졸업논문청구논문

ScanDal 분석 결과를 활용한 안드로이드 어플리케이션에서의 개인정보 유출 제어

Controlling personal information leakage of android application using ScanDal analysis result

박 현 민 (朴 賢 旻 Park, Hyeon Min)
13045

과학영재학교 경기과학고등학교

2015

ScanDal 분석 결과를 활용한 안드로이드 어플리케이션에서의 개인정보 유출 제어

Controlling personal information leakage of android application using ScanDal analysis result

[논문제출 전 체크리스트]

1. 이 논문은 내가 직접 연구하고 작성한 것이다. ■
2. 인용한 모든 자료(책 • 논문 • 인터넷자료 등)의 인용표시를 바르게 하였다. ■
3. 인용한 자료의 표현이나 내용을 왜곡하지 않았다. ■
4. 정확한 출처제시 없이 다른 사람의 글이나 아이디어를 가져오지 않았다. ■
5. 논문 작성 중 도표나 데이터를 조작(위조 혹은 변조)하지 않았다. ■
6. 다른 친구와 같은 내용의 논문을 제출하지 않았다. ■

Controlling personal information leakage of android application using ScanDal analysis result

Advisor : Teacher Jeon, Hyun-Seok

by

13045 **Park, Hyeon-Min**

Gyeonggi Science Highschool for the gifted

A thesis submitted to the Gyeonggi Science Highschool in partial fulfillment of the requirements for the graduation. The study was conducted in accordance with Code of Research Ethics[1].

2015. 11. 30.

Approved by

Teacher Jeon, Hyun-seok

[Thesis Advisor]

---

1) Declaration of Ethical Conduct in Research: I, as a graduate student of GSHS, hereby declare that I have not committed any acts that may damage the credibility of my research. These include, but are not limited to: falsification, thesis written by someone else, distortion of research findings or plagiarism. I affirm that my thesis contains honest conclusions based on my own careful research under the guidance of my thesis advisor.

ScanDal 분석 결과를 활용한 안드로이드 어플리케이션에서의 개인정보 유출 제어

박 현 민

위 논문은 과학영재학교 경기과학고등학교 졸업논문으로
졸업논문심사위원회에서 심사 통과하였음.

2015년 11월 30일

심사위원장 이 광 근 (인)

심사위원 이 영 준 (인)

심사위원 전 현 석 (인)

Controlling personal information leakage of android application using ScanDal analysis result

Abstract

Nowadays, as a result of the rapid spread of the smartphone, most people use mobile application. However, the Android platform, the most dominant mobile operating system, makes it hard for its users to know the exact information applications request because of the limitation of the permission system, which is asked once during installation. It is impossible to deny some of the permissions requested, and it is also hard to determine whether the acquired information is used only internally or not. To address this problem, the PrivateManager project that asks the users in a speculated situation predicted by the result of the ScanDal - which analyzes the Android application statically - and provides management of private information was suggested. In this study, the statistic service that collects user acceptance or rejection and provides it to other users was added to the project to judge the dangerousness.

ScanDal 분석 결과를 활용한 안드로이드 어플리케이션에서의 개인정보 유출 제어

초 록

스마트폰의 빠른 보급에 따라 거의 대부분의 사람들이 모바일 어플리케이션을 이용하는 시대가 되었다. 그러나 가장 많은 점유율을 가진 안드로이드 플랫폼 상에서의 어플리케이션은 설치할 때 한 번만 물어보는 권한 시스템의 한계점으로 인해 어떤 정보를 요구하는지를 잘 알기 어렵다. 요구하는 정보들 중 일부만 거부하는 것도 불가능하며, 획득된 정보가 기기 내에서만 사용되는지, 외부로 전송되는지도 알 수 없는 것이 현실이다. 이러한 문제를 해결하기 위한 방법으로 안드로이드 어플리케이션을 정적으로 분석하는 ScanDal의 분석 결과를 토대로 예측된 개인정보가 유출될 수 있는 부분에서 사용자의 확인을 받고, 개인정보 관리 기능을 제공하는 PrivateManager 프로젝트가 진행된 바 있다. 본 연구에서는 이 프로젝트에 각 항목에 대한 사용자들의 수락 여부를 수집하고 이를 다른 사용자들에게 제공하도록 하는 기능을 추가하여 더 쉽게 위험성을 판단할 수 있도록 개선하였다.

목차

그림 목차

Ⅰ. 서론

스마트폰이 대중화됨에 따라 원래의 목적과는 다르게 사용자 몰래 개인정보를 유출할 수 있는 악성 어플리케이션이 증가하고 있으며, 악성 어플리케이션이 아니라도 사용자 위치 기반 광고 서비스 등의 부가 서비스를 위해 사용자의 위치 정보 등 민감한 개인정보 영역에 접근하는 경우가 많이 늘어나고 있다.

2014년 인터넷이용실태조사[1]에 따르면 만 6세 이상 인구의 78.6%는 스마트기기를 보유하고 있다. 이 외에도 여러 통계 자료로 볼 때, 우리의 일상에서 이미 스마트폰은 떼려야 뗄 수 없는 중요한 전자 기기가 되어 있다. 또한, 2012년 하반기 스마트폰이용실태조사 결과[2]에 따르면 스마트폰 이용자의 1인 평균 설치된 어플리케이션의 개수는 46.1개로 상당히 많은 수준임을 알 수 있다.

