Enhancing Security of Android based Smart Devices

Nisha Shah
Research Scholar, Gujarat Technological University
Department of Computer / IT Engineering
nisha.vipul1@gmail.com
Cont.:+919824256211

Dr. Nilesh Modi,
Dr. Babasaheb Ambedkar Open University
drnileshmodi@yahoo.com
Cont.:+919662640500

In the current era of smart devices, mobile phones are rapidly emerged and increasingly being used as primary computing, communication device with sensing capabilities and running more performance intensive task. Secure and healthy working environment of this smarty is required to be maintained, that present number of security and privacy alarming concerns. Though sufficient peripheral protection mechanisms described, authentication and access control are not alone sufficient to provide integral protection against intrusions. So there is a need for more intelligant and sophisticated security controls, and for that intellegent Intrusion Detection / Prevention System are essential. These arise need for smart analysis techniques, particularly in application code, to materialize. One need to rely on carefully controlled dynamic analysis techniques to detect potentially dangerous pieces of code. There are many security detective and preventive solutions available in market, but still this research field is immature and unexplored in depth. Apart from that there are many challenges in building effective Smartphone security solutions.

Majority of solutions provided in area of Smartphone handle specific issue for particular device and environment. In one of the recent work researchers suggested having better solution to control permissions before installing the application to the device. Intended to work in the same direction, we define a framework aimed to help, identify and warn users for the resources going to acquire by the applications downloaded to install on smart devices. That way, it will try to intimate the users for the resources going to acquire in future, at runtime by application processes directly or indirectly. So in advance the users will come to know about hard and soft resources

going to utilize by application and can uncover the malicious intention of resource access hidden in the application and the wicked objective of application-owner will be exposed. Having this in mind, our solution will establish a strong footprint in device security by preventive alarm. For the same we focused on Android based smart devices looking to the popularity, availability and download statistics of android app, also due to the open Android's philosophy, benign or malignant applications can be published easily with limited controls; Android is having very high risk against security.

Key Words: Device security, Access permission, Intrusion, Malware, Dynamic analysis, Security risk

1. Introduction

Smartphone usage is on the rise and Smart devices are becoming more popular furnishing replacement of laptops and desktop computers for a diversity of needs. Range of Smart devices (Smart phones, tablets) and OS are available. Looking to the statistics of Smartphone sales vendor wise and operating system wise, Android Smartphone are in leading position amongst all [0]. Statistics says Android app store is having highest no of apps and the number of available apps in the Google Play Store surpassed 1 million apps in July 2013 and was 2.6 million apps in December 2016[1]. Similar is the trend in app download for Android. Android users have downloaded almost double (in number) apps in a year than iOS. Worldwide statistical report projects increase in about 25% rise every year in mobile app download with free app download is about 85 to 90% more than paid app [2].

Moreover Android application can be easily published by anybody on Google Play store by paying small amount for the registration, requiring all the applications must be digitally signed. On the contrary there are no warranties that applications are not malicious. In addition, due to the open Android's philosophy, applications can also be published on un-official markets, or distributed through several other channels where no control is performed.

A major source of security problems in Android is the ability to incorporate third-party applications from available online markets. Determining which applications are malignant and which are not is still a formidable challenge, as those constitutes a threat to user for security and privacy.

The growth and popularity has exposed mobile devices to increase number of security threats. Though sufficient peripheral protection mechanisms are described, authentication and access

control are not alone sufficient to provide integral protection against intrusions. So there is a need for more intelligant and sophisticated security controls, and for that intellegent Intrusion Detection and Prevention System are essential. As prevention is better than cure, we intended to provide a preventive measure by our proposed framework, warning the smart users for resources going to access by the app in future while the app start establishing its footprint into the device passing through installation.

2. Related Work

Several researches are done in the field of Smartphone intrusion detection, where it can be seen that promising approach involved cloud based techniques to reduce resource usage to detect attack at the cost of cloud services, network connectivity and communication to maintain real-time synchronization of device in cloud [4, 5]. Other approaches involved non-human behaviour analysis instead of relying on known signatures for malware detection but fail to detect instantaneous and abrupt attack [6, 7, 8]. Even rigorous surveys are done from 2011 to 2015 in the area of Smartphone security challenges, android security architecture and its issues, malware evolution and penetration threats, and highlight desirable security features, security mechanisms and solutions available and provided suggestions for defence, detection, protection and security [9, 10, 11, 12]. Schlegel, Roman, et al. talked about stealing of high-valued information through on-board sensors [13]. Suarez-Tangil, Guillermo, et al. described a dynamic analysis tool to detect hidden malware components distributed as a part of an app package [14]. In [3] it is shown that how the extra permissions can be used for malicious intention and suggested to have better solution to control permissions before installing the application on the device. In [15], it is talked about assessment of hosted android applications as benign or malicious using proposed dynamic security analysis framework.

