Volume 3, Issue 11, November 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Enhanced Secured Cloud Oriented Detection Mechanism for Android Applications

Mr. Vishal S. Patil[1], Mr. Sushant A. Patinge[3]
ME 2ND Year, Dept of CSE
P R Patil College of Engg. & Tech.,
Amravati -444605, India

Mr. Chetan J. Shelke[2]
HOD Dept of IT
P R Patil College of Engg. & Tech.,
Amravati -444605, India

Abstract: ***As in recent era of computers and internets, mobiles devices, Smartphone's plays a vital role in human day to day life. Also nowadays Smartphone's, tablets are becoming very popular especially android OS based Smartphone's are gaining much more popularity as compared to Apple's iOS. These Smartphone's having various apps and features based on only internet but these new emerging features of these devices give opportunity to new malwares & threats. Android is comparatively new operating system hence its makes very hard to detect and prevent these viruses and malwares attacks by using some traditional mechanisms. So security of these Smartphone's is now becoming very popular issue of researchers. The lack of standard security mechanism in Android applications is very advantages to hackers. So to overcome these various pitfalls we use cloud services as a security weapon for providing decent security system for Android applications.***

Keywords: Android OS, Smartphone's, Malwares, Cloud Services, Applications Security.

I. INTRODUCTION

Recently the use of Smartphone's based on Android OS has increased rapidly hence providing better security policies is becoming most important area of research. As Smartphone's devices are being rapidly utilized by enterprises, and various government agencies also in military services, security plays an important role, because many users uses these devices to hold their valuable sensitive data, attackers may use this sensitive information with wrong intent. Mobile viruses can cause many types of damages like, private data leakage, remote listening etc. also they can congest the servers by sending many unwanted messages and spam's and reduces the efficiency of communication network. Hence in order to control these malware attacks in Smartphone's some crucial steps must be taken to provide some efficient mechanism for controlling the growth and productions of these viruses.

Anti-virus research is recently ongoing process for identifying and analyzing new and unknown malware for extracting possible detection scheme that can be used within some anti-virus software. There exits some virus and malware detector software that can scan and block viruses, Trojans that are infecting Android applications. Most malwares is being detected by scanning in signature database. For generating the reports and special signatures the infected application need to be analyzed and carefully observed so that we can collect some meaningful pattern about the specific malware.

One approach to transfers the limited functionality of Smartphone's, is to off-load workload into the cloud. Taking advantage of the cloud is a very good approach, since a service in the cloud can be changed as needed, but modifications to the Smartphone's devices are very difficult. There are various applications like CloneDroid [1] which introduces the idea of offloading parts of programs into a cloud for speeding-up and saving power. Also ParanoidAndroid [2] offers a system in which the device is replicated into the cloud, and various security applications are applied on the replicas that had been created. One big advantage of shifting the security mechanism into the cloud is the almost indefinite processing power and "battery" capacity. This makes it possible to run every resource intense security services that would not be offered by the phone. If the phone is replicated in the cloud, this also allows the developer of a security service to extend this service without changes on the phone. The security service can examine the phone not only from inside its system but it can also monitor the replica itself which runs the cloud This can further improve the chances of detecting malicious software and open up possibilities that would not be provided by the device itself. [1, 2].

II. LITERATURE REVIEW

Following are the various research related to the topic which had been previously done which includes

A. Applying Behavioral Detection on Android-Based Devices

Shabtai A. and Elovici Y. present a light-weight, behavioral-based detection framework called Andromaly for Android Smartphone's, which realizes a Host-based Intrusion Detection System (HIDS). The detection system runs directly on the device and monitors various features and events on the Smartphone and classifies them as benign or malicious. They evaluate their framework by testing game and tool applications, where the classification algorithm is able to distinguish between those two kinds of applications. The authors evaluate several combinations of

classification algorithms and feature selections and conclude that the proposed anomaly detection is feasible on Android devices [3].