실제로 삼성 갤럭시S 내의 '거울' 위젯 어플리케이션이 동작하는 기능에 비해 엄청난 권한을 요구하고 있던 것[3]이 밝혀진 바 있으며, 유명 손전등 어플리케이션에서 유심 칩 번호 등의 중요한 개인정보를 외부로 유출한다는 것[4]이 드러난 바가 있다. 삼성 갤럭시 시리즈의 펌웨어 업그레이드시 함께 설치되며, 비활성화가 불가능한 시스템 어플리케이션 '스마트 매니저' 역시 과도한 권한을 요구하여[5] 논란이 되고 있기는 마찬가지이다.

본 연구에서는 정적 분석의 결과를 이용하여 어플리케이션이 개인정보에 접근하고 정보를 유출할 수 있는 부분에서 사용자에게 물어볼 수 있도록 하는 PrivateManager 프로젝트[6]에 사용자들의 승인 여부 통계를 제공하는 기능을 추가하여 신뢰성과 사용성을 향상시키고자 하였다.

Ⅱ. 이론적 배경

2.1 iOS와 Android

일반적으로 사람들이 널리 사용하는 스마트폰의 운영체제는 크게 iOS와 안드로이드로 구분된다. iOS에서는 어플리케이션이 요청하는 모든 권한에 대해 각 권한이 처음 요청되었을 때 해당 권한에 대한 승인 여부를 물어보는 팝업 창을 띄우고 버튼을 통해 사용자의 응답을 받아 그대로 동작한다. 이렇게 사용자 주도로 개인정보를 관리하며, 그림 1처럼 설정에서 각 동작의 승인 여부를 쉽게 변경할 수 있도록 되어 있다.

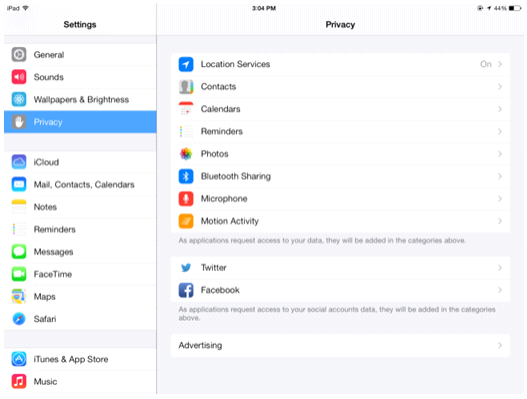


그림 1 iOS의 개인정보 접근 관리 화면

이에 반해, 2014년 1월 기준으로 대한민국 스마트폰 사용자의 93.4%가 사용하는 플랫폼인 Android[7]은 6.0 Marshmallow 이전까지는 각 어플리케이션이 그림 2처럼 처음에 설치할 때에 단 한 번, 이 어플리케이션이 어떠한 개인정보에 접근할 수 있음을 선언할 뿐이다. 그마저도 이 중 하나라도 거부한다면 그 어플리케이션은 설치조차 되지 않기에, 사용자가 그 어플리케이션을 이용하고 싶다면 어플리케이션이 요구하는 권한을 모두 수락하는 수밖에 없다. 한편, 어플리케이션이 특정 권한을 획득한다면, 그 이후부터는 사용자에게 알려지는 것 하나 없이

개인정보에 쉽게 접근할 수도 있다.

날로 늘어가는 개인정보 유출 사고와 위험성을 인지하고 6.0 Marshmallow에서는 새로운 권한 모델이 적용되어 개인정보를 안전하게 관리할 수 있지만, 출시된 지 얼마 되지 않아 보급률도 크지 않으며, 그 전 버전들에 대해서는 전혀 관리가 되고 있지 않은 것이 사실이다. 따라서 예전 버전의 안드로이드 상에서도 어플리케이션이 개인정보를 사용할 수 있도록 하는 권한을 각 유형별로 사용자가 관리할 수 있도록 해줄 필요가 있다.

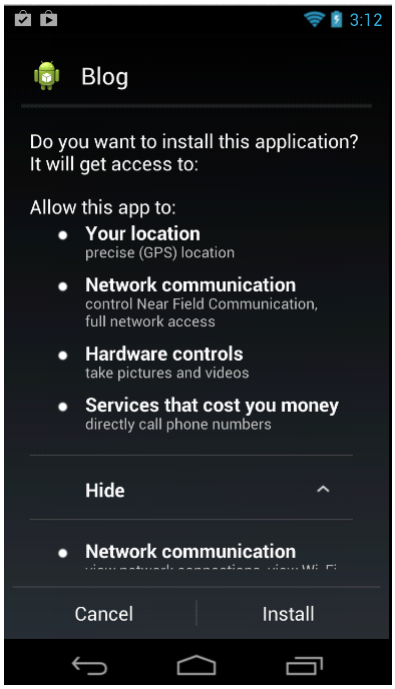


그림 2 안드로이드 상에서의 어플리케이션 설치 시 화면

이러한 필요성을 바탕으로 만들어진 TaintDroid[8] 프로젝트는 안드로이드 시스템 코드를 수정하여 개인정보 차단을 운영 체제 차원에서 막을 수 있는 기능을 제공한다. 그러나 이는 동적으로 개인정보에 대한 접근을 감시하는 방식이기에 필연적으로 성능 하락이 발생한다. 또한 펌웨어를 직접 수정하는 방식의 특성상

다양한 기기를 지원하지 못하며, 지원하는 버전도 한정되어 있는 등 큰 한계점이 있다.

