Available online at www.elixirpublishers.com (Elixir International Journal)

Network Engineering

Elixir Network Engg. 80 (2015) 30835-30838

ISSN: 2229-712X

Permissions based malware detection system for android a review and surveys

Sagar R. Aradwad, Sagar N. Tulsani and Bhushan S. Chaudhari
Sandip Foundation, Nashik, 422013, India.

ARTICLE INFO

Article history:
Received: 27 September 2014;
Received in revised form:
19 February 2015;
Accepted: 28 February 2015;

Keywords
Malwares, Android,
SmartPhones, Permissions,
Maachine learning,
MADAM, RADS,
Andromaly, Crowdroid.

ABSTRACT

Number of smartphones users is increasing rapidly and Android is currently the most popular Smartphone operating system. However, users feel their private information at threat, facing a rapidly increasing number of malwares for Android which significantly increasing that of other platforms. There are large number of apps available for the ease and use of the smartphone users. When a user installs any application from the google play store he/she is asked to grant some permissions to function the particular application properly. User either has to accept all those permissions in order to install the application on his/her device or he/she has to deny all those permission and terminate the installation of the application. A normal smartphone user is not aware of most of the permissions asked during installation so he/she tends to accept those all permissions in order to use the application. This introduces a potential threat to the users device. With this smartphones usage, mobile malware attacks are also growing. The application that we are developing will help user to identify the malicious applications that are installed on the device. And if a user finds any malicious activity being performed by any application then he/she can change the necessary permissions to avoid the malicious activity being done by the application. All this will be done post the installation of any application. So user will first have to accept all those permissions and get the app installed on his/her device from the Google play store. And then user can modify (allow/deny) the permissions the application is using. Our proposed application will have a scanning activity which will tell the user which applications are malicious and may harm the device. The application will use machine learning approach to some extent for scanning the applications to determine the application is malicious or not.

Introduction

Usage of the Smartphone is increasing day by day. All these functionalities gives opportunities to the attackers to get attracted towards the smartphones. Smartphone use is now not just limited to personal conversation but has expanded to financial transactions, internet banking and for storing personal data. This results in the vulnerability of malware attacks with the target for information and identity theft. In year 2004[1], the researchers from Kaspersky Lab first found the malware for mobile phones. That malware was known as called Cabire.

Thus from that time onwards the malwares in the phones increased largely depending on how popular that phone is. This paper mainly focuses on the mobile malwares and their analysis with various detection and prevention techniques.

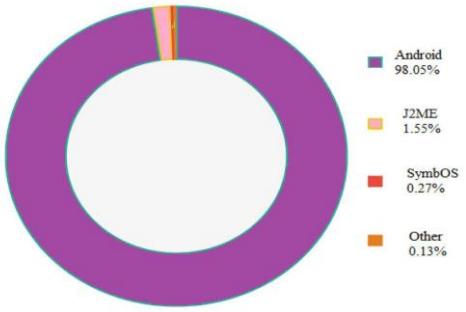

Fig 1. OS wise malware distribution

Basic Terms

Malware

It is the worldwide epidemic whose objective is to subvert the intended function.

Mobile Malware

Malicious software targets the devices in order to damage or removes and changes the entire system. These malwares targeted the Symbian OS [1] in year 2004. Such nefarious codes installs themselves or sticks up and comes in with the package we are installing. Further thus they perform functions without the users knowledge or permission. The goals of these mobile malwares are key logging, phishing, unwanted advertisements, spying, etc. [2].

Viruses and Trojans

Trojans in mobiles affects the devices by replicating themselves to smooth and unharmed programs. Thus later these Trojans which gets installed with the various apps carries the malicious actions. There is the great similarity between Trojans and the mobile viruses. Various third parties may use the malicious code in order to root the phone and gain the super authentication to access flash memory and various files.