B. Crowdroid: Behavior-Based Malware Detection System for Android

Burguera et al. present a framework for obtaining and analyzing Smartphone application activities called Crowdroid. Their framework monitors system calls of applications on the Smartphone's of many users, and analyzes these samples at a central server. Scope of the framework is to differentiate between benign applications and their corresponding malware versions. Since Smartphone users can install applications not only from the official application market, but e.g., from the Internet, there can exit's copies of benign applications, with added malware functionality. Burguera et al. show that their framework is a promising approach to distinguish between a benign application and the corresponding malicious version [4].

C. Detection of Smartphone Malware

Schmidt A.-D.'s dissertation gives a detailed overview of the evolution and present status of smartphone malware. The dissertation introduces dynamic and static analysis concepts to detect malware. For dynamic analysis, a user behavior- and application behavior-based concept is described and evaluated on Symbian OS, Windows Mobile and Android. He
also states that function and library calls can be used to successfully detect malware for Android and Symbian OS [5].

D. A cloud-based intrusion detection and response system for mobile phones

Houmansadr et al. propose a cloud-based intrusion detection and response architecture. Its objectives are transparent operations to the user, light resource usage, and real time and accurate intrusion detection and response. The architecture emulates a smartphone in the cloud and uses a proxy to duplicate all traffic between the smartphone and the Internet. Intrusion detection on the emulated smartphone is done using resource intense off-the-shelf intrusion forensics and detection systems. To keep the device and the emulated device synchronized, the system replicates the user's input in the cloud. Once misbehavior is detected, the architecture automatically decides upon the best countermeasure, and sends it to the device. A prototype of the forensics engine in the cloud uses a set of intrusion detection systems and the logging of system calls to analyze the installed application [6].

E. Paranoid Android: versatile protection for Smartphone's

Portokalis et al. present a prototype called Paranoid Android for security checking of Android Smartphone's on remote servers hosting exact replicas of the phones. The prototype uses previously recorded system traces to replay the actions of the real smartphone in the replicas. The remote servers can then perform security scans on the replicas, including anti-virus scans and dynamic taint checking. An evaluation of the prototype showed that the transmission overhead can be kept below 2.5 KiBps, but the battery life is reduced by about 30%. The authors explain how the battery consumption could be improved significantly and conclude that the architecture is suitable for protection of mobile phones [7].

F. Monitoring Smartphones for Anomaly Detection

Schmidt et al. demonstrate how a smartphone running Symbian OS can be monitored to extract features for anomaly detection. The features are sent to a remote server to perform analysis using intrusion detection systems on the data. The paper shows the data extracted from different applications, and how this data can be interpreted [8].

G. Virtualized In-Cloud Security Services for Mobile Devices

Oberheide et al. introduce a model for moving anti virus functionality to an off-device network service which employs multiple malware detection engines. They argue that this
model has three benefits: better detection through multiple detection engines, reduced on device
resource consumption through offloading of computation and reduced on-device software complexity, since all malware detection is done in the network. A prototype for this model is developed for Nokia N800 and N95 devices running Symbian OS. They show that their approach is feasible and effective for the current generation of Smartphone [9].

H. XManDroid: A New Android Evolution to Mitigate Privilege Escalation Attacks

Bugiel et al. propose a security framework called XManDroid to detect and prevent application- level privilege escalation attacks at runtime. Their prototype for Android OS dynamically analyzes the applications' permission usage with only minimal overhead. It is able to detect covert channels which can be established using Android's system services or content providers. They evaluate the prototype against known application-level privilege attacks and conclude that their prototype is capable of detecting several attacks, but also reports some false positives [11].

I. Security as a Service in Cloud for Smartphones

Lakshmi S. proposed a generic architecture for a security service for smartphones and use cases how the service can be used. The architecture was analyzed in terms of its security aspects and experimental performance and battery measurements are presented, which show the benefits of such a service in the cloud [10].