2.2 안드로이드 어플리케이션 파일의 구조

안드로이드 시스템에서 어플리케이션 파일은 APK라는 확장자를 갖는다. 이 APK 파일은 일반적으로 사용되는 압축 파일 형식인 ZIP 파일과 같은 구조를 가지고 있고, 그림 3에서 나타난 것과 같이 컴파일된 바이너리들로 이루어진 classes.dex 파일, 어플리케이션의 컴포넌트 목록·권한 등과 같은 정보를 포함하고 있는 AndroidManifest.xml 파일, 이미지·음악 등의 리소스 파일 등으로 이루어져 있다.

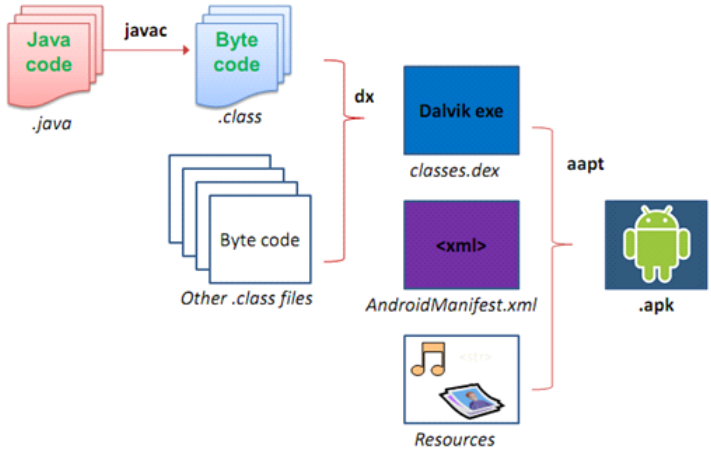


그림 3 안드로이드 어플리케이션 파일의 구조[9]

2.3 Dalvik VM 및 smali

안드로이드 어플리케이션은 Dalvik VM이라는 가상 머신 위에서 실행되는데, 이에 필요한 명령 코드들이 classes.dex 파일에 포함되어 있다. 여러 java 소스 코

드들로부터 컴파일된 class 파일들이 Dalvik opcode로 바뀌고 그것들이 합쳐져 classes.dex 파일로 만들어지는 것이다.

한편, 이렇게 생성된 바이너리 파일은 사람이 읽을 수 없기에 사람이 쉽게 볼 수 있도록 하는 변환 작업이 필요하다. 그림 4와 같이 baksmali라는 과정을 통하면 classes.dex 파일은 사람이 읽을 수 있도록 const(상수 지정 명령), move-result(함수의 실행 결과를 레지스터로 복사), invoke-static(정적 멤버 함수 호출) 등으로 간단하게 풀어 쓰여 있는 smali 코드 형태로 바뀐다. 이를 통해 쉽게 의미를 파악하고 특정 부분을 수정할 수 있으며, 그 후에는 smali라는 툴을 이용하여 변경된 smali 코드를 다시 classes.dex로 만들 수 있다.

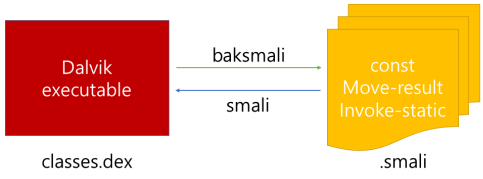


그림 4 smali와 baksmali의 동작 모식도

2.4 ScanDal[10]

ScanDal은 달빅 가상머신 언어로 기술되어 있는 안드로이드 어플리케이션을 분석 대상으로 하는 정적 분석기이다. 달빅 프로그램에 대해 분석한다는 것은 자바 역 컴파일러 등의 툴을 이용하지 않는다는 뜻이다.

악성 행동을 의도한 어플리케이션의 경우 달빅 바이트코드 수준에서 코드의 수정이 있을 수 있고, 그 경우 자바로의 역 컴파일러가 제대로 작동하지 못 할 수 있다. 따라서 달빅 바이트코드의 실행 의미를 직접 분석하면 개인정보를 누출시키는 지의 여부를 어느 정도 분석해 낼 수 있게 된다.

ScanDal은 어플리케이션이 개인정보를 누출시키는지의 여부를 파악하기 위해, 정보의 소스(source; 개인정보를 운영체제로부터 꺼내오는 API 함수 호출 위치)로부터 싱크(sink; 임의의 데이터를 기기 밖으로 내보낼 수 있는 API 함수 호출 위치)로 데이터 흐름의 존재를 개인정보의 누출로 정의하여 요약 해석 기법을 통해 구현된 도구이다.

