Consciousness about Mobile App Permissions

Uma H R , Rashmi G R, Bindushree V

Abstract*: This paper gives us the attentiveness on opening files from unknown sources as sometimes it may cause damage to our mobile phones. In almost all the mobile apps after downloading it will ask some of the permissions to allow clicking for the allow button only we can able to access anything in that application otherwise we are unable to use all the features of that application. Many popular android apps including Facebook messenger, WhatsApp, Skype, Twitter, Share it, Instagram and other party apps get user permission after the installation. By allowing these permissions they can recording with the phone audio and video at any time, they can see contacts and modifying the USB storage contents(files). Lack of knowledge and awareness about permissions to the people may cause significant negative consequences. This research evaluates effectiveness of a demo app with visual ques to increase permissions awareness and avoid negative consequences.

Keywords: Mobile applications, Permissions, Android, awareness, education, empirical study, Mobile app permission disadvantage.

I. INTRODUCTION

Mobile apps playing an important role in our daily lives. Permissions in Android apps is an either or proposition . Agree with the permission request or we can't able to use all the features of that particular application. There is no middle ground. Many popular Android apps including Face book Messenger, whatsApp, Skype, Twitter, Share it and Instagram get user permissions during installationon. By allowing these permissions they can record with the phone audio and video at any time, they can see contacts and modifying the USB storage contents (files). EX: Truecaller mobile application will be working like this only by copying all the contacts information to their database on cawed allow the contact permission in their app. The2018smart phone market share shows Androidat74. 15%,Apple at 23. 28%,Windows at 0.29%, KAIOS at 0.96%, Samsung at 0.29% and 0.42% for all others. Apple and Blackberry review permissions prior to store approval [1]. Because of the significantly large Android market share and because of its –take-it-or-leave-it permissions structure focuses only on Android permissions. Our smart phones have a lot of sensitive data including personal information, bank account information, and client-information. A cyber criminal or a nation state that can purchase user's sensitive data from an app provider installed on the smart phone can cause significant damage, and often without their knowledge. We are providing an idea, to limit these data mining in our phones by using some application (bouncer). Here we can grant permissions temporarily to the app. It uses an accessibility service. It activates when you grant permission and gives you the option to remove it. When you go home, it will open the app's settings and remove the permission for you extremely quickly.

Manuscript published on November 30, 2019.
* Correspondence Author

Uma H R*, Assistant Professor , Department of CSE, BGSIT, Mandya, India.
Rashmi G R, Assistant Professor , Department of CSE, BGSIT, Mandya, India.
Bindushree V, Assistant Professor , Department of CSE, BGSIT, Mandya, India.

II. THEORETICAL BACKGROUND

Prior research confirms that Android permission warnings are often ignored and do not help most users make correct security decisions. While requesting the app permissions is totally on the discretion of the developer a multitude of permissions are usually requested may vary from generic permission like accessing your application information to more privacy invasive permissions like accessing the camera and personal information.

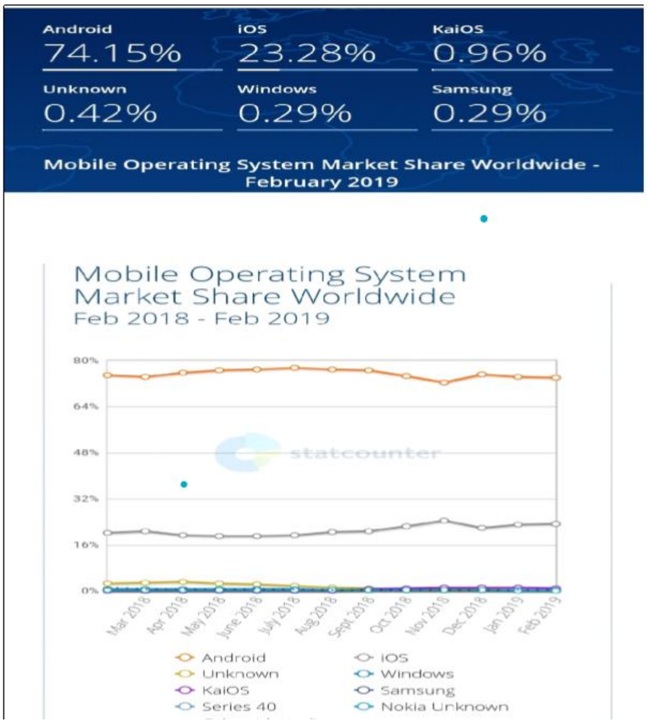
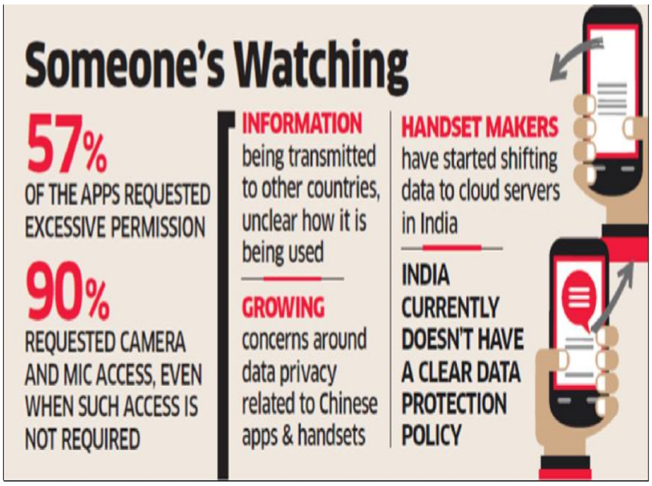


