

# Demo: DroidNet - An Android Permission Control Recommendation System Based on Crowdsourcing

Pulkit Rustgi Carol Fung

Department of Computer Science, Virginia Commonwealth University, Richmond, VA, USA  
{rustgip, cfung}@vcu.edu

**Abstract**—Mobile and web application security, particularly the areas of data privacy, has raised much concerns from the public in recent years. Most applications, or apps for short, are installed without disclosing full information to users and clearly stating what the application has access to, which often raises concern when users become aware of unnecessary information being collected. Unfortunately, most users have little to no technical expertise in regards to what permissions should be turned on and can only rely on their intuition and past experiences to make relatively uninformed decisions. To solve this problem, we developed DroidNet, which is a crowd-sourced Android recommendation tool and framework. DroidNet alleviates privacy concerns and presents users with high confidence permission control recommendations based on the decision from expert users who are using the same apps. This paper explains the general framework, principles, and model behind DroidNet while also providing an experimental setup design which shows the effectiveness and necessity for such a tool.

**Keywords**—Privacy, Permission, Android, Smartphone, Recommendation, App, Application, Crowdsourcing, Data mining

## I. INTRODUCTION

The current permission management for privacy control on the Android OS heavily depends on users. Users have to decide what permissions an application can access, before or after an application is installed. Applications are free to request users to give access to whatever resources they claim to need. Permissions requested by these apps are often displayed to users through a dialog window with little information disclosed to users. This has proved to be ineffective since users may not entirely understand what resource an application is requesting access and/or they have no time to look into what consequence it may cause to accept a permission request. Only a small percentage (3%) of users pay attention and make correct answers to permission granting questions [1].

To help users alleviate their privacy concerns, we designed and developed a tool called DroidNet, which is a successor to the previously proposed RecDroid [3] and its implementation [2]. DroidNet is a permission control system that exams users' app permission decisions and compare them with recommended decisions. When mismatches are found, the DroidNet raises alerts and notify users so that they can revise their decisions. The recommended permission decisions are crowdsourced based on expert users who use the same apps [4].

DroidNet allows users to easily view requested permissions as well as manage them. The system framework provides the following major functionalities:

978-3-903176-15-7 © 2019 IFIP

- A front-end user interface and launcher pages to indicate which apps DroidNet is currently monitoring. This functionality is directly interacting with users.
- A back-end engine to collect each user's installed application and its corresponding permissions and responses, from which recommendations are made on whether a permission should be granted or not.
- A recommendation system and display to guide users with permission granting decisions done by serving users with recommendations from expert users on the DroidNet network.
- A user-based ranking algorithm to rank security risks of each mobile application as well as their permissions.

In the rest of this paper, we will describe the architecture design of the system and then provide use cases on how to use Droidnet.

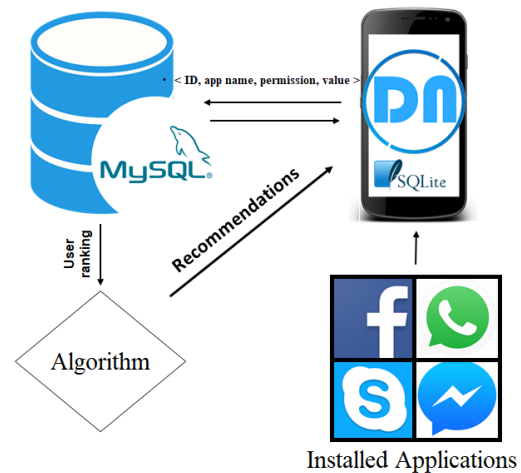


Figure 1: DroidNet architecture

## II. ARCHITECTURE DESIGN AND IMPLEMENTATION

As shown in Figure 1, DroidNet consists of a client-side DroidNet app, a server-side database and a permission recommendation algorithm. The major difference between this work and our previous implementation [2] is that the front-end implementation is realized completely through an app without any OS patch, which is a huge leap towards the deployability of the system.

