REFERENCES

Acoca, B., 2008. Online identity theft. Organ. Econ. Coop. Dev. OECD Obs. 12.

Ahmed, R., Dharaskar, R.V., 2008. Mobile forensics: an overview, tools, future trends and challenges from law enforcement perspective, in: 6th International Conference on E-Governance, ICEG, Emerging Technologies in E-Government, M-Government. pp. 312–23.

Angelopoulou, O., 2012. Analysis of digital evidence in identity theft investigations.

Aresu, M., Ariu, D., Ahmadi, M., Maiorca, D., Giacinto, G., 2015. Clustering android malware families by http traffic, in: 2015 10th International Conference on Malicious and Unwanted Software (MALWARE). IEEE, pp. 128–135.

Arora, A., Garg, S., Peddoju, S.K., 2014. Malware detection using network traffic analysis in android based mobile devices, in: Next Generation Mobile Apps, Services and Technologies (NGMAST), 2014 Eighth International Conference on. IEEE, pp. 66–71.

Arp, D., Spreitzenbarth, M., Hubner, M., Gascon, H., Rieck, K., 2014. The DREBIN Dataset [WWW Document]. URL http://user.informatik.uni-goettingen.de/~darp/DREBIN/ (accessed 5.18.16).

Au, K.W.Y., Zhou, Y.F., Huang, Z., Lie, D., 2012. Pscout: analyzing the android permission specification, in: Proceedings of the 2012 ACM Conference on Computer and Communications Security. ACM, pp. 217–228.

Ayyub, B.M., 2014. Risk analysis in engineering and economics. CRC Press.

Babu Rajesh, V., Reddy, P., Himanshu, P., Patil, M.U., 2015. DROIDSWAN: DETECTING MALICIOUS ANDROID APPLICATIONS BASED ON STATIC FEATURE ANALYSIS. Comput. Sci. Inf. Technol. 163.

Barrera, D., s Kayacık, H.G., van Oorschot, P.C., Somayaji, A., 2010. A methodology for empirical analysis of permission-based security models and its application to android. In Proc. of the ACM conference on Computer and Communications Security 1.

Batten, L.M., Moonsamy, V., Alazab, M., 2016. Smartphone Applications, Malware and Data Theft, in: Computational Intelligence, Cyber Security and Computational Models. Springer, pp. 15–24.

Becher, M., Freiling, F.C., Hoffmann, J., Holz, T., Uellenbeck, S., Wolf, C., 2011. Mobile security catching up? revealing the nuts and bolts of the security of mobile devices, in: Security and Privacy (SP), 2011 IEEE Symposium on. IEEE, pp. 96–111.

Berghel, H., 2002. Hijacking the web. Commun. ACM 45, 23–27.

Bhati, S., Sharma, S., Singh, K., n.d. Review On Google Android a Mobile Platform. IOSR J. Comput. Eng. IOSR-JCE E-ISSN 2278–661.

Bilge, L., Strufe, T., Balzarotti, D., Kirda, E., 2009. All your contacts are belong to us: automated identity theft attacks on social networks, in: Proceedings of the 18th International Conference on World Wide Web. ACM, pp. 551–560.

Burguera, I., Zurutuza, U., Nadjm-Tehrani, S., 2011. Crowdroid: behavior-based malware detection system for android, in: Proceedings of the 1st ACM Workshop on Security and Privacy in Smartphones and Mobile Devices. ACM, pp. 15–26.

Castelluccia, C., De Cristofaro, E., Perito, D., 2010. Private information disclosure from web searches, in: Privacy Enhancing Technologies. Springer, pp. 38–55.

Chekina, L., Mimran, D., Rokach, L., Elovici, Y., Shapira, B., 2012. Detection of deviations in mobile applications network behavior. ArXiv Prepr. ArXiv12080564.

Chellappa, R.K., Sin, R.G., 2005. Personalization versus privacy: An empirical examination of the online consumer's dilemma. Inf. Technol. Manag. 6, 181–202.

Chen, Z., Han, H., Yan, Q., Yang, B., Peng, L., Zhang, L., Li, J., 2015. A first look at android malware traffic in first few minutes, in: Trustcom/BigDataSE/ISPA, 2015 IEEE. IEEE, pp. 206–213.

Chikofsky, E.J., Cross, J.H., others, 1990. Reverse engineering and design recovery: A taxonomy. Softw. IEEE 7, 13–17.

Commission, I.E., Standardization, I.O. for, 2008. BS ISO/IEC 27005:2008, British Standard. BSI Group.