2.5 TaintDroid

TaintDroid는 Android Open Source Project(AOSP)를 기반으로 하여 제작된 운영체제로, 실행되는 어플리케이션이 어떤 정보에 접근하는지를 실시간으로 감시한다. 이를 통해 개인정보에 접근하는 것이 확인될 경우에 사용자에게 통지하거나 작동 여부를 물어볼 수 있도록 하는 것이 이 프로젝트의 역할이다.

그러나 동적으로 감시하는 이 시스템의 특성상 실제로 어플리케이션을 동시에 실행해야 하며, 필연적으로 그 속도도 느려지게 되어 있다. IPC 벤치마크를 사용하여 성능을 평가했을 때 원래의 안드로이드 운영체제에 비해 27% 더 느린 것으로 나타났다.[8]

2.6 정적 분석[9]

정적 분석은 프로그램을 실행시켜 보지 않고 원하는 결과를 얻어내는 것으로, 분석기가 완성되면 사람의 손을 거치지 않고 분석기가 스스로 대상 프로그램을 분석할 수 있다. 요약 해석에서 제안하는 조건들을 만족하는 분석기를 디자인할 경우, 그 분석기는 해당 실행 의미에 대해 모든 실행과정을 안전하게 포섭하게 된다. 이 방법은 임의의 언어와 임의의 성질에 대해 활용할 수 있고, 디자인과 구현에 따라 다양한 정밀도를 얻어낼 수 있다.

Ⅲ. 연구 방법

3.1 구현 내용

3.1.1 통계 대상

본 연구에서는 이전 연구에서의 PrivateRepacker를 통해 패치된 앱을 사용하는 사용자들이 개인 정보에 대한 접근(source)과 개인 정보 유출 가능성이 있는 행위(sink)에 대해 얼마나 이 행위를 많이 접했으며, 얼마나 이 행위에 동의했는지에 대한 통계를 수집한다.

이를 통해 다른 사람이 이에 접근했을 때 현재 사용자들이 얼마나 동의했는지의 여부를 인지시키는 것을 목표로 한다.

3.1.2 통계 생성

통계 생성은 PrivateManager 내부에서 이루어진다. 최초 의심 행위 발생시 생성되는 팝업 창에서 수집된 수락/거부의 수, 이후 PrivateManager 상에서 수락/거부 여부를 변경하며 수집된 데이터를 어플리케이션 내부 데이터베이스에 보관한다. 각 어플리케이션 파일의 고유한 해시값을 통해 정확히 해당 어플리케이션에 대한 데이터만 저장할 수 있도록 테이블을 분리했다.

3.1.3 통계 수집

많은 디바이스에서 쉽게 통계를 수집하기 위해 인터넷을 이용했다. 일반적인 웹 서버에 많이 사용되는 Nginx, PHP, MySQL 등의 환경을 통해 각 어플리케이

션에 대한 데이터를 수집하고 저장한다. 통계 수치가 변경되는 모든 동작이 발생할 때마다 통계 수집을 위해 인터넷 연결을 시도한다. 모바일 기기의 특성상 인터넷이 연결되지 않은 상태가 지속될 수 있으므로, 내부 데이터베이스에 변화한 양을 모두 기록하며, 서버에서 처리가 완료되었다는 긍정적인 답변을 받았을 때 이를 내부 데이터베이스에서 제거함으로써 잠시 인터넷 환경이 좋지 못할 때에 발생된 통계 자료도 문제없이 생성하고 서버에서 정확하게 수집할 수 있도록 했다.

3.1.4 통계 확인

사용자들은 PrivatePatcher를 통해 패치된 어플리케이션을 이용하면서 sink나 source로 분석된 지점에 도달할 경우 팝업 창을 통해 9초 내에 이 행위를 승인할 것인지를 판단해야 한다. 이 때 PrivateManager에서는 인터넷에 연결하여 통계 제공 서비스를 통해 사용자의 작업에 따른 수락/거절 통계 자료를 얻어온다.

모바일 환경의 특성상 인터넷 망에 연결되어 있지 않을 수 있으며, 인터넷 망에서도 접속이 차단되는 등의 경우가 있을 수 있으므로 처음부터 인터넷에서 완전히 정보를 얻어온 후 팝업 창을 표시하기에는 무리가 있다. 따라서 통계 자료를 얻어오는 작업은 백그라운드에서 진행되며, 통계 저장 서버로부터 정상적인 응답이 오는 순간 팝업 창에 추가적인 메시지를 보여주는 방식으로 구현하였다.

3.2 구현 방법

3.2.1 통계 자료 구조

통계 저장 서버와 PrivateManager 어플리케이션 모두에서 통계 자료는 SQLite를 통해 데이터베이스의 형태로 저장된다. 데이터베이스에는 여러 개의 테이블이

존재한다. 패치된 어플리케이션의 해시값을 통해 테이블을 생성한다. 이 때 SQLite상에서 숫자로만 이루어진 테이블명은 허용되지 않으므로, 혹시라도 해시값이 모두 숫자로 이루어질 경우에 대비하여 해시값 앞에 '_'라는 문자를 붙인다.

