ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

Seeing Unseen: Detecting Malware Attack Vulnerablity in Android Smartphones

Rasika Deodhar[1], Isha Deshpande[1], Rutuja Gandhi[1], Suraj Jadhav[1,] Shital Kakad[2]

B. E Students, Department of Information Technology, Marathwada Mitra Mandal's College of Engineering Pune, Savitribai Phule Pune University, Pune India.[1]

Professor, Department of Information Technology, Marathwada Mitra Mandal's College of Engineering Pune, Savitribai Phule Pune University, Pune India.[2].

ABSTRACT: Android has become the most widespread mobile device OS today. Due to this popularity and also to its open source nature, Android-based smartphones are now an ideal target for attackers. There exists malicious software (malware) that affects the smartphones. Many ways have been introduced for a safer environment, yet vulnerabilities are seen. The malware threat for mobile phones is likely because of the permissions that an app carries with it. Often users download apps without checking the permissions. These permissions provide various accesses of the smartphones. These permissions make the smartphones vulnerable the most. This paper proposes an approach to detect vulnerability of malware attacks in Android Smartphones.

KEYWORDS: Risk communication**,** Mobile, Malware, Mobile Security

I. INTRODUCTION

[1]In recent years smart phones have become ubiqutious. Right from children to the elderly, naïve to skilled all around the world, there are different user base for mobile devices. More than 50 percent are smartphones now,this statistic excludes tablets and other mobile phones based system. The ubiquitous usage of these mobile devices poses new privacy and security threats. Our entire digital lives are often stored on the devices, which contain contact lists, email messages, passwords, and access to files stored locally and in the cloud.[2] Unfortunately, the increasingadoption of smartphones comes with the growing prevalence of mobile malware. Possible access to this personal information by unauthorized parties puts users at risk, and this is not where the risksend.In Android an appmust request a specific permission to be allowed access to a given resource. Depending on these permissions, different usage access gets provided, for eg. Usage of camera, Location, Media Access, etc. [3]These access results in Energy consumption. Often these Energy Consumption levels are controlled, but if the application turns malicious, energy consumption can increase drastically.

[4] Due to the risks of privacy-invasive spyware andmalware in traditional computing environments, newer platformsof permissions-based models have been switched to. Before installing applicationsAndroid warns the user about permissions. Therefore, it is important to communicate the risk of installing an app to usersso as to help them make a good decision about whether to install a given app or not.Android's current risk communication mechanism has been shown to be of limited effectiveness. Studies have demonstrated that users tend to ignore the permissions that an app requests and some recent work has attempted to overcome some of these limitations.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

II. LITERATURE SURVEY

1. Seeing the Unseen-

The colluding applications exchanges the data through local communication channel to built within the device to access sensitive data. Sender accesses the data but is not permitted to use the network; therefore colluding application which acts as a receiver, accesses the network and exfiltrates the information received, to external server.

Several covert channel are proposed to set between the sender and receiver - Type of Intent, File Lock, System Load, Volume Settings,Unix Socket Discovery, File Size,Memory Load.

Framework based on artificial intelligence tools, such as neural networks and decision trees, to detect the presence of malware using information hiding techniques based on power measurements is developed. Battery Consumption Evaluation is done on the basis of the above Artificial Intelligence techniques.

2. Catch me if you can

DroidChameleon, which is a systematic framework for evaluation of existing anti-malware softwares is developed. It has several common transformation techniques for Android applications.The applications are transformed automatically.Known malwares are passed through this framework to reproduce variants of the malware, further verified for original malware functionality.

3. Time and Location Power Based Malicious Code Detection Techniques for Smartphones

Detection of malware is foundation of Individual Power Consumption profiles. Three techniques which are designed, implemented and evaluated on Google's Android Platform are introduced, and are tested and with collection of data.

This paper focused on detecting malicious code on a smartphone without impacting its battery or hindering user interaction (by putting a strain on the processor), through a location-based detection technique that was designed to work within the capabilities of smartphones.

