Awareness of App Usage and Security Issues among Smartphone Users in India

Dr. Aruna Deoskar[1] *Pradnya Khalane*[2]

ABSTRACT

As per the survey reports (the Hindu Feb 2016) India has become the second biggest smart phone users. Numbers of users have become habitual of using Internet and various mobile Applications. Whether it is business App, entertainment App or consumer App, user is using all such Apps very frequently. But basic challenge is that user is downloading such Apps for ease and comfort might be free or by paying, without bothering for agreement terms and security issues. The purpose of this study is to understand and explore the awareness of Indian Smartphone users about security and privacy issues related with free Smartphone Apps. The study focuses on various free Android apps downloaded by users, awareness about permissions to be granted while installing free apps, and problems faced by users. Research study is conducted and primary data is gathered from users of all age groups.

Keywords **:** Smartphone Apps, security, privacy, threats, Android, permissions

I INTRODUCTION

Technological advancements made user more and more techno savvy. In past few years number of Smartphone users has increased drastically. Mobile phone has become an integral and necessary part of each and every individual. With the connection of word 'SMART' with mobile phones, users are interested to become more and more 'SMART'. Smart phones are mobile phones with lot of user friendly additional features. Availability of more and more on line applications, has made user life simpler and easier. But at the same time it has increased the complication among individual life unknowingly. 'SMART' phones are providing 'SMART' features and making user 'SMART' and also creating 'SMART' problems. Such unknown 'SMART' problems could be eased off by increasing the security awareness among users. Smart phones stores huge amount of user's personal and professional data, thus may pose serious security and privacy threats. User might not be interested in making such information to be public, but for signing certain site user provides the minimum required information which unknowingly becomes public. While installing free APPs as provided by the smart phone, user grant the permission(s) to APP provider but little he/she is aware about that for what they are granting the permission. This can be reduced if user would be aware of Smartphone APPS and various security issues. Through this paper the researcher is trying to analyze such security awareness among various smart phone users.

1. *Professor MCA, ATSS IICMR*
Email:aadeoskar@gmail.com
2. *Assistant Professor, Modern College*
Shivaji Nagar Pune

II LITERATURE REVIEW

Smartphone stores heterogeneous data related to user's personal and/or professional information. This increases serious privacy threats. Such data, if maliciously collected by intruders then can be used by attackers for wrong intentions. Various service providers collect user data as per the defined policy, but details which they are collecting no one knows that for what purpose their personal data has been gathered by third party. Whenever user is downloading an App, he has to sign an agreement by accepting their terms and conditions. In such cases most of the

time our submitted data/information is been transmitted to the app-maker and/or to third-party advertisers. Some apps may track user location. Location-based services like Google maps, Yelp or Foursquare need user location in order to function properly. However, there are apps that do not need user location to function but may still be tracking it. Apps may also be infected with malware (malicious software that can pose a threat to your Smartphone). Many mobile apps do not have privacy policies, and when they do, they are often long and difficult to understand.[1]

Android holds the largest market share 81% in 2016 in Smartphone market. Analysis of more than 7 million mobile apps during 2014 showed that mobile users face risks on many fronts including: [2]

Malicious apps that steal information

- Malicious apps that steal information
- Benign apps written in an insecure manner
- Benign apps that use insecure or aggressive ad libraries
- Apps that enable attackers to steal users' identity
- Apps that profit attackers by calling for-fee phone numbers and texting services [2]

Researchers warn that a surprisingly high percentage of Smartphone apps may threaten user privacy[3].In October 2010, joint research by Intel Labs, Penn State and Duke University found that 15 out of 30 Android apps analyzed sent geographic information to remote ad servers without users' knowledge. Seven of them also sent the unique phone identifier; in some cases, the actual phone number and serial number were sent to app vendors. This can enable app vendors and/or advertisers to create comprehensive profiles about user likes and dislikes, the places user visit when he/she carry phone, user Web surfing habits and more. They can then use those profiles however they want or sell them to others. Meanwhile, in June 2010, security vendor Smartphone Mobile Systems found that 20% of Android apps allowed third parties (that is, companies other than the app vendors themselves) to get access to private or sensitive information. In addition, the report warned, 5% of the apps could make phone calls by themselves without user intervention and 2% could send an SMS text message to a premium, for-pay number -- again without the user making the call.[3]

Table 1: Smart Phone Apps

Existing Android permission model

Android Apps	
Third Party Apps	**Pre-installed Apps**
Apps are available for download from Google Play and Amazon. These Android apps are developed by individual third-party developers	Apps come along with phone from the vendors. They are developed and loaded in the phone before it reaches to user.

