IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
PP 05-09

Insidious Vulnerabilities on Mobile Applications – Security Measures

K.Berlin, Dr.S.S.Dhenakaran
Ph.D Research Scholar Department of Computer Science Alagappa University, Karaikudi Tamil Nadu, India berlinjenson@gmail.com
Professor Department of Computer Science Alagappa University, Karaikudi Tamil Nadu, India ssdarvind@yahoo.com

Abstract: *The digitalization of business processes and practices is inevitable. One trend, of interest to both business and hackers, is the increasing number of mobile versions of enterprise applications for employees and customers. Mostly, Apps developers particularly focused on application functionalities, not security. This is the main reason helping hackers hack apps, repackage apps, malicious code and reloading apps. It gives very harsh issues to customer's sensitive data. Applications not using encryption can be affected by such problems. The best thing is that mobile apps developer has to use the encryption framework to protect the user's data which makes at most impossible to crack the data. Bad data storage, outdated of antivirus and lack of encryption principles are the causes vulnerabilities on mobile applications. This paper outlines best practices to avoid mobile app vulnerabilities and secure its information.*

Keywords: *Mobile applications, Anti-malware, Encryption, Vulnerabilities, Sensitive data, Security.*

I. INTRODUCTION

Nowadays, the whole world has entirely relied upon the technological developments. So the people desire to do process their needs within the hand. Everyone has been using mobile phone for their sophisticated life. Internet is first thing to process the mobile based tasks in mobile Applications. Both internet and Apps are act as backbone to functioning mobile phones. Every day people browse many things through the several websites, but how many of them feel comfortable about security. We are living in connected world, where information leaks happen every day and the biggest question is whether all of these websites are safe? The answer is no.

Vulnerabilities have entered into the devices in abundance manner from security point basis. Application developers have only concentrated on Apps functionalities more than the security. So hacker easily changes Application functionality as per their wish even with knowing of main server.

Google play store and Apple App store provide variety of Apps for android mobiles. Google and Apple companies are two big traders in the Smartphone market. Both stores have offer at least 1 million Apps and gets downloads in the range of billions [1]. Compare these two; both are having pros and cons. Apple store grants only top quality apps to the users for the better excellence. But from the web developer's point of view, they need to spend more time to reach the apple's standard. On the other hand, Google play store allows very low quality Apps too. It gives the chance to the users being installed the buggy apps and causing more security issues too. This research paper signifies the security issues over the Smartphone apps and gives better solutions to avoid user's data from the unwanted vulnerabilities.

Mobile Applications

Distinct mobile Application providers have been controlling the Smartphone market. Five of them are listed here Google play, Apple App store, Windows phone store, Amazon App store, BlackBerry world. From these providers top downloaded Apps are listed with its security issues.

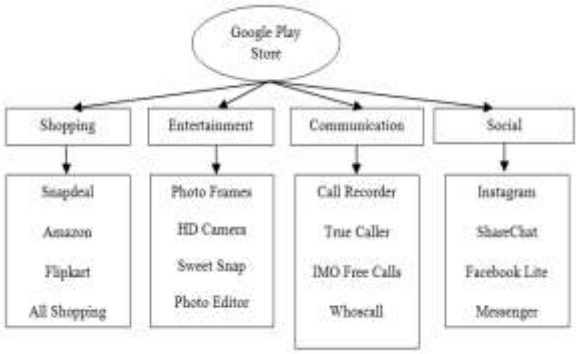

Figure 1: Top downloaded Apps

Shopping

Online shopping plays a big role in e-commerce; it provides immediate services to consumers directly over the internet. For shop, Google play service plenty of Apps without knowing the issues of security. After downloading, Apps need to access some of the data which has stored on devices for the installation. Users should remember one thing that is how many times they have clicked "I agree" to accept the terms and conditions of the appropriate Apps.

Table 1: Apps used to shopping

Name of the App	Description	Needed data to install
Snapdeal[2]	Indian e-commerce company for online shopping	Activity on the device, which Apps are running, browsing history, Bookmarks.
Amazon	American e-commerce company over the world wide	Identity, Contacts, Location
Flipkart	Indian company for online shopping over the India	Device & App history, Identity, contacts.
ALL SHOPPING	All online shopping Apps are controlled within one App	Identity, SMS, Device ID and Call Information, receive data from internet.

