Android Mobile Malware Detection Using Fuzzy AHP

[1]Juliza Mohamad Arif, [1]Mohd Faizal Ab Razak, [1]Sharfah Ratibah Tuan Mat, [1] Suryanti Awang, ,
[1]Nor Syahidatul Nadiah Ismail, [1]Ahmad Firdaus

[1]Faculty of Computing
Universiti Malaysia Pahang
26600 Pekan, Pahang, Malaysia

juliza.m.arif@gmail.com , faizalrazak@ump.edu.my , sharfah0206@gmail.com,
suryanti@ump.edu.my , nadiahismail@ump.edu.my, firdausza@ump.edu.my,

Abstract— Android mobile is very challenging because it is an open-source operating system that is also vulnerable to attacks. Previous studies have shown various mobile malware detection methods to overcome this problem, but still, there is room for improvement. Mobile users mostly ignore long lists of permissions because these are difficult to understand. Therefore, to distinguish benign or malware applications and the probability of each permission request is understood, it is necessary to evaluate Android mobile applications. This research proposed a multi-criteria decision-making based (MCDM) mobile malware detection system using a risk-based fuzzy analytical hierarchy process (AHP) approach to evaluate the Android mobile application. This study focuses on static analysis, that uses permission-based features to assess the mobile malware detection system approach. Risk analysis is applied to increase the awareness of the mobile user in granting any permission request to contain a high-risk level. The evaluation used 10,000 samples taken from Drebin and AndroZoo. The results show a high accuracy rate of 90.54% values that can effectively classify the Android application into four different risk levels.

Keywords: Android mobile, mobile malware detection system, fuzzy analytical hierarchy process, risk analysis

1. Introduction

The use of mobile devices is growing every year. Statista revealed that the number of mobile users has increased from 2.7 billion in 2012 to 3.2 billion in 2019. It foresees a rise of up to 3.8 billion in 2021 (Statista, 2020). Mobile applications are no longer limited to communication and are also widely used in education, social media, shopping, industry, and banking. Its widespread use causes large quantities of data containing highly-sensitive information to be provided. This scenario presents an opportunity for a malicious code explosion designed to target mobile devices. Over 30 million mobile malwares were detected in 2018 (Mcaffee, 2019). Based on Nokia Threat Intelligence Report 2019 (Nokia, 2019), Android has recorded a higher percentage of malware among smartphone devices. Android smartphones accounted for the highest percentage, with malware applications, and researchers need to focus on these results to improve the security of Android mobile.

In the future, a comparative study between fuzzy AHP and other MCDM approaches can be conducted to validate the significant methods to improve mobile malware detection systems. Moreover, as one of the steps to increase awareness among Android users, the security vulnerabilities of Android applications that exposed users at risk of malware attacks should also be considered to be extended by this study. Furthermore, it is strongly recommended to use updated real-world data and applications existing in App Stores to assess the performance of the developed model, and it will be extremely important to evaluate the Android mobile malware detection system in the future.

The limitation of this study is that it only focused on permission-based features. Additional static features such as Java code and the intent filter can be select to expand the research. The results of this study will assist future researchers in improving the Android mobile malware detection system.

Acknowledgement

The work is funded by the Ministry of Higher Education FRGS under RACER (Project ID: RDU192601 (RACER/1/2019/ICT02/UMP//1) and PGRS200392.

References

Adewole, K. S., Anuar, N. B., Kamsin, A., Varathan, K. D., & Razak, S. A. (2017). Malicious accounts: Dark of the social networks. *Journal of Network and Computer Applications*, *79*, 41–67. https://doi.org/10.1016/j.jnca.2016.11.030

Alali, M., Almogren, A., Hassan, M. M., Rassan, I. A. L., & Bhuiyan, M. Z. A. (2018). Improving risk assessment model of cyber security using fuzzy logic inference system. *Computers and Security*, *74*, 323–339. https://doi.org/10.1016/j.cose.2017.09.011

Alazab, M., Alazab, M., Shalaginov, A., Mesleh, A., & Awajan, A. (2020). Intelligent mobile malware detection using permission requests and API calls. *Future Generation Computer Systems*, *107*, 509–521.

https://doi.org/10.1016/j.future.2020.02.002

Allix, K., Bissyandé, T. F., Klein, J., & Le Traon, Y. (2016). AndroZoo: Collecting millions of Android apps for the research community. *Proceedings - 13th Working Conference on Mining Software Repositories, MSR 2016*, 468–471. https://doi.org/10.1145/2901739.2903508