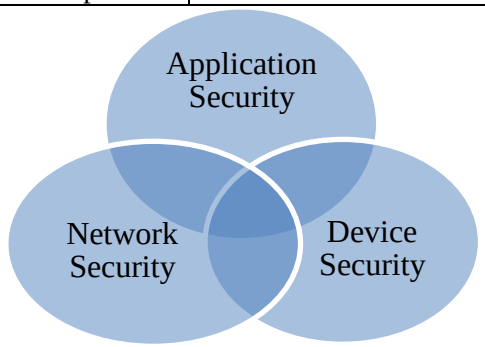


Fig. 1: Smartphone Security

Smartphones are incorporated with various security permissions. User has to check these permissions before accessing and downloading any application. In general smart phone provide mobile security at Application level, Device level and Network level. By default, an Android app can only access a limited range of system resources. Access to sensitive resources is protected through a security mechanism known as Permissions.

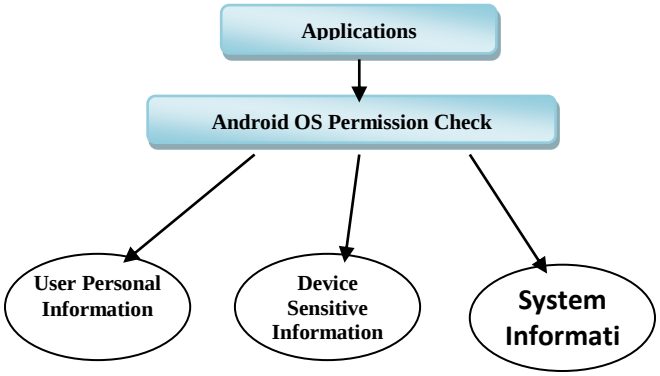
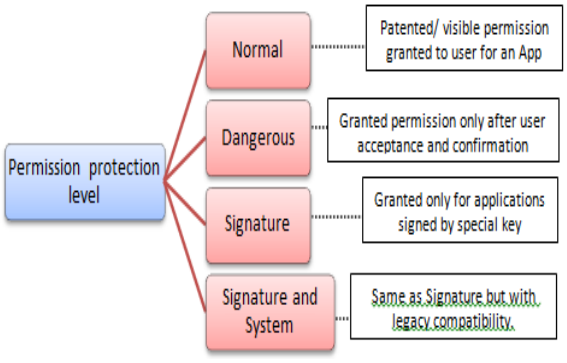


Fig. 2: Android Permission Check

It provides protected Android Permission Interface for the sensitive resources. To make use of the protected Interface, an application must declare associated permissions in a manifest and these permissions are agreed upon by user at the time of App installation. Android ranks these permissions according to threat level. Various permission protection levels are: Normal, Dangerous, Signature and Signature or System. Normal permission are patented and visible for every application. Dangerous permissions are displayed to users to get their acceptance and confirmation. However, there is still great variance within Dangerous permissions. Dangerous permissions let an application perform such actions which may cost the user pertaining to feasibility aspect or related to private information On the other hand, Dangerous permissions also guard the ability to connect to paired Bluetooth devices, modify audio settings, and get the list of currently running applications automatically.



III RESEARCH METHODOLOGY

An explorative study has been conducted by the author to study the awareness of security and privacy issues related with Smartphone apps. Respondents who have Smart phones are considered for this study. Survey method with random sampling is used to collect the primary data. Primary data has been gathered from 34 valid respondents out of total 38 respondents. Questionnaire technique is used to collect the data. The questionnaire is being designed in two sections; a) general information and b)awareness about security and privacy related issues, free app usage, user expectations from app providers, and Indian Government.

Secondary data is gathered from articles and research papers published in books and journals.

