Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 12, December 2015, pg.330 – 334

Mobile Malware Detection through Analysis of Web Application Network Behavior

Himgouri P. Barge
PG Student, Department of Computer Engineering, Flora Institute of Technology, Khopi, Pune, India
gouribarge.8@gmail.com

Prof. Pankaj R.Chandre
Guide, Department of Computer Engineering, Flora Institute of Technology, Khopi, Pune, India
Pankajchandre30@gmail.com

Abstract – Our system detects mobile malware by identifying suspicious network activities through real-time traffic analysis, which only requires connection establishment packets. Specifically, our detection algorithms are implemented as modules inside the Open Flow controller, and the security rules can be imposed in real time. We present a new behavior-based anomaly detection system for detecting meaningful deviations in a mobile application's network behavior. More specifically, we attempt to detect a new type of mobile malware with self-updating capabilities that were recently found on the official Google Android marketplace. Malware of this type cannot be detected using the standard signatures approach or by applying regular static or dynamic analysis methods. The detection is performed based on the application's network traffic patterns only. For each application, a model representing its specific traffic pattern is learned locally (i.e., on the device). Semi-supervised machine-learning methods are used for learning the normal behavioral patterns and for detecting deviations from the application's expected behavior. These methods were implemented and evaluated on Android devices. The evaluation experiments demonstrate that: (1)various applications have specific network traffic patterns and certain application categories can be distinguished by their network patterns; (2) different levels of deviation from normal behavior can be detected accurately; (3)in the case of self-updating malware, original (benign) and infected versions of an application have different and distinguishable network traffic patterns that in most cases, can be detected within a few minutes after the malware is executed while presenting very low false alarms rate; and local learning is feasible and has a low performance overhead on mobile devices.

Keywords: Android Malware, Smart-Phones Security, Network Traffic.

1. INTRODUCTION

Along with the significant growth in the popularity of smart phones and the number of available mobile applications, the amount of malware that harm users or compromise their privacy has also dramatically increased .mobile phones are most widely used in every aspect of our life including personal, official, political, social and educational as well as. That is the reason mobile phones are used not only for making calls, but also making important business decisions in professional life, internet services like online shopping , online ticket

booking ,online social network etc. There are number of apps available for various mobile operating systems to these services. Internet banking is one of the most increasing areas where mobile devices (i. e banking app.) are widely used now days.

Mobile Security deals with the techniques to secure the mobile devices from malicious files and applications. There are three main properties of security based on how the data can be secure:

1. Confidentiality is about preventing the data from unauthorized users. The data stored in mobile device must not be used by anyone except mobile user.

2. Integrity is about prevention of unauthorized modification of information or data. Mobile data must be fix by unauthorized users.

3. Availability is about preventing unauthorized withholding of information . Mobile's applications and services must be available and accessible to the authorized mobile user.

Use of mobile phones for sensitive and important services like mobile net banking, are increasing so Mobile security is must needed. Mobile security is challenging job since the malicious applications are created every day. So basic understanding about various viruses and malwares for mobile user is must necessary.

Malware or malicious software is a software program or mobile application which exhibits malicious behavior. This is a general term used to refer to a variety of intrusive applications and are characterized into virus, bonnets, worm, Spyware, Adware, Root kit and Trojan horse based on their behavior of affecting the mobile device. Malwares are most widely used by black hat hackers to access the personal data and sensitive information of a mobile device. They can also use the malwares to gather the sensitive data of a corporate or government websites. Malwares can be written in programming languages like Perl.

A virus is a software program that can destroy the personal data, applications of mobile device. Viruses have the properties of self-modification, encryption which makes its detection very difficult to an antivirus application. A bonnet is the most severe threat to the information society at present. It can control Internet Relay Chat (IRC) or can also send spam emails. Bonnets are used to thief information data from a computer such as different login IDs, application serial number, financial information such as credit cards number etc .worms are the stand alone software applications that can run without a host and have the capacity to self –replicate and propagate around in the network. Worms are also used by the bonnets to control the computers connected to internet which are used by spam sender for sending junk emails. will send the Caribe.sis file to other device. The worm is harmless because it does not perform any malicious activity but due to the continuous searching for other Bluetooth device, it reduces the battery life. a spyware is a software program that gathers person and organization information and can also send the information to another entity without the permission of user. Key logger is Spyware software which is used to store the key struck on a keyboard. It stores all key interactions without the permission of user. Hackers use this software to get passwords and usernames of a computer. Trojan horse is a category of Spyware that can reach a computer system via online games, internet driven applications.