Alshahrani, H., Mansourt, H., Thorn, S., Alshehri, A., Alzahrani, A., & Fu, H. (2018). DDefender: Android application threat detection using static and dynamic analysis. *2018 IEEE International Conference on Consumer Electronics, ICCE 2018*, *2018-Janua*, 1–6. https://doi.org/10.1109/ICCE.2018.8326293

Alshehri, A., Hewins, A., McCulley, M., Alshahrani, H., Fu, H., & Zhu, Y. (2017). Risks behind Device Information Permissions in Android OS. *Communications and Network*, *09*(04), 219–234. https://doi.org/10.4236/cn.2017.94016

Arp, D., Spreitzenbarth, M., Hübner, M., Gascon, H., & Rieck, K. (2014). Drebin: Effective and Explainable Detection of Android Malware in Your Pocket. *NDSS*, *August*. https://doi.org/10.14722/ndss.2014.23247

Arslan, R. S., Dogru, I. A., & Barisci, N. (2019). Permission-Based Malware Detection System for Android Using Machine Learning Techniques. *International Journal of Software Engineering and Knowledge Engineering*, *29*(1), 43–61. https://doi.org/10.1142/S0218194019500037

Bai, H., Xie, N., Di, X., & Ye, Q. (2020). FAMD: A Fast Multifeature Android Malware Detection Framework, Design, and Implementation. *IEEE Access*, *8*, 194729–194740. https://doi.org/10.1109/access.2020.3033026

Baraiya, D., & Diwanji, P. H. (2017). A Survey on Android Malware Detection Techniques. *DEStech Transactions on Computer Science and Engineering*, *3*(wcne), 143–147. https://doi.org/10.12783/dtcse/wcne2016/5088

Bernardi, M. L., Cimitile, M., Martinelli, F., & Mercaldo, F. (2017). A fuzzy-based process mining approach for dynamic malware detection. *IEEE International Conference on Fuzzy Systems*. https://doi.org/10.1109/FUZZ-IEEE.2017.8015490

Buchanan, W. J., Chiale, S., & Macfarlane, R. (2017). A methodology for the security evaluation within third-party Android Marketplaces. *Digital Investigation*, *23*, 88–98. https://doi.org/10.1016/j.diin.2017.10.002

Chen, Z., Yan, Q., Han, H., Wang, S., Peng, L., Wang, L., & Yang, B. (2018). Machine learning based mobile malware detection using highly imbalanced network traffic. *Information Sciences*, *433–434*, 346–364. https://doi.org/10.1016/j.ins.2017.04.044

D'Angelo, G., Ficco, M., & Palmieri, F. (2020). Malware detection in mobile environments based on Autoencoders and API-images. *Journal of Parallel and Distributed Computing*, *137*, 26–33. https://doi.org/10.1016/j.jpdc.2019.11.001

Feizollah, A., Anuar, N. B., Salleh, R., & Wahab, A. W. A. (2015). A review on feature selection in mobile malware detection. *Digital Investigation*, *13*, 22–37. https://doi.org/10.1016/j.diin.2015.02.001

Hasegawa, C., & Iyatomi, H. (2018). One-dimensional convolutional neural networks for Android malware detection. *Proceedings - 2018 IEEE 14th International Colloquium on Signal Processing and Its Application, CSPA 2018*, *March*, 99–102. https://doi.org/10.1109/CSPA.2018.8368693

Jerlin, M. A., & Marimuthu, K. (2018). A New Malware Detection System Using Machine Learning Techniques for API Call Sequences. *Journal of Applied Security Research*, *13*(1), 45–62. https://doi.org/10.1080/19361610.2018.1387734

Karbab, E. M. B., Debbabi, M., Derhab, A., & Mouheb, D. (2018). MalDozer: Automatic framework for android malware detection using deep learning. *DFRWS 2018 EU - Proceedings of the 5th Annual DFRWS Europe*, *24*, S48–S59. https://doi.org/10.1016/j.diin.2018.01.007

Kaspersky. (2016). *EXPLOIT.LINUX.LOTOOR*. https://threats.kaspersky.com/en/threat/Exploit.Linux.Lotoor/#:~:text=Linux.,Lotoor&text=This program is a conditionally,CVE-2009-1185).