Objective of Study:

The main objective of this study is

- To understand the user awareness about App usages and security issues

Sub objectives :

- To understand the App usages among Smart phone users.
- To understand the user awareness about security issues related to free Apps.

IV DATA ANALYSIS

Data is gathered through questionnaire by interacting with various smart phones users. Primary data is analyzed to know the degree of user awareness about App usages. Thirty four (34) valid responses were received from all age group of people. IT and Non IT user are analyzed to know the degree of awareness and its association with Information Technology literacy level. Gathered data is analyzed and following results are summarized:

- 53% IT users prefer Android system, 9% user prefers Windows. 41% Non –IT user prefers Android OS,
- Almost all IT user prefers to select an App based on features and ratings. But Non IT user selects an App based on cost and availability.
- Most of the user prefers Apps which are freely available and having maximum features. Various Factors association with App selection among users

	Table.2:App Selection Factors					
	Free	Paid	Cost	Features	Availability	Ratings
IT User	53%	9%	3%	44%	26%	21%
Non IT	35%	6%	9%	18%	21%	15%

- User awareness about App permissions before downloading them

	Table 3: App Permission Status					
	Ignore	Allow App provider to access mobile resources	Don't Know	Like to share personal data	Don't Like	Don't Care
IT User	30%	50%	20%	15%	75%	10%
Non IT	36%	50%	14%	7%	86%	7%

Irrespective of IT literacy most of the smart phone users allow App provider to access their phone information to down load available App on their mobile phone. This shows that user is not bothering about serious security issues while downloading various available Apps. Majority of users do not like to share their personal data with App providers.

- Users after downloading free App as per the requirement; expects that App should work as per the defined features. But faces lot of problems while using them after downloading successfully.

	Table. 4:User Expectations			
	Security	Privacy Protection	Easy Access	App Should occupy minimum Storage
IT User	41%	38%	35%	24%
Non IT	32%	29%	24%	12%

	Table. 5: Problems Faced By the User			
	Slow	Memory Full	Mobile Hang	App Crashes
IT User	29%	3%	6%	18%
Non IT	21%	26%	3%	11%

- Depending upon responses as given by smart phone users, all positive responses are considered as indication towards awareness among users. It has been observed that IT literate users are more aware towards such security and permission policies compared to Non IT professionals. 61% IT professionals are checked yes of knowing the gravity of security policies and permissions to be understood by user before downloading any App. Whereas for Non IT users this percentage turned out as 32% only. But despite of having such awareness user is

involved in downloading desired App by neglecting all such security checks.

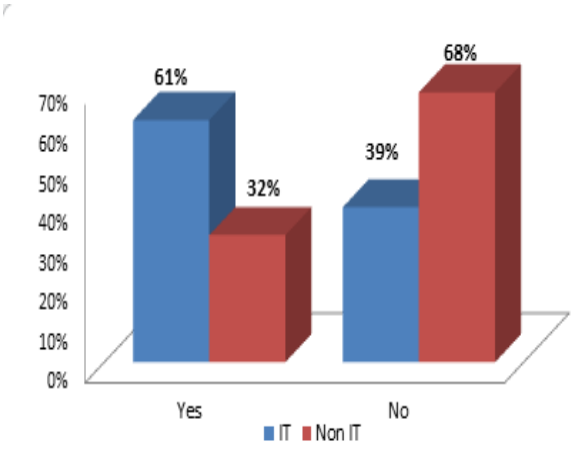


Fig. 4:Security Awareness Among Users

V. CONCLUSION

Smart phone users are interested in downloading mostly free Apps. They are least bothered about various consequences of neglecting security issues.

This study has analyzed that how much such security awareness s there among smart phone users. Irrespective of IT proficiency smart phone users are facing lot of problems while using such Apps. App providers are ensuing of protecting user data and assuring to users of fulfilling their expectations from such downloaded Apps, but most of the Apps not as per the expectations. IT users compared to Non IT users are much well versed and aware of security policies related to Apps but neglects them.

REFERENCES

[1]Smartphones and privacy, InfoWorld | Jul 17, 2015

[2]Out of Pocket: A Comprehensive Mobile Threat Assessment of 7 Million iOS and Android Apps, February 2015

[3]joint research by Intel Labs, Penn State and Duke University, October 2010