

An Analysis of Mobile Applications Security, Issue and Aspects from the User's Perspective

Ashish A Kulkarni¹, Shivaji R. Madan²

¹Assistant Professor, MIT School of Management Pune, Maharashtra, India

²Research Guide, Dr. Babasaheb Ambedkar Marathada University, Aurangabad, Maharashtra, India

Abstract: *Today's era more sound to be mobile era every one attacked through shape size functionality of cell phones, we found even illiterate person uses mobile features such as Internet etc. even literate person has some more advanced way to use the functionality such as auto save passwords, installing Mobile APPS for each and every work even downloading data form unsafe sides, many user thinks that once they install antivirus and if they regular update that antivirus there is no need to take any other security measures. But this assumption is not correct many times our own mistakes lead to unsafe transaction over cell phones. The researcher found some common issues which can take user to unsafe and unsecure transaction without knowing to him*

Keywords: Mobile APPS, Antivirus, Wifi Network

1. Introduction

Today's smartphone is the same as the Desktop we used in 2000, but with better graphics, more memory and better connectivity 90% of the top mobile apps have access to local files that can contain sensitive customer data, corporate intellectual property, and personally identifiable information. No wonder Gartner and other industry experts now recommend mandatory security testing and remediation of all enterprise mobile applications — including internally-developed and third-party applications and mobile applications downloaded from app stores that may come from unverified sources. Even if mobile app developers are not malicious, they may have unintentionally incorporated third-party components and libraries that violate security policies (such as capturing sensitive information for error logging).

Mobile Apps: A mobile application, most commonly referred to as an app, is a type of application software designed to run on a mobile device, such as a smartphone or tablet computer. Mobile applications frequently serve to provide users with similar services to those accessed on PCs. Apps are generally small, individual software units with limited function. This use of software has been popularized by Apple Inc. and its App Store, which sells thousands of applications for the iPhone, iPad and iPod Touch. A mobile application also may be known as an app, Web app, online app, iPhone app or smartphone app.

Mobile Web: The mobile Web refers to the use of the Internet through handheld mobile devices. Increasingly, smartphones and other devices with wireless data access structures access the same "full" Internet traditionally accessed on desktop or laptop computers.

A mobile website is similar to any other website in that it consists of browser-based HTML pages that are linked together and accessed over the Internet (for mobile typically WiFi or 3G or 4G networks). The obvious characteristic that distinguishes a mobile website from a standard website is the fact that it is designed for the smaller handheld display and touch-screen interface.

Like any website, mobile websites can display text content, data, images and video. They can also access mobile-specific features such as click-to-call (to dial a phone number) or location-based mapping.

Apps are actual applications that are downloaded and installed on your mobile device, rather than being rendered within a browser. Users visit device-specific portals such as Apple's App Store, Android Market, or Blackberry App World in order to find and download apps for a given operating system. The app may pull content and data from the Internet, in similar fashion to a website, or it may download the content so that it can be accessed without an Internet connection.

2. Methodology

- **Research methodology:** Exploratory and Descriptive research
- **Sample Element:** Mobile Users
- **Sampling Technique:** Convenience sampling
- **Location :** Pune , Maharashtra
- **Sample size :** 500
- **Instrument :** A Well structured Questionnaire
- **Data Analysis:** Analysis was done by using simple frequency tables, cross tabulation, percentages

Objectives

- 1) To check the security of mobile apps
- 2) To check users awareness about common security features of Mobile Apps .
- 3) To check much improved mobile security mechanism

3. Results

Table 1: Mobile Password

Pattern Password	268
Text Password	121
No Password	25
Other	85
TOTAL	500

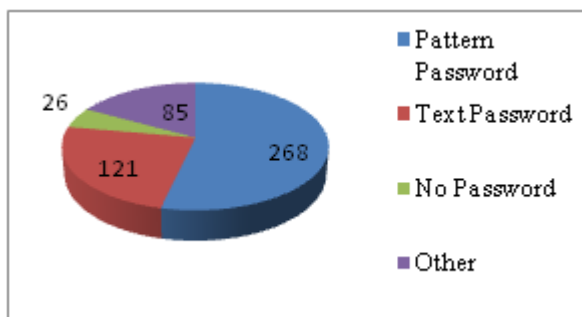


Table 2: Mobile Operating System

_Android	220
Mobile OS	165
Microsoft	90
Other	25
TOTAL	500

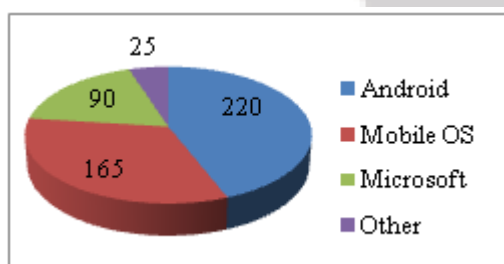


Table 3: Antivirus Program Installed on Mobile

Yes	350
No	150
TOTAL	500

Table 4: Uses of WIFI Network on Cell Phone

Daily	325
Monthly	27
Weekly	124
Never	24
TOTAL	500

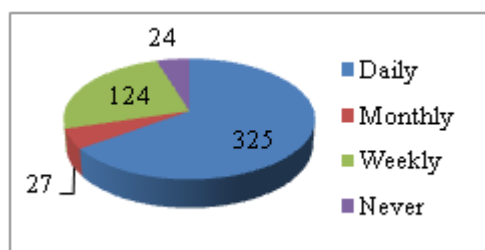


Table 5: Downloading APPS form Apps Store

Daily	175
Monthly	121
Weekly	180
Never	24
TOTAL	500

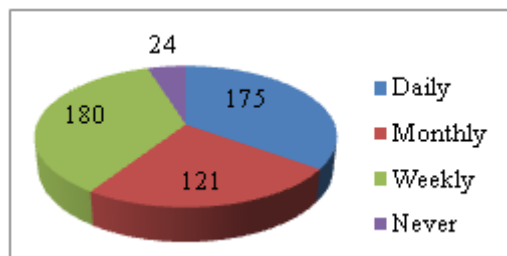


Table 6: Yes/No answer questions

Question	Yes	NO
Habitual to save password in mobile	231	269
Installing Security apps	400	100
Storing data on cloud platform	150	350
Sending confidential data such as Email	250	250

4. Discussion and Conclusions

Table 1 shows that distribution of respondent according to their current mobile Password the pattern password, text password and other kind of password

Table 2 shows the operating system which user is using android is leader among that but it is found that Android is unsafe as compare to other operating system .

Table 3 represent the number of user who are using mobile antivirus.

Table 4 represent the wifi abdication among users it is found that as we increases wifi uses there should increases in security risk

Table 5 represent the downloader form mobile store. There is fare amount of chances for downloading unwanted files security break falls while downloading apps from apps store

Further Table 6 represents few yes no type question where user has to pay attentions as sending data on mobile is not in encrypted format even data stored on cloud can be accessed from your mobile anywhere anytime

References

- [1] https://www.owasp.org/images/c/cf/ASDC12-Mobile_Application_Security_Who_how_and_why.pdf
- [2] <http://www.veracode.com/products/mobile-application-security>