International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 03 | Mar 2020 www.irjet.net p-ISSN: 2395-0072

System to Identify AND Define Security Threats TO THE Users ABOUT THE Illegitimate Installed Applications

Shashank Machare[1], Mahesh Patil[2], Ashwini Bansode[3], Tanvi Pawar[4], Mr. A.N Gedam[5]

[1,2,3,4]*Student, Dept. of Computer Engineering, A.I.S.S.M.S. Polytechnic, Pune, Maharashtra, India*
[5]*Lecturer, Dept. of Computer Engineering, A.I.S.S.M.S. Polytechnic, Pune, Maharashtra, India*

Abstract – *Mobile security is one of the most important aspect when it comes to keeping our data secure from any external attack like phishing, data hacking and many other attacks that can have very disastrous effects that may also lead to social disturbance, as in one's private data can be made public by the attackers. Indeed, one of the main reason for such attacks to get executed, the hacker need to get into the victim's mobile phone's system through which it can look for the loopholes that will lead him/her to the data that could be extracted by using the hacking techniques. Access to a very large amount of data in various formats like images and videos can be gained by simply getting inside the phone memory through a third-party application that has access to the phone's memory. Hence, there's a need of an application software that will detect such applications by scanning throughout the phones memory and inform the user about the possible threats posed by them.*

***KeyWords*: Application, Software, Security, Memory, third-party applications, scanning.**

1. INTRODUCTION

The android systems are usually found to be vulnerable to the external threats as the mobile devices are all the time exposed to the spywares and malwares that are spread throughout the internet abundantly. The hackers can easily gain access to a mobile phone which is connected to the internet through the website which the device is currently logged on. Hacker does the work of gaining access in the user's mobile device by using various techniques and harmful spywares. Data can be observed, and also exploited by the hackers easily. This can also be done by getting into the victim's phone's operating system through an .apk file. Usually, the applications are downloaded from the android play store which comes with the very famous google play protect scanning feature that helps in keeping the platform free from such applications that carry special encoded software programs to intentionally observe and steal user data from the phone memory. Of course everyone are aware that the play store is not the only source to download applications from, one such platform is the infamous 'Internet', by using an application browser we can access the web which is daily flooded with so many harmful applications that have been specially designed to steal the user data. Applications downloaded from the internet through a browser usually are not scanned for malwares, hence putting the user data at risk. These applications may carry specialized codes, on execution may look for private user data from the system memory and send it to the hacker's servers through the internet connection. We usually refer to such application as third-party applications and are installed by the user themselves unaware of the threats they may pose. Many times the applications are auto downloaded or installed in the phone memory whenever we visit a harmful website. Hence it is necessary to have an application that does the work of detecting such applications files lying inside the phone memory or are installed without the user knowledge.

1.1 PROBLEM DEFINITION

The main purpose of making an application that can scan through the phone memory and identify the underlying applications files that have been downloaded and are present in the system storage without the user's knowledge is to completely nullify the possibility of a security threat i.e data loss or hacking by the hackers.

1.2 LITERATURE SURVEY

All the modern devices come with in-built system to fight against the already acknowledged viruses by the operating system developers, which is updated through the regular security patches. But one main features missing in it is about finding the applications that have been installed or only downloaded and are yet to be installed in the phone memory from the unknown sources and could be easily identified as illegitimate application files that may potentially harm a device. So here we propose a 'System to identify and define security threats to the users about the illegitimate installed applications'. By using 'MobiSecure' application, the users can find the applications files that have been downloaded into their phone's memory without their knowledge.

2. PROPOSED METHODOLOGY

The proposed framework is an application that has all the ability to look throughout the phone memory for the application files usually with '.apk' extension. The main reason behind the development of application is the ability to offer real-time diagnosis of latest installed or downloaded files that can lead to cyber-attacks. The normal mobile phone users should be aware of every

installed application and their corresponding threats, which ideally are not known to majority of them, hence we aim at providing the users information about the threats a latest installed application software or file may contain.

