**Available Online at www.ijcsmc.com**

**International Journal of Computer Science and Mobile Computing**

**A Monthly Journal of Computer Science and Information Technology**

**ISSN 2320–088X**
**IMPACT FACTOR: 6.199**

*IJCSMC, Vol. 9, Issue. 3, March 2020, pg.58 – 63*

# PROTECTING SECRET FILES IN MOBILE FROM MALICIOUS APP

**Mrs. B.SATHYABAMA[1]; Mr. D.VINOTHKUMAR[2]**
[1]Assistant Professor, [2]Final MCA Student
PG and Research Department of Computer Application, Hindusthan College of Arts and Science, Coimbatore, Tamil Nadu, India
[1] msathyaimpossible@gmail.com

---

***ABSTRACT: Android has been a major target of malicious applications. How to detect and keep the malicious app out of the app markets is an ongoing challenge. One of the central design points of Android security mechanism is permission control that restricts the access of apps to core facilities of devices. However, it imparts a significant responsibility to the app developers with regard to accurately specifying the requested permissions and to the users with regard to fully understanding the risk of granting certain combinations of permissions. Android permissions requested by an app depict the app's behavioral patterns. In the projected system, providing password for individual files into that folder and making access control to move, copy or delete those files and folders. If a user who knows the password can able to access, move, copy or delete that file. And also, providing extra facilities as if an unauthorized user trying to access our file and he attempting to give wrong as times means there is an alert message will send to the respective user of that file.***
***Keywords– Malicious App, Android Security, Hacking***

---

## I. INTRODUCTION

As mobile device usage increases in ubiquity and capability, so will the need for increased security and privacy. Mobile devices are now being used for tasks once primarily under taken on personal computers and notebooks. Paying bills, banking, ordering items online and others can now be done entirely on a smart phone. With the increase in the amount of sensitive information stored on a mobile device, user privacy becomes an important, if somewhat forgotten, factor.

 

The Rise in the number of task performed on mobile devices means sensitive information is stored on the devices. Android devices are a potential vector for criminal exploitation. Some of the malicious app which involve in stealing contact and privacy details from the mobile user even without the knowledge of the user. So there must be app validator for monitoring and controlling the app permission and accessible limits.

## II. IMPLEMENTATION

- Adding files module
- File protection
- Warning Message
- Request File access
- Removing File Permission

### Adding Files Module

This module is used to add the files to list which is to be protected. We can add single files or multiple files to this list. Files can also be included later after creating the file. In this case, the old files file will be deleted and the new file will be created when including some files to your project list.

### File Protection

When adding single or multiple files, password can be given to each file to protect the access of unknown users from viewing the file. Any type of files can be added to the project by selecting the files. while adding files there is an additional features as adding security questions when user forgot means and also enabling message alert when an unauthorized user trying for password attack

### Show Warning Message

When any malicious app is accessing protected files through this app, the warning message will be displayed in both app.

### Request File Access

If the app is not a malicious app and it needs to access the protected files, the app can send the access request to the malicious protection app. the main app will show the request details. The mobile user can grant permission or can block access again.

### Remove File Permission

This module describes about remove file permission from existing locked files. The user can release permission from already secured files.

 

## III. OFFERED SYSTEM AND ANTICIPATED SYSTEM

### OFFERED SYSTEM

In existing systems for such services, usually all the users directly publish their complete profiles for others to search. However, in many applications, the users' personal profiles may contain sensitive information that they do not want to make public. Due to the increasing openness and popularity, android phones have been an attraction to most of the malicious applications and an attacker can easily embed its own code into the code of a benign application. Therefore, malwares attacking the android application are growing at an alarming rate and under these circumstances, security of the devices and the assets these devices allow access to, be at stake. In addition, android itself has some distinct characteristics and limitations due to its mobile nature.

### DRAWBACKS OF OFFERED SYSTEM

- Opens up the possibility for hackers to commit fraud and launch spam and virus attacks.
- Increases the risk of people falling prey to online scams that seem genuine, resulting in data or identity theft.
- The existence of third party application stores contribute in spreading malwares.
- The users are not aware enough of the threat endangered.
- Trust either the application store or the popularity of the application.
- The security of data is less.
- A permission is a restriction limiting access to a part of the code or to data on the device
- The limitation is imposed to protect critical data and code that could be misused to distort or damage the user experience.