The related work conveys that in depth and thorough work is required to assess apps installed on smart device and permissions required by the apps [3, 14, 15]. With the intention to contribute in these immature areas we propose a framework to assess applications, aiming to install on the device.

3. Android Framework and security

Google's Android is a Linux based operating system having four layered architecture as application, application framework, libraries and anroid runtime, linux kernel from top to bottom

respectively. Because of its open architecture, its Application Programming Interface is popular in developer community. Self signed certified application can be installed to the android device very easily. As no central certificate authority is needed, malignant applications can be introduced easily into the market, moreover due to the open Android's philosophy, application can also be published on un-official markets or distributed through several other channels. Android's this strategy does not provide adequate level of security.

Previous research work on Smartphone conveys that majority of contribution is found in area of intrusion detection, security and privacy. Where in researchers worked in vicinity to find footprints left by intruders, viruses, malwares and Trojans applying different data mining techniques like classification, clustering, machine learning, neural network, and pattern recognization depend upon type of analysis to do on which kind of data, runtime configuration environment of Smartphone, input provided and the output required.

Our study also shows that widely held researches do not capture runtime environment context and majority of time they are demonstrated in emulated / simulated environment.

4. Proposed framework to enhance security

With the objective in mind to improve security of Android devices by providing intelligent, resource intensive and robust solution we propose a framework. Our goal is to provide a preventive measure by warning the smart users for resources going to access by the app in future when the app start establishing its footprint into the device passing through installation. Here the purpose is by providing alarming notification, user can judge about the resources actually required by the application, risk associated with it and that way the illogical access control permission acquisition intention will be exposed and misuse of resource can be reduced. But it again depend on alerness of the smart device user only. Our idea is to reduce the damage going to take place to the device, by maliciour activity performed by processes running on device as a result of application execution than to identify and take recovery actions after device is harmed by attacking application. In later case recovery and cure will not be 100% sure and even it needs extra efforts.

We proposed a monitoring and detection framework to maintain and provide the stable and safe working environment in Android base smart devices. It will reside in application and application framework layer of four layer Android architecture.

Figure 1 shows monitoring and detection framework design proposed by us, which shows the projected workflow. It is targeted to identify malignant intense hidden in the application in prior, as once the application is installed on device, anytime by any means it can harm the device, so that the attack / hateful activity can be prevented. That way it will be an intrusion preventive solution.

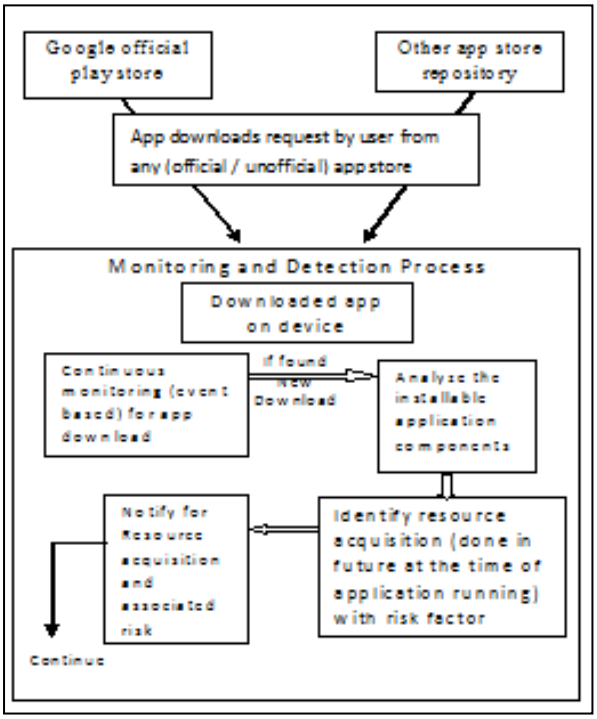

Figure 1: Workflow of Application Monitoring and Detection Framework

Our design will continuously monitor the app download activity and as it will found any download, it will first convert the installable app form to the form which can be easily assessed. From this form it will identify all the resources required by the app at run time in future after it gets installed. The objective behind resource requirement assessment is to identify needless resource acquisition dynamically which can be used for malicious purposes. Our aspiration is to prevent such misuse and that way provide security. Resource requirement will be notified with associated risk and if found acceptable then the application will retain on the device. Our intention behind this work can be clearly understood by taking one example. If one user wants to install some game on his device, it will be downloaded from the app store by him. If contact /

