International Journal of Engineering Research and Science & Technology

ISSN : 2319-5991
Vol. 1, No. 2
April 2015

2nd National Conference on "Recent Advances in Science Engineering & Technologies" RASET 2015

Organized by

Department of EEE, Jay Shriram College of Technology, Tirupur, Tamil Nadu, India.

www.ijerst.com

Email: editorijerst@gmail.com or editor@ijerst.com

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
Special Issue, Vol. 1, No. 2, April 2015
2nd National Conference on "Recent Advances in Science, Engineering&Technologies" RASET-2015

Research Paper

ANALYSIS OF SUSPICIOUS BEHAVIORS OF MALWARE IN ANDROID

S R Ruthra Devi[1]*, S Kayathiri[1], G Arun Prassath[1], M Sivasankari[1] and M Nandhini[1]

*Corresponding Author: ***S R Ruthra Devi***

Android based Smartphone are now a day's getting more popular. With the use of Smartphone, user must always concern about the security breaching and malicious attacks. The phone security still faces many challenges in securing highly confidential contents. Introducing an approach for proactive malware detection working by abstraction of program behaviors. Suspicious actions are detected by comparing trace abstractions. The trace abstraction helps to eradicate the malware from the device. Analyze the programs or applications, then represented them as footprint languages, which are abstracted by altering with respect to elementary behavior patterns. The extraction is done by Static analysis and Dynamic analysis. The device will automatically detect and prevents the spread of malware beyond its early stage. The "Analysis of Suspicious Behaviors of Malware in Android" an automatic containment strategy aimed at existing approaches to protect mobile devices against the classes of attacks into varoius categories, based upon the track down principles, architectures, collected data and operating systems. The model detects and prevents the malware at their early stage from spreading into the other applications. The malwares get eradicated from the device without affecting the ongoing process in the mobile phone. The traffic and non-traffic worm scan is performed for detecting and trashing the malwares from spreading.

Keywords: Smartphone, Malware, Attacks, Static Analysis, Dynamic Analysis, Traffic and non-traffic worm scan

INTRODUCTION

Mobile devices, such as smart phone or Personal Digital Assistant have become more and more widespread, and often essential in our everyday life. Usually the mobile devices contain lots of sensitive information such as a list of contacts, ingoing/outgoing call, text messages, and on latest model a calendar of our schedule, emails, our current position (if the phone has embedded GPS). Latest models feature a complete OS, but for many people they are no more than phones, so there is a derogation of the risk connected to phone security. The user does not know about the security threats and damages of data due to the lack of phone security. This makes Phones an interesting target for malicious users. The

[1] Department of Information Technology, SNS College of Technology, Coimbatore, TamilNadu, India.

malicious users access the user's personal data illegally and damage their contents.

The security threats include physical security, access passwords and prying eye protection. Damages that a user can sustain are loss of money, privateness and arrest the processing speed, battery life. Sometimes user's personal details can also get damaged by the malicious users. Reverse Engineering of Malware Analysis is a process which is used by forensic investigators and system engineers to analyses the flow, operation, functionality of malware. So it is important to have an anti-virus application for all mobile devices to prevent the malicious attacks in the early stage. The anti-virus application prevents and eradicates the malware from being spreading to other applications. The anti-virus application eliminates the malware without affecting the process of the mobile device. It will eliminate the malware at their early stage.

PROBLEM DEFINITION

In order to detect malware, a combination of the deterministic epidemic model and a general stochastic epidemic model is used to model the effect of large-scale malware attacks. The complexity of the general stochastic epidemic model makes it difficult to derive insightful results that could be used to contain the malware. It is difficult to prevent malwares in large-scale. The stochastic epidemic model is used to detect the presence of a malware by identifying the trend, not the rate of the observed invalid scan traffic.

The model will not differentiate the non-traffic worm scan from the traffic worm scan. The applications get damaged due to the lack in scanning security of malware. The anti-virus application may also get damage due to the malware. In those situation it is difficult to prevent malware with the damaged anti-virus application. So self-scanning is needed to detect and eliminate the malware at the early stage.

PROPOSED SYSTEM

Review of behavior of malware analysis model leads to the development of an automatic malware containment strategy that prevents the spread of a malware beyond its early stage. It automatically detects and eradicate the malware before it starts spreading to other applications. Obtaining the probability that the total number of hosts that the malware infects is below a certain level. If the probability goes beyond the certain limit, the device will automatically scans for malware detection. The strategy can effectively contain both fast scan malware and slow scan malware without knowing the worm signature in advance or needing to explicitly detect the malware.

