Detect and Prevent the Mobile Malware

Abdullah Mohammed Rashid & Ali Taha Al-Oqaily

Basrah University, Basrah Iraq
College of IT, University Tenaga Nasional Kajang, Selangor, Malaysia

Abstract- Mobile devices such as mobile phones have become one of the most needed and important device for everyone living in the 21st century. This is due to their ability in accommodating people with information and effective communication that make people's life easier and more meaningful. However, the conveniences offered by the devices come with security concern: mobile malware. There are many incidents caused by mobile malware that downgrade organization's reputation or financial lost. The mobile malware represent a security threats to mobile devices, there are many types of mobile malware compromising the security platform. This paper discusses techniques to effectively detect and prevent the mobile malware and propose an improvement towards current techniques which gives better mobile malware detection and prevention.

Index Terms- Malware; mobile Malware; Detection and Prevent.

I. INTRODUCTION

Mobile devices have become one of the most important needs in the 21st century living era [17 & 9]. This is shown, for example, when many organizations started to convert their computing resources such as Personal Computer (PC) to mobile phones due to many convenient features offered by mobile phones; lighter, excellent connectivity to Wi-Fi, portable and accessible anywhere. According to C Laudon in THRTEENTH EDITION the General Electric (GE) is one of the world largest companies, producing aircraft engines and other transportation purely convert to use the I phone device to perform the employees activities such report and data analysis . Nowadays, mobile computing is adopted in many purposes such as keep contact numbers, data storage, transaction process, internet access and checking the emails [4]. According to the Ericsson report, there are around 6.7 billion mobile subscriptions at the moment and, approximately 9.3 billion mobile subscriptions at the end of 2019 [22].

One of the security threats over the use of mobile devices is SMS fraud which is a common threat in Android, IOS and Apple. It works like this: the users receive a message asking them to subscribe in daily, weekly or monthly service. The users usually have tendency to subscribe by providing personal information such as credit card number because the service is initially made as a free of charge. After several period, the service begins to charge the users without their knowledge [6 & 22]. Another type of security threats is Spyware, which steals data from the mobile device without user's permission [7].

One way to prevent the mobile devices from these threats (malware), users need to use antimalware tools. These tools identify, attract and catch the known malware and notify the users of further action to be taken. However, some of the new malware cannot be recognized by normal software or tools an improvement on the detection technique is required.

Mobile malware threat is a real challenge in mobile devices [12 & 10]. This threat is exacerbated with the increasing number of mobile devices accessing to the internet as a basic and daily service. Some of the malwares are harmful to the mobile devices in many ways, such as exhausting the battery use, destructing files and fraudulently send SMS or email to the contacts without the knowledge of the mobile device owner [22 & 14].

The main objective of this study is to discuss several techniques that can be used to detect and prevent mobile malwares from attacking mobile devices. Then, the comparisons between various techniques are given and that leads towards our recommendations to improve the current detection and prevent techniques.

II. RELATED WORKS

A. Related Methods of Mobile Malware Detection

Many researchers use various methods and software to detect , attack and prevent mobile malware. The table below reviews some of these methods, which are described in details in Related Works section.

No.	Methods	Description
1	ESET	An antivirus application used to detect and prevent mobile malware.
2	F-Secure	An antivirus application used to detect and prevent mobile malware.
3	Kasper sky	An antivirus application used to detect and prevent mobile malware.
4	McAfee	An antivirus application used to detect and prevent mobile malware.
5	Norton	An antivirus application used to detect and prevent mobile malware.
6	Trend Micro	An antivirus application used to detect and prevent mobile malware.
7	Pre Crime	A proactive defensive approach produced by Haibo Li et al. (2014) that use mirror synchronization to delay system events and speculate user events for detecting mobile malware.
8	Dynamic analysis	Collecting data related to calls and analysis the collected data in different tools.
9	Static analysis	Collecting data related to the names of the functions and calls appearing at the

		output; collecting the next responses, then follows certain mechanisms for analysis.
10	Cloud service	Used to predict the next event of a mobile or maintain a copy from the mobile event.
11	Monitoring	Key the eyes within mobile to monitor many things such as power expenditure.

B. **Existing Techniques**

Previous researchers have proposed a number of models, methods, and mechanisms to detect and prevent malware in mobile devices [2 & 18]. Most of these methods are summarized as static analysis, dynamic analysis, cloud computing, and signature-based. First, antivirus application system is a traditional technique that uses signature-based approach to detect malware such as ESET, F-Secure, Kasper sky, McAfee, Norton, and Trend Micro [12].

