References

1. Rasthofer, S., Arzt, S. and Bodden, E., 2014, February. A Machine-learning Approach for Classifying and Categorizing Android Sources and Sinks. In *NDSS*.
2. Ramachandran, R., Oh, T. and Stackpole, W., 2012, June. Android anti-virus analysis. In *Annual symposium on information assurance & secure knowledge management* (pp. 35-40).
3. Jamil, Q. and Shah, M.A., 2016, August. Analysis of machine learning solutions to detect malware in android. In *Innovative Computing Technology (INTECH), 2016 Sixth International Conference on* (pp. 226-232). IEEE.
4. Yu, T., Jan, T., Simoff, S. and Debenham, J., 2007. Incorporating prior domain knowledge into inductive machine learning. *Unpublished doctoral dissertation Computer Sciences*.
5. Aman, W., 2014. A framework for analysis and comparison of dynamic malware analysis tools. *arXiv preprint arXiv:1410.2131*.
6. Bläsing, T., Batyuk, L., Schmidt, A.D., Camtepe, S.A. and Albayrak, S., 2010, October. An android application sandbox system for suspicious software detection. In *Malicious and unwanted software (MALWARE), 2010 5th international conference on* (pp. 55-62). IEEE.
7. Zhuo, L., Zhimin, G. and Cen, C., 2017, July. Research on Android Intent Security Detection Based on Machine Learning. In *2017 4th International Conference on Information Science and Control Engineering (ICISCE)* (pp. 569-574). IEEE.
8. Ankita Kapratwar, August 2016, 'Static and Dynamic Analysis for Android Malware Detection', Msc thesis, San Jose State University, California USA.
9. Gascon, H., Yamaguchi, F., Arp, D. and Rieck, K., 2013, November. Structural detection of android malware using embedded call graphs. In *Proceedings of the 2013 ACM workshop on Artificial intelligence and security* (pp. 45-54). ACM.
10. Mas' ud, M.Z., Sahib, S., Abdollah, M.F., Selamat, S.R. and Yusof, R., 2014, May. Analysis of features selection and machine learning classifier in android malware detection. In *Information Science and Applications (ICISA), 2014 International Conference on* (pp. 1-5). IEEE.
11. Rieck, Konrad, Philipp Trinius, Carsten Willems, and Thorsten Holz. "Automatic analysis of malware behavior using machine learning." *Journal of Computer Security* 19, no. 4 (2011): 639-668.
12. Percoco, N.J. and Schulte, S., 2012. Adventures in bouncerland, failures of automated malware detection within mobile application markets. *Trustwave Holdings, Inc., Tech. Rep*.
13. Peng Guojun, Cheng Dezhi, Zhao Haodong, Shen Shiqi, Li Jingwen. UI Automatic Triggering and Testing Method for Android Software Dynamic Behavior Monitoring [J]. Secrecy Science and Technology, 2014(10):29-35
14. Wang, X., Zhang, D., Su, X. and Li, W., 2017. Mlifdect: Android Malware Detection Based on Parallel Machine Learning and Information Fusion. *Security and Communication Networks, 2017*.
15. Mila Parkou, Contagio Mobile, viewed 11 January 2018, < http://contagiominidump.blogspot.com/ >
16. VirusShare, viewed 11 January 2018

< https://virusshare.com/about.4n6>

17. VirusTotal Malware Intelligence Services viewed 11 January 2018
< https://www.virustotal.com/en/about/ >
18. ADMIRE, Android Marketplaces & Developers Intelligence and Reputation Engine, viewed 11 January 2018
< http://admire.necst.it/about >
19. Ashish Bhatia, android-malware samples, viewed 11January 2018
< https://github.com/ashishb/android-malware>
20. Technische Universität Braunschweig, the DREBIN dataset, viewed 11 January 2018.
< https://www.sec.cs.tu-bs.de/~danarp/drebin/ >
21. Santuko Linux, viewed 11 January 2018
< https://santoku-linux.com/about-santoku/ >
22. Aptoid downloader, viewed 11 January 2018
< https://en.aptoide.com/installer >
23. Reverse engineering Android applications, viewed 10 October 2017.
<https://pentestlab.blog/2017/02/06/reverse-engineering-android-applications/>
24. Axmlprinter, viewed 12 January 2018. <https://github.com/rednaga/axmlprinter>
25. Drozer: Comprehensive security and attack framework for Android, viewed 12 January 2018 <https://labs.mwrinfosecurity.com/tools/drozer/>
26. Zhuo, L., Zhimin, G. and Cen, C., 2017, July. Research on Android Intent Security Detection Based on Machine Learning. In *2017 4th International Conference on Information Science and Control Engineering (ICISCE)* (pp. 569-574). IEEE.
27. Yerima, S.Y., Sezer, S. and Muttik, I., 2015. High accuracy android malware detection using ensemble learning. *IET Information Security*, *9*(6), pp.313-320.
28. Maier, D., Müller, T. and Protsenko, M., 2014, September. Divide-and-conquer: Why android malware cannot be stopped. In *Availability, Reliability and Security (ARES), 2014 Ninth International Conference on* (pp. 30-39). IEEE.
29. Apvrille, A. and Strazzere, T., 2012. Reducing the window of opportunity for Android malware Gotta catch'em all. *Journal in Computer Virology*, pp.1-11.
30. Yuan, Z., Lu, Y. and Xue, Y., 2016. Droiddetector: android malware characterization and detection using deep learning. *Tsinghua Science and Technology*, *21*(1), pp.114-123.
31. Londoño, S., Urcuqui, C.C., Cadavid, A.N., Amaya, M.F. and Gómez, J., 2015. SafeCandy: System for security, analysis and validation in Android. *Sistemas & Telemática*, *13*(35), pp.89-102.
32. Backes, M. and Nauman, M., 2017, April. LUNA: Quantifying and Leveraging Uncertainty in Android Malware Analysis through Bayesian Machine Learning. In *Security and Privacy (EuroS&P), 2017 IEEE European Symposium on* (pp. 204-217). IEEE.
33. Friedman, J., Hastie, T. and Tibshirani, R., 2001. *The elements of statistical learning* (Vol. 1, pp. 241-249). New York: Springer series in statistics.