

Understanding the Relationship Between Quality and Security in Android Applications: A Large Scale Analysis of Reverse Engineered Android Applications

XXXXXXXXXXXXXXXXXXXX
XXXXXXXXXX
XXXXXXXXXX
XXXXXXXXXX
XXXXXXXXXX, XX, XXX
XXXXXX@XXXXX.XXX

ABSTRACT

Android applications (apps) are not immune to the problems which also plague conventional software including security vulnerabilities, quality defects, permission misuse, and numerous other issues. Many developers even intentionally create vulnerable or malicious apps (malware) for often highly lucrative purposes. We need to better understand current trends in app quality and security order to create higher quality software, and more effectively battle malware. In order to gather this critical information, we collected and reverse engineered 70,785 Android apps from the Google Play store, along with 1,420 malicious apps from other sources. Each app was analyzed using several static analysis tools to record a variety of information about each of them including requested permissions, size (LOC), possible defects and permission misuse. Our findings conclude that: 1) app categories substantially differ in terms of permissions misuse; 2) that there is no significant correlation between an app's quality and security; 3) that malware typically requests more permissions and suffers in several quality related metrics in comparison to benign apps; 4) that malware and benign apps are annually growing both in terms of LOC and requested permissions. We also present an easy to use, robust website and dataset for others to use in their own research.

1. INTRODUCTION

References

- [1] Contagio mobile. <http://contagiomindump.blogspot.com>.
- [2] Number of apps available in leading app stores as of november 2015. <http://www.statista.com/statistics/266210/number-of-available-applications-in-the-google-play-store/>.
- [3] Manifest.permission. <http://developer.android.com/reference/android/Manifest.permission.html>, July 2014.
- [4] T. Armendariz. Fortinet's fortiguard labs reports 96.5% of all mobile malware tracked is android based, symbian is distant second at 3.45blackberry, palmos, and windows together

represent less than 1 http://www.fortinet.com/press_releases/2014/fortiguard-quarterly-labs-reports.html.

- [5] A. Bartel, J. Klein, Y. Le Traon, and M. Monperrus. Automatically securing permission-based software by reducing the attack surface: An application to android. In *Proceedings of the 27th IEEE/ACM International Conference on Automated Software Engineering, ASE 2012*, pages 274–277, New York, NY, USA, 2012. ACM.
- [6] I. Burguera, U. Zurutuza, and S. Nadjm-Tehrani. Crowddroid: behavior-based malware detection system for android. In *Proceedings of the 1st ACM workshop on Security and privacy in smartphones and mobile devices*, pages 15–26. ACM, 2011.
- [7] B. Chess and G. McGraw. Static analysis for security. *IEEE Security & Privacy*, (6):76–79, 2004.
- [8] David and M. Kleidermacher. Using coding standards to improve software quality and security. <http://www.embedded.com/design/safety-and-security/4418986/Using-coding-standards-to-improve-software-quality-and-security>.
- [9] A. P. Felt, E. Chin, S. Hanna, D. Song, and D. Wagner. Android permissions demystified. In *Proceedings of the 18th ACM Conference on Computer and Communications Security, CCS '11*, pages 627–638, New York, NY, USA, 2011. ACM.
- [10] A. P. Felt, K. Greenwood, and D. Wagner. The effectiveness of application permissions. In *Proceedings of the 2Nd USENIX Conference on Web Application Development, WebApps'11*, pages 7–7, Berkeley, CA, USA, 2011. USENIX Association.
- [11] Y. Feng, S. Anand, I. Dillig, and A. Aiken. Apposcopy: Semantics-based detection of android malware through static analysis. In *Proceedings of the 22Nd ACM SIGSOFT International Symposium on Foundations of Software Engineering, FSE 2014*, pages 576–587, New York, NY, USA, 2014. ACM.
- [12] M. C. Grace, W. Zhou, X. Jiang, and A.-R. Sadeghi. Unsafe exposure analysis of mobile in-app advertisements. In *Proceedings of the Fifth ACM Conference on Security and Privacy in Wireless and Mobile Networks, WISEC '12*, pages 101–112, New York, NY, USA, 2012. ACM.
- [13] D. Kleidermacher and M. Kleidermacher. *Embedded Systems Security: Practical Methods for Safe and Secure Software and Systems Development*. Newnes, Newton, MA, USA, 1st edition, 2012.
- [14] D. E. Krutz, M. Mirakhorli, M. S. A., A. Ruiz, J. Peterson, A. Filipski, and J. Smith. A dataset of open-source android applications. In *Proceedings of the 12th Working Conference on Mining Software Repositories*. ACM, 2015.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