Once the malware got detected, the device will automatically prevents the malware from spreading. Before the device starts scanning the application, the anti-virus application scans itself to detect whether the application shows any misbehavioral activities. If the anti-virus application detects itself to be affected by malware, it automatically scans itself and prevents the malware from spreading. After eradicating the malware from the application, the device starts scanning the other applications installed in the mobile phones. The application mainly concentrate on the running applications. The frequently used applications given more preference than other applications. Suspicious behaviors are detected by comparing with the malware database provided. The automatic malware containment schemes effectively contain the malware and stop its spreading.

GETTING INSTALLED APPS

Android has a growing selection of third party applications, which can be acquired by users either through an app store such as Google Play or the Amazon Appstore, or by downloading and installing the application's APK file from a third-party site. The Play Store application allows users to browse, download and update apps published by Google and third-party developers, and is pre-installed on devices that comply with Google's compatibility requirements. The app filters the list of available applications to those that are compatible with the user's device, and developers may restrict their applications to particular carriers or countries for business reasons. But most of the users download the APK files from third party servers and installed into mobiles. Most of the apps from trusted sources are not malware, but the third party server provide malwares in modified APK. So user has the power to list all the apps installed in their mobile, then user can identifies the Application is malware.

GETTING RUNNING TASKS

In Android, processes and Applications are two different things. An app can stay "running" in the background without any processes eating up your phone's resources. Android keeps the app in its memory so it launches more quickly and returns to its prior state. When your phone runs out of memory, Android will automatically start killing tasks on its own, starting with ones that you haven't used in frequently.

Mostly malwares are running in the background without the user knowledge, so that can be send and receive anonymous data to any remote server. User can detect the application and remove it, If the user not opened any app but they automatically running in the background, its known as malware.

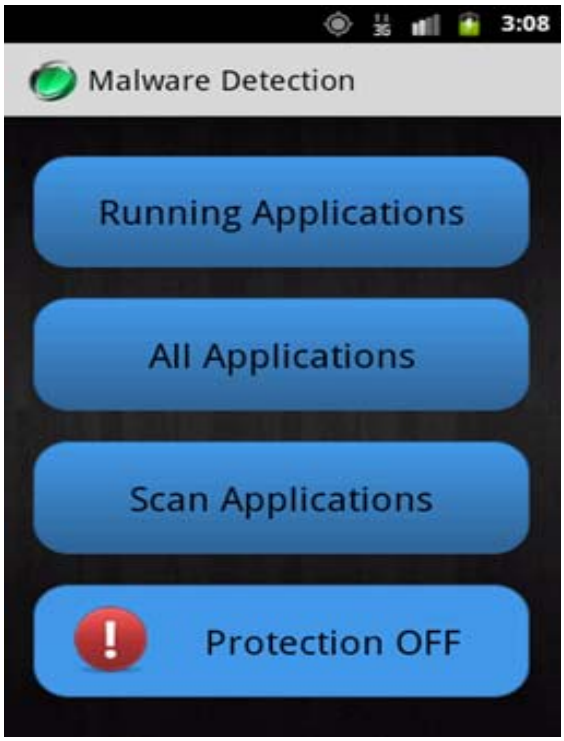
EXTRACT INFORMATION

Android security model highly relies on permission-based. There are about 130 permissions that govern access to different resources. Whenever the user installs a new app, he would be prompt to approve or reject all permissions requested by the application. In this module if user select's any running application its Manifest permissions are shown to the user. It can be easy for the user to identify the malware. For example a gaming application requires SMS permission, but there is no need for SMS in that application. So the application can send premium rated SMS to any number in background.