Conrow, E.H., Shishido, P.S., 1997. Implementing risk management on software intensive projects. IEEE Softw. 14, 83.

Delosières, L., García, D., 2013. Infrastructure for detecting Android malware, in: Information Sciences and Systems 2013. Springer, pp. 389–398.

Developers, A., 2011. System Permissions. http://developer.android.com/guide/topics/security/permissions.html, Permission Group.

Dictionary, W., 1913. Webster's revised unabridged dictionary. C. & G. Merriam Co. Springfield, Massachusetts, USA.

Duda, R.O., Hart, P.E., Stork, D.G., 2012. Pattern classification. John Wiley & Sons.

Elenkov, N., 2012. Certificate pinning in Android 4.2.

Enck, W., Ongtang, M., McDaniel, P., 2009. Understanding android security. IEEE Secur. Priv. 50–57.

Erturk, E., 2015. Two Trends in Mobile Security: Financial Motives and Transitioning from Static to Dynamic Analysis. ArXiv Prepr. ArXiv150406893.

Erturk, E., 2012. A case study in open source software security and privacy: Android adware, in: Internet Security (WorldCIS), 2012 World Congress on. IEEE, pp. 189–191.

Feller, W., 1950. An introduction to probability theory and its applications. Vol. I.

Felt, A.P., Chin, E., Hanna, S., Song, D., Wagner, D., 2011a. Android permissions demystified, in: Proceedings of the 18th ACM Conference on Computer and Communications Security. ACM, pp. 627–638.

Felt, A.P., Finifter, M., Chin, E., Hanna, S., Wagner, D., 2011b. A survey of mobile malware in the wild, in: Proceedings of the 1st ACM Workshop on Security and Privacy in Smartphones and Mobile Devices. ACM, pp. 3–14.

Felt, A.P., Ha, E., Egelman, S., Haney, A., Chin, E., Wagner, D., 2012. Android permissions: User attention, comprehension, and behavior, in: Proceedings of the Eighth Symposium on Usable Privacy and Security. ACM, p. 3.

Feng, Y., Anand, S., Dillig, I., Aiken, A., 2014. Apposcopy: Semantics-based detection of android malware through static analysis, in: Proceedings of the 22nd ACM SIGSOFT International Symposium on Foundations of Software Engineering. ACM, pp. 576–587.

Gates, C.S., Li, N., Peng, H., Sarma, B., Qi, Y., Potharaju, R., Nita-Rotaru, C., Molloy, I., 2014. Generating summary risk scores for mobile applications. Dependable Secure Comput. IEEE Trans. On 11, 238–251.

Gercke, M., 2007. Internet-Related Identity Theft. Econ. Crime Div. Dir. Gen. Hum. Rights Leg. Aff. Strasbg. Fr.

Gianazza, A., 2013. PuppetDroid: a remote execution environment and UI exerciser for Android malware analysis.

Google Android : CVE security vulnerabilities, versions and detailed reports [WWW Document], n.d. URL http://www.cvedetails.com/product/19997/Google-Android.html?vendor_id=1224 (accessed 6.9.16).

Grace, M., Zhou, Y., Zhang, Q., Zou, S., Jiang, X., 2012. Riskranker: scalable and accurate zero-day android malware detection, in: Proceedings of the 10th International Conference on Mobile Systems, Applications, and Services. ACM, pp. 281–294.

Greene, S., 2014. Security Program and Policies: Principles and Practices. Pearson Education.

Gross, R., Acquisti, A., 2005. Information revelation and privacy in online social networks, in: Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society. ACM, pp. 71–80.

Haseman, C., 2008. Android Essentials. Apress.

Hoar, S.B., 2001. Identity theft: The crime of the new millennium. Rev 80, 1423.

Hoffman, S.K., McGinley, T.G., 2010. Identity theft: a reference handbook. ABC-CLIO.

Hogben, G., Dekker, M., 2010. Smartphones: Information security risks, opportunities and recommendations for users. Eur. Netw. Inf. Secur. Agency 710.

Hoofnagle, C.J., 2007. Identity theft: Making the known unknowns known. Harv. J. Law Technol. 21.

Hoog, A., 2011. Android forensics: investigation, analysis and mobile security for Google Android. Elsevier.

Iland, D., Pucher, A., Schauble, T., 2011. Detecting android malware on network level. Univ. Calif. St. Barbara 12.

ISO, I., 1994. IEC 7498-1: 1994 information technology–open systems interconnection–basic reference model: The basic model. ISO Stand. ISOIEC 7498–1.

Jakobsson, M., Myers, S., 2006. Phishing and countermeasures: understanding the increasing problem of electronic identity theft. John Wiley & Sons.