Kaspersky. (2019). *Mobile malware evolution 2018*. https://securelist.com/mobile-malware-evolution-2018/89689/

Kaspersky. (2021). *TROJAN-SMS.ANDROIDOS.FAKEINST*. https://threats.kaspersky.com/en/threat/Trojan-SMS.AndroidOS.FakeInst/

Kedziora, M., Gawin, P., Szczepanik, M., & Jozwiak, I. (2019). Malware Detection Using Machine Learning Algorithms and Reverse Engineering of Android Java Code. *International Journal of Network Security & Its Applications*, *11*(01), 01–14. https://doi.org/10.5121/ijnsa.2019.11101

Kim, H., Cho, T., Ahn, G. J., & Hyun Yi, J. (2018). Risk assessment of mobile applications based on machine learned malware dataset. *Multimedia Tools and Applications*, *77*(4), 5027–5042. https://doi.org/10.1007/s11042-017-4756-0

Kim, K., Kim, J., Ko, E., & Yi, J. H. (2020). Risk Assessment Scheme for Mobile Applications Based on Tree Boosting. *IEEE Access*, *8*, 48503–48514. https://doi.org/10.1109/ACCESS.2020.2979477

Kouliaridis, V., Kambourakis, G., Geneiatakis, D., & Potha, N. (2020). Two anatomists are better than one-Dual-level android malware detection. *Symmetry*, *12*(7), 1–21. https://doi.org/10.3390/sym12071128

Kouzinopoulos, C. S., Spathoulas, G., B, K. M. G., Votis, K., Pandey, P., Tzovaras, D., Katsikas, S. K., Collen, A., & Nijdam, N. A. (2018). Security in Computer and Information Sciences. In *Security in Computer and Information Sciences* (Vol. 821). https://doi.org/10.1007/978-3-319-95189-8

Kumar, K. A., Raman, A., Gupta, C., & Pillai, R. R. (2020). The recent trends in malware evolution, detection and analysis for android devices. *Journal of Engineering Science and Technology Review*, *13*(4), 240–248. https://doi.org/10.25103/jestr.134.25

Li, J., Sun, L., Yan, Q., Li, Z., Srisa-An, W., & Ye, H. (2018). Significant Permission Identification for Machine-Learning-Based Android Malware Detection. *IEEE Transactions on Industrial Informatics*, *14*(7), 3216–3225. https://doi.org/10.1109/TII.2017.2789219

Liu, K., Xu, S., Xu, G., Zhang, M., Sun, D., & Liu, H. (2020). A Review of Android

Malware Detection Approaches Based on Machine Learning. *IEEE Access*, *8*, 124579–124607. https://doi.org/10.1109/ACCESS.2020.3006143

Liu, X., Lin, Y., Li, H., & Zhang, J. (2020). A novel method for malware detection on ML-based visualization technique. *Computers and Security*, *89*. https://doi.org/10.1016/j.cose.2019.101682

Malleswari, D. N., Dhavalya, A., Sai, V. D., & Srikanth, K. (2018). A detailed study on risk assessment of mobile app permissions. *International Journal of Engineering and Technology(UAE)*, *7*(1.1 Special Issue 1), 297–300. https://doi.org/10.14419/ijet.v7i1.1.9706

Martinelli, F., Mercaldo, F., Nardone, V., Santone, A., & Vaglini, G. (2020). Model checking and machine learning techniques for HummingBad mobile malware detection and mitigation. *Simulation Modelling Practice and Theory*, *105*(March), 102169. https://doi.org/10.1016/j.simpat.2020.102169

Mat, S. R. T., Razak, M. F. A., Kahar, M. N. M., Arif, J. M., Mohamad, S., & Firdaus, A. (2021). Towards a systematic description of the field using bibliometric analysis: malware evolution. In *Journal of Scientometrics* (Issue 0123456789). Springer International Publishing. https://doi.org/10.1007/s11192-020-03834-6

Mathur, A., Podila, L. M., Kulkarni, K., Niyaz, Q., & Javaid, A. Y. (2021). NATICUSdroid: A malware detection framework for Android using native and custom permissions. *Journal of Information Security and Applications*, *58*(January), 102696. https://doi.org/10.1016/j.jisa.2020.102696

Mcaffee. (2019). *McAfee Mobile Threat Report Q1*. https://www.mcafee.com/enterprise/en-us/assets/reports/rp-mobile-threat-report-2019.pdf

Mercaldo, F., & Santone, A. (2020). Deep learning for image-based mobile malware detection. *Journal of Computer Virology and Hacking Techniques*, *16*(2), 157–171. https://doi.org/10.1007/s11416-019-00346-7

Naderi, H., & Kiani, B. (2020). Security Challenges in Android Mhealth Apps

Permissions: A Case Study of Persian Apps. *Frontiers in Health Informatics*, 1–6. https://doi.org/10.30699/fhi.v9i1.224

