International Journal of Scientific and Technical Advancements
ISSN: 2454-1532

Detecting Malicious Apps from Play Store

Akshay Bhardwaj [1], A.J. Singh[2,#]
[1] Department of Computer Science, Himachal Pradesh University, Himachal Pradesh, India-171003
[2] Department of Computer Science, Himachal Pradesh University, Himachal Pradesh, India-171003
[#]Email: akshay117@gmail.com, aj.hpucs@gmail.com

Abstract—With the advent of Android as the most popular mobile operating system more and more users are adding into its realm. But being an open platform it is not without its fair share of problems, the deadliest of which stem from the play store. We try through this paper to devise a mechanism that can help not only the experts but even the naïve users to find out how to know if an app is safe. We present a classification system for knowing this.

Keywords— Android;security;malicious apps;play store;classification.

I. INTRODUCTION

Society is ending up increasingly innovatively progressed with each passing year. In 2014, 1 out of 5 individuals on the planet had an advanced mobile phone (Heggestruen). The Android Operating System represents 84.1% in overall advanced mobile phone piece in pie in the second quarter of 2014 (IDC). The ubiquity of Android OS makes it an alluring focus for nefarious hackers. The effect of one malevolent Android app is sweeping, putting more portable clients in danger contrasted with different OS. There is a 388% ascent in malignant apps in Android showcase from 2011 to 2013 (Gendron). Such a tremendous increment is because in way the larger part of portable clients utilizes Android OS, luring nefarious hackers to it. The principle Android app commercial center, Play Store, likewise doesn't authorize strictness over submitted apps. In spite in fact Android gadgets just permit the establishment of marked apps, this measure is circumvented by essentially utilizing a self-marked testament (Android). Such tolerant approach permits nefarious hackers to circulate their malevolent apps to people in general considerably more effectively.

II. CURRENT SCENARIO AND THE PROBLEM

There are a wide range of sorts of noxious apps. Malevolent apps take on the appearance of true blue apps are one in more noticeable versatile dangers in 2014 (F-Secure). Here is a regular situation in which a malevolent disguising app is made. Right off the bat, the nefarious hacker downloads a genuine app from the Android advertise. Furthermore, the nefarious hacker figures out the true blue app, includes a noxious payload and solicitations for more consents to encourage the assault. The nefarious hacker may likewise refresh the adaptation number. In conclusion, the nefarious hacker will repackage app and distribute it back to people in general. At the point when a client introduces the repackaged app supposing it is the most recent adaptation in honest to goodness app, the nefarious hacker will have the capacity to do malevolent assaults on the client utilizing the extra authorizations allowed. Some basic assaults include: taking secret information, for example, messages and contact records utilizing the "READ_SMS" and "READ_CONTACTS" consents separately and taking cash by sending SMS or calling paid rate numbers utilizing the "SEND_SMS" and "CALL_PHONE" authorizations individually. The effect of such noxious apps is exceptionally critical as it allows nefarious hackers to make full utilization in rundown of authorizations to encourage their assaults (Sophos). Portable clients, particularly non-IT smart clients, are falling prey to such pernicious apps because over dependence on the Android advertise or the notoriety or fame in apps. Most tech specialists suggest clients just download apps from the official Play Store, Play Store since apps from other obscure sources are perilous (Marchant). Despite the fact this guidance is right, it can delude clients, especially non-IT clever ones, into feeling the apps from the official Play Store will dependably be protected. There have been situations where noxious apps were effectively distributed to Play Store and Play Store (Paganini). In this way clients still must be ready while downloading apps from the Play Store. A decent case of a legitimate and mainstream app is the diversion

Akshay Bhardwaj and A J Singh, "Detecting Malicious Apps from Play Store," *International Journal of Scientific and Technical Advancements*, Volume 4, Issue 1, pp. 35-42, 2018.