4. Dissecting Android Malware: Characterization and Evolution

Systematic categorization of malwares is done. Threefold representation is reported-

i. presentation of first large collection of 1260 Android malware samples in 49 different malware families.

ii. timeline analysis of discovery was obtained based on the collected malware samples. Then they were thoroughly characterized based on theircomplete detailed behavior breakdown.

iii. evolution-based study of representative Android malware was performed, which showed that the malwares were rapidly evolving and the existing anti-malware solutions were seriously lagging behind.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

III. PROPOSED SYSTEM ARCHITECTURE

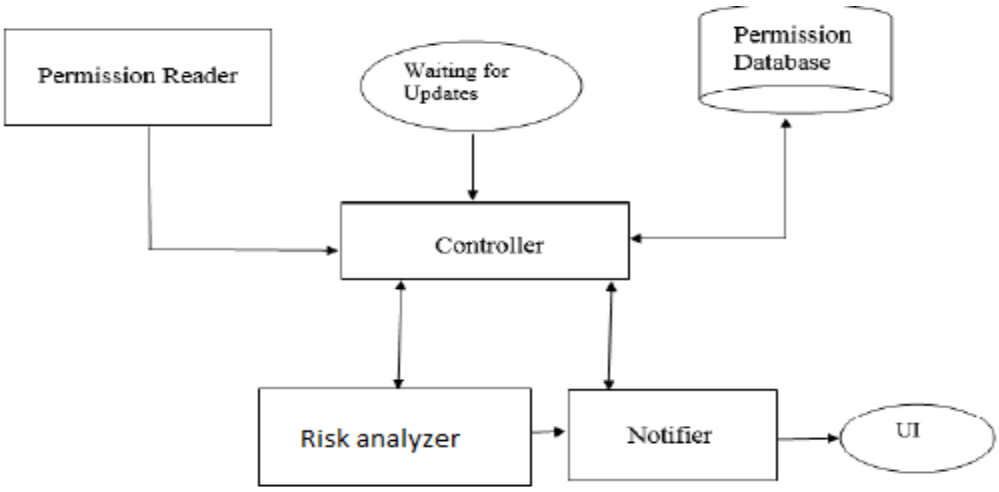

Fig A Proposed System Architecture

The mobile users are carrying mobile devices with positioning functionality. These mobile devices also can 1) communicate with the LBS database servers through the help of base stations; 2) communicate with other mobile users via wireless LAN or ad hoc network routing protocols, . In this paper, we assume that the mobile users are trusted and mean no harm to the system. But the LBS database servers are not trustworthy. Thus in order to preserve location privacy, users must query the servers with a cloaked region instead. So the LBS database servers do not have the knowledge of the exact location of mobile users but a cloaked region which may contain at least *k* anonymity.

IV. EXPERIMENTAL SET UP AND RESULTS

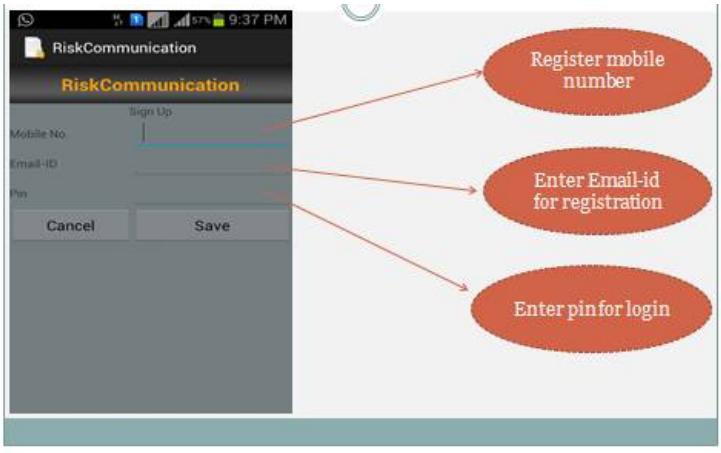

Fig. 1: Module 1: Registration/Login Page. First page – Userwould be asked for Mobile Number, Email-id and Pin for signing up, all for basic login purpose.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