'System to identify and define security threats to the users about the illegitimate installed applications' has following features:

- User and Device Interface
- File scanning function
- Threat finding feature
- Suggestion of threats to the user
- Listing the application files that are system-default hidden

3. SYSTEM ARCHITECTURE AND FUNCTIONING

The application developed is capable of running on minimum API 19 level that is it will support 97.3% android devices. The application has 2 main modules namely, Home page and Result display page. Our application is designed to scan for illegitimate applications that have been installed from unknown sources eg. Browser, shared through different media sharing platforms etc. Such application acts as the medium for various cyber attacks that would be executed by the hackers.

Explaining the modules:

1. Home page

Home page consist of a short summary to our application and its features and a scan button which on clicked starts to look for .apk files that usually don't come from a legitimate source, provided the data on the phone memory is accessible.

2. Result page

As soon as the scan is complete, the results from the scan i.e list of application is displayed on the result page with a short description. Also to make it more convenient for the users to take action on those applications, we provide with an option that will trigger the deletion of that specific application file from the phone memory hence nullifying all the risk the user were first exposed to.

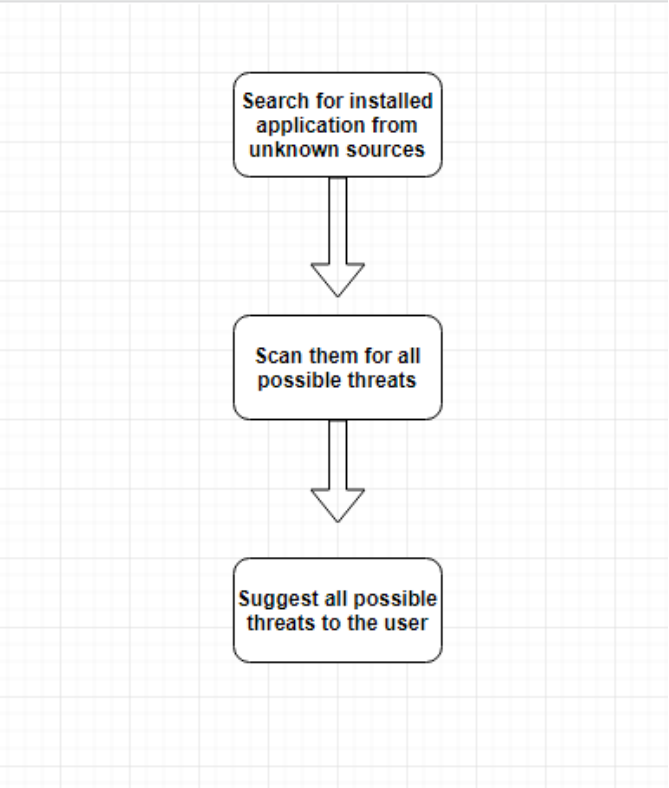

Fig -1: System Architecture

4. CONCLUSION

Using mobile application that has the capability of identifying the applications that may contain malware can substantially decrease the threat of various cyber attacks that are drastically increasing in this growing world of computers. 'MobiSecure' can nullify the risk of cyber attacks by identifying the applications that have been installed from illegitimate sources and providing the user an option to delete those applications from the phone memory.

5. REFERENCES

[1] P.K.Dixit, "Android", 2014.

[2] Philip K. Dick, "Do Androids Dream Of Electric Sheep?: The inspiration behind Blade Runner and Blade Runner 2049" , 16 Feb 2012

[3] Dave Maclean, Satya Komatineni, Grant Allen "Pro Android 5 (Apress)" , 2015

[4] Anubhav Pradhan,Anil V. Deshpande, "Composing Mobile App, Learn | Explore | Apply" , 2014

[5] Clifton ,"Andriod User Interfce Design: Implementing Material Design for Developers" , 3 Mar 2016

[6] Jon Erickson, "Hacking: The art of exploitation", 2nd Edition

[7] Steven Furnell, "Mobile Security: A pocket guide", July 2009