"Irate Bird". Because of its prominence, there have been numerous pernicious apps taking on the appearance in diversion "Irate Bird". In this way, a famous app has been played by numerous clients does not really liken to a completely safe app in light in fact there exist malevolent repackaged renditions in first app. Truth be told, clients ought to be considerably more cautious while downloading famous apps as they have a tendency to pull in nefarious hackers. Our goal is to give an answer for non-IT astute versatile clients from falling prey to noxious portable apps have been expanding in the course of recent years. This goal was not completely met by some other existing strategies or procedures proposed by different scientists. For instance, the work done by (Cerbo et al.) is more particular and limited. They just broke down SMS related operations accomplished by Java APIs. What we need to accomplish is to identify each classification of malevolent exercises, not simply SMS-related issue, e.g. making telephone calls to paid numbers or taking client's close to home data. Their approach is viable in distinguishing any noxious exercises emerging from SMS-related operations. Our approach enables us to have a free app won't be influenced by any adjustment in the gadget equipment/programming in this circumstance. Lei et al. utilize an authorization based behavioral foot printing plan and heuristics-based sifting plan to recognize noxious apps. Their plan considers each app with the consents can have conceivable malignant action. For instance, apps require "SEND_SMS" consent will be restricted by their plan. Be as it may, this will cause issue with informing app, for example, WhatsApp. The inquiry is the manner by which to choose whether it is a genuine app requiring "SEND_SMS" authorization. We utilized app's classification to deal with this issue. Lei's strategy is significantly more tedious and asset escalated as they filter the app to discover how the app acts, what APIs the app calls and what work parameters are set by the app et cetera.

III. Our Proposal

Our revelation of utilizing the app's classification as a component in discovery criteria implies our framework is as lightweight as conceivable without doing such escalated examines likes their plan in (Lei et al) (Zhou et al) characterize the apps into high hazard, medium hazard and okay utilizing an arrangement of examination modules. So they can organize to put more exertion on assessing the high hazard apps. We additionally characterize the apps into high/medium/generally safe with the goal ideally the client can comprehend the level of effect and potential harm the app is equipped for causing. In any case, their identification strategy is not quite the same as our own. They dissect the app's code marks and furthermore figured out DVM bytecode. So indeed, their strategy additionally winds up noticeably out of date. Time and asset may be of worry as they expresses it processes 118,318 aggregate apps in under 4 days. Yet, will the client still have the capacity to utilize his/her telephone with such program running? A perfect arrangement is to make a security app recognizes malignant apps in light of consents asked for by apps being introduced on gadgets. A conceivable path is to make a boycott of possibly unsafe consents, for example, the SEND_SMS" authorization, which when conceded enables the app to send SMS messages to subjective beneficiaries, including paid rate numbers. At the point when an app is identified asking for any in consents in the boycott, it will raise a caution and mark the app as hazardous. Notwithstanding, there are circumstances where the "SEND_SMS" consent isn't perilous. Informing apps will require the "SEND_SMS" consent with a specific end goal to work. We should have the capacity to decide when asked for consents are authentic and when they are malevolent.

IV. Other Recommendations

In the following area, we portray the philosophy used to answer this inquiry.

The Working in Classification

This area exhibits an investigation and proposes our approach of taking care in issue.

A. Inspecting of portable apps

Keeping in mind the end goal to make a security app distinguishes noxious apps in view of asked for consents, we led an investigation on portable apps' asked for authorizations. This enabled us to pick up a more profound comprehension of which authorizations are generally asked for by apps. There are a sum of 25 classifications of utilizations in the Android Market, Play Store. They are "Books and Reference", "Business", "Funnies", "Correspondence", "Training", "Amusement", "Back", "Diversions", "Wellbeing and Fitness", "Libraries and Demo", "Way of life", "Media and Video", "Restorative", "Music and Audio", "News and Magazines", "Personalization", "Photography", "Efficiency", "Shopping", "Social", "Games", "Instruments", "Transportation", "Travel and Local" and "Climate". Every class is part amongst free and paid apps. In this manner to

Akshay Bhardwaj and A J Singh, "Detecting Malicious Apps from Play Store," *International Journal of Scientific and Technical Advancements*, Volume 4, Issue 1, pp. 35-42, 2018.

guarantee our investigation covers all cases, the asked for consents of 50 free and 50 paid utilizations of every class were gathered. In outline, the aggregate example measure in our investigation was 2,500 apps ((50+50)*25). There are 261 distinct authorizations at the season of composing and they are partitioned among 14 consent gatherings, "In-app buys", "Gadget and app history", "Cell information settings", "Character", "Contacts/Calendar", "Area", "SMS", "Telephone", "Photograph/Media/File", "Camera/Microphone", "Wi-Fi association", "Bluetooth association", "Gadget ID and Call data" and "Other". The recovered authorizations are merged into a table with the separate groupings for every class as appeared in Table 1.1. The greatest consider is 50 we considered 50 apps in every classification. As appeared in Table 1.1, the normal authorizations for an app in the "Books and Reference" classification are "Read the substance of your USB stockpiling", "Alter or erase the substance of your USB stockpiling" from the "Photograph/Media/File" gathering and "Full system get to", "View organize associations", "Keep gadget from dozing" thefrom "Other" gathering.

