IJCSE International Journal of Computer Sciences and Engineering Open Access
Survey Paper Vol.-7, Special Issue-17, May 2019 E-ISSN: 2347-2693

Issues and Protection of Mobile Application Security

M. Angelin Rosy[1*], N.Shilpa[2], M. Felix Xavier Muthu[3]

[1,2]Dept. of MCA, Er.Perumal Manimekalai College of Engineering, Anna University, Hosur, India
[3]Dept. of Mechanical Engineering, St.Xavier's Catholic College of Engineering, Anna University, Nagercoil, India

Corresponding Author: angel_rosym@yahoo.co.in, Tel. - 9944579754

Available online at: www.ijcseonline.org

Abstract— Now a days, people give more important to the smartphones. Smartphone users are increasing day by day. Mobile device contains sensible data and hackers easily access our data. Avoid installing more free apps and cyber criminals to avoid cyber crime. All the vulnerabilities are increasing by the hackers. Use block option in some applications to block the camera. Use pin code, patterns, finger prints and iris scanner to secure Smartphone applications. Android platform will be made available under apache software and open source licence. To avoid cyber crime use antivirus software and firewalls keep them to update. Don't open email or attachment from unknown sources.

Keywords: Smartphone security, Mobile application development, Cyber crime.

I. INTRODUCTION

Now a days, people give more important to the smartphones. Smartphone users are increasing day by day. Mobile device contains sensible data and hackers easily access our data. Avoid installing more free apps and cyber criminals to avoid cyber crime. All the vulnerabilities are increasing by the hackers. Use block option in some applications to block the camera. Use pin code, patterns, finger prints and iris scanner to secure Smartphone applications. Android platform will be made available under apache software and open source license. To avoid cyber crime use antivirus software and firewalls keep them to update. Don't open email or attachment from unknown sources. Mobile devices like smartphones have found their means into our personal lives. To facilitate communication, orientation and provide mobile access to the Internet. Using smartphones during a business context appears to be a logical consequence. Smartphones, particularly in camera closely-held, area unit employed in all reasonably organizations, freelance of the corporate.

II. LITERATURE SURVEY

W.ENCK, D.octeau, PMC Daniel and s .chaudhri. They introduce decompiler in this mobile application security for recreate the source code in free applications. Dr.B.B.meshram, surveyed of Smartphone security the application developers are misbehaving the user's data.

III. EXISTING WORK

In mobile application development they are many platforms are there such as, Black berry os, ios, Android and Microsoft windows. In this mobile app security has some existing protection of Smartphone applications to enhance security. In this paper, existing mobile applications developers are generating the source code as visible in free applications. Patterns, pin codes and passwords are used to secure the applications. Smartphone apps security introduced a iris scanner to secure the applications. Iris scanner is used to hide photos, videos, text messages etc. It protects the user's data. so, there is no possible ways to hack our data .Avoid more installing free apps from apps store. Purchase and download the licensed apps, licensed apps are too secure. There is no way to hack our data while using licensed apps ,source code is not visible in these applications. use decompiler to recreate the source code fig 1.

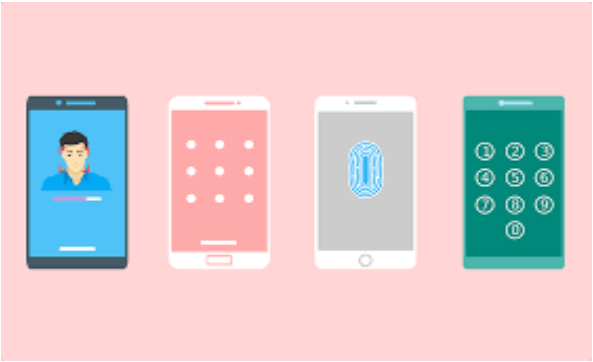

Figure 1. Mobile Application Security

IV. PLATFORM PROTECTION

OS protection policy is based on the user-applications run as the user and can access all the user's files. In

smartphones OS protection policy is based on applications. By default, each Smartphone application is isolated, e.g., sandbox policies in ios, and in Android. Permissions An isolated and unprivileged application has very limited functionality. Therefore, Smartphone platforms permit access to individual sensitive resources e.g., address book, GPS exploitation permissions, A permission could be a style of capability. In contrast to capabilities, they do not always support delegation. Each platform uses permissions in slightly different ways. Compare the differences between the most prominent platforms. There are 2 general forms of permissions: time-of-use and install-time. A time of use permission is approved by the user once the applying executes a sensitive operation, e.g., iOS's prompt to permit associate application access to location. Install-time permission is approved by the user when the application is installed fig 2. There are many platforms in smartphones they are:

- Black berry os
- Android os
- IOS
- Microsoft windows

Figure 2. Mobile Application Security

V. APPLICATION ANALYSIS

Android has available hundreds of thousands of applications .most of the apps are useless in the apps store. It is safer than any other source. Beyond this, there is a class of dangerous functionality that many reputable applications include, specifically disclosing privacy sensitive information such as geographic location and phone identifiers without informed consent by the user. There are limits to the security protections that can be provided by markets However, recent advancements in application analysis are moving towards more automated certification.

