Original Research Paper

Volume - 7 | Issue - 5 | May - 2017 | ISSN - 2249-555X | IF : 4.894 | IC Value : 79.96

Engineering

Permission based malware detection by using k means algorithm in Android OS

Chetan J. Shelke Asst. Professor, Dept.ofIT, P.R.Patil College of Engineering, Amravati, India

Pravin Karde Asst. Professor, Dept of IT, Govt. Polytechnic, Amravati, India

V. M. Thakre HOD, Dept.of Computer science SGBAU Amravati University Amravati, India

ABSTRACT In the developing market now a days cashless transaction are increasing day by day same time its difficult to manage security while online transaction through android phone as the many application downloaded from market which is freely available may leak private information or some important information like banking transaction details ,bank account number ,etc ,now a days smartphones are vulnerable for app containing malware ,camera based attack ,SMS based attack may steal your private information .permission based method for malware detection is presented to detect malware from app. decision can be taken that downloaded app is malicious or not is done by k means algorithm k means algorithm form a cluster to classify malicious app .the proposed methodology is useful when the signature of app is not present in malware dataset .system describe the process of extracting features of android apk file in order to detect the malware by using android manifest file. The main aim of this proposed system is to develop an accessible and comprehensive Eclipse structure application, can potentially able to check which applications are using malicious permission or requesting for that permission.

KEYWORDS : Android OS, Smart phones, Malwares, permission, Applications Security.

I. INTRODUCTION

Smartphone are helpless to malicious attack The small size of android devices, fond of with people's hasty procedure, increase the probability of malicious software injection onto smart phones. They can be compromised in three respects: confidentiality, integrity, and availability [3].technological safety measures, such as firewalls, antivirus, and encryption, are infrequent on mobile phones, and mobile phone operating systems are not rationalized as commonly as those on personal computers. Mobile social networking applications sometimes lack the detailed privacy controls of their PC counterparts. Recent innovations in mobile commerce have enabled users to conduct many transactions from their smartphone, such as purchasing goods and applications over wireless networks, redeeming coupons and tickets, banking, processing point-of-sale payments, and even paying at cash registers.

II. LITERATURE REVIEW

Amir Houmansadr, Saman A. Zonouz, and Robin Berthier.[11] has proposed 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. AsafShabtai and Yuval Elovici[12] present a light-weight, behavioural-based detection framework called Andromaly for Android smartphones, which realizes a Host-based Intrusion Detection System (HIDS). Byung-Gon Chun and PetrosManiatis[13] introduces an architecture called CloneCloud for seamless partial off-loading of program execution from the smartphone to a computational infrastructure hosting smartphone clones IkerBurguera, UrkoZurutuza, and Simin N. Tehrani.[14] monitors system calls of applications on the smartphones of many users, and analyzes these samples at a central server. Aubrey-Derrick Schmidt, Frank Peters, Florian Lamour, and Sahin Albayrak.[16] demonstrate how a smartphone running Symbian OS can be monitored to extract features for anomaly detection. Lakshmisub Ramanian.[17] 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.

III. PERMISSION BASED DETECTION

In Permission based detection permission are extracted from android manifest xml database is created which contain permission required for malicious app. system extract the permission and then matched with permission database. Few malicious permission are as follows

1)Broadcast_sms 2)read_sms 3)receive_sms 4)write_sms 5)read_phone 6)call_phone 7)change_configuration.

The selected features are collected into the signature database and divided into training data and test data and used by standard machine learning techniques to detect the android malware applications. In the first step we have used K-Means clustering to obtain k disjoint clusters on training datasets each cluster depicts a region of similar features instances in terms of Euclidean distances between the instances and their cluster centroids. We consolidate Market 2011 and Malware dataset into one dataset, and haphazardly select some portion of this dataset as a preparation dataset. The dataset is spoken to as (Xi,Yi),

where i= 1, 2, ,n and
Xi speaks to a n-dimensional vector (x1,x2, ,xn) and Yi= –1, 1 speaks to the relating class mark with 1 for generous and –1 for malware.

For K-implies grouping, we set the info parameter k as the quantity of bunches, and segment the preparation dataset that contains n application consents into k groups.

The k groups have two qualities: the intra bunch closeness is high, however the entomb group similitude is low. The mean estimation of the question comparability in a bunch is characterized as the group similitude, which is the group "centroid" or the focal point of gravity. We utilize the Weighted Euclidean separation to give the similitude between two applications. It is processed as takes after:

$$d(i,j)=\sqrt{\omega_1|x_{i1}-x_{j1}|^2+\cdots+\omega_n|x_{in}-x_{jn}|^2}$$

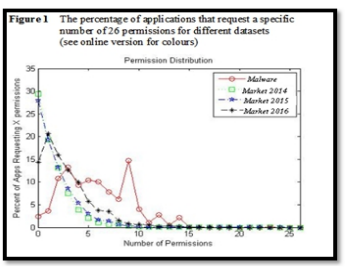


Figure 1 The percentage of applications that request a specific number of 26 permissions for different datasets (see online version for colours)