The two asked for consents in the "Photograph/Media/File" gather enable the app to peruse and spare information, for example, books and references to the telephone. "Full system access" and "View arrange associations" authorizations enable the app to get to the Internet to peruse and recover books and references. "Keep gadget from dozing" consent keeps the gadget screen from darkening or killing because of latency on the screen in light in fact the client may read without touching the screen for quite a while. In this way, these asked for authorizations are sensible and honest to goodness for a "Books and Reference" app. An app will be profoundly suspicious in the event it demands consents with zero checks or authorizations don't exist in Table 1.1. Note the "Other" consent gather contains more than a hundred authorizations. For quickness, we overlooked consents in this classification were not asked for by any app. Subsequent to dissecting every one in 25 tables from their individual classifications, we reasoned the most normally asked for authorizations over all classifications are "Read the substance of your USB stockpiling", "Change or erase the substance of your USB stockpiling" from "Photograph/Media/File" gathering and "Full system get to", "View arrange associations" from the "Other" gathering. This is on account of most apps require Internet and edit access to the gadget stockpiling to spare information onto the telephone. We delivered a reference chart for the information in each table by plotting the consent mean something negative for the diverse authorization bunches with bars speaking to the consents asked for by free and paid apps. The chart gives a visual portrayal enables us to watch any contrast amongst free and paid utilizations of every classification as appeared in Fig. 1.1. Indeed, the most extreme tally is 50 for every rendition.

From Fig. 1.1, we watch the example of asked for authorizations with the expectation of complimentary apps intently takes after the example of asked for consents for paid apps. In the wake of investigating every one in 25 reference diagrams from their individual classifications, we infer the consents asked for both free and paid apps from a similar class by and large have a similar example. Notwithstanding, we watched some striking things.

The "Play Store permit check" authorization seemed more in paid apps rather than in free apps, as paid apps require this consent to check if the client has made any installment. Just few free apps made solicitations for this consent. Free apps have a tendency to insert notices as a wellspring of wage for engineers. Therefore, extra consents are required to encourage the use of promotions in the free apps.

Paid apps created by business organizations or experts tend to better comprehend the idea of authorizations and hence ask for consents shrewdly, which prompt less asked for consents. A learner engineer may ask for excess consents because of vulnerability over the need of different authorizations and we watched this in a few free apps.

B. Connection between every app's class and consents

With the required information on the consents of various classes accumulated, we would then be able to endeavor to discover contrasts in authorizations asked for by apps in various classifications. As the information gathered includes both free and paid apps, they will be gathered and utilized into a single unit in our resulting investigation. We plot consent means something negative for authorization bunches with each line shading speaking to a classification of authorizations in Fig. 1.2. The most extreme check is 100 since we've summed up means both free and paid apps. Unmistakably consents in both the "Photograph/Media/File" and "Other" classifications are regularly asked for each in 25 classifications of utilizations. This outcome is in accordance with the conclusion we attracted the past segment, where we watched the most normally asked for authorizations over all classifications are "Read the substance of your USB stockpiling", "Adjust or erase the substance of your USB stockpiling" from

Akshay Bhardwaj and A J Singh, “Detecting Malicious Apps from Play Store,” *International Journal of Scientific and Technical Advancements*, Volume 4, Issue 1, pp. 35-42, 2018.

"Photograph/Media/File" gathering and "Full system get to", "View organize associations" from the "Other" gathering. It can be watched there are near zero consent mean each in 25 classifications for "Cell information settings" and "Bluetooth association" gatherings, which is because of an adjustment in the authorization approach by Android. These consents have been reassigned - both "BLUETOOTH" and "BLUETOOTH_ADMIN" authorizations are currently under the "Other" gathering.