Fig [1]: Mobile Operating System Market Share Worldwide.

The study, commissioned by the Economic Times in the second week of January, reviewed the permissions sought and data shared by these apps among themselves or with third parties outside India.

DOI:10.35940/ijrte.D4237.118419

It also covered the various permissions sought by the apps to access features on user’s phones such as contacts camera, microphone, sensors, location and text messages.Given the proliferation of Chinese apps in India, the study focused specifically on the privacy aspects of mobile apps-these called “Dangerous permissions” being taken by the apps and the data being shared with external parties. Social platform TIKTOK, and UC Browser owned by Chinese ecommerce giant Alibaba have hundreds of millions of user’s accessing these apps every day. UC Browser has over 130millionof its global 430 million users in India, according to the company.



Someone’s Watching

57% OF THE APPS REQUESTED EXCESSIVE PERMISSION

90% REQUESTED CAMERA AND MIC ACCESS, EVEN WHEN SUCH ACCESS IS NOT REQUIRED

INFORMATION being transmitted to other countries, unclear how it is being used

GROWING concerns around data privacy related to Chinese apps & handsets

HANDSET MAKERS have started shifting data to cloud servers in India

INDIA CURRENTLY DOESN’T HAVE A CLEAR DATA PROTECTION POLICY

Fig [2]: Survey regarding data protection.

The study found that on an average, these apps transfer data to around seven outside agencies, with69% of the data being transferred to the US. TIKTOK sends data to China Telecom; Vigo Video to TENCENT; Beauty Plus to MEITU; and QQ and UC Browser to its parent owned by Alibaba.

There is no privacy law in India today whereas in the US, there is some legal requirement and in Europe, (there) is the stringent GDPR REGIM[2].

III. EXPERIMENTS CONDUCTED

ARANDOM sample of 1021Android apps was taken into consideration. During the study, various categories of Android apps like Games, Tools. Entertainment Social& Communication, Music and Video, Personalization Productivity,Photography ,Education and eBook and life style were ANALYZED .The data set included the catgory of App and the lists of permissions that this app requested during installation [6]. The apps have been classified in to two categories depending on the permissions requested. The first category includes those apps that request Genericc Permissions and those that request Privacy invasive Permission. Figure4: shows the percentage of apps that rrequested for generic permissions like the Audio settings, SYNC settings, wallpaper, reading internet history and so on. From Figure 3, can be seen that more than 95% of the apps request. NetworkCommunication.72%requestStorage and 42 % requested your app info permission[4].