이 테이블 내에서 source/sink 등의 항목은 각 행별로 나누어진다. 이에 대해 allow, disallow, type이라는 열에 수락한 수(숫자), 거부한 수(숫자), 이 항목에 대한 간략한 설명(문자열)을 저장한다. 개인정보에 접근하는 부분(source)은 id, geo 등의 항목별로 분류되며, 유출 가능한 부분(sink)은 같은 항목이라도 호출되는 지점에 따라 번호를 붙여 다르게 분류된다. 그림 5와 6은 터미널 상에서 확인할 수 있는 테이블과 그 내부의 구조를 나타낸 것이다.

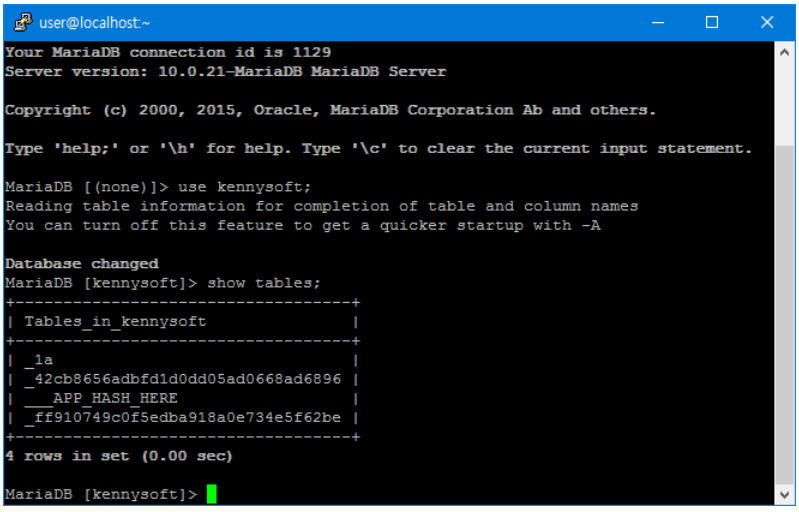


그림 5 서버에서 테이블의 구조

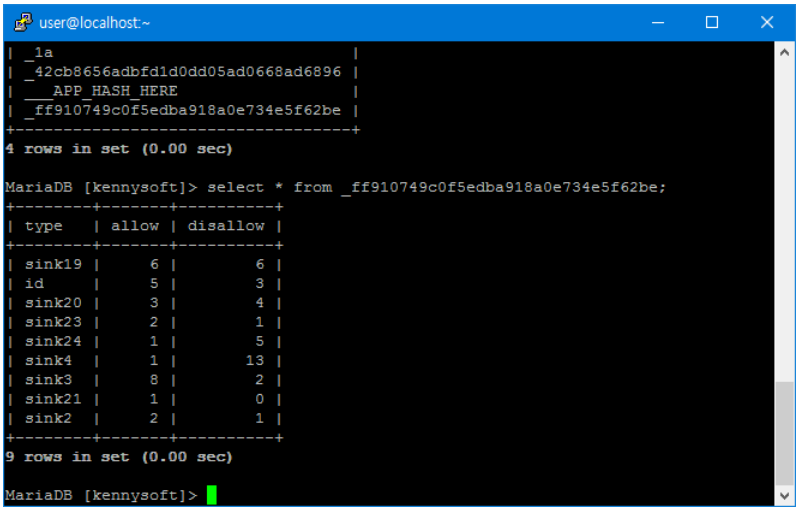


그림 6 서버에서 테이블 내부의 구조

통계 자료에 대한 접근은 각각의 시스템에서 지원하는 기능을 활용하였다. 서버에서는 PHP에서 제공하는 mysql 함수들을 이용했고, PrivateManager에서는 안드로이드에서 제공하는 SQLiteOpenHelper 및 SQLiteDatabase 등을 사용해 구현하였다.

3.2.2 서버와의 통신

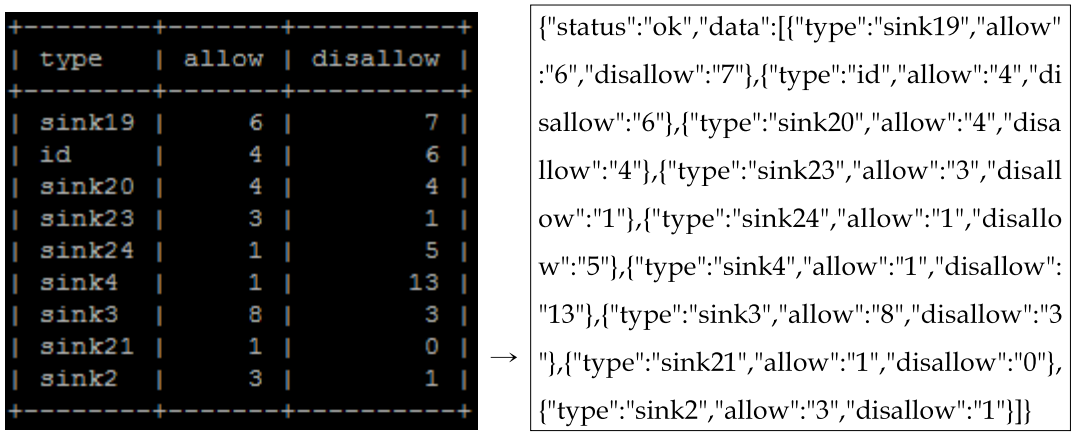
PrivateManager은 서버와 통신하기 위해 UrlConnection을 사용한다. 이 통신은 그 목적이 통계 자료를 가져오기 위한 것(get)인지, 설정하기 위한 것(set)인지에 따라 다르다. GetUrlConnection에서는 획득된 통계 자료를 유연하게 활용할 수 있도록 자료 취득 성공시 호출되는 함수를 설정할 수 있게 구현하였다.