Jansen, W., Ayers, R., 2007. Guidelines on cell phone forensics. NIST Spec. Publ. 800, 101.

Janson, W., Scarfone, K., 2008. Guidelines on cellphone and PDA security: Recommendations of the National Institute of Standards and Technology NIST Special Publication 800-124. Gaithersburg MD.

Jarmoc, J., Unit, D., 2012. SSL/TLS interception proxies and transitive trust. Black Hat Eur.

Jeon, W., Kim, J., Lee, Y., Won, D., 2011. A practical analysis of smartphone security, in: Human Interface and the Management of Information. Interacting with Information. Springer, pp. 311–320.

Jing, Y., Ahn, G.-J., Zhao, Z., Hu, H., 2014. Riskmon: Continuous and automated risk assessment of mobile applications, in: Proceedings of the 4th ACM Conference on Data and Application Security and Privacy. ACM, pp. 99–110.

Kearney, P., Brügger, L., 2007. A risk-driven security analysis method and modelling language. BT Technol. J. 25, 141–153.

Kondakci, S., 2010. A causal model for information security risk assessment, in: Information Assurance and Security (IAS), 2010 Sixth International Conference on. IEEE, pp. 143–148.

Kong, D., Cen, L., Jin, H., n.d. Towards Automatic Ranking App Risks via Heterogenous Privacy Indicators.

Konings, B., Bachmaier, C., Schaub, F., Weber, M., 2013. Device names in the wild: Investigating privacy risks of zero configuration networking, in: Mobile Data Management (MDM), 2013 IEEE 14th International Conference on. IEEE, pp. 51–56.

Krishnamurthy, B., Wills, C.E., 2009. On the leakage of personally identifiable information via online social networks, in: Proceedings of the 2nd ACM Workshop on Online Social Networks. ACM, pp. 7–12.

Lederm, T., Clarke, N.L., 2011. Risk assessment for mobile devices, in: Trust, Privacy and Security in Digital Business. Springer, pp. 210–221.

(LEFG), L.E.F.G., America, U.S. of, 2013. Smartphone Thefts and Robberies: Growing Trends and Promising Practices.

Lever, C., Antonakakis, M., Reaves, B., Traynor, P., Lee, W., 2013. The Core of the Matter: Analyzing Malicious Traffic in Cellular Carriers., in: NDSS.

Lindorfer, M., Neugschwandtner, M., Platzer, C., 2015. MARVIN: Efficient And Comprehensive Mobile App Classification.

Lindorfer, M., Neugschwandtner, M., Weichselbaum, L., Fratantonio, Y., van der Veen, V., Platzer, C., 2014. ANDRUBIS-1,000,000 Apps Later: A View on Current Android Malware Behaviors, in: Proceedings of the the 3rd International Workshop on Building Analysis Datasets and Gathering Experience Returns for Security (BADGERS).

Liu, J., Yu, J., 2011. Research on Development of Android Applications, in: 2011 Fourth International Conference on Intelligent Networks and Intelligent Systems. IEEE, pp. 69–72.

Liu, Q., Sun, X., 2012. Research of Web Real-Time Communication Based on Web Socket.

Lo, N.-W., Yeh, K.-H., Fan, C.-Y., 2014. Leakage Detection and Risk Assessment on Privacy for Android Applications: LRPdroid.

Maker, F., Chan, Y., 2009. A survey on android vs. linux. Univ. Calif. 1–10.

Mansfield-Devine, S., 2012. Android architecture: attacking the weak points. Netw. Secur. 2012, 5–12.

Mercuri, R.T., 2006. Scoping identity theft. Commun. ACM 49, 17–21.

Mylonas, A., Theoharidou, M., Gritzalis, D., 2013. Assessing privacy risks in android: A user-centric approach, in: Risk Assessment and Risk-Driven Testing. Springer, pp. 21–37.

Newman, G., McNally, M.M., 2005. Identity theft literature review. Citeseer.

Oberheide, J., Miller, C., 2012. Dissecting the android bouncer. SummerCon2012 N. Y.

Olofsson, P., Andersson, M., 2012. Probability, statistics, and stochastic processes. John Wiley & Sons.

Padmakar, E.P., Shivaji, R.L., n.d. A Review on Risk Score Based App Classification Using Enriched Contextual Information of App Context.

Patel, A., 2011. Identifying network path including network proxies. Google Patents.

Peng, H., Gates, C., Sarma, B., Li, N., Qi, Y., Potharaju, R., Nita-Rotaru, C., Molloy, I., 2012. Using probabilistic generative models for ranking risks of android apps, in:

Proceedings of the 2012 ACM Conference on Computer and Communications Security. ACM, pp. 241–252.

