과도한 권한을 요구하는 안드로이드 앱 탐지

배경륜[O*], 이연재[*], 김의연[*], 태규빈[*], 김형종[*], 이해영[**]
[o*]서울여자대학교 정보보호학과
[**](주)두두아이티
e-mail: hkim@swu.ac.kr[*]

Detection of Android Apps Requiring Excessive Permissions

Gyeongryoon Bae[O*], Yonjae Lee[*], Euiyeon Kim[*], Gyubin Tae[*], Hyung-Jong Kim[*], Hae Young Lee[**]
[o*]Dept. of Information Security, Seoul Women's University
[**]DuDu IT, Inc.

● 요 약 ●

안드로이드 운영체제는 앱을 설치하거나 실행할 때 사용자가 해당 앱이 요청하는 권한들을 승인하도록 하고 있으나, 일반적인 사용자들은 이를 주의 깊게 확인하지 않고 승인하는 경우가 많으며, 과도한 권한들을 요구하는 앱의 실행은 프라이버시 침해 문제로 이어질 수 있다. 본 논문에서는 제공하는 기능들에 비해 과도한 권한들을 요구하는 안드로이드 앱들을 탐지하는 모델을 제안한다. 먼저 손전등, 다이어리, 지불(페이) 및 채팅 앱 207개를 대상으로 요구하는 권한들을 조사하여 정리하였다. 조사 결과를 기준으로 설치 또는 실행하려는 앱이 어느 정도의 권한들을 요구하는지 가늠할 수 있다. 설치된 앱들의 요구 권한들을 조회할 수 있는 앱 프로토타입을 개발하였으며, 향후 모델의 구체화 및 검증을 거쳐, 프로토타입에 적용할 계획이다.

키워드: 모바일 프라이버시(mobile privacy), 모바일 보안(mobile security), 안드로이드(Android)

I. Introduction

안드로이드(Android) 운영체제는 사용자에게 앱 설치 시 혹은 실행 시 해당 앱이 요구하는 권한들(permissions)을 확인하여 승인 또는 거부할 수 있도록 하고 있으나, 일반적인 사용자들은 이러한 권한 요청들을 주의 깊게 확인하지 않고 승인하는 경우가 많다[1]. 안드로이드의 공식 앱 마켓인 구글 플레이 스토어(Google Play Store)에 제공하는 기능들에 비해 과도한 권한들을 요구하는 앱들(예를 들어, 자세한 위치, 통화 기록, 주소록 등의 접근 권한들을 요구하는 손전등 앱)이 다수 존재하며, 이는 심각한 프라이버시 침해 문제로 이어질 수 있다.

연구의 목표는 과도한 권한들을 요구함으로써 프라이버시 침해 우려가 있는 안드로이드 앱들을 식별하기 위한 기술을 개발하는 것이다. 이를 위한 첫 단계로, 본 논문에서는 제공하는 기능들에 비해 과도한 권한들을 요구하는 안드로이드 앱들을 식별하기 위한 모델을 제안한다. 앱 종류별로 요구하는 권한들이 다를 수밖에 없으므로, 앱 종류별로 권한들을 조사하였다. 4가지 종류 207개의 앱들을 대상으로, 종류별 앱들이 요구하는 권한들을 조사하였다. 조사 결과는 종류별로 과도한 권한들을 요구하는 앱들을 식별하는데 기준으로 활용할 수 있다. 설치된 앱들을 대상으로 요구 권한들을 조회할 수 있는 앱 프로토타입을 개발하였으며, 향후 조사 결과를 반영하여 사용자가 과도한 권한을 요구하는 앱들을 식별하는데 도움이 될 수 있도록 확장할 것이다.