camera or any such resources acquisition request is there in the app code, which is in reality not essential but for malicious purpose it may be defined, can create havoc.

5. Conclusion and future work

In this paper we gave an overview on how an android based smart device can be securely used. We presented Android security mechanisms available, tools and techniques used and pros and cons of each. To overcome the loopholes in presented work where major work is done in the area of intrusion detection and very less amount of work is done in the vicinity of intrusion prevention, we proposed dynamic preventive architecture for android security. Our work will be new step in direction of android intrusion prevention. We are working on the proposed design and in near future the implementation scenario and the research results will be published. The results will be tested on range of android based smart devices to get the assurance of the proposed work. We are sure that our work will be a strong new step in the direction of android security by prevention.

References

[0] http://www.gartner.com/newsroom/id/3323017

[1] https://www.statista.com/statistics/276623/number-of-apps-available-in-leading-app-stores/

[2] http://www.gartner.com/newsroom/id/2592315

[3] Jain, A. (2016, March). Android security: Permission based attacks. In *Computing for Sustainable Global Development (INDIACom), 2016 3rd International Conference on* (pp. 2754-2759). IEEE.

[4] Houmansadr, A., Zonouz, S. A., & Berthier, R. (2011, June). A cloud-based intrusion detection and response system for mobile phones. In *Dependable Systems and Networks Workshops (DSN-W), 2011 IEEE/IFIP 41st International Conference on* (pp. 31-32). IEEE.

[5] Zonouz, S., Houmansadr, A., Berthier, R., Borisov, N., & Sanders, W. (2013). Secloud: A cloud-based comprehensive and lightweight security solution for smartphones. *Computers & Security*, *37*, 215-227.

[6] Xie, L., Zhang, X., Seifert, J. P., & Zhu, S. (2010, March). pBMDS: a behavior-based malware detection system for cellphone devices. In *Proceedings of the third ACM conference on Wireless network security* (pp. 37-48). ACM.

[7] Dini, G., Martinelli, F., Saracino, A., & Sgandurra, D. (2012, October). MADAM: a multi-level anomaly detector for android malware. In *International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security* (pp. 240-253). Springer, Berlin, Heidelberg.

[8] Shabtai, A., Kanonov, U., Elovici, Y., Glezer, C., & Weiss, Y. (2012). "Andromaly": a behavioral malware detection framework for android devices. *Journal of Intelligent Information Systems*, *38*(1), 161-190.

[9] Wang, Y., Streff, K., & Raman, S. (2012). Smartphone security challenges. *Computer*, *45*(12), 52-58.

[10] La Polla, M., Martinelli, F., & Sgandurra, D. (2013). A survey on security for mobile devices. *IEEE communications surveys & tutorials*, *15*(1), 446-471.

[11] Suarez-Tangil, G., Tapiador, J. E., Peris-Lopez, P., & Ribagorda, A. (2014). Evolution, detection and analysis of malware for smart devices. *IEEE Communications Surveys & Tutorials*, *16*(2), 961-987.

[12] Faruki, P., Bharmal, A., Laxmi, V., Ganmoor, V., Gaur, M. S., Conti, M., & Rajarajan, M. (2015). Android security: a survey of issues, malware penetration, and defenses. *IEEE communications surveys & tutorials*, *17*(2), 998-1022.

[13] Schlegel, R., Zhang, K., Zhou, X. Y., Intwala, M., Kapadia, A., & Wang, X. (2011, February). Soundcomber: A Stealthy and Context-Aware Sound Trojan for Smartphones. In *NDSS* (Vol. 11, pp. 17-33).

[14] Suarez-Tangil, G., Tapiador, J. E., Lombardi, F., & Di Pietro, R. (2014). Thwarting obfuscated malware via differential fault analysis. *Computer*, *47*(6), 24-31.

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