It can give the access of targeted computer to a hacker that can use the machine as a part of bonnet, can theft the sensitive data, can download any malicious files, and can upload any file into target machine. It can also control the whole computer system remotely. In general, any malware can be downloaded and executed on a device using such a "remote payload" technique. Specifically, in the case of Drop dialer Trojan, the downloaded malicious package sent SMS messages to premium-rate numbers. The download action can be scheduled for both specific and random time in the future, or may even be initiated remotely by sending a command message to the devices, using, for instance, Google's push notification service (GCM or former C2DM). Several different techniques allowing Android application update from a remote location exist. These techniques are elaborated in Self-updating malware section.

2. IMPLEMENTATION

In this project we have developed an Antivirus application to detect the infected files. The application is in two modes, first is a standalone application, user can download this application from the internet and can install it in mobile device. This application has two versions, one is developed in J2SE and another is in J2ME. Mobile devices can use the version based on the application requirements and compatibility with mobile device. Both versions provide the facility to scan the device. J2SE version has more facilities than J2ME. The second mode of application is a web based client - server application. The application can be used when the device is

connected to internet. User can register his/her device, can scan file online, can report a file as thread, and can also download updates for Antivirus application. Securing mobile devices is a challenging task. People use mobiles for net banking, online shopping and many other works. Security of mobile devices is very much important since, if a device has infected file(virus) , its data will no longer be safe , virus files can control the mobile data , also can send the critical data while connected to net.

Web Client:

To study various antivirus solutions available in the literature. to design and develop an application to detect the infected files (virus) in a mobile device using J2SE and J2ME.extend the application as a web application that will provide the facility for user to scan the mobile files online, other services to report a file as thread.

The responsibility of the client side software is to monitor the applications that are already installed and running on the device, learn their user specific local models and detect any deviations from the observed "normal" behavior. The Collaborative Learning Server is responsible for collecting and aggregating data reported by various mobile devices and deriving collaborative models, which represent the common traffic patterns of numerous users for each application.

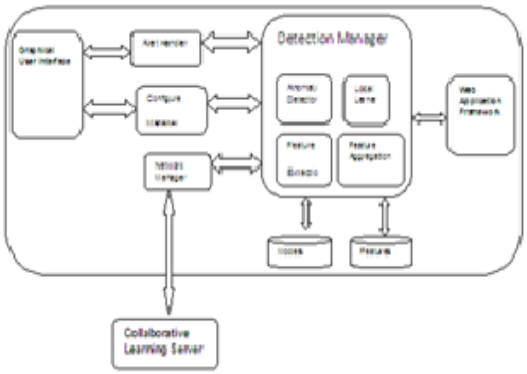

Fig. 1. Architecture of malware detection system.

The general system architecture consists of a client component installed on the Android mobile device and a server component. The responsibility of the client-side software is to monitor the applications that are already installed and running on the device, learn their user specific local models and detect any deviations from the observed "normal" behavior. The Collaborative Learning Server is responsible for collecting and aggregating data reported by various mobile devices and deriving collaborative models, which represent the common traffic patterns of numerous users for each application. Any application or file which copies its files into root directory of device or makes new directory while user may not be aware about it, is Malware application. there are many other heuristic rules to report a suspicious file as Malware. Number of Malwares are created, modified and edited every day which makes their detection difficult. So it is not easy task to detect all the malicious applications of a device.

The analysis and detection of Android malware has been a vivid area of research in the last years. Several concepts and techniques have been proposed to counter the growing amount and sophistication of this malware. An overview of the current malware landscape is provided in the studies of Felt et al and Zhou &.

2.1 Detection using Static Analysis

The first approaches for detecting Android malware have been inspired by concepts from static program analysis. Several methods have been proposed that statically inspect applications and disassemble their code .For example, the method Kirin checks the permission of applications for indications of malicious activity. Similarly, Stowaway analyzes API calls to detect over privileged applications and Risk Ranker statically

identifies applications with different security risks. Common open-source tools for static analysis are Smali and Androguard, which enable dissecting the content of applications with little effort.

