A New Approach to Secure Smartphone Applications

Jemima Abraham[1], Sneha Ambhore[2], Kanika Kapoor[3]
[1, 2,3]*Ajeenkya D.Y. Patil University*

***Abstract* -** In the 21st Century, smart phones are widely used in our day to day lives. As the use of smart phones increase, its features and its applications also increase simultaneously. Mobile applications cater to various smart phone users' problems. For every problem, there is at least one application that acts as a solution for the user. However, it is necessary to keep a check on which applications are running in the users' smart phones, as anyone can install or uninstall any application in the users' phone.

***Keywords* -** Application, Attacks, Installation, Security, Pin, Un-installation, Smart Phone

I. INTRODUCTION

Increase in smart phones and mobile application; have made human life very smooth and easy- running. However, the applications that the user downloads in his/ her smart phone have to be downloaded with the knowledge of the user. With the increase in mobile application, various monitoring applications, hacking applications are also evolving; this threatens the user for being monitored by another person.

Illustrations: The above mentioned situation can be illustrated with the help of two scenarios.

i). If a person 'A' has given his mobile to person 'B' for a particular purpose, there is no guarantee that person 'B' will not install any monitoring/hacking applications in person A's smart phone.

ii). If a person 'Y' has private photo album application installed in his mobile and person 'Z' finds out and uninstalls the application, this will cause a loss of data for person 'Y'.

In a smart phone, a person can directly install and uninstall applications in simple steps. This causes a threat of any unknown, hidden monitoring application to be installed in your system by a known/ unknown person as shown in illustration I. There is also a threat of losing private or important data by uninstalling any applications by known/unknown person as shown in illustration II.

Attacks: Based on the above mentioned threats following attacks can take place:

Data Theft: This attack can take place if the attacker has the intention of stealing any of the users' information stored in any application. By uninstalling the application in which the user has stored his/her information, it is impossible for the user to regain the data back if there is no backup.

- Man-In-Middle: By installing any spyware applications in the users' smart phone, the attacker can keep a watch on the user by performing passive attack.
- Spoofing: Spoofing can also take place if an attacker has installed a monitoring application in the victim's smart phone.

II. LITERATURE SURVEY

To protect smart phone users from any such attacks, the manufactures have come up with various applications and settings to protect their users from data breach. Many authors have researched on the smart phone security, privacy and protection of the users' information or data from unauthorized persons. [2].

A. AppLock - It is an application that was built to lock application, so that any unauthorized person cannot open it and read or edit any data [2]. Although at the time of creation the application had few vulnerabilities, in the recent days it's doing good in the market as the vulnerabilities have been considered and blocked. AppLock had recently introduced a security feature that makes sure that uninstallation of the AppLock will first confirm if the user is the authenticated person by asking for a pin or pattern that was set by the authorized user.

B. Two Factor Authorization - This system combines two authentication methods. For example location and biometrics can be combined. In GPS these options are used, where it helps in tracking the location of the user. Then the fingerprint authentication algorithm is used. This uses encryption in exchange of data after authentication [5].

C. Linux Kernel - It is used in Android as their system level security. It grants the operating system a user-based permissions model, process isolation, a secure mechanism for IPC, and the ability to remove any unnecessary or potentially insecure parts of the kernel [4].

D. Biometrics - It makes breaking into a system very difficult as it measures the unique characteristics of the user like, voice recognition, fingerprint, retina scan, etc. Fingerprint is said to be the most efficient authentication methods that follows three steps:

1. Enrolment
2. Searching
3. Verification

This system also provides secondary authentication by accepting pin from the user. Various online applications provide this security to authenticate their users [4].

E. One Time Password - OTP is another popular security feature used in online services. Many mobile applications such as WhatsApp, hike, WeChat also requests the user to enter the OTP before they start the application to check that the authorized person is using the application by sending a password to the users given phone number. OTP is generated based on time and location which makes it difficult for the hackers to know the exact details of the GPS application of the authorized person [5].

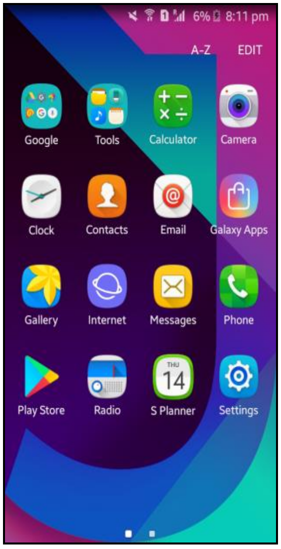
III. PROPOSED SYSTEM

Many such features and applications are being introduced on a regular basis by the manufactures, to keep their users safe from any attacks. In this paper, I have proposed another such security feature that will keep smart phone users from any unauthorized person from installing or uninstalling any application from Play Store. This feature is called as 'setting installation/uninstallation pin'. When the user has sent his/her installation/uninstallation pin, every time he/ she installs or uninstalls any application from their smart phone, they will be asked to enter the installation/uninstallation pin to confirm their action as an authorized user. The feature of setting the installation/uninstallation pin can be found by following these steps:

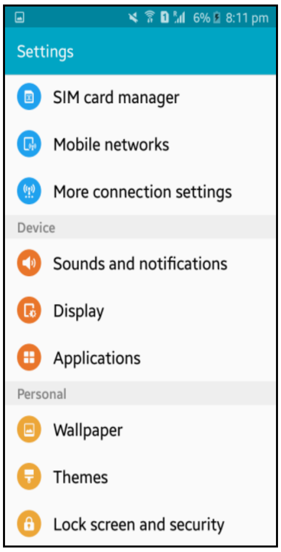
Setting -> Applications -> Application Manager ->More ->Set Installation/Uninstallation Pin.