Aside from the focuses over, each in 25 classifications has a particular example of asked for authorizations as showed by each line design in the line chart. Review the "Other" gathering envelops over a hundred authorizations. Accordingly to additionally demonstrate the distinctive examples between each in 25 classifications, a more profound examination is required. We analyze the asked for consents of 25 classes of uses for the "Other" gathering, and we think this will yield helpful outcomes. A line chart is made by plotting consent means something negative for the distinctive authorization bunches with each line shading speaking to the consents from every class of uses as appeared in Fig.1.3. By and by, the most extreme check is 100 because of accumulation over free and paid apps. Everyone in lines are high on the left side on the ground. The initial two authorizations are "Full system access" and "View arrange associations", which are regularly asked for over all classifications: this outcome has additionally strengthened the perception. Distinctive classes have diverse pinnacles and examples in the diagram. From both line charts, we infer there is a remarkable example of asked for authorizations for each in 25 classifications. Among authorizations, there are no two lines cover each other precisely. Along these lines, each example can be utilized to distinguish a specific class. At long last, the issue brought beforehand up in this segment on the best way to decide when authorization is true blue or pernicious would now be able to be comprehended. Every classification has a specific example, so the example can be utilized to decide whether the consent is pernicious or not in unique situation. Furthermore, using these examples will guarantee a superior recognition rate and furthermore less false positives contrasted with utilizing one general channel, for example, the general boycott strategy, for each.

On the off chance an app demands consent where its classification's line in the figure tops, this demand will be regarded real. On the off chance the app demands authorization where the line is most minimal in the figure then the app is exceedingly suspicious as this is strange conduct.

C. Risk level channel: Each example will beutilized as the gauge for its separate classification and we tailor a danger level channel particularly for class. There are 3 risk levels for the channel: "Safe", "Mellow" and "Threat". A survey for each in authorizations found in the separate examples is performed to additionally distribute them to the proper danger levels. Authorizations in the "Protected" danger level are those are required to complete an app's expected center functionalities. For example, an informing app won't be hailed as possibly malignant for asking for the "SEND_SMS" consent. Consents in the "Gentle" danger level are those may not be fundamental for the app's essential functionalities and may raise protection issues, for example, recovering data about the client and gadget. In any case, the potential for malignant movement is still low. A case in this class is an app recovers data for an installed outsider ad benefit. Authorizations in the "Risk" danger level are those can cause some type of harm/misfortune to the telephone or/and the client and are not required for the center usefulness in app. For instance, the "CALL_PHONE" consent enables an app to make telephone calls without client intercession. An app not in the "Correspondence" class demands this consent might take cash by calling paid-rate numbers. Authorizations are anomalous, for example, those with zero include or those not Table 1.1 above, are likewise in the "Risk" danger level as a matter of course as they show malignant movement.

The authorizations with their particular danger levels are then examined into Table 1.1I. As specified, any authorization not showed inside Table 1.1 is as a matter of course in the "Risk" danger level.

At the point when an app is being filtered for vindictive plan, the risk level table in individual app's class is utilized. The scanner will look into each in app' asked for authorizations and check the comparing mapped risk level in Table 1.1. In the event there is a deviation from the acknowledged standard, a ready will be activated, requesting therapeutic activity, for example, the expulsion in conceivably vindictive app.

Akshay Bhardwaj and A J Singh, “Detecting Malicious Apps from Play Store,” *International Journal of Scientific and Technical Advancements*, Volume 4, Issue 1, pp. 35-42, 2018.