In terms of cloud service [18 & 15] used cloud as a service to detect and prevent mobile malware. [18] produced the Pre Crime proactive malware detection system that is employed to predict the behavior of mobile devices and compare with the next event to ensure that the next event is normal or abnormal.[15] used cloud infrastructure to perform complex analysis methods in order to detect malware families by periodically updating the database for detection.

Another methods used by [12 ; 7 & 17] placed several steps to detect and prevent mobile malware. [12] used the method of monitoring power consumption, increasing platform diversity and enforcing hardware and box; [7] used antivirus application to be aware of battery and network, checking device setting and downloading applications from trusted providers; [17] developed a protective model from five stages to detect and prevent mobile malware, which are caution, investigate, monitor, update and remove.

Vast number of researchers focused on static analysis, dynamic analysis or both of them [13; 16 &11] . Aubrey-Derrick Schmidt collected the names of the functions and calls appearing at the output and next responses, and then follows certain mechanisms for analysis; [16] developed a framework which uses only dynamic analysis to detect malware in the Android platform; [11] is a combination of static analysis and dynamic analysis, in which the static analysis detects malicious code and the dynamic analysis identifies malicious packet structure.

Finally, [8] used only the monitoring method to detect mobile malware by observing the electric power of the mobile device and energy consumption history, since mobile malware open channels, such as Wi-Fi and Bluetooth consume mobile power. Also [3 & 5] monitored and detected malicious malware by observing power consumption.

In conclusion, researchers used four methods to detect and prevent mobile malware, which are cloud service, model-based stage, static and dynamic analysis and power consumption observation.

C. **Mobile Malware Behaviors**

There are many malwares that attack mobile devices such as SMS Zombie, Worm, and Spyware. The most popular and malicious malware is Trojan. Trojan malware infects mobile devices through separate malicious mobile applications, free apps or purchased from non-authentic resource, p2p file sharing, download from website or e-mail distribution. This kind of malware can : (1) Collect private data from current mobile device or install other malicious apps like worms. (2) Send SMS to contact numbers in the infected mobile device. (3) Trojans can be used to commit phishing activities. This situation disrupts the financial for banking companies, organizations and individual users, for example financial loss to the sender and receiver, sender is charged for sending SMS, and receiver receives SMS that tells them to subscribe daily or monthly service [20 ;19 & 21].

III. DISCUSSION

From the result of the previous review, the cloud used in the PreCrime scheme keeps the mobile performance stable as it predicts run in the cloud. However, this method can only detect malware but cannot prevent the malware [18]. Also, the cloud infrastructure is used for complex analysis and detecting malware families, reducing storage space usage and reducing complex processing [1]. This method requires standard access to the Internet, consumes mobile battery, and not precise in detecting the malware alone [1 & 15].

Using the steps to detects and prevents malware is time consuming because it requires periodical monitoring, checking and changing or updating the mobile operating system.

Static analysis is fast and easy to detect malware but it cannot catch malicious malware that uses blackout, where as dynamic analysis can detect the malware even with blackout, but consumes storage capacity [1].

Montoring mobile battery consumption can detect malware, but the major challenges for this monitoring method are that it identifies more technical details and consumes mobile storage due to storage of power history [8].

IV. RECOMMENDATION

Dynamic analysis can detect and prevent malware, but this method consumes storage space. On the other hand, the Pre Crime cloud service scheme can detect malware but cannot prevent malware and keep efficient mobile performance.

The integration between the dynamic analysis method and the Pre Crime cloud service scheme could be proposed as an efficient solution of both methods weaknesses. The result of dynamic analysis storage in cloud space solves the storage challenge in dynamic analysis and uses cloud to predict the mobile behavior, as compared to the dynamic analysis result. The proposed method can detect, prevent ,and provide storage space to dynamic analysis and use the cloud service.

V. CONCLUSION

As long as technology continues to develop mobile malware are also developed continuously in line with new technology. Users are affected through the development of malware, for that measures need to be developed early before

new malware emerges. The main contribution of the proposed solution is to produce a new model, method and technique to detect and prevent malware through a combination of cloud service and dynamic analysis.

REFERENCES

[1] Mohd Zaki Mas`ud, Shahrin Sahib, , Mohd Faizal Abdollah, Siti Rahayu Selamat and Robiah Yusof, 2014. Android Malware Detection System Classification. Research Journal of Information Technology, 6: 325-341.

[2] Rastogi, V., Chen, Y., & Enck, W. (2013, February). Appsplayground: automatic security analysis of smart phone applications. In Proceedings of the third ACM conference on Data and application security and privacy (pp. 209-220). ACM.