One pin can be used for confirming both installing and unstalling an application.

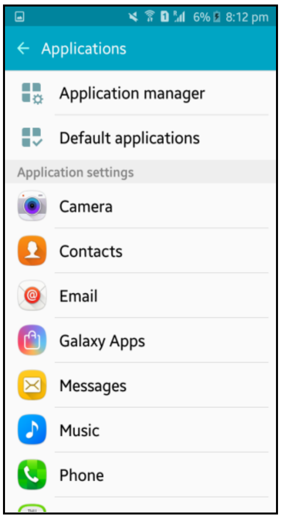
Steps 1 to 4 include click 'Settings' icon, select 'Applications', go to 'Application manager', and click on 'more option, respectively.



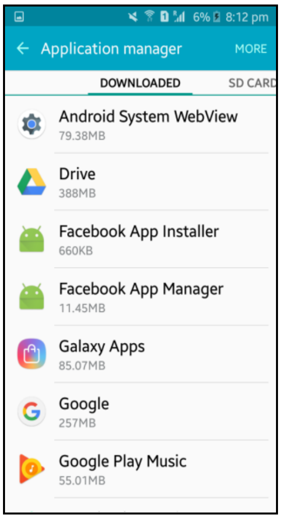
STEP 1



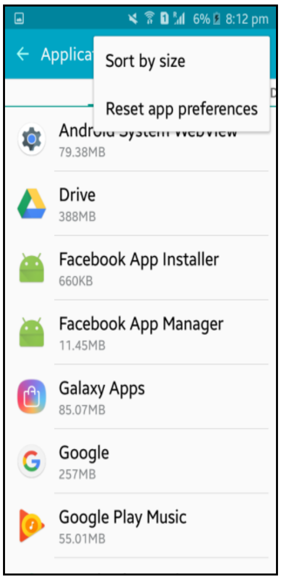
STEP 2



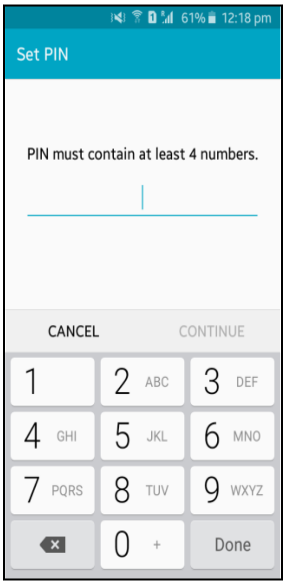
STEP 3



STEPS 4



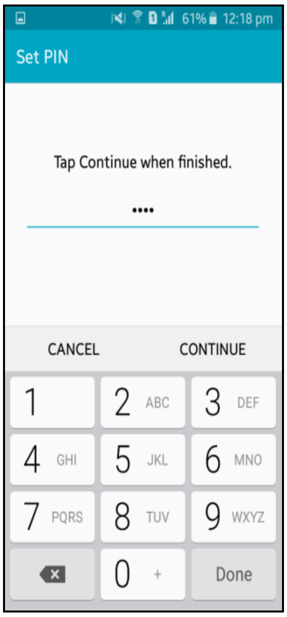
STEP 5



PIN must contain at least 4 numbers.

STEPS 6

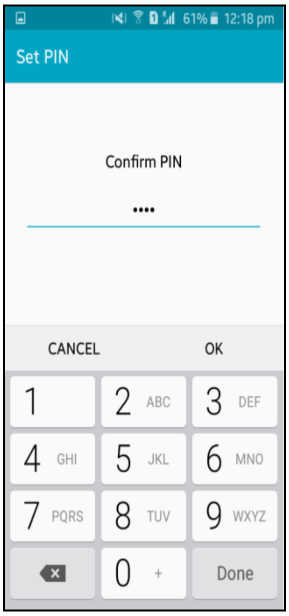
In Step 5, **installation/uninstallation** pin option can be added along with the two other settings that already exist within the 'more' option which can be found in the 'Application Manager'. Once the pin is set, every time the user installs any application from Play Store, he/she will be asked to confirm his/her installation by entering the installation pin.



Tap Continue when finished.