II. Detection Model

안드로이드에서 제공하는 권한들은 보호 수준을 기준으로 일반(normal), 위험(dangerous), 서명(signature), 서명 및 특권(signature and privileged)의 4가지로 나뉜다. 일반 권한들은 사용자의 승인 없이 사용이 가능하며, 위험 권한들은 보안 또는 프라이버시 문제로 사용자의 승인이 필요하다. 서명이나 서명 및 특권 권한들도 사용자의 승인 없이 사용이 가능하나, 해당 권한들은 안드로이드 개발사 및 기기 제조사들이 개발한 앱들에서만 사용이 가능하다. 안드로이드 앱들 중 손전등, 다이어리, 지불(페이) 및 채팅 앱 207개를 조사하였으며, 일반 및 위험 권한들만을 대상으로 하였다. 조사 결과 앱 종류별로 요구한 위험 및 일반 권한들의 수의 평균값, 중간값(median), 최솟값 및 최댓값을 Table 1에 정리하였다.

Table 1. Number of permissions

종류		손전등	다이어리	지불	채팅
개수		100	65	23	19
Dangerous	평균값	1.60	2.10	5.63	5.04
	중간값	1	2	6	5
	최솟값	0	0	3	2
	최댓값	6	6	8	7
Normal	평균값	0.16	0.14	0	0.04
	중간값	1	0	0	0
	최솟값	0	0	0	0
	최댓값	2	1	0	1

정리된 결과는 종류별로 과도한 권한들을 요구하는 앱들을 식별하는데 활용할 수 있다. 예를 들어, 손전등 앱은 위험 권한을 요구하지 않더라도 기능의 제공이 가능하므로 위험 권한을 요구하지 않는 앱의 사용이 권장되며, 2개 이상의 위험 권한들을 요구하는 앱의 사용은 보안 또는 프라이버시 측면에서 위험할 수 있다.

III. Implementation

설치된 앱들을 대상으로, 앱 종류별, 앱별, 권한별로 요구하는 권한들이나 앱들을 조회할 수 있는 프로토타입을 개발하였다. 오픈 소스인 권한 탐색기(Permission Explorer)[1]를 기반으로 구현하였다.

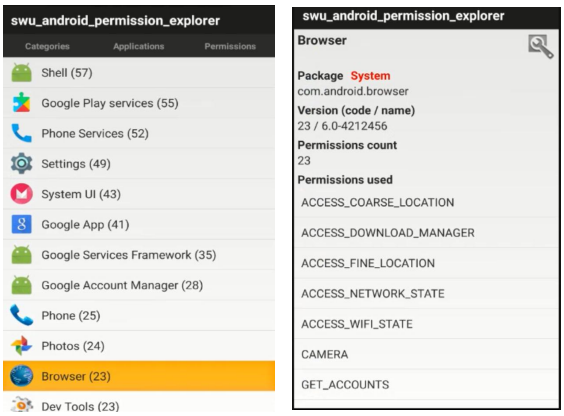

Fig. 1. Prototype Implementation

IV. Conclusions and Future Work

본 연구에서는 과도한 권한들을 요구하는 앱들을 탐지하는 모델을 제안하였다. 향후에는 모델의 구체화 및 검증을 수행할 예정이다. 앱들의 요구 권한들을 분석하여 보안 관점에서 위험한 앱들을 식별하는 기존 기술들[3,4]과는 달리, 프라이버시 관점에서 위험한 앱들을 식별하는데 초점을 맞출 계획이다.

Acknowledgement

이 연구는 2017년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(NRF-2017R1D1A1B03034644).

REFERENCES

[1] A.P. Felt *et al*, "Android permissions: user attention, comprehension, and behavior," Proc. of SOUPS '12, July 2012.

[2] Permission Explorer. https://github.com/ruippeixotog/permission-explorer

[3] S. Kang, J.W. Yoon, "Probabilistic K-nearest neighbor classifier for detection of malware in android mobile," J. of KIISC, Vol. 25, No.4, pp. 817-827, August 2015.

[4] H.R. Ryu, Y. Jang, T. Kwon, "Malware Classification System to Support Decision Making of App Installation on Android OS," J. of KIISE, Vol. 42 No. 12, pp. 1611-1622, December 2015.