Applications that are Phishing

Similar to the PC attacks, the malware attackers creates the phishing apps for the mobile. These apps seem to be legitimate services but they steal credentials in order to perform financial frauds. For an instance, recently there was one fake security app developed for Facebook, which assured that it would provide the

Tele:
E-mail addresses: sagar.aradwad@gmail.com

security to the Facebook users accounts, but rather have stolen the information of users.

Adware and Spyware

Spyware is the thing which collects the information that is confidential. It collects all this information from the user secretly and transfers this information to the third party. They also might advertise the information and hence referred to as the adware. It mainly accesses the information like location, browsing history, messaging habits, contacts and the downloading preferences. As the hardwares information it accesses the version of the OS, IMEI number, IMSI number, product ID which can be used as weapons for further more haphazard.

Botnets

Malwares mainly plays their role by affecting the programs that run in background. These malwares waits for the event to occur so that they can push themselves up into it and can do their intended tasks. They execute without letting the user know about their presence.

Who creates the malware?

Malware creators are also called as the hackers, crackers, or even the black hats. During the lifecycle of the software there are two checkpoints were the malicious code can be inserted. They are pre-release phase and post release phase. The hacker inserts the internal threat into the code before the release of the software. Later, the other people from the organization may inject the malware at the post release phase of the software.

Detectors of Malware

The malware detector shields the system by detecting malicious behavior. The malware detector performs its functions through various techniques. They accept two inputs namely information of malicious behavior, which comes from the phase called as learning and the other input is the program under inspection.

Malware Detection Techniques

Malwares detection techniques can be broadly differentiated into two main types signature based and the anomaly based. Signature detection focuses on the characterization of the maliciousness of the code which is to be inspected. Whereas the detection technique based on the anomaly refers to the knowledge information of the code under inspection. Anomaly detection is also called as detection based on the specification. It deals with the specific specification or the particular set of rules to detect what is the valid behavior so as to decide the programs malware nature. Programs which violate the mentioned specifications are treated as malicious.

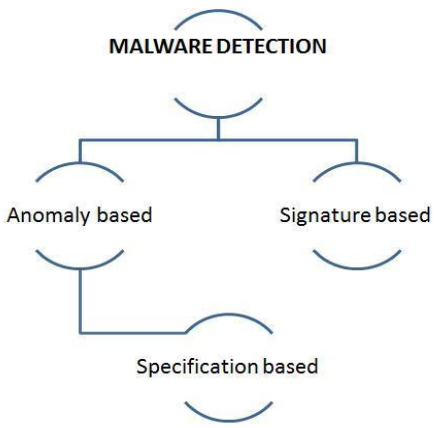

Fig. 2. Malware Detection Techniques

Various Markets

Smartphone users can download or buy the applications from various markets. Various Smartphones companies like Apple, Google, and Nokia focuses on the various markets for downloading various applications. Apple iOS phones permits the users using these phones to install applications only from the Apple App Store [4], also applications in the App Store are rated by Apple iOS for security. In case the users wish to install the apps from the other markets then they have to do jail breaking of their devices. But there exists ample risk in this process as it violates the phones warranty. In the same way Android provides their users with an official application Store the Android Market [2]. Android allows its users for installing apps from unofficial stores, although they are warned that this may cause malware. For Nokia phones they have appstore called as Ovi. Ovi is the authorized and official markets from installing applications from other sources presently.[16]

Related Permissions

Smartphone prevents the users by alerting them before installing any sensitive information. Permissions are not responsible to inject the spyware as the malware attacker gives the permissions while installation itself.

The permission system of Android is very extensive. Users often approve the permissions like access to contacts, Bluetooth, camera, messages, gallery, etc.