한편, SetUrlConnection에서는 설정을 위한 각 연결에 대해 고유한 id를 저장하여 서버와 성공적으로 통신이 이뤄짐을 확인한 후 자체 데이터베이스에서 제거할 수 있도록 하였다. 이를 통해 인터넷에 접속할 수 없거나, 다른 이유로 서버에 접근하지 못했을 때 반영되지 않은 통계 자료를 함부로 제거할 수 없게 하

였다.

서버로 데이터를 보낼 때에는 별다른 절차 없이도 쉽게 처리할 수 있도록 URL에 특정 값의 이름과 그 데이터를 그대로 기술하는 GET 메서드를 사용한다. 한편, 서버에서 데이터를 보낼 때에는 json 방식을 사용한다. 필요한 값이 없거나 오류가 생길 경우 status에 error임을 표시하고, 성공적으로 처리되었을 경우에는 status를 ok로 설정한다.

get 명령인 경우 data 배열에 type, allow, disallow로 구성된 오브젝트들을 나열하여 데이터를 전달하며, PrivateManager에서는 이를 JSONObject를 통해 가공하여 처리한다. 그림 7은 json 형태의 통계 자료 예시를 나타낸 것이다.



type	allow	disallow
sink19	6	7
id	4	6
sink20	4	4
sink23	3	1
sink24	1	5
sink4	1	13
sink3	8	3
sink21	1	0
sink2	3	1

→

{"status":"ok","data":[{"type":"sink19","allow":"6","disallow":"7"},{"type":"id","allow":"4","disallow":"6"},{"type":"sink20","allow":"4","disallow":"4"},{"type":"sink23","allow":"3","disallow":"1"},{"type":"sink24","allow":"1","disallow":"5"},{"type":"sink4","allow":"1","disallow":"13"},{"type":"sink3","allow":"8","disallow":"3"},{"type":"sink21","allow":"1","disallow":"0"},{"type":"sink2","allow":"3","disallow":"1"}]}

그림 7 json 형태의 통계 자료

3.2.3 통계 생성

PrivateManager는 두 가지 상황에서 통계를 생성한다. 첫 번째는 source나 sink 상황에 처음 직면했을 때 나타나는 팝업 창(PrivateRequestActivity)에서이다. 사용자가 수락/거부 버튼을 누르거나, 9초가 지나 자동으로 거부 처리가 되

었을 경우 미리 생성된 SQLite 데이터베이스에 기록하도록 요청한다. 이 경우 신규로 생성되는 통계 자료이므로, A(Allow; 수락)+D(Disallow; 거부)의 값은 1이다.

두 번째는 PrivateManager 어플리케이션을 직접 실행시켜 특정 어플리케이션에 대한 설정을 변경할 때이다. 스위치의 상태가 변경될 때 호출되는 함수에서 원래의 값과 변경되는 값을 알 수 있으므로 이에 따라 통계 자료를 조정하도록 한다. 이 경우는 이미 수집된 통계에서 변동 사항이 생기는 것이므로, A+D의 값은 0이다.

3.2.4 통계 확인

통계 확인 역시 두 가지 상황에서 이루어진다. 첫 번째로는 팝업 창에서 버튼을 누르기 전 현재 상황을 파악할 수 있도록 값을 보여준다. 두 번째는 어플리케이션별 설정을 확인하고 변경할 때에 현재 상황을 실시간으로 보여주는 것이다. 이는 사용자가 스위치 조작을 통해 값을 변경할 때 set 쿼리가 완료된 후 바로 get 쿼리를 보내 실시간 수치가 반영되어 정확한 값을 보여줄 수 있도록 한다.

모든 경우에 대해 모바일 환경의 특성상 인터넷 상태가 좋지 않을 수 있다. 따라서 팝업 창에서는 기본 메시지 형태가 있고, 서버와의 연결에 성공하여 정상적으로 값을 얻어 온 경우에는 기본 메시지 아래에 추가로 내용을 붙여 팝업 창을 갱신한다. 어플리케이션별 설정을 보는 화면에서는 기본적으로 각 항목에 대한 개략적인 설명을 크게 표시해 놓으며, 역시 정상적으로 값을 얻어 온 경우에만 이 아래에 공간을 확보하여 그 내용을 보여준다.

Ⅳ. 연구 결과 및 분석

4.1 연구 결과

통계를 활용하는 기능 및 번역을 추가하고 새로운 Material 디자인을 사용하여 이전과 달라진 부분을 찾을 수 있다. 그림 8과 9는 이전 버전과 비교한 것이다.