### A. DroidNet App

The main purpose of DroidNet app is to provide an integrated UI that allows users to quickly and efficiently view



Figure 2: Permissions portal

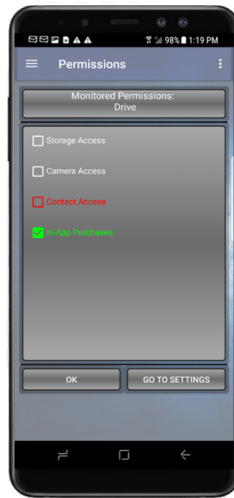


Figure 3: Permissions display



Figure 4: Recommendation display

applications and their requested permissions while also giving them quick access to potentially change them if they so desire. In addition, DroidNet app logs every applications requested permissions and then uploads what decision the user has in place (grant or deny) for them on a server.

### B. Databases

User data collection is done through the phones built in SQLite database as well as an online MySQL based database. Each client-side installation will come with a SQLite database that stores local information of permission decisions which will be synced with server. The server-side database is implemented using a MySQL hosted on GoDaddy web service. the purpose of the database is to store information about users' permission decisions as well as recommended permission decisions after the crowdsourcing recommendation algorithm.

### C. Back-end Services and Recommendation Algorithm

In order to identify when a user makes changes to an application, DroidNet employs a synchronization process that examines the online database where the users data is stored and compares it to the local SQLite database on the device.

A recommendation algorithm is responsible for providing the user with a reliable recommendation regarding whether a permission is necessary. Users receive up-to-date advice through notifications on what permission should be allowed for which application. The recommendation algorithm is established based on a crowdsourcing approach, where the permission control decisions from expert users using the same apps will be collected and aggregated and recommended to other users. Start from a set of seed expert users, the system searches for other expert users based on the similarity of their permission decisions [3], [4].

## III. A USER CASE STUDY

### A. User Interaction

In this section we provide a case study on how a user can use DroidNet to manage permission control. Our DroidNet app

can be found in Google play store and is available for free download. To help with understanding, we will use the apps "Drive" (Google Drive) and "Smart Switch" as example apps in our case study.

When a user launches the DroidNet app, the default permission page will show up as shown in Figure 2, where a list of installed apps are listed. If a user selects an app from the list, a set of its requested permissions will be shown as in Figure 3 and the user can select some of them to be monitored resources. A Permission labeled with green or red color means the permission decision does or does not match DroidNet recommendations, respectively. For every installed app that DroidNet is monitoring, users can use the DroidNet permission control UI to view each apps installed permissions, and if they so choose modify them through the Android OS settings page. The user can also choose to go to the notification center to check notifications about newly discovered permission mismatches, as seen in the screenshot Figure 4.

## IV. REQUIRED TOOLS AND DEVICES

The live demonstration will utilize one laptop as well as up to 3 Android phones ranging from the Nexus 4 to the Galaxy S8. We will potentially require Wi-Fi access to provide the best user experience, as well as a presentation table. If possible, a larger screen that is able to display HDMI-based input would also help.

## REFERENCES

- [1] What is the price of free? <https://www.cam.ac.uk/research/news/what-is-the-price-of-free>.
- [2] B. Rashidi, C. Fung, G. Bond, S. Jackson, M. Pare, and T. Vu. RecDroid: An Android Resource Access Permission Recommendation System. In *The ACM International Symposium on Mobile Ad Hoc Networking and Computing (ACM MobiHoc 2015)*, 2015.
- [3] B. Rashidi, C. Fung, and T. Vu. Dude, ask the experts!: Android resource access permission recommendation with recdroid. In *Integrated Network Management (IM), 2015 IFIP/IEEE International Symposium on*, pages 296–304.
- [4] B. Rashidi, C. Fung, and T. Vu. Recdroid: A resource access permission control portal and recommendation service for smartphone users. In *Proc. of the ACM MobiCom Workshop on Security and Privacy in Mobile Environments (SPME '14), Maui, Hawaii, USA*, pages 13–18. ACM, September.