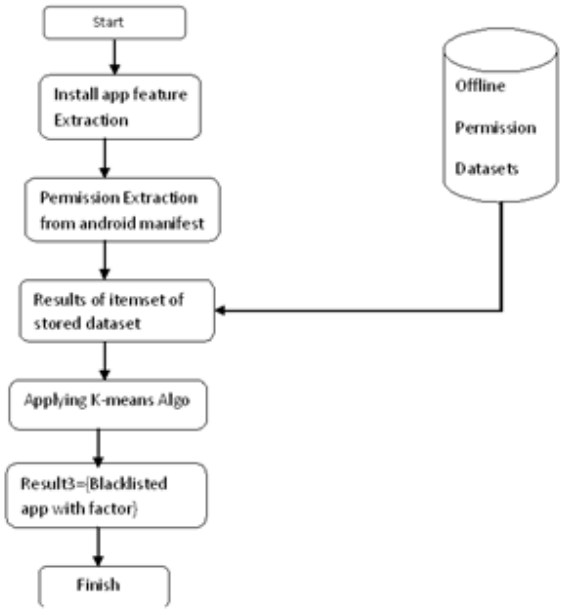
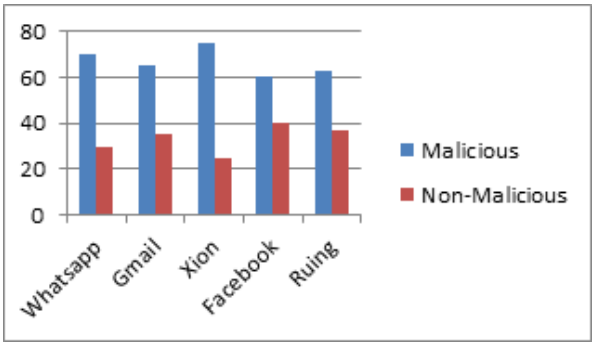


Figure 1 Permission Based Detection

IV. RESULT ANALYSIS

App name	Malicious Permissions	Non malicious permission ration
Whats App	70%	30 %
Gmail	65%	35%
Xion	75%	25 %
Face book	60%	40%
Ruing	63%	37 %

Table 1: Permission based Monitoring for spy detection



REFERENCES

[1.] Thomas Bla¨sing, Leonid Batyuk, Aubrey-Derrick Schmidt, Seyit Ahmet Camtepe, and Sahin Albayrak, "An Android Application Sandbox System for Suspicious Software Detection",www.dailabor.de/fileadmin/Files/Publikationen/Buchdatei/Thomas_AAS_Malware2010.pdf(retrieved at 2013-08-20).

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

[3.] Lakshmisub Ramanian. Security as a service in cloud for smartphones. Master's thesis, Fraunhofer Institute for Secure Information Technology, 2011.

[4.] IDC Deutschland. IDC-studie. Excerpt available http://www.idc.de/press/presse_mc_security2011.jsp, (retrieved at 2014-03-13).

[5.] Juniper Networks Global Threat Center. 2011 malicious mobile threats report.http://www.juniper.net/us/en/local/pdf/additional-resources/jnpr-2011-mobile-threats-report.pdf, (retrieved at 2014-03-13).

[6.] 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.

[7.] AVG Mobilation. Antivirus free. https://play.google.com/store/apps/details?id=com.antivirus, (retrieved at 2014-03-13).

[8.] Ramon Llamas, Ryan Reith, and Michael Shirer. Apple Cedes Market Share in Smartphone Operating System Market as Android Surges and Windows Phone Gains, According to IDC.http://www.idc.com/getdoc. jsp?containerId=prUS24257413, Aug. 2013.

[9.] Kindsight Security Labs Malware Report - Q2 2013. Alcatel-Lucent, Jul. 2013.

[10.] FortiGuard Midyear Threat Report. Fortinet, Aug. 2013.

[11.] 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 Networks Workshops, DSNW '11,pages 31–32,Washington, DC, USA, 2011. IEEE Computer Society.

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

[13.] 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.

[14.] 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.

[15.] A D Schmidt. Detection of Smartphone Malware. PhD thesis, Technischen University at Berlin, 2011.

[16.] 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 Middle WARE, Operating Systems, and Applications, MOBILWARE '08, pages 40:1–40:6, ICST, Brussels, Belgium, Belgium, 2007. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering).

[17.] Lakshmi subRamanian. Security as a service in cloud for smartphones. Master's thesis, Fraunhofer Institute for Secure Information Technology, 2011.

[18.] Eric Y. Chen and Mistutaka Itoh. Virtual smartphone over ip. In Proceedings of the 2010 IEEE International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2010.

[19.] 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.

[20.] Faruki P, Bharmal A, Laxmi V, Ganmoor V, Gaur MS, Conti M, Rajarajan M (2015) Android security: a survey of issues, malware penetration, and defenses. Commun Surv Tutor IEEE 17(2):998–1022

[21.] Lindorfer M, Neugschwandtner M, Platzer C (2015) MARVIN: efficient and comprehensive mobile app classification through static and dynamicanalysis[J]. http://www.iseclab.org/papers/marvin_compsac15.pdf

[22.] Petsas T, Voyatzis G, Athanasopoulos E, Polychronakis M, Ioannidis S (2014) Rage against the virtual machine: hindering dynamic analysis of android malware, In: Seventh European Workshop on System Security, pp 1–6. doi:10.1145/2592791.2592796

[23.] Sufatrio, Tan DJJ, Chua T-W, Vrizlynn LL (2015) Securing android: a survey, taxonomy, and challenges. ACM Comput. Surv 47(4):58. doi:10.1145/2733306

[24.] Tam K, Khan SJ, Fattori A, Cavallaro L (2015) CopperDroid: automatic reconstruction of android malware behaviors. In: Proceedings of the Network and Distributed System Security Symposium (NDSS'15), San Diego .Internet Society

[25.] Zhauniarovich Y, Ahmad M, Gadyatskaya O, Crispo B, Massacci F (2015) StaDynA: addressing the problem of dynamic code updates in the security analysis of android applications. In: ACM Conference on Data and Application Security and Privacy (CODASPY)