Dataset for mobile malware

This is the review on various well known iOS, Symbian, and Android malware, based on data which is gathered from public anti-malware databases. This section mainly focuses on the methodology and the literature survey

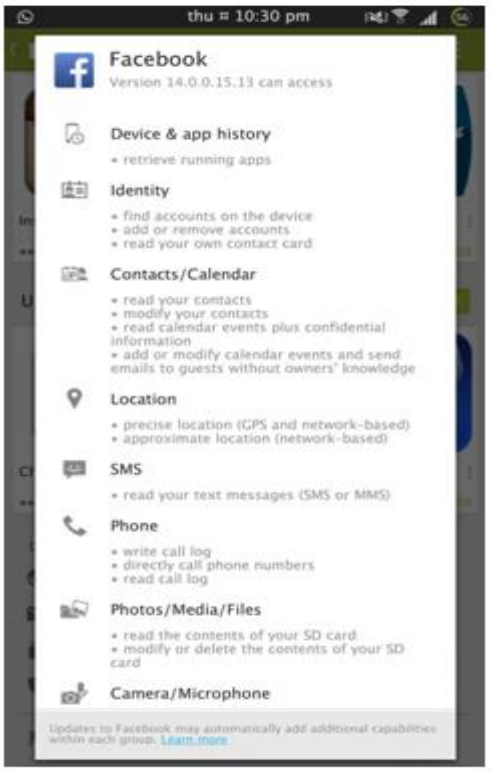

Fig. 3. Permission Required By Facebook App

Methodology Study

To find information about known mobile malware, the public databases of anti-virus companies is merged. The existence of each piece of malware is confirmed by at least two anti-virus vendors, and compared malware reports to identify cases where researchers had used different names for the same piece of

malware. Main focus of this review is to collect statistics about malware and the related work performed in past for the same.

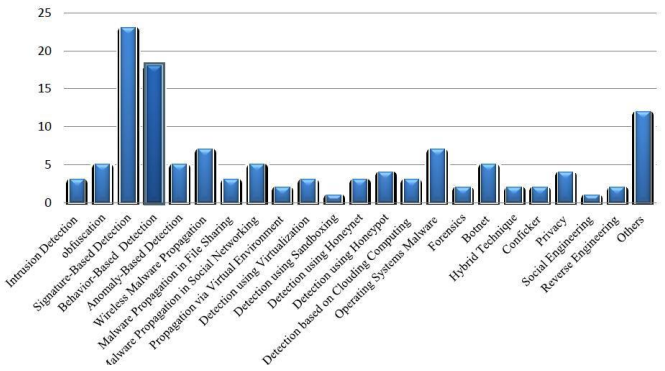

Fig. 4. Statistical Survey Of Malware Detection Techniques [14]

Related Work

Four malicious applications were developed to evaluate the ability to detect anomalies. MADAM: a Multi-Level Anomaly Detector for Android Malware [5] uses 13 features to detect android malware for both kernel level and user level. MADAM has been tested on real malware found in the wild and uses a global-monitoring approach that is able to detect malware contained in unknown applications, i.e. not previously classi-fied. [6]MADAM is the framework which attempts malicious actions performed by real malware on Android platform. The framework exploits a multi-level approach i.e. that combines features at the kernel-level and at the application level, and is based upon machine learning techniques. The first prototype of MADAM for Android Smartphone has managed to detect all the 10 monitored real malware, with an impact on the user experience due to the few false positives issued per day. Crowdroid [2] is a machine learning-based framework that recognizes Trojan-like malware on Android smartphones, by analyzing the number of times each system call has been issued by an application during the execution of an action that requires user interaction. A genuine application differs from its trojanized version, since it issues different types and a different number of system calls. Crowdroid builds a vector of m features (the Android system calls). Another IDS that relies on machine learning techniques is Andromaly [3] which monitors both the smartphone and users behaviors by observing several parameters, spanning from sensors activities to CPU usage. 88 features are used to describe these behaviors; the features are then pre-processed by feature selection algorithms. T Monitors smartphones to extract features that can be used in a ma-chine learning algorithm to detect anomalies. The framework includes a monitoring client, a Remote Anomaly Detection System (RADS) and a visualization component. RADS is a web service that receives, from the monitoring client, the monitored features and exploits this information, stored in a database, to implement a machine learning algorithm.[7] proposes a behavior-based malware detection system (pB-MDS) that correlates users inputs with system calls to detect anomalous activities related to SMS/MMS sending. [8][9] Propose Kirin security service for Android, which performs lightweight certification of applications to mitigate malware at install time. Kirin certification uses security rules that match undesirable properties in security configuration bundled with applications.[10] Performs static analysis on the executables to extract functions calls usage using various techniques.[12]