Permissions group	Individual permission	Requested count (Free App)	Requested count by groups (Free App)	Requested count (Paid App)	Requested count by groups (Paid App)
In-app purchases	Ask to make purchases	12	12	12	12
Device & app history	Retrieve running apps	6	6	8	8
	Read sensitive log data	4		2	
	Read your web bookmarks and history	0		0	
	Retrieve system internal state	0		0	
Cellular data settings	Change/Intercept network settings and traffic	0	0	0	0
Identity	Find accounts on the device	10	10	8	8
	Add or remove accounts	2		0	
	Read your own contact card	0		0	
	Modify your own contact card	0		0	
Contacts/ Calendar	Read your contacts	2	2	0	0
	Modify your contacts	0		0	
	Read calendar events plus confidential information	0		0	
	Add or modify calendar events and send email to guests without owners' knowledge	0		0	
Location	Approximate location (network-based)	8	8	8	10
	Precise location (GPS and network-based)	6		10	
	Access extra location provider commands	0		0	
SMS	Send SMS messages; this may cost you money	0	0	0	0
	Receive text messages (SMS)	0		0	
	Read your text messages (SMS or MMS)	0		0	
	Receive text messages (MMS, picture or video message)	0		0	
	Edit your text messages (SMS or MMS)	0		0	
	Receive text messages (WAP)	0		0	
Phone	Read call log	2	2	0	2
	Directly call phone numbers; this may cost you money	0		2	
	Reroute outgoing calls	0		0	
	Write call log	0		0	
	Modify phone state	0		0	
	Make calls without your intervention	0		0	
Photo/ Media/File	Read the contents of your USB storage	40	40	44	44
	Modify or delete the contents of your USB storage	40		42	
	Access USB storage filesystem	0		0	
	Format external storage	0		0	
	Mount or unmount external storage	0		0	
Camera/ Microphone	Take pictures and videos	4	4	2	2
	Record audio	0		0	
	Record video	0		0	
Wi-Fi connection	View Wi-Fi connections and names of connected devices	14	14	14	14
Bluetooth connection	Can control Bluetooth on your device, and broadcast to or get information of nearby devices	0	0	0	0
Device ID & Call info	Read phone status and identity	24	24	18	18
Other	Full network access	46	46	48	48
	View network connections	44		46	
	Prevent device from sleeping	26		14	
	Receive data from Internet	12		6	
	Control vibration	10		12	
	Run at startup	8		2	
	Google Play license check	6		20	
	Modify system settings	6		2	
	Install shortcuts	6		2	
	Uninstall shortcuts	4		0	
	Read Google service configuration	4		0	
	Send sticky broadcast	4		0	
	Control system backup and restore	2		2	
	Create accounts and set passwords	2		0	
	Use accounts on the device	2		0	
	Toggle sync on and off	2		0	
	Draw over other apps	0		2	
	Connect and disconnect from Wi-Fi	0		2	
	Bind to an accessibility service	0		2	
	Allow Wi-Fi Multicast reception	0		2	
	Set wallpaper	0		2	