Peng, S., Yu, S., Yang, A., 2014. Smartphone malware and its propagation modeling: A survey. Commun. Surv. Tutor. IEEE 16, 925–941.

Shabtai, A., Fledel, Y., Kanonov, U., Elovici, Y., Dolev, S., Glezer, C., 2010. Google android: A comprehensive security assessment. IEEE Secur. Priv. 35–44.

Shin, W., Kwak, S., Kiyomoto, S., Fukushima, K., Tanaka, T., 2010. A small but non-negligible flaw in the Android permission scheme, in: Policies for Distributed Systems and Networks (POLICY), 2010 IEEE International Symposium on. IEEE, pp. 107–110.

Singh, S.K., Mishra, B., Gera, P., 2015. A Privacy Enhanced Security Framework for Android Users, in: IT Convergence and Security (ICITCS), 2015 5th International Conference on. IEEE, pp. 1–6.

Son, K.-C., Lee, J.-Y., 2011. The method of android application speed up by using NDK, in: Awareness Science and Technology (iCAST), 2011 3rd International Conference on. IEEE, pp. 382–385.

Spreitzenbarth, M., Freiling, F., Echtler, F., Schreck, T., Hoffmann, J., 2013. Mobile-sandbox: having a deeper look into android applications, in: Proceedings of the 28th Annual ACM Symposium on Applied Computing. ACM, pp. 1808–1815.

Stoneburner, G., Goguen, A., Feringa, A., 2001. NIST Special Publication 800-30. Risk Manag. Guide Inf. Technol. Syst.

Stuart, A., Ord, J.K., 1994. Kendall's Advanced Theory of Statistics, Volume 1: Distribution Theory, Edward Arnold. Lond. UK.

Su, M.-Y., Chang, W.-C., 2014. Permission-based malware detection mechanisms for smart phones, in: Information Networking (ICOIN), 2014 International Conference on. IEEE, pp. 449–452.

Theoharidou, M., Mylonas, A., Gritzalis, D., 2012. A risk assessment method for smartphones, in: Information Security and Privacy Research. Springer, pp. 443–456.

UI/Application Exercise Monkey [WWW Document], n.d. URL http://developer.android.com/tools/help/monkey.html (accessed 10.21.15).

Varga, J., Muska, P., 2014. Presenting Risks Introduced by Android Application Permissions in a User-Friendly Way. Tatra Mt. Math. Publ. 60, 85–100.

Voas, J., Quirolgico, S., Michael, C., Scarfone, K., 2015. Vetting the Security of Mobile Applications. NIST NIST Spec. Publ. 800–163.

Wang, J., 2009. Computer network security: theory and practice. Springer Publishing Company, Incorporated.

Wang, W., Wang, X., Feng, D., Liu, J., Han, Z., Zhang, X., 2014. Exploring permission-induced risk in android applications for malicious application detection. Inf. Forensics Secur. IEEE Trans. On 9, 1869–1882.

Wei, M., Gong, X., Wang, W., n.d. Claim What You Need: A Text-Mining Approach on Android Permission Request Authorization.

Wichers, D., 2013. OWASP Top-10 2013. OWASP Found. Febr.

Wong, M.Y., Lie, D., 2016. IntelliDroid: A Targeted Input Generator for the Dynamic Analysis of Android Malware 1.

Xu, W., Zhang, F., Zhu, S., 2013. Permlyzer: Analyzing permission usage in android applications, in: Software Reliability Engineering (ISSRE), 2013 IEEE 24th International Symposium on. IEEE, pp. 400–410.

Yang, Z., Yang, M., Zhang, Y., Gu, G., Ning, P., Wang, X.S., 2013. Appintent: Analyzing sensitive data transmission in android for privacy leakage detection, in: Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security. ACM, pp. 1043–1054.

Zhang, C., Sun, J., Zhu, X., Fang, Y., 2010. Privacy and security for online social networks: challenges and opportunities. Netw. IEEE 24, 13–18.

Zhang, Y., Luo, X., Yin, H., 2015. Dexhunter: toward extracting hidden code from packed android applications, in: Computer Security–ESORICS 2015. Springer, pp. 293–311.

Zheng, M., Sun, M., Lui, J., 2013. Droid analytics: A signature based analytic system to collect, extract, analyze and associate android malware, in: Trust, Security and Privacy in Computing and Communications (TrustCom), 2013 12th IEEE International Conference on. IEEE, pp. 163–171.