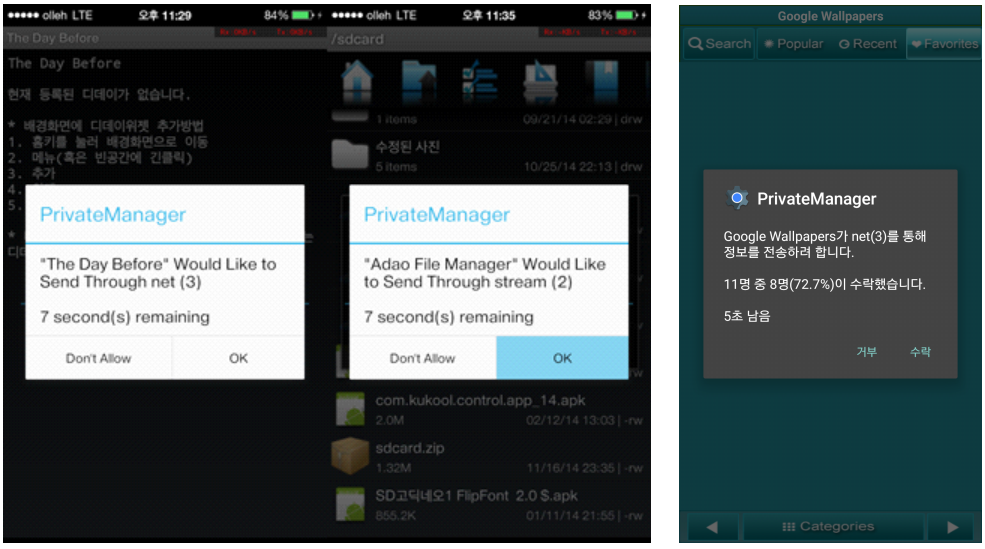


그림 8 팝업 창의 이전 모습 및 번역과 통계 기능을 추가한 현재 모습

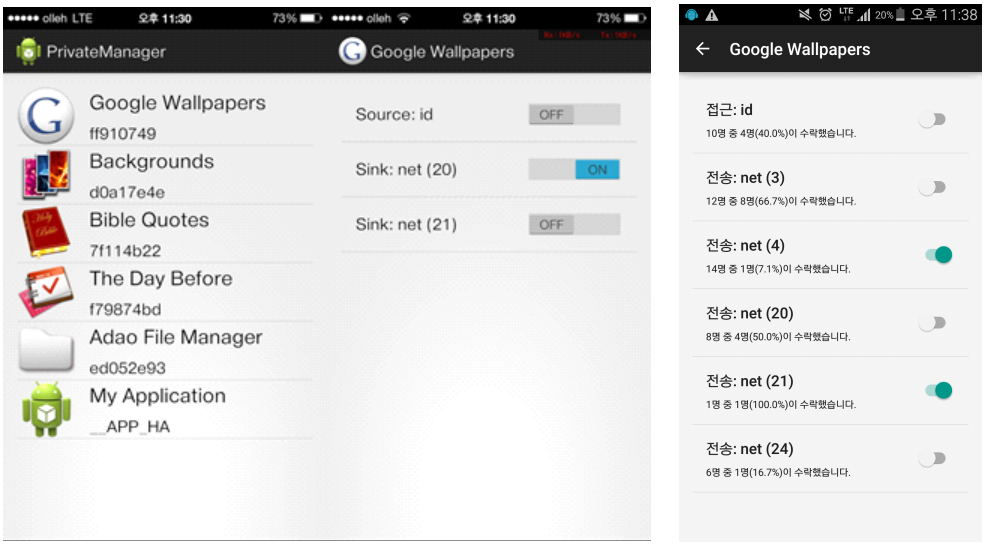


그림 9 설정 창의 이전 모습 및 번역과 통계 기능을 추가한 현재 모습

모바일 환경의 특성상 인터넷 환경이 좋지 않을 수 있는데, 이럴 때에도 기존의 레이아웃 느낌을 그대로 가져갈 수 있도록 설계하여 큰 이질감이 느껴지지 않도록 하였다. 그림 10은 네트워크 상황에 따른 화면 구성 변경을 나타낸 것이다.

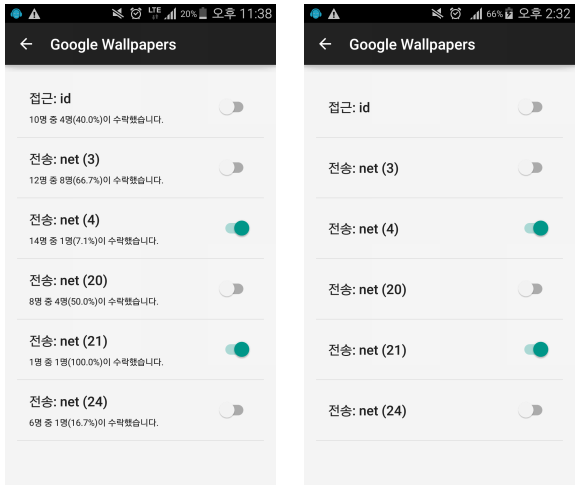


그림 10 통계 서버에 연결할 수 있을 때와 없을 때의 차이

4.2 한계점 및 발전 가능성

본 연구의 한계점으로는 ScanDal을 이용해 분석된 지 얼마 되지 않은 어플리케이션들에 대해서는 통계 자료가 존재할 수 없다는 점이 있다. 따라서 누군가는 최초로 실행해보며 안전한 행위인지를 검증해가며 권한을 조정해 주어야 한다.