Table1.1.Table of top 50 free and also paid "books & reference" apps

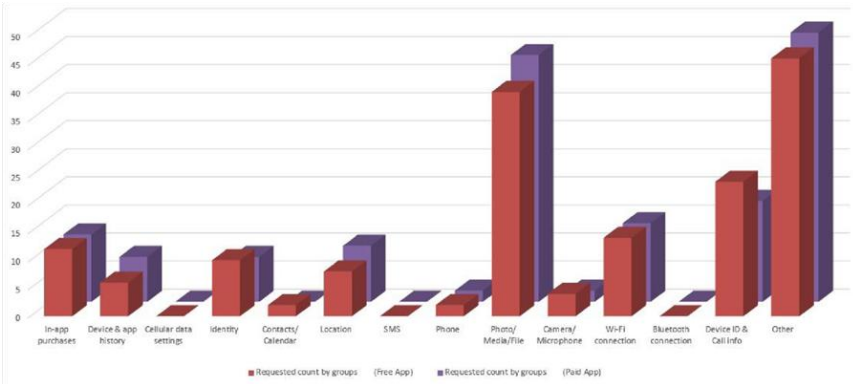

Figure 1.1. Top 50 free and paid "Books & Reference" Apps

ISSN: 2454-1532

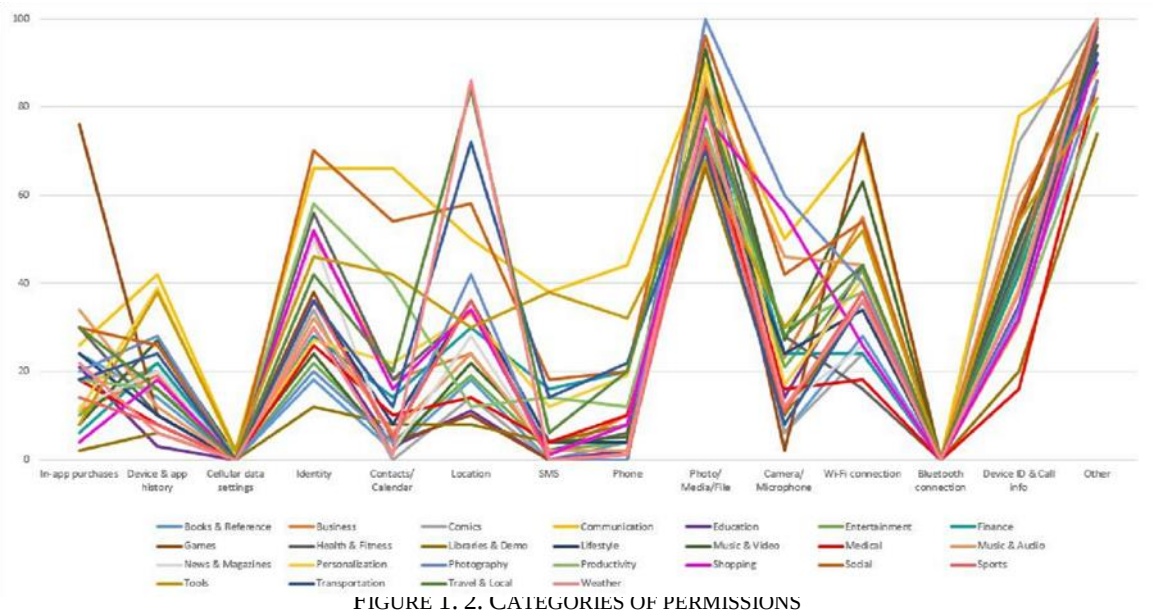

FIGURE 1. 2. CATEGORIES OF PERMISSIONS

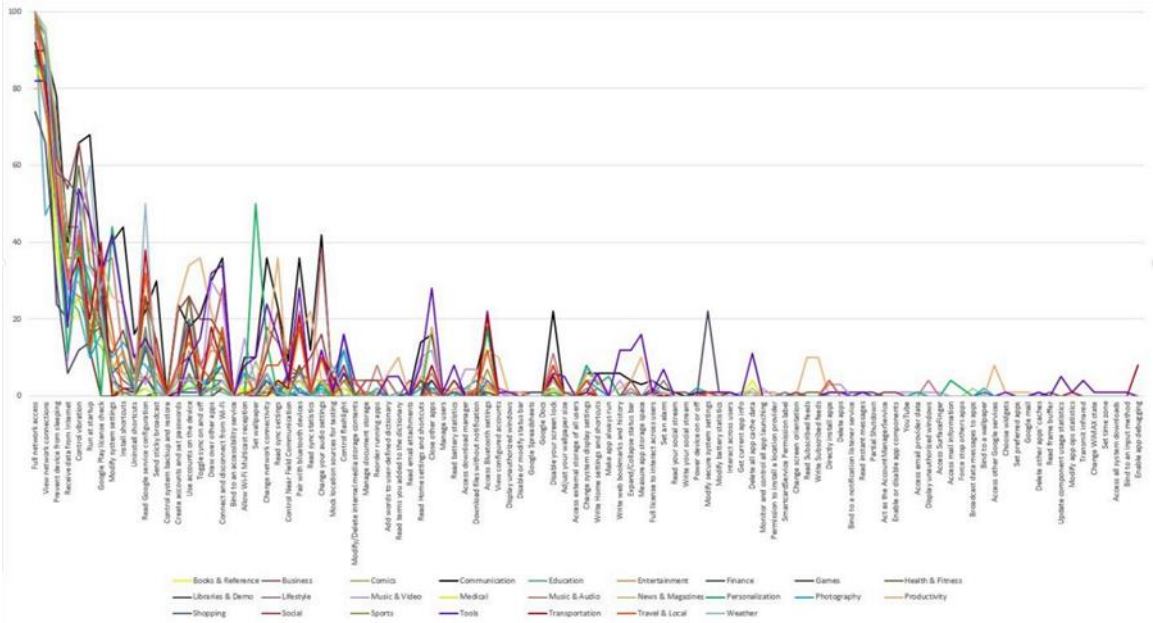

Figure 1.3. 25 permissions categories for "Other" group only

Akshay Bhardwaj and A J Singh, "Detecting Malicious Apps from Play Store," *International Journal of Scientific and Technical Advancements*, Volume 4, Issue 1, pp. 35-42, 2018.