[3] Kim, H., Smith, J., Shin, K.G.: Detecting energy- greedy anomalies and mobile malware variants. In: Proceeding of the 6th international conference on Mobile systems,applications, and services, pp. 239–252 (2008)

[4] Pousttchi, K., Weizmann, M., & Turowski, K. (2003). Added value-based approach to analyze electronic commerce and mobile commerce business models.

[5] Liu, L., Yan, G., Zhang, X., Chen, S.: Virusmeter: Preventing your cellphone from spies. In: Proceedings of the 12th International Symposium On Recent Advances In

[6] Mikko Hypponen. Malware goes mobile. Nov. 2006

[7] Mu, J., Cui, A., & Rao, J. (2013, July). Android Mobile Security–Threats and Protection. In International Conference on Computer, Networks and Communication Engineering (ICCNCE 2013). Atlantis Press.

[8] Ghallali, M., El Ouadghiri, D., Essaaidi, M., & Boulmalf, M. (2011, December). Mobile phones security: the spread of malware via MMS and Bluetooth, prevention methods. In Proceedings of the 9th International Conference on Advances in Mobile Computing and Multimedia (pp. 256-259). ACM.

[9] Nadji, Y., Giffin, J., & Traynor, P. (2011, December). Automated remote repair for mobile malware. In Proceedings of the 27th Annual Computer Security Applications Conference (pp. 413-422). ACM.

[10] Mu, J., Cui, A., & Rao, J. (2013, July). Android Mobile Security–Threats and Protection. In International Conference on Computer, Networks and Communication Engineering (ICCNCE 2013). Atlantis Press.

[11] Malhotra, A., & Singh, P. P. (2014). Android Malware: Study and Analysis for Privacy Leak in Ad-Hoc Network. IJCSNS, 14(6), 92.

[12] Yan, Q., Li, Y., Li, T., & Deng, R. (2009). Insights into malware detection and prevention on mobile phones. In Security Technology (pp. 242-249). Springer Berlin Heidelberg.

[13] Schmidt, A. D., Bye, R., Schmidt, H. G., Clausen, J., Kiraz, O., Yuksel, K. A., ... & Albayrak, S. (2009, June). Static analysis of executables for collaborative malware detection on android. In Communications, 2009. ICC'09. IEEE International Conference on (pp. 1-5). IEEE.

[14] Felt, A. P., Finifter, M., Chin, E., Hanna, S., & Wagner, D. (2011, October). A survey of mobile malware in the wild. In Proceedings of the 1st ACM workshop on Security and privacy in smartphones and mobile devices (pp. 3-14). ACM.

[15] Milosevic, J., Dittrich, A., Ferrante, A., & Malek, M. (2014, September). A Resource-optimized Approach to Efficient Early Detection of Mobile Malware. In Availability, Reliability and Security (ARES), 2014 Ninth International Conference on (pp. 333-340). IEEE.

[16] Burguera, I., Zurutuza, U., & Nadjm-Tehrani, S. (2011, October). Crowdroid: behavior-based malware detection system for android. In Proceedings of the 1st ACM workshop on Security and privacy in smartphones and mobile devices (pp. 15-26). ACM.

[17] Pieterse, H., & Olivier, M. S. (2013, August). Security steps for smartphone users. In Information Security for South Africa, 2013 (pp. 1-6). IEEE.

[18] Tan, C., Li, H., Xia, Y., Zang, B., Chu, C. K., & Li, T. (2014, June). PreCrime to the rescue: defeating mobile malware one-step ahead. In Proceedings of 5th Asia-Pacific Workshop on Systems (p. 5). ACM.

[19] Dunham, K. (2008). Mobile malware attacks and defense. Syngress.

[20] Delac, G., Silic, M., & Krolo, J. (2011, May). Emerging security threats for mobile platforms. In MIPRO, 2011 Proceedings of the 34th International Convention (pp. 1468-1473). IEEE.

[21] Fleizach, C., Liljenstam, M., Johansson, P., Voelker, G. M., & Mehes, A. (2007, November). Can you infect me now?: malware propagation in mobile phone networks. In Proceedings of the 2007 ACM workshop on Recurring malcode (pp. 61-68). ACM.

[22] (2013, November). [Online]. vailable: http://www.ericsson.com/res/docs/2013/ericsson-mobility-report-november-2013.pdf

AUTHORS

First Author – Abdullah Mohammed Rashid, College of IT, University Tenaga Nasional Kajang, Selangor, Malaysia, Email: abdalla_rshd@yahoo.com, ST21977@utn.edu.my
Second Author – Ali Taha Al-Oqaily, College of IT, University Tenaga Nasional Kajang, Selangor, Malaysia, Email: Oqli83@yahoo.com