### ANTICIPATED SYSTEM

In this system, we overcome the above challenges and make the following main contributions. The privacy preservation problem of profile. Two levels of privacy are defined along with their threat models, where the higher privacy level leaks less profile information to the adversary than the lower level. This research proposes the use of permissions removal, wherein a reverse engineering process is used to remove an app's permission to a resource. The repackaged app will run on all devices the original app supported. Our findings that are based on a study of seven popular social networking apps for Android mobile devices indicate that the difficulty of permissions removal may vary between types of permissions and how well-integrated a permission is within an app.

### ADVANTAGES OF ANTICIPATED SYSTEM

- Every App are restricted in the permission level
- The malicious app cannot retrieve privacy data
- Targets a wide audience, making it a useful and effective recruitment tool.
- Improves business reputation and client base with minimal use of advertising.

 

## IV. INPUT DESIGN & OUTPUT DESIGN

Input Design is one of the most expensive phases of the operation of computerized system and it is often the major problem of a system. A large number of problems with a system can usually be tracked backs to fault input design and method. Needless to say, therefore, that the input data is the life blood of a system and have to be analyzed and designed with utmost case and consideration. The decisions made during the input design are

- To provide cost effective method of input.
- To achieve the highest possible level of accuracy.


FIG 1: Login Page

 

