에 따라 앱 스토어에 관한 연구도 아래와 같이 진행되어야 한다.

(1) 앱 탐지 도구 : 최근 다양한 은닉화 기법을 사용한 악성 앱이 많이 등장으로 기존의 정적, 동적 및 휴리스틱 분석을 통해서 탐지가 쉽지 않다. 때문에 보다 고도화된 기법이 연구되어야 한다.

(2) 앱 검증 : 악성 사용자는 다양한 네트워크 공격을 통해 정보를 가로채거나 변조한다. 때문에 기존의 연구는 인증서를 통한 프로토콜 구축이 수반된다.

(3) 앱 업데이트 : 앱의 기능, 요구 권한, 안전성 등 다양한 상황에 따라 안전하게 이루어져야 한다. 하지만 기존 연구는 앱의 업데이트 요구 시, 눈으로 확인 할 수 있는 정보에 한정되어 있다. 따라서 보다 세밀한 정책 또는 앱 내부 비교 분석을 통한 연구가 필요하다.

(4) 앱 정보 분석 : 기존의 연구는 다양한 관점을 통해 분석이 이루어졌다. 하지만 분석한 결과가 실제 환경에서 악성 상황 분석이 미비하다. 따라서 실제 환경에 맞추어 연구가 진행되어야 한다.

8. Acknowledgement

이 논문은 2016년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(2015R1D1A1A01058928)

참고문헌

[1] Ericsson. 2013. Ericsson Mobility Report. Retrieved February 10, 2015, from http://www.ericsson.com/res/docs/2013/ericsson-mobility-report-november-2013.pdf

[2] Kaspersky. 2014. Mobile cyber threats October 2014 http://media.kaspersky.com/pdf/Kaspersky-Lab-KSN-Report-mobile-cyberthreats-web.pdf

[3] Faruki, Parvez, et al. "Android security: a survey of issues, malware penetration, and defenses." Communications Surveys & Tutorials, IEEE 17.2 (2015): 998-1022.

[4] Vidas, Timothy, and Nicolas Christin. "Sweetening android lemon markets: measuring and combating malware in application marketplaces." Proceedings of the third ACM conference on Data and application security and privacy. ACM, 2013.

[5] Zhou, Wu, et al. "Detecting repackaged smartphone applications in third-party android marketplaces." Proceedings of the second ACM conference on Data and Application Security and Privacy. ACM, 2012.

[6] Yang, Chao, et al. "Detecting money-stealing apps in alternative Android markets." Proceedings of the 2012 ACM conference on Computer and communications security. ACM, 2012.

[7] Lindorfer, Martina, et al. "AndRadar: fast discovery of android applications in alternative markets." Detection of Intrusions and Malware, and Vulnerability Assessment. Springer International Publishing, 2014. 51-71.

[8] Lortz, Steffen, et al. "Cassandra: towards a certifying app store for android." Proceedings of the 4th ACM Workshop on Security and Privacy in Smartphones & Mobile Devices. ACM, 2014.

[9] Vidas, Timothy, and Nicolas Christin. "Sweetening android lemon markets: measuring and combating malware in application marketplaces." Proceedings of the third ACM conference on Data and application security and privacy. ACM, 2013.

[10] Ernst, Michael D., et al. "Collaborative verification of information flow for a high-assurance app store." Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security. ACM, 2014.

[11] Möller, Andreas, et al. "Update behavior in app markets and security implications: A case study in google play." Proc. of the 3rd Intl. Workshop on Research in the Large. Held in Conjunction with Mobile HCI. 2012.

[12] Sanders, Craig, Ayush Shah, and Shengzhi Zhang. "Comprehensive analysis of the android google play's auto-update policy." Information Security Practice and Experience. Springer International Publishing, 2015. 365-377.

[13] Tian, Yuan, et al. "Supporting Privacy-Conscious App Update Decisions with User Reviews." Proceedings of the 5th Annual ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices. ACM, 2015.

[14] Harman, Mark, Yue Jia, and Yuanyuan Zhang. "App store mining and analysis: MSR for app stores." Proceedings of the 9th IEEE Working Conference on Mining Software Repositories. IEEE Press, 2012.

[15] Petsas, Thanasis, et al. "Rise of the planet of the apps: A systematic study of the mobile app ecosystem." Proceedings of the 2013 conference on Internet measurement conference. ACM, 2013.

[16] Liu, Yuhong, and Yan Sun. "Can reputation manipulation boost app sales in Android market?." Acoustics, Speech and Signal Processing (ICASSP), 2013 IEEE International Conference on. IEEE, 2013.

[17] Fu, Bin, et al. "Why people hate your app: Making sense of user feedback in a mobile app store." Proceedings of the 19th ACM SIGKDD international conference on Knowledge discovery and data mining. ACM, 2013.