MALWARE DETECTION

There are many malwares floating in the web that

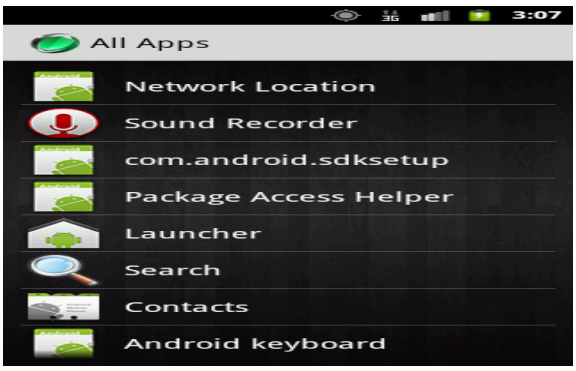
Protection Mode Off



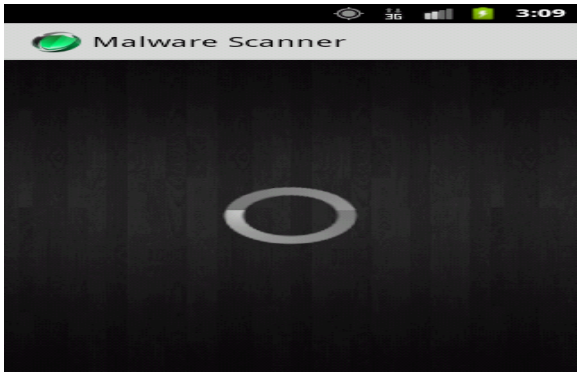
Protection Mode On

Scanning Running Applications

Scanning All Installed Applications



Scanning Of Applications



can be affecting the android OS, maintaining a huge collection of malware database used to find the identified malwares. If the user scan the entire application installed in their mobile each application will be compared to the malware database, if any app found malware, the system shows error and instruct the user to uninstall the particular application.

User no need to scan for every time for malware when installing any application, system automatically scan the newly installed application for malware whenever user install any new application. If the application is found malware. It shows error notification.

CONCLUSION

Every personalized gadget faces certain levels of threats in its security level. On enhancing malware detection with self-scanning as an additional feature, highly promotes the system to a safer side than usual. Implementing this feature can also be effective in defending any application by itself, when self-scanning is made a part of its module. So that no other separate defender would be required to secure its privacy. Self-scanning plays a vital role in eliminating the malwares at the early stage and prevents the malware from

spreading into other applications. Thus malware detection for android is very efficient by providing a barrier at the initial stage rather than a massive spread.

FUTURE WORK

Self-scanning feature when applied as a part in every application can provide high security level in combination with a separate scanner application. Malicious software are being developed to attack the private contents benefiting the worm developers with ransom or other cyber wars. Self-scanning would be an effective idea for defending the untrusted contents entering the security part, when made as an inbuilt feature in every emerged or emerging software, safeguarding the system and when safeguarding the system as a whole, it acts as a double protection to the entire gadget which would become tough for the hackers to find the loop holes.

REFERENCES

1. Mariantonietta la Polla, Fabio Martinelli, and Daniele Sgandurra, a survey on security for mobile devices" IEEE communications surveys & tutorials, accepted for publication" 1553-877x/12/ 2012 IEEE.
2. Emre Erturk" A Case Study in Open Source Software Security and Privacy: Android Adware" World Congress on Internet Security (WorldCIS-2012). 978-1-908320-04/9/$25.00©2012 IEEE.
3. Addodil Jo Elv Arg Hese, pro. F Stuart Walker, dissecting Andro malware, 2011 The Sans Institute.
4. Drienne Porter felt, Matthew Finifter, Erika Chin, Steven Hanna, and David Wagner, a survey of mobile malware in the wild, Acm 78-1-4503-1000/11/10, october 17, 2011, chicago.
5. Rajdeep Chakraborty, "detailed analysis of the continuously evolving threat of malwares", retrieved, last accessed: 24 august, 2011.
6. Dennis Distler, 'Detailed analysis of the continuously evolving threat of malwares', retrieved Last Accessed:24 August, 2011.
7. Google android http://developer.android.com/guide/basics/what-is-android.html.
8. Troy Vennon, "Threat analysis of the android market",http://www.globalthreat center.com/wpcontent/uploads/2010/06/android-market-threat-analysis-6-22-10-v1.pdf,last accessed: 24 august, 2011.
9. Johannes Kinder, Stefan Katzenbeisser, Christian Schallhart, and Helmut Veith. Proactive detection of computer worms using model checking. IEEE transactions on dependable and secure computing, 7:424{438, October 2010.
10. Dong-Jie wu1, Ching-Hao mao2 "Droidmat: android malware detection through manifest and API calls tracing"2012 seventh Asia joint conference on information security. 978-0-7695-4776-3/12 /IEEE.
11. Takamasa Isohara, Keisuke Takemori and Ayumu Kubota" kernel-based behavior analysis for android malware detection" 2011 seventh international conference on computational intelligence and security 978-0-7695-4584-4/11 2011 IEEE.

International Journal of Engineering Research and Science & Technology
Hyderabad, INDIA. Ph: +91-09441351700, 09059645577
E-mail: editorijlerst@gmail.com or editor@ijerst.com
Website: www.ijerst.com