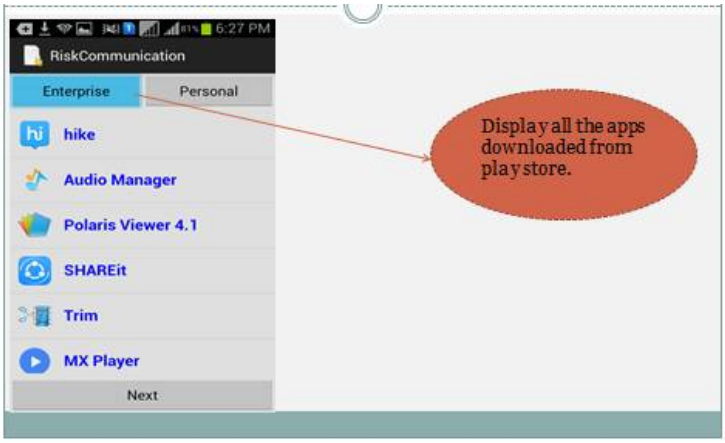

Fig. 2: Module 2: After selecting Enterprise Button, all the applications except thesmartphone's inbuilt ones would be listed.

Fig. 3: Module 2:Similarly, if Personal Button is clicked, all the personally designed applications (ex, designed apk files) would be listed

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

Fig. 4: Module 3 Part 1: If any application from any list is being clicked, user would see the details like- the Package name, Sevarity count and Vulnerability

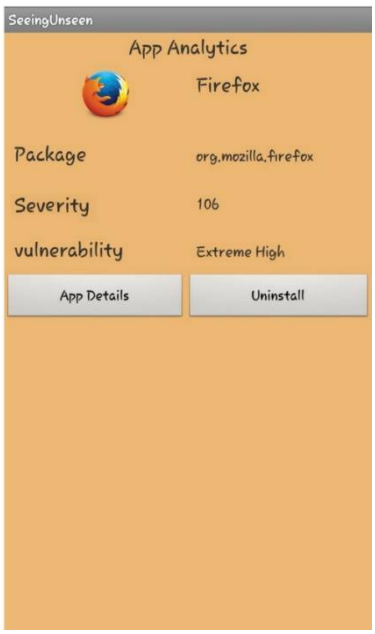

Fig. 5: Module 3 Part 2: If any application from any list is being clicked, user would see the details like- the Package name, Severity count and Vulnerability

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

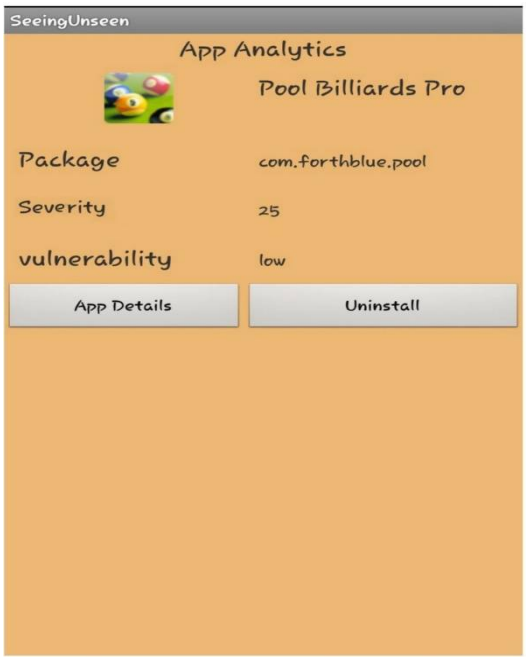

Fig. 6: Module 3 Part 2: If any application from any list is being clicked, user would see the details like- the Package name, Severity count and Vulnerability