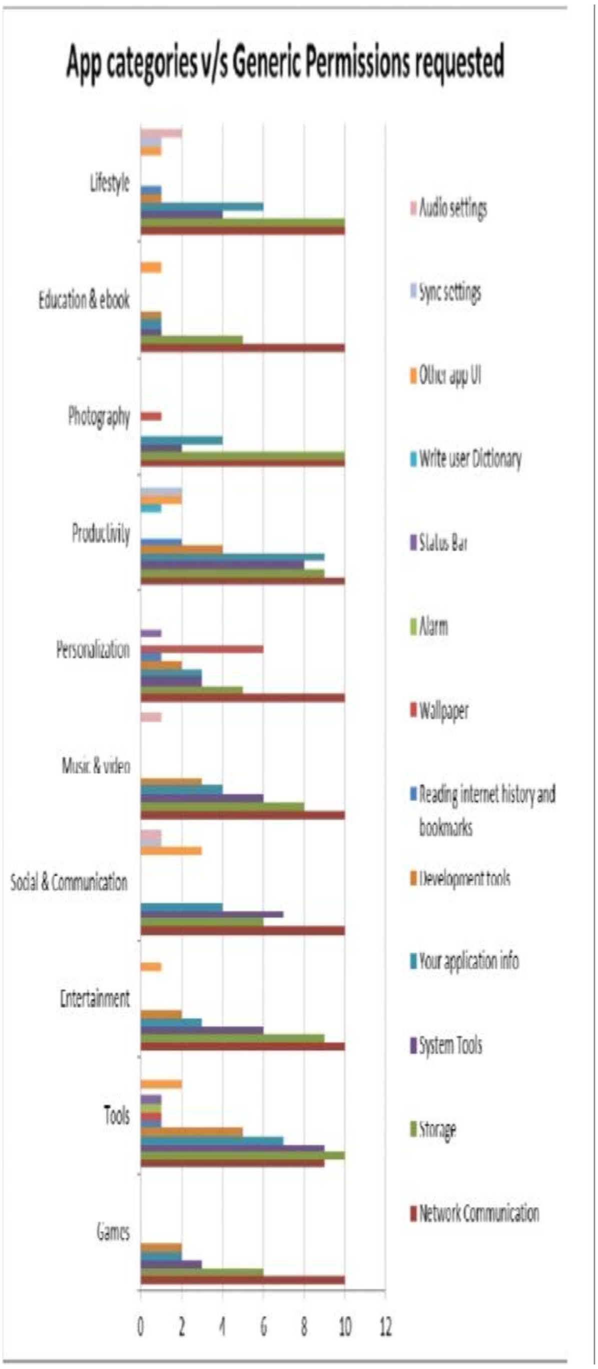


Fig [3]: Percentage of apps requesting Generic permissions.

IV. CONCLUSION

By using bouncer app we can give permission to the unknown source temporarily, it will automatically remove permission after we close the application. Hence it will not cause damage to mobile phone. Though most of the apps request a multitude of generic as well as privacy invasive permissions, a conscious decision on the part of the user is essential before installing the apps. The user should in advertently read the permissions requested and their implications there of before granting access. This can help the user in preventing the revelation of personal information.

REFERENCES

1. https://gs.statcounter.com/os-market-share/mobile/worldwide
2. https://economictimes.indiatimes.com/tech/internet/chinese-apps-seeking-way-more-information-than-needed-survey/articleshow/67633562.cms
3. Mobile Technology Fact Sheet , Pew Research Centre , http: / / www. Pcw intermittent org/ fact sheets/ mobile technology fact sheet.
4. .https://www.google.com/search?q=app+categories+v/s+generic+permissions+requested&newwindow=1&sxsrf=ACYBGNTsGgoows-864qI4RuKW2EO84KWzg:1574754007680&source=lnms&tbm=isch&sa=X&ved=2ahUKEwjX2vHpr4fmAhXXAnIKHQAKAWMQ_AUoAnoECA4QBA&biw=1024&bih=657
5. Why does this Android app needs many Permissions? , http: / / www. lifehacker.com/ 5991099/ why-does-this-app need-so-many permissions.
6. http: / / www. statista. com/ statistics 281106 number- of-android downloads-from-google-play The Economic Times IEEE Paper - How privacy invasive android apps are?
7. IEEE Paper - Mining android apps to recommend permission

AUTHORS PROFILE

UMA H R, working as Assistant Professor at BGSIT. I have done Mtech in computer science and engineering

Rashmi G R, working as Assistant Professor at BGSIT. I have done Mtech in computer science and engineering

Bindushree V, working as Assistant Professor at BGSIT. I have done Mtech in computer science and engineering. I am a member of “association of engineers group”. I have published a paper on “image processing”