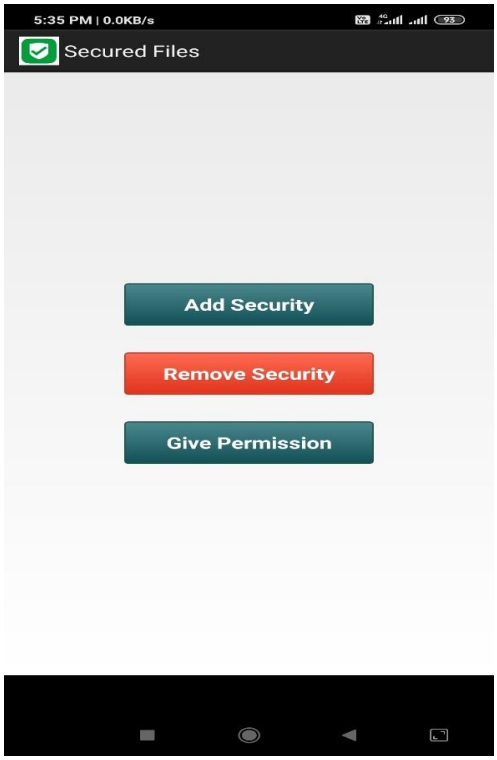


FIG 2: Home Page

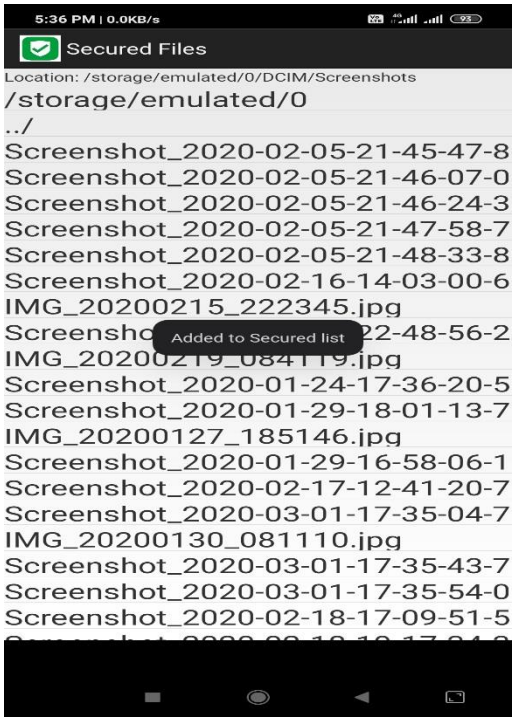


FIG 3: Add to Security

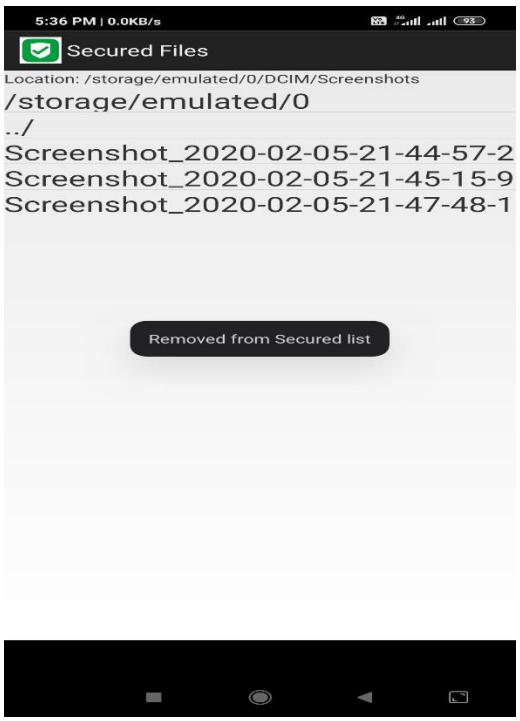


FIG 4: Remove From Security

 

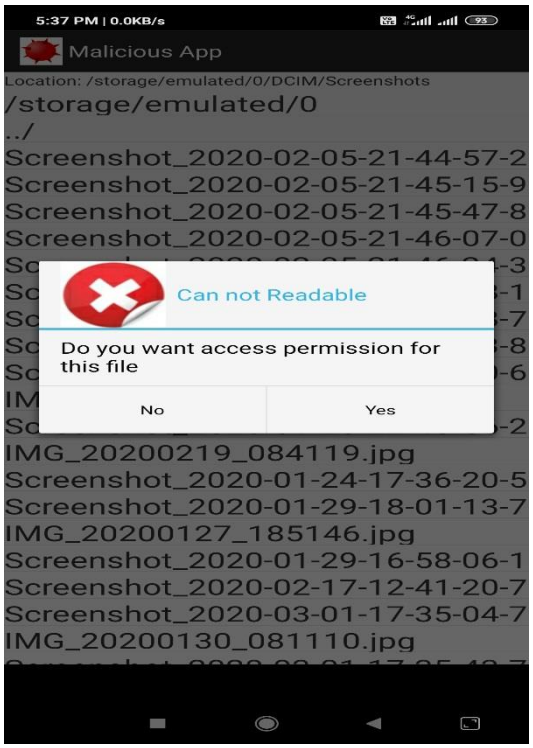


FIG 5: Non Access Image Files

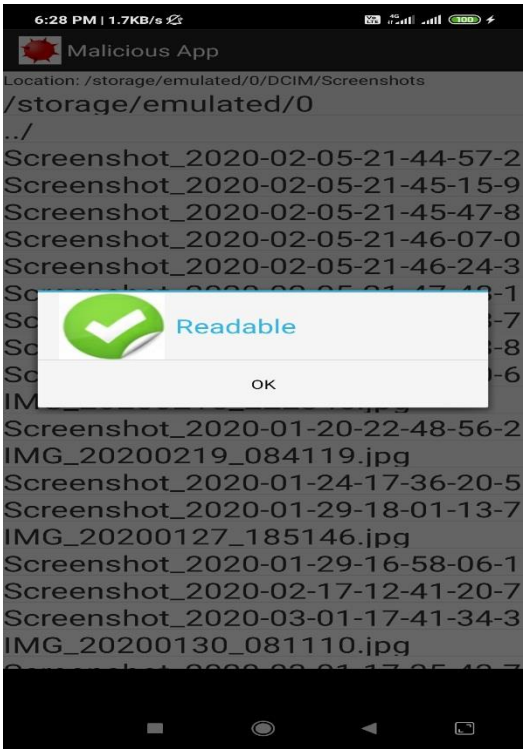


FIG 6: Access Image Files

## V. CONCLUSION

From the apps that were studied in this process, it was found that access_file_location could be removed from social networking apps without requiring direct source code changes. The only change required was to actually remove the permission request from the AndroidManifest.xml file and then recompile the app. The apps with the location permissions removed, were functionally stable after the permission removal. To prevent apps from reading contacts information generally requires some code changes in order to prevent the app from crashing or stalling. Bb studying this paper we come to know that the security on the android mobiles can be enhanced if we remove the permission access on our devices.

# REFERENCES

[1]. Ed Burnette, **"Hello Android Introducing Google's Mobile Development Platform",** Third Edition.
[2]. Herbert Scheldt, **"Java: The Complete Reference"**, Seventh edition, Tata McGraw Hill Publishing Company.
[3]. Vivian Sianhaan, Rismon Hasiholan Sianipar **"SQLite with JDBC for Beginners"**, 2019.

 