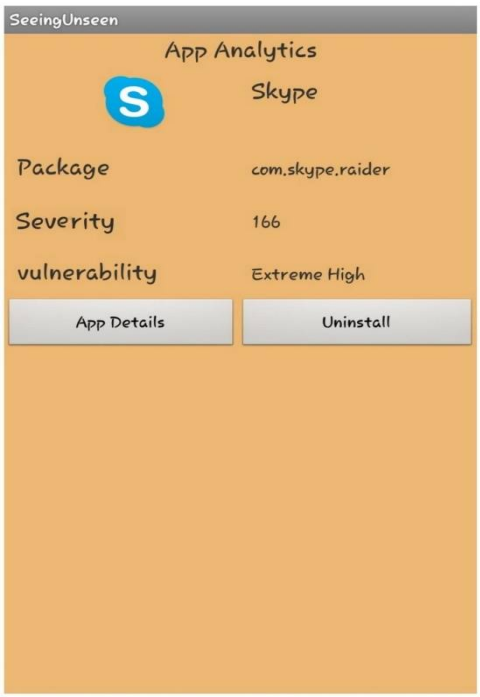

Fig. 7: Module 3 Part 3: If any application from any list is being clicked, user would see the details like- the Package name, Severity count and Vulnerability

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

V. FUTURE SCOPE

I. Reduce the false ration of system
II. Provide the positioning functionality to the mobile users.
III. Provides location detecting devices for the users.
IV. Developing in a system level

VI. CONCLUSION

In this paper, we have proposed a system which would detect the Malware attack vulnerability, based on the values of severity calculated by Decision Tree Algorithm. The applications on user's smartphone would be checked for the permissions they access. The severity value is calculated on the basis of rank given to the permission level, in a training matrix. The more severity value, more is the vulnerability level. Thus, maximum permission access leads to maximum consumption of battery and more vulnerability to exploit.

REFERENCES

[1]NiranjanBalasubramanian, ArunaBalasubramanian, ArunVenkataramani, "Energy Consumption in Mobile Phones: A Measurement Study and Implications for Network Applications," 2009 ACM 978-1-60558-770-7/09/11, November 4–6, 2009.
[2] (2011) Smartphone Shipments Tripled Since '08. DumbPhones Are Flat. http://tech.fortune.cnn.com/2011/11/01/smartphone-shipments-tripled-since-08-dumb-phones-areflat.
[3] IshaDeshpande, RasikaDeodhar, SurajJadhav, Rutuja Gandhi, ShitalKakad, "Malware Detection Using Energy Consumption In Smartphones ",I2CT
[4] Kevin Benton, L. Jean Camp, VaibhavGarg, "Studying the Effectiveness of Android Application Permissions Requests"
[5] Aaron Carroll, GernotHeiser, "An Analysis of Power Consumption in a Smartphone"
[6] NiranjanBalasubramanian, ArunaBalasubramanian, ArunVenkataramani, "Energy Consumption in Mobile Phones: A Measurement Study and Implications for Network Applications," 2009 ACM 978-1-60558-770-7/09/11, November 4–6, 2009.
[7] Yajin Zhou, Xuxian Jiang, "Dissecting Android Malware: Characterization and Evolution," 2012 IEEE Symposium on Security and Privacy, 2012.
[8] V. Rastogi, Y. Chen, and X. Jiang, "Catch me if you can: Evaluating Android anti-malware against transformation attacks," IEEE Trans. on Information Forensics and Security, vol. 9, no. 1, pp. 99–108, Jan. 2014.
[9] H.-A. Jacobsen, A.K.Y. Cheung, G. Li, B. Maniymaran, V. Muthusamy, and R.S. Kazemzadeh, "The PADRES Publish/ Subscribe System," Principles and Applications of Distributed Event-Based Systems. IGI Global, 2010.
[10] J. Bethencourt, A.Sahai, and B. Waters, "Ciphertext-Policy Attribute-Based Encryption," Proc. IEEE Symp. Security and Privacy, 2007.]
[7] Aaron Carroll, GernotHeiser, "An Analysis of Power Consumption in a Smartphone"
[11] W.C. Barker and E.B. Barker, "SP 800-67 Rev. 1. Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher," technical report, Nat'l Inst. of Standards & Technology, 2012.[9] Yajin Zhou, Xuxian Jiang, "Dissecting Android Malware: Characterization and Evolution," 2012 IEEE Symposium on Security and Privacy, 2012.