Threat Level	Permissions group	Individuals permission	Purpose
Safe	In-app purchases	Ask to make purchases	To allow in-app purchases
	Location	Approximate location (network-based)	To access approximate location derived from network location sources such as cell towers and Wi-Fi
		Precise location (GPS and network-based)	To access precise location from location sources such as GPS, cell towers, and Wi-Fi
	Photo/ Media/File	Test access to protected storage	To read from external storage, such as SD card
		Modify or delete the contents of your USB storage	To write/delete to external storage, such as SD card
	Wi-Fi connection	View Wi-Fi connections and names of connected devices	To check the state of connection before accessing the internet
	Device ID & Call info	Read phone status and identity	To read the phone state by accessing the device identifiers (to know if a call is in progress)
	Other	Full network access	To open network sockets to access the Internet
		View network connections	To access information about networks to check the state of network before connecting to the Internet
		Control vibration	To control the vibrate function of the phone
		Prevent device from sleeping	To keep device and screen active without requiring the user to tap it every minute
		Modify system settings	To read or write the system settings which are common for personalization applications
		Run at startup	To run the application every time upon the phone's startup which is required by some personalized launcher
		Set wallpaper	To personalize the wallpaper
		Install shortcuts	To install shortcuts in homescreen
		Close other apps	To kill the background process of other apps (use to kill apps that cause conflicts when personalizing)
		Connect and disconnect from Wi-Fi	To change Wi-Fi connectivity state
		Access Bluetooth settings	To discover and pair bluetooth devices
		Write Home settings and shortcuts	To write settings and shortcuts in homescreen
		Make app always run	To make the app's activities always active
Mild	Device & app history	Retrieve running apps	To get information about the currently or recently running tasks which will reveal what apps are running on the device
		Read sensitive log data	To read the low-level system log files which include the log files of other applications and might contain sensitive and personal data
		Read your web bookmarks and history	To read the user's browsing history and bookmarks
	Identity	Find accounts on the device	To access the list of accounts in the Accounts Service to choose for use with the app for authentication purposes
		Read your own contact card	To read the user's personal profile data to use as default values or profile picture for some apps
	Contacts/ Calendar	Read your contacts	To read the user's contact lists
		Read calendar events plus confidential information	To read the user's calendar information
	SMS	Read your text messages (SMS or MMS)	To read SMS messages for facilitating the checking of special codes sent by the app to the device
	Phone	Read call log	To read the user's call log, the permission is implicitly granted by "Read your contacts"
	Camera/ Microphone	Take pictures and videos	To access the camera of the device which can be use to take photos to use as wallpaper for personalization
		Record audio	To record audio which can be use in voice search functions provided by some personalized interface
	Other	Change system display settings	To modify the current configuration such as locale
		Receive data from Internet	To accept messages sent by the app's service
		Change network connectivitiy	To change network connectivity state
		Access mail information	To access email information which can be used by personalized notification apps that require email notification
		Change your audio settings	To change the phone audio settings
Danger	Device & app history	Retrieve system internal state	To retrieve the phone internal state dump information from system services. Not common to be requested for "Personalization" apps
	Cellular data settings	Change/Intercept network settings and traffic	To change network settings and to intercept and inspect all network traffic which can potentially monitor, redirect or modify any network packets. Not common to be requested for "Personalization" apps
	Identity	Modify your own contact card	To modify the user's profile. Not common to be requested for "Personalization" apps
		Add or remove accounts	To manage the list of accounts in AccountManager. Not common to be requested for "Personalization" apps
	Contacts/ Calendar	Modify your contacts	To write to user's contact lists but not common to be requested for "Personalization" apps
		Add or modify calendar events and send email to guests without owners' knowledge	To write to user's calendar information but not common to be requested for "Personalization" apps
	Location	Access extra location provider commands	Not common to be requested for "Personalization" apps
	SMS	Edit your text messages (SMS or MMS)	To write SMS messages. Not common to be requested for "Personalization" apps
		Receive text messages (SMS)	To monitor incoming SMS messages which can be recorded or being modified by the app. Not common to be requested for "Personalization" apps
		Receive text messages (MMS, picture or video message)	To monitor incoming MMS messages which can be recorded or being modified by the app. Not common to be requested for "Personalization" apps
		Send SMS messages; this may cost you money	To send an SMS without the user knowing. Not common to be requested for "Personalization" apps
		Receive text messages (WAP)	To monitor incoming WAP push messages which are used by MMS. Not common to be requested for "Personalization" apps
	Phone	Write call log	To modify phone's incoming and outgoing call log which can be used to hide unauthorized calls made. Not common to be requested for "Personalization" apps
		Reroute outgoing calls	To monitor, modify, or drop outgoing calls. Not common to be requested for "Personalization" apps
		Modify phone state	Modify the status of phone functionality which can be used to intercept incoming calls. Not common to be requested for "Personalization" apps
		Directly call phone numbers; this may cost you money	To make calls without user's knowledge or approval. Not common to be requested for "Personalization" apps
	Camera/ Microphone	Record video	To record video. Not common to be requested for "Personalization" apps
	Other	Modify secure system settings	To modify the secure system settings which should only be used by system apps. Not common to be requested for "Personalization" apps
		Access email provider data	To access your email database, including inbox, sent messages, usernames and passwords. Not common to be requested for "Personalization" apps
		Force stop others apps	To force terminate other apps which should only be used by system apps. Can be misused to stop security apps. Not common to be requested for "Personalization" apps
		Download files without notification	To download files without showing any notification. Not common to be requested for "Personalization" apps
		Power device on or off	To power the device on or off. Not common to be requested for "Personalization" apps