III. SOLUTIONS

As our main area of discussion is android application security hence we will try to overcome some of the shortcomings of the various present security policies. In this system we use cloud as a security scanner device which helps android operating system to enhance their application security. In this system when user actually download any application available on application market that contains viruses or any malware than the users provides some specific report regarding that particular application or feedback , that feedback report will be transferred to cloud server and saved permanently. When any other person try to install same application then cloud server just restrict that user and

informs in advance that application is malicious and harmful. For this one web service will be available as a background process which checks each time about malicious application.

The main objectives of our system are

1. A proposed system detect the malwares from different security algorithm .The our system implements the some security algorithms like pattern checking and signature.
2. Provides the cloud services for the android application. The cloud provides the software as a service to deploy the security algorithms that validate the android application security.
3. The System also maintains the centralized database over cloud to maintain the log of different kinds of malware that further used for the security checks.

IV. CONCLUSION

This paper introduced a security service for Smartphone's, which offloads the detection of malicious applications from the Smartphone into the cloud. As Smartphone's are very much prone to viruses and malwares hence we introduces new approach of using cloud as a security weapon for providing security. Also literature review section covers all the related work which has been previously carried out related to this topic. Also we provided some possible solutions to the problems of malwares in Android applications.

REFERENCES:

[1] Byung-Gon Chun and Petros Maniatis. Augmented smartphone applications through clone cloud execution. In Proceedings of the 12th conference on Hot topics in operating systems, 2009.

[2] Georgios Portokalidis, Philip Homburg, Kostas Anagnostakis, and Herbert Bos. Paranoid android: versatile protection for smartphones. In Proceedings of the 26th Annual Computer Security Applications Conference, 2010.

[3] Asaf Shabtai and Yuval Elovici. Applying behavioral detection on android-based devices. In MOBILWARE, pages 235–249, 2010.

[4] A D Schmidt. Detection of Smartphone Malware. PhD thesis, Technischen Universit¨at Berlin, 2011.

[5] Amir Houmansadr, Saman A. Zonouz, and Robin Berthier. A cloud-based intrusion detection and response system for mobile phones. In Proceedings of the 2011 IEEE/IFIP 41st International Conference on Dependable Systems and NetworksWorkshops, DSNW '11, pages 31–32,Washington, DC, USA, 2011. IEEE Computer Society.

[6] Iker Burguera, Urko Zurutuza, and Simin N. Tehrani. Crowdroid: behavior-based malware detection system for Android. In Proceedings of the 1st ACM workshop on Security and privacy in smartphones and mobile devices, SPSM '11, pages 15–26, New York, NY, USA, October 2011. ACM.

[7] Georgios Portokalidis, Philip Homburg, Kostas Anagnostakis, and Herbert Bos. Paranoid android: versatile protection for smartphones. In Proceedings of the 26th Annual Computer Security Applications Conference, 2010.

[8] Aubrey-Derrick Schmidt, Frank Peters, Florian Lamour, and Sahin Albayrak. Monitoring smartphones for anomaly detection. In Proceedings of the 1st international conference on MOBILe Wireless MiddleWARE, Operating Systems, and Applications, MOBILWARE '08, pages 40:1–40:6, ICST, Brussels, Belgium, Belgium, 2007. ICST

[9] Jon Oberheide, Kaushik Veeraraghavan, Evan Cooke, Jason Flinn, and Farnam Jahanian. Virtualized In-Cloud Security Services for Mobile Devices. In Workshop on Virtualization in Mobile Computing (MobiVirt '08), Breckenridge, Colorado, June 2008.

[10] Philipp Stephanow Lakshmi Subramanian, Gerald Q. Maguire Jr. An architecture to provide cloud based security services for smartphones, 2011.

[11] Sven Bugiel, Lucas Davi, Alexandra Dmitrienko, Thomas Fischer, and Ahmad-Reza Sadeghi. Xmandroid: A new android evolution to mitigate privilege escalation attacks. Technical report, Technische Universit¨at Darmstadt, 2011.