Mathematical Model

Step 1: User will download the application from playstore
User: U
Application: A
Playstore: P
Permission manager: Pm
Scanner: S
Permissions: Ps
Downloads(U, A)
2 U(User(U)) ! downloads(AppfromP laystore(P))

Step 2: When the user installs the applicaton, the Scanner checks the app installed on the user phone.
2 S(Scanner(S)) ! Checks(Application(A))
S(Scanner(S)) ! Scans(ApplicationContents)
S(Scanner(S)) ! P rompts(MaliciousContents)
S(Scanner(S)) ! diverts(P ermissionManager(P m))

Step 3: Permission manager lists all the permissions of the application. Also it will give the chance to user to toggle those permissions.

2 P m(P ermissionManager(P m))! Checks(ApplicationConents)

2 P m(P ermissionManager(P m))! Lists(P ermissions(P s))

2 P m(P ermissionManager(P m))! P romptschange(P ermissions(P s))

Step 4: User changes the Permissions prompted by the permission manager.
2 U(User(U)) ! Changes(P ermissions(P s)) 2 U(User(U)) ! Installs(Application(A))

A. Sequence Diagram

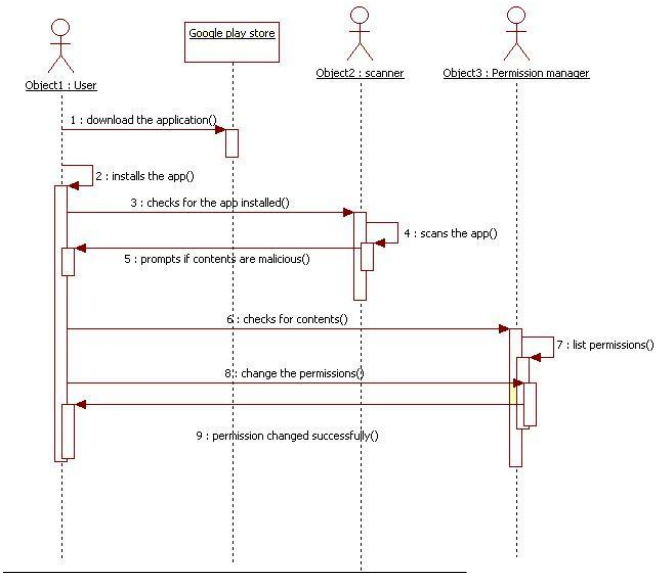

Fig. 5. Use Case Diagram for the System

Fig 4. shows the sequential flow amongst the various objects in the system.

Literature Survey

Analysis Of Malaware Detection Techniques Table

Table I. Analysis of malaware detection techniques table

Sr.No	Name Of Project	Techniques
1	Crowdriod[2]	ML
2	Andromaly[3]	SML
3	MADAM[6]	ML
4	RADS[7]	BBML

Conclusion

Rapid increase is seen in phones these days. Android OS is the leading market. There are various testing methods available but it requires large scale of testing required. Users running our application will be able to see their own Smartphone behavior. They could even alert the users when one of their applications shows an abnormal trace. The system can also act as an early warning system, capable of detecting malicious or abnormally behaving applications in the early stages of propagation.