Table 1.2. Threat level table for personalization category

V. CONCLUSION

We have just come up with a different way to classify play store threats. The plus point with our approach is that it benefits savvy and naïve users alike.

REFERENCES

1. O. Celestino "Mobile Apps: New Frontier for Cybercrime" http://www.trendmicro.com/vinfo/us/threatencyclopedia/webattack/119/mobile-apps-newfrontier-for-cybercrime. [retrieved: Oct, 2015]
2. F- Secure. "Mobile Threat Report Q1 2014" http://www.fsecure.com/documents/996508/1030743/Mobile_Threat_ Report_Q1_2014.pdf

3. M. Gendron (Ed.). "RiskIQ Reports Malicious Mobile Apps in Google Play Have Spiked Nearly 400 Percent" 2014 http://www.riskiq.com/company/pressreleases/riskiq-reportsmalicious- mobile-appsgoogle-play-have-spiked-nearly-400.
4. J. Heggestuen, (2013). "One In Every 5 People In The World Own A Smartphone, One In Every 17 Own A Tablet " 2013.http://www.businessinsider.com/smartphoneand-tabletpenetration-2013-10.
5. IDC." IDC: Smartphone OS Market Share" http://www.idc.com/prodserv/smartphone-os-marketshare.jsp.
6. P. Marchant, "Top 10 Android security tips", http://www.computerweekly.com/feature/Top-10Android-securitytips [retrieved: Oct, 2015]
7. P. Paganini, "Phishing goes mobile with cloned banking app into Google Play", http://securityaffairs.co/wordpress/26134/cybercrime/phishing-goes-mobile-cloned-banking-app-googleplay.html. [retrieved: Oct, 2015]
8. Sophos,"Sophos Security Threat Report 2014" http://www.sophos.com/enus/medialibrary/PDFs/other/sophossecurity- threatreport-2014.pdf, pp. 9.
9. L Lei, Y. Wang, J. Jing, Z. Zhang and X. Yu.,"MeadDroid: Detecting Monetary Theft Attacks in Android by DVM Monitoring", Information Security and Cryptology - ICISC 2012, LNCS 7839, 2013, pp 78-91
10. Y. Zhou, Z. Wang, W. Zhou and X. Jiang.,"Hey, You, Get Off of My Market:Detecting Malicious
11. Apps in Official and Alternative Android Markets" Proceedings of the 19th Network and Distributed
12. System Security Symposium (NDSS 2012), 2012.

Akshay Bhardwaj and A J Singh, "Detecting Malicious Apps from Play Store," *International Journal of Scientific and Technical Advancements*, Volume 4, Issue 1, pp. 35-42, 2018.