Figure 3. Mobile Application Security

Permission Analysis

Permissions articulate protection policy, but they describe what an application can do once installed the first to use Android permissions to identify dangerous functionality. To break dangerous practicality down into the permissions needed to perform it.If associate application doesn't have a requisite permission, the attack cannot occur applications, five of that were questionable once reviewing their purpose. They report an exponential decay in the number of applications requesting individual permissions fig 4.

Figure 4. Mobile Application Security

VI. PROTECT ANDROID APPLICATION USERS

Smartphone users should use trusted applications and use factor of authentication. Most of the users ignore this security features. Trusted applications are safer than the other applications, lock every app in your Smartphone by password, patterns, pin code and iris scanner. Android platform provides security features but there will be a risk if the user install suspicious apps or to allow permission to an applications. Android application needs permission from the user at the time of installation Use only apps from apps store, If you're not using Wi-Fi or

Bluetooth, turn them off Besides saving some battery life, network connections are often accustomed attack you. The Blue Borne Bluetooth hackers are still alive well, and ready to break your day. Don't give it a chance.

VIII. SOURCE CODE RECOVERY VALIDATION

Performed extensive validation testing of compiler. The included tests recovered the source code for small, medium and large open source applications and found no errors in recovery. In most cases the recovered code was virtually identical from the original source code. A trend to area unit restricted by the state of the art in decompilation. In order to understand the impact of decompiling retargeted classes verses ordinary Java class files, To perform a parallel study to guage Soot on Java applications generated with ancient Java compilers. A variety of packages, indicating we cannot do better while using Soot for decompilation. A possible way to improve this is to use a different decompiler.

VII. RESEARCH FINDING

Android using two types of security enforcement. At first, applications run as linux processes with their own user IDS and thus are separated from each other. The way of vulnerability in one application does not affect other applications. Android provides IPC mechanisms, which we need to secure a second enforcement mechanisms comes into play. Android implements a reference monitor to mediate access to application parts supported permission. If AN application tries to access another part, the tip user should grant the suitable permissions at installation time. Phone identifiers are leaked through plaintext requests. Phone identifiers used as device fingerprints. Phone identifiers, specifically the IMEI, square measure won't to track individual users. The IMEI is tied to personally identifiable information (PII). Not all phone identifier use leads to ex-filtration. Phone identifiers square measure sent to advertising and analytics servers.

Figure 5.Mobile Application Security

VIII. CONCLUSION

In this paper established how to secure applications in smartphones. Users can recreate the source Code in this paper establish Mobile applications. Use IRIS scanner to secure the applications. Do not allow to access the data to free applications buy the licensed App store metadata is plentiful and public although difficult to access. Many studies report this drawback, particularly in accessing information from Google Play. Majority of apps is Several studies tried together and mix ASCII text file with alternative app information. .Datasets of app store knowledge and executables have the advantage that they're independent of licensing of the application source code. Data from marketplaces can be scraped for free while APK archives can be downloaded from app stores.

REFERENCES

[1] A Study of Android Application Security William Enack, Damien Octeau, Patrick Mcdaniel, And Swarat Chaudhri Systems And Internet Infrastructure Security Laboratory.

[2] Mobile Application Security Platforms Survey Sardasht M.Mahmood, Bakhitier M.Amen, Rebwar M.Nabi International Journal Of Computer Applications (0975-8887).

[3]Security Risks and Their Prevention Capabilities in Mobile Applications Development Aneta of Information Technology, Lodz University Of Technology, Poland Information Systems In Management (2015).Vol.4123-134.

[4]The Role Of Mobile Networks-Apps Security Using Network Techniques S,Amutha International Journal Of Engineering And Techniques And Volume4 Issue1,Feb 2018.

[5]Defending Users Against Smartphone Apps: Techniques And Future Directions, William Enck North Carolina State University.

[6]A Survey Of Android Technology Shivam1,Ranjana Sharma2 International Conference On Advanced Computing(Icac-2016).