There is a survey done on the behaviour of current mobile malware payloads. Presently, mobile malware is motivated primarily by a desire to send premium-rate SMS messages and sell information. There is also survey made on the permissions of Android malware. Android malware commonly requests the ability to directly send SMS messages, which is uncommon among non-malicious applications. Information more importantly user should be careful enough rather than blindly downloading an application.[15]

Future Scope

User will be able to detect a high risk malware app while installation.

User will be able to change the permissions it has granted after installation.

User will get a warning to not install the app.

Protecting the mobile from unauthorized access and securing its data and its contents.

Acknowledgement

We would like to thank our guide Prof. Bhushan Chaudhari for the guidance and support.

Reference

[1] Trend Micro. A Brief History of Mobile Malware .

[2] Dupaul, N. Common Mobile Malware Types: Cyber security 101 , Oct 2013.

[3] I. Burguera, U.Z., Nadijm-Tehrani, S.: Crowdroid: Behavior- Based Malware Detection System for Android. In: SPSM11, ACM(October 2011)

[4] A. Shabtai, U. Kanonov, Y. Elovici, C. Glezer, Y.Weiss: Andromaly: a behavioral malware detection framework for android devices. Journal of Intelligent Information Systems 38(1) (January 2011) 161-190.

[5] G. Dini, F.Martinelli, A. Saracino, D. Sgandurra: MADAM: a Multi-Level Anomaly Detector for Android Malware

[6] Schmidt, A.D., Peters, F., Lamour, F., Scheel, C.Camtepe, s.A., Albayrak, S.: Monitoring smartphones for anomaly detection. Mob. Netw.Appl. 14(1)(2009) 92-106

[7] Xie,L.,Zhang,X.,Seifert, J.P.,Zhu, S.: pBMDS: a behavior-based malware detection system for cellphone devices. In: Proceedings of the Third ACM Conference on Wireless Network Security, WISEC 2010, Hoboken, New Jersey, USA, March 22-24 2010, ACM(2010) 37-48

[8] Enck,W., Ongtang, M., McDaniel, P.: On lightweight mobile phone application certification.In: CCS 09: Pro-ceedings of the 16th ACM conference on Computer and Communication Security, New York, NY, USA, ACM (2009) 235-245

[9] Ongtang, M., McLaughlin, S., Enck, W., McDaniel, P.: Semantically Rich Application- Centric Security in An-droid. In: Computer Security Applications Conference, 2009. ACSAC 09. Annual.(Dec 2009) 340-349

[10] Schmidt, A.D., Bye, R., Schmidt, H.G., Clausen, J.H., Kiraz, O., Yuksel, K.A., Camtepe, S.A., Albayrak, S.: Static Analysis of Executables for Collaborative Mal-ware Detection on Android. In: Proceedings of IEEE International Conference on Communications, ICC 2009, Dresden, Germany, 14-18 June 2009, IEEE (2009) 1-5

[11] International Journal of Electronic and Electrical Engineering. ISSN 0974-2174 Volume 7, Number 7 (2014), pp. 717-722 International Research Publication House

[12] Literature Analysis on Malware Detection

[13] A Survey on Techniques in Detection and Analyzing Malware Executables International Journal of Advanced Research in Computer Science and Software Engineering

[14] Survey on mobile malware : A war without end MADAM: a Multi-Level Anomaly Detector for Android Malware International Journal of Computer Science and Business Informatics ISSN: 1694-2108 —vol. 9, No. 1. JANUARY 2014

[15] A Survey On Malware Propogation,Camtepe, s.A., Albayrak, S.: Monitoring smartphones for anomaly detection. Mob. Netw.Appl. 14(1)(2009) 92-106 ANALY-SIS, AND DETECTION International Journal of Cyber-Security and Digital Forensics (IJCSDF) 2(4): 10-29. The Society of Digital Information and Wireless Communications 2013 (ISSN: 2305-0012)

[16] Permission Based Andriod Malware detection,Zarni Aung, Win Zaw;