Entertainment

Several distinct android Apps are approved by Google play store especially Apps which have entertaining the users in different aspects. The picture editing App access device camera and media files to edit picture which has stored on devices [3]. Paul Oliveria, researcher at cyber security says, permissions by themselves are harmless, because it may be better to give good mobile experience to the users. But in the aspect of security, users should read carefully of terms and conditions when installing android Apps. Belongs to the entertaining category few of them described.

Table 2: Apps related to Entertainment

Name of the App	Description	Needed access to install
Photo Frames[4]	Used to show the images as different beautiful view	Images, videos or audio, device's external storage.
HD camera	Utilized all advantage of devices. Quick snaps, easy photos and videos.	Location, images, videos or audio, device's external storage, camera, microphone.
Sweet Snap	Live Face filter, selfie camera edit	Location, images, videos or audio, device's external storage, camera, Microphone, wifi connection information, Device ID and call information, read settings and shortcuts, receive data from internet.
Photo Editor	Used to edit photos on devices	Images, videos or audio, device's external storage, wifi connection information, receive data from internet.

Communication

Plenty of apps designed by the developers to improve the communication as fast and replace the existing settings of old one for increase the customers To improvise the communication of android tools, much more Apps are designed by distinct developers.

Table 3: Apps related to Communication

Name of the App	Description	Needed data to install
Call recorder[5]	Automatic call recorder and save any phone calls	Contacts, phone, images, videos or audio, device's external storage, Microphone, wifi connection information, device ID, call information, receive data from internet.
True caller	To identify unknown calls	Identity, contacts, Location, SMS, Phone, Photos/Media/Files, Camera, Wifi connection information, Device ID and call information, read voice calls, write voice calls, MMS wakeup.
IMO free calls	Unlimited voice, video calls and messages.	Identity, contacts, location, SMS, phone, photos/media/files, camera, Microphone, wifi connection information, Device ID and call information, receive data from the internet.

Social

According to the Google play store, among several categories, Apps under social having highest downloads. Android mobile phone users have engaged with social Apps like Facebook, twitter, Messenger, ShareChat, Instagram etc. such Apps are discussed.

Table 4: Social Network related Apps

Name of the App	Description	Needed data to install
Instagram[6]	To capture and share world moments	Device and App history, Identity, contacts, Location, SMS, photos/media/files, camera, microphone, device ID and call information, receive data from internet.
ShareChat	Share videos, jokes, Gifs, audio, images within India	Identity, contacts, location, SMS, photos/media/files, camera, wifi connection information, device ID and call information, download files without notification, manage document storage, receive data from internet.
Facebook Lite	Keeping up with friends is faster and easier.	Device and App history, Identity, calendar, cantacts, location, SMS, phone, photos/media/files, camera, microphone, wifi connection information, device ID and call information, download files without notification, receive data from internet.
Messenger	Instantly connect with people.	Identity, contacts, location, SMS, Phone, photos/media/files, camera, photos/media/files, camera, microphone, wifi connection information, device ID and call information, download files without notification, receive data from internet.

Security Issues of Mobile Applications

While compared iphones and ipads android is fully open source platform for Apps and games. In section 2, describes in detail about, what are the personal information of customers is needed to install android apps. Apps read customer's contact list, messages include bank transaction passwords, gallery, control device, camera etc. Google Play store supports millions of Apps without the checking of SSL certification. By this chance hackers develop duplicate copy of professional Apps and access customer's details easily. So lack of encryption is one of the considerable mater here. Based on the customer ratings mobile Apps which has top ranking discussed in the security aspects.

Table 5: Security issues of most downloaded Apps

Name of the App	Name of the Attack	Hack via	Installs	Customer Rating
Amazon	ViperRat	Malicious website links, phishing attempts.	100,000,000+	4.3
Flipkart	Map of maps	Links from third party websites	100,000,000+	4.4
Facebook	Malware apps	Dubbed GhostTeam using WebView code	1,000,000,000+	4.1
Instagram	Brute force	Brute force password cracking tool.	1,000,000,000+	4.5
Whatsapp	Sophisticated hacker hack group chats	Control the whatsapp server through the insertion of new number into group chat without admin permission.	1,000,000,000+	4.4

Map of maps also called as National security threat, it makes huge data vulnerable by the mercenaries from different countries. It access entire server of e-commerce through the digital black market includes Flipkart. There are 56 malware applications designed to hack facebook login details [7]. Hackers upload the malicious Apps into Google Play with some utilities like flashlight, QR code scanner. Once this malware app installed, it gets device administrator permissions to access all the details on the device.