이러한 한계점을 해결하기 위해서 고안한 개선 방법으로는, 관리자를 두어 새로운 어플리케이션에 대한 테스트를 해 보도록 하거나, 위험한 서버들의 리스트를 정해 놓고 이에 대한 인터넷 작업은 자동으로 취소하는 방법을 사용할 수 있을 것이다. 또한 제목이나 아이콘 등으로부터 자연어 처리를 통해 어플리케이션의 기본 목적을 파악하고, 관련이 없는 항목에 대해서는 자동으로 일부 거부 처리를 하는 방법을 도입할 수 있을 것이다.

Ⅴ. 결론 및 토의

본 연구에서는 안드로이드 어플리케이션을 정적으로 분석하여 개인정보 유출 위험을 줄이는 PrivateManager 프로젝트의 각 동작에 통계적 분석 기능을 추가하여 사용자들이 특정 기능에 대해 신뢰할 수 있는 근거를 만들고자 하였다.

안드로이드에서 지금까지는 어플리케이션의 설치를 위해 수동적으로 모든 권한을 수락할 수밖에 없었던 상황이었지만, PrivateManager 프로젝트로 인해 특정 권한이 필요할 때에 능동적으로 수락과 거부를 할 수 있도록 되었기에 어플리케이션의 목적과 전혀 관계없이 수집되는 항목들에 대해서 많은 사용자들이 거부를 할 수 있게 되었다. 다만 미처 고려하지 못한 사용자들이 있을 수 있으므로, 대부분의 사용자의 경향성을 알려 주기 위해서 서버를 사용해 통계 자료를 수집하도록 하였고, 이를 통해 개인정보 보호 측면에서 더 좋은 효과를 나타낼 수 있도록 하였다.

다만 출시되지 얼마 되지 않거나 새로 업데이트되는 등의 이유로 충분한 통계 자료가 존재하지 않을 수 있다. 이럴 경우를 대비하여 초기에 테스트를 수동으로 해 주거나, 위험 서버 리스트를 두어 이를 자동으로 차단하거나, 자연어 처리를 통해 어플리케이션의 카테고리, 제목 등과 관련 권한을 분석하여 요청하는 기능이 목적과 관련이 크지 않으면 자동적으로 거부하는 등의 시스템을 도입하면 더욱 효율적으로 개인정보를 보호할 수 있을 것이다.

Ⅵ. 참고 문헌

[1] 한국인터넷진흥원 (2013), “2013년 인터넷이용실태조사 결과 발표”, Web site: http://isis.kisa.or.kr/board/?pageId=060200&bbsId=3&itemId=801

[2] 한국인터넷진흥원 (2013), “2012년 하반기 스마트폰이용실태조사 결과발표”, Web site: http://isis.kisa.or.kr/board/index.jsp?pageId=060200&bbsId=3&itemId=799

[3] 동아일보 (2011), “삼성 갤럭시S ‘거울’앱 속에 당신의 정보 몰래 보는 ‘눈’이 있다”, Web site: http://news.donga.com/3/all/20111205/42360234/1

[4] MBC (2014), “[단독] ’손전등 앱’ 개인정보 훔쳐가…유심칩 번호까지 유출”, Web site: http://imnews.imbc.com/replay/2014/nwdesk/article/3553208_13490.html

[5] 전자신문 (2015), “삼성전자 ‘스마트 매니저‘ 앱 권한 보니 "발신전화를 가로채기 할 수 있다"”, Web site: http://www.etnews.com/20151118000374

[6] 박현민, 이재범 (2014), “모바일 어플리케이션의 정적 분석을 통한 개인정보 유출 차단”, 경기과학고등학교.

[7] 연합뉴스 (2014), “한국은 세계 1위 안드로이드 공화국…93.4%가 사용”, Web site: http://www.yonhapnews.co.kr/it/2014/01/19/2405000000AKR20140119057700017.HTML

[8] William Enck, Peter Gilbert, Byung-gon Chun, Landon P. Cox, Jaeyeon Jung, Patrick McDaniel, and Anmol N. Sheth. (2010) “TaintDroid: An Information-Flow Tracking System for Realtime Privacy Monitoring on Smartphone

s", Symposium on Operating Systems Design and Implementation (OSDI), pp.11-12.

[9] Ajinkya Saswade (2014), "Decompile and Secure android apk", Web site: http://decompileandsecureapk.wordpress.com/2014/05/10/decompile-and-secure-android-apk/

[10] 윤용호 (2013), "안드로이드 앱에서 개인정보 누출을 검출하는 정적분석기 설계", 공학석사 학위논문, 서울대학교.

Summary

Controlling personal information leakage of android application using ScanDal analysis result

// TODO

감 사 의 글

논문의 지도를 맡아주신 전현석 선생님께 가장 먼저 감사의 말씀을 드립니다. 또한 정적 분석을 잘 사용할 수 있도록 도와주신 프로그래밍 연구실의 윤용호 조교님과 주제에 큰 관심을 보여주신 이광근 교수님께도 감사의 말씀을 드립니다. 3년간 함께 연구를 진행하며 굉장히 많은 코드 기여를 한 이재범 학생에게도 감사의 뜻을 전합니다.