Nokia. (2019). Nokia Threat Intelligence Report – 2019. *Network Security*, *2019*(12), 4. https://doi.org/10.1016/s1353-4858(18)30122-3

Olukoya, O., Mackenzie, L., & Omoronyia, I. (2020). Security-oriented view of app behaviour using textual descriptions and user-granted permission requests. *Computers and Security*, *89*, 101685. https://doi.org/10.1016/j.cose.2019.101685

Pan, Y., Ge, X., Fang, C., & Fan, Y. (2020). A Systematic Literature Review of Android Malware Detection Using Static Analysis. *IEEE Access*, *8*, 116363–116379. https://doi.org/10.1109/ACCESS.2020.3002842

Rashidi, B., Fung, C., & Bertino, E. (2017). Android resource usage risk assessment using hidden Markov model and online learning. *Computers and Security*, *65*, 90–107. https://doi.org/10.1016/j.cose.2016.11.006

Razak, M. F. A., Anuar, N. B., Othman, F., Firdaus, A., Afifi, F., & Salleh, R. (2018). Bio-inspired for Features Optimization and Malware Detection. *Arabian Journal for Science and Engineering*, *43*(12), 6963–6979. https://doi.org/10.1007/s13369-017-2951-y

Razak, M. F. A., Anuar, N. B., Salleh, R., & Firdaus, A. (2016). The rise of “malware”: Bibliometric analysis of malware study. *Journal of Network and Computer Applications*, *75*, 58–76. https://doi.org/10.1016/j.jnca.2016.08.022

Razak, M. F. A., Anuar, N. B., Salleh, R., Firdaus, A., Faiz, M., & Alamri, H. S. (2018). “Less Give More”: Evaluate and zoning Android applications. *Measurement: Journal of the International Measurement Confederation*, *133*, 396–411.

Salah, A., Shalabi, E., & Khedr, W. (2020). A lightweight android malware classifier using novel feature selection methods. *Symmetry*, *12*(5), 1–16. https://doi.org/10.3390/SYM12050858

Salah, Y., Hamed, I., Nabil, S., Abdulkader, A., & Mostafa, M. M. (2019). Mobile Malware Detection : A Survey. *International Journal of Computer Science and*

Information Security, *17*(1).

Sayadi, H., Patel, N., D, S. M. P., Sasan, A., Rafatirad, S., & Homayoun, H. (2018). Ensemble learning for effective run-time hardware-based malware detection. *2018 55th ACM/ESDA/IEEE Design Automation Conference (DAC)*, 1–6. https://doi.org/10.1145/3195970.3196047

Sharma, A., Gandotra, E., Bansal, D., & Gupta, D. (2019). Malware Capability Assessment using Fuzzy Logic. *Cybernetics and Systems*, *50*(4), 323–338. https://doi.org/10.1080/01969722.2018.1552906

Sharmeen, S., Huda, S., Abawajy, J., & Hassan, M. M. (2020). An adaptive framework against android privilege escalation threats using deep learning and semi-supervised approaches. *Applied Soft Computing Journal*, 106089. https://doi.org/10.1016/j.asoc.2020.106089

Statista. (2020). *Smartphone users worldwide 2016-2021 Published by S. O'Dea, Dec 10, 2020 How many people have smartphones worldwide? The number of smartphone users worldwide today surpasses three billion and is forecast to further grow by several hundred million in the n*. https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/

Taheri, R., Ghahramani, M., Javidan, R., Shojafar, M., Pooranian, Z., & Conti, M. (2020). Similarity-based Android Malware Detection Using Hamming Distance of Static Binary Features. *Future Generation Computer Systems*, *105*, 230–247. https://doi.org/10.1016/j.future.2019.11.034

Wang, S., Chen, Z., Yan, Q., Yang, B., Peng, L., & Jia, Z. (2019). A mobile malware detection method using behavior features in network traffic. *Journal of Network and Computer Applications*, *133*(January), 15–25. https://doi.org/10.1016/j.jnca.2018.12.014

Yan, P., & Yan, Z. (2018). A survey on dynamic mobile malware detection. *Software Qual J*, *May 2017*, 891–919. https://doi.org/10.1007/s11219-017-9368-4

Zaburko, J., & Szulzyk-Cieplak, J. (2019). Information security risk assessment using the AHP method. *IOP Conference Series: Materials Science and Engineering*, *710*(1). https://doi.org/10.1088/1757-899X/710/1/012036