No application is fully safe from the hackers; even huge company like apple had hacking experience in the past. So the people who are having skeptical feel about bank details and personal data, they advised as please don't share your data on websites.

Analysis of Mobile Apps Statistics

Launching of mobile applications is in increasing mode by Google Play, Apple App Store and Amazon store. In Google play applications are available either at a cost or free of charge. The available applications are directly downloaded via play store App. The statistical report of Google play provided mobile applications is listed below.

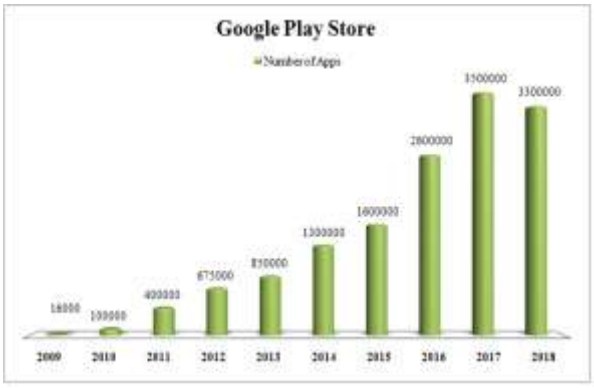

Figure 2: Google play store applications count.

Apple Inc., provides digital application forum called as App store. App store allows users to download mobile apps designed with iOS software development kit. Apple mobile apps supports only to iPhone, iPod Touch handheld systems, iPad, Apple TV. The statistical analysis of Apple App store mobile applications are pictorized in yearly wise.

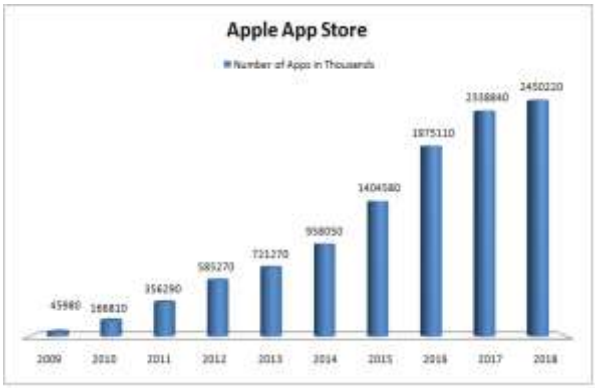

Figure 3: Apple App store Application count

Amazon App store provides mobile applications for android devices which are maintained by Amazon team. Offer free mobile applications on some festival days to customer, which means on the whole day the android users can download mobile apps unconditionally for free of cost. Mobile applications supported by Amazon App store is depict clearly.

Figure 4: Amazon App store Application count

II. CONCLUSION

Consumers have always afraid of security against hacking and identity happening every day. Hackers and cyber attacks get more active to hack secured data. Before starts the installation, essential to check whether the particular App has SSL certificate. SSL is a crypto-technique, by exchanging symmetric key it establishes secured cryptographic link between server and clients. The elementary reason for using SSL is to preserve the consumer's sensitive data with encrypted connection. So during the online purchases people should aware of cautious and advised to don't save banking details on the website. Nothing is perfectly secured, to safe devices from the malicious hacking people should regularly update passwords and keep security settings tight.

REFERENCES

[1] https://www.androidauthority.com/google-play-store-vs-the-apple-app-store-601836/ (refer for the second chapter)
[2] Available at https://play.google.com/store/apps/category/shopping
[3] https://economictimes.indiatimes.com/small-biz/security-tech/technology/why-mobile-apps-require-access-to-your-dataand-device-tools/articleshow/52138161.cms
[4] Available at https://play.google.com/store/apps/category/entertainment
[5] https://play.google.com/store/apps/category/communication
[6] https://play.google.com/store/apps/category/social
[7] https://thehackernews.com/2018/01/facebook-password-hacking-android.html

Author Profile

K. Berlin, received her M.Phil degree in Alagappa University, Tamil Nadu. Now she is pursuing her Ph.D (Computer Science) research in the same university. The field of her research is data security in cryptography. Four Research papers are published in Journals and Conferences.

S.S.Dhenakaran, a faculty member is working in the Department of Computer Science, Alagappa University, Tamil Nadu, India. He has acquired a doctoral degree in Computer Science and Engineering during 2008. Completed post graduation in mathematics during 1984, PG degree in computing during 2003. To his credit, he has more than 95 articles in international journal and conference. His field of research is Data Security using Cryptography. His familiar research fields are Optimization Techniques, Algorithms and Data mining.