••••

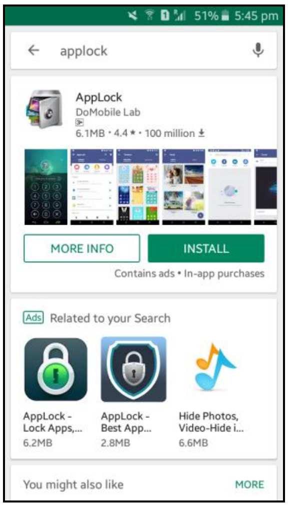
STEP 7



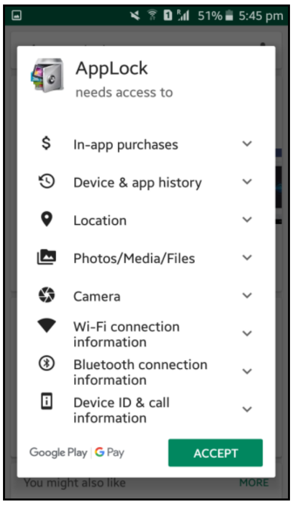
Confirm PIN

••••

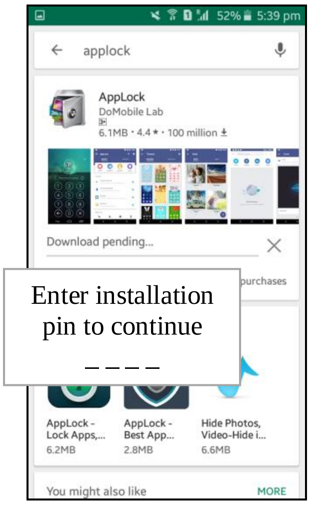
STEP 8



STEP 9



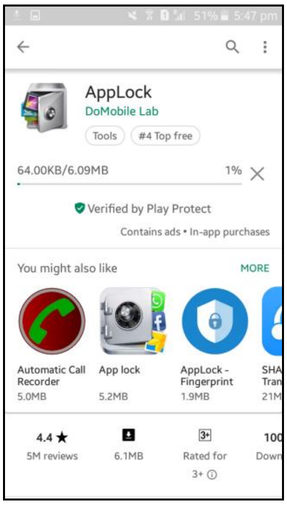
STEP10



Enter installation pin to continue

_ _ _ _

STEP 11



STEPS 12

IV. FUTURE SCOPE

This security feature that I have proposed helps in securing users from unauthorized persons from installing or uninstalling applications. In future if need arises, different pins can be set for installing and uninstalling just like setting different wallpapers for the mobile lock screen and home screen. Further, to make the security more complex, instead of pins, passwords can also be set.

V. CONCLUSION

This paper focuses on the security features and applications provided in smart phones to protect their users from any kind of attacks. However applications can be installed and uninstalled by anyone from Play Store. This creates a fear of any monitoring or tracking application being installed in the users' smart phone without his/her knowledge. This threat can be easily solved by implementing the above mentioned solution of installation/uninstallation pin, thus protecting the smart phone users from unauthorized person from installing and uninstalling any application.

VI. ACKNOWLEDGMENTS

I thank my guide Ms. Sneha Ambhore, for her ideas and knowledge on the topic that helped me complete this paper successfully.

VII. REFERENCES

[1]. https://www.cse.wustl.edu/~jain/cse571-11/ftp/mobiles.pdf

[2]. Mahmoud, A. Y., & Mahdi, A. O. (2016). Comments On Multi-window Against Mobile Application Lock. *Journal of Multidisciplinary Engineering Science Studies (JMESS)*, *2*(5), 494-497.

[3]. Jain, A. K., Flynn, P., & Ross, A. A. (Eds.). (2007). *Handbook of biometrics*. Springer Science & Business Media.

[4]. Ahvanooey, M. T., Li, Q., Rabbani, M., & Rajput, A. R. (2017). A survey on smartphones security: software vulnerabilities, malware, and attacks. *Int. J. Adv. Comput. Sci. Appl.*, *8*(10), 30-45.

[5]. http://www.pcworld.com/article/2010278/10-common-mobile-security-problems-to-attack.html

[6]. Woongryul Jeon, Jeeyeon Kim, Youngsook Lee, and Dongho Won, A Practical Analysis of Smartphone Security, Springer Verlag Berlin Heidelberg ,2011.

[7]. Yajin Zhou and Xuxian Jiang.Dissecting androidmalware: Characterization and evolution.Security and Privacy, IEEE Symposium on, 2012.

[8]. Yong-Tae Kim, Yoon-Su Jeong and Gil-Cheol Park,Analysis of Smartphone Security Problem - Android and iPhone, International Journal of Advancements in Computing Technology(IJACT) Volume 5, Number 11, July 2013.

[9]. Poornima Mahesh, AshwiniJayawant and Geetanjali Kale,Smartphone Security: Review of Attacks,Detection And Prevention, International Journal of Advanced Research in Computer Science and Software Engineering,Volume 5, Issue 3,March 2015.

Jemima Abraham,
Student of Ajeenkya D.Y. Patil University, Perusing the degree of BCA and Specializing on Cloud Technology and Information Security.