2.2 Detection using Dynamic Analysis

A second branch of research has studied the detection of Android malware at run-time. Most notably, are the analysis system Taint Droid and Droid Scope that enable dynamically monitoring applications in a protected environment, where the first focuses on taint analysis and the later enables introspection at different layers of the platform. While both systems provide detailed information about the behavior of applications, they are technically too involved to be deployed on smart phones and detect malicious software directly. As a consequence, dynamic analysis is mainly applied for offline detection of malware, such as scanning and analyzing large collections of Android applications. For example, the methods Droid Ranger , Apps Playground , and Copper Droid have been successfully applied to study applications with malicious behavior in different Android markets. A similar detection system called Bouncer is currently operated by Google. Such dynamic analysis systems are suitable for filtering malicious applications from Android markets. Due to the openness of the Android platform, however, applications may also be installed from other sources, such as web pages and memory sticks, which requires detection mechanisms operating on the smart phone. Paranoid Android is one of the few detection systems that employs dynamic analysis and can spot malicious activity on the smart phone. To this end, a virtual clone of the smart phone is run in parallel on a dedicated server and synchronized with the activities of the device. This setting allows for monitoring the behavior of applications on the clone without disrupting the functionality of the real device. The duplication of functionality, however, is involved and with millions of smart phones in practice operating Paranoid Android at large scale is technically not feasible.

3. CONLUSION

In this paper, we presented a novel system for detecting meaningful deviations in a mobile application's network traffic patterns that can be used for detecting an emerging type of malware with self-updating capabilities that allow for stealing user data or spying on users. The presented system, although initially planned as a host-based part of a client server system, is a fully-functioning, stand-alone monitoring application for mobile devices, which can be used alone or in conjunction with other methods. One of the main capabilities of the proposed system is protection of mobile device users from malicious attacks on their phones. The detection is performed based only on the application's network traffic patterns.

As future work, we will further study the characteristics of mobile malware, investigate more malware detection techniques and explore the possibilities of employing them in the context of SDN. In addition, we plan to take better advantage of GENI infrastructure and test our system at an even larger scale in order to optimize our system design.

REFERENCES

[1] A.P. Felt, et al., "A Survey of Mobile Malware In The Wild," 1st Workshop on Sec. & Privacy in Smart phones and Mobile Devices, 2011.

[2] L. Chekina, et al., "Detection of Deviations in Mobile Applications Network Behavior," available on http://arxiv.org/corr/home

[3] Y.-A. Huang, et al., "Cross-feature analysis for detecting ad-hoc routing anomalies," Int. Conf. on Distributed Computing Systems, 2003.

[4] Gartner identifies the top 10 strategic technology trends for 2013. [Online]. Available: http://www.gartner.com/it/page.jsp?id=2209615

[5] M. Hypponen, "Malware goes mobile," Scientific American, vol. 295,no. 5, pp. 70–77, 2006.

[6] T. Bradley. (2011) DroidDream becomes android market nightmare. [Online]. Available: http://www.pcworld.com/article/221247/droiddream becomes android market nightmare.html

[7] D. Goodin, "Backdoor in top iPhone games stole user data, suit claims,"The Register, 2009.

[8] C. Guo, H. Wang, and W. Zhu, "Smart-phone attacks and defenses," in HotNets III, Nov 2004.

[9] J. Jamaluddin, N. Zotou, R. Edwards, and P. Coulton, "Mobile phone vulnerabilities: a new generation of malware," in IEEE International Symposium on Consumer Electronics, Sept 2004, pp. 199–202.

[10] Emerging cyber threats report 2012. [Online]. Available: http://www.gtisc.gatech.edu/doc/emerging cyber threats report2012.pdf

[11] Aukasz Machnik, “Documents Clustering techniques", in Annales UMCS Informatica Lublin-Polonia Sectio AI,p 401

[12] P. Porras, H. Saidi, and V. Yegneswaran, “An analysis of the iKee.B iPhone botnet,” Security and Privacy in Mobile Information and Communication Systems, pp. 141–152, 2010.

[13] D. Damopoulos, G. Kambourakis, and S. Gritzalis, “iSAM: An iPhone stealth airborne malware,” Future Challenges in Security and Privacy for Academia and Industry, pp. 17–28, 2011.

[14] Open Networking Foundation. Software-Defined Networking: The new norm for networks. [Online].Available: https://www.opennetworking.org/images/stories/downloads/white-papers/wp-sdn-newnorm.pdf