SAC'17, April 3-7, 2016, Marrakech, Morocco.

Copyright 2017 ACM 978-1-4503-3739-7/16/04...\$15.00.

<http://dx.doi.org/xx.xxxx/xxxxxxx.xxxxxx> ...\$15.00.

- [15] S.-H. Lee and S.-H. Jin. Warning system for detecting malicious applications on android system. In *International Journal of Computer and Communication Engineering*, 2013.
- [16] X. Li. Using peer review to assess coding standards-a case study. In *Frontiers in education conference, 36th annual*, pages 9–14. IEEE, 2006.
- [17] X. Li and C. Prasad. Effectively teaching coding standards in programming. In *Proceedings of the 6th Conference on Information Technology Education, SIGITE '05*, pages 239–244, New York, NY, USA, 2005. ACM.
- [18] P. Pearce, A. P. Felt, G. Nunez, and D. Wagner. Addroid: Privilege separation for applications and advertisers in android. In *Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security, ASIACCS '12*, pages 71–72, New York, NY, USA, 2012. ACM.
- [19] R. Pressman. *Software Engineering: A Practitioner's Approach*. McGraw-Hill, Inc., New York, NY, USA, 7 edition, 2010.
- [20] V. Rastogi, Y. Chen, and X. Jiang. Droidchameleon: Evaluating android anti-malware against transformation attacks. In *Proceedings of the 8th ACM SIGSAC Symposium on Information, Computer and Communications Security, ASIA CCS '13*, pages 329–334, New York, NY, USA, 2013. ACM.
- [21] A. Reina, A. Fattori, and L. Cavallaro. A system call-centric analysis and stimulation technique to automatically reconstruct android malware behaviors. *EuroSec, April*, 2013.
- [22] N. Rutar, C. B. Almazan, and J. S. Foster. A comparison of bug finding tools for java. In *Software Reliability Engineering, 2004. ISSRE 2004. 15th International Symposium on*, pages 245–256. IEEE, 2004.
- [23] B. P. Sarma, N. Li, C. Gates, R. Potharaju, C. Nita-Rotaru, and I. Molloy. Android permissions: A perspective combining risks and benefits. In *Proceedings of the 17th ACM Symposium on Access Control Models and Technologies, SACMAT '12*, pages 13–22, New York, NY, USA, 2012. ACM.
- [24] A. Shabtai, U. Kanonov, Y. Elovici, C. Glezer, and Y. Weiss. "andromaly": a behavioral malware detection framework for android devices. *Journal of Intelligent Information Systems*, 38(1):161–190, 2012.
- [25] R. Stevens, J. Ganz, V. Filkov, P. Devanbu, and H. Chen. Asking for (and about) permissions used by android apps. In *Mining Software Repositories (MSR), 2013 10th IEEE Working Conference on*, pages 31–40, 2013.
- [26] M.-Y. Su and W.-C. Chang. Permission-based malware detection mechanisms for smart phones. In *Information Networking (ICOIN), 2014 International Conference on*, pages 449–452, Feb 2014.
- [27] K. A. Talha, D. I. Alper, and C. Aydin. Apk auditor: Permission-based android malware detection system. *Digital Investigation*, 13:1–14, 2015.
- [28] T. Vidas, N. Christin, and L. F. Cranor. Curbing android permission creep. In *In W2SP*, 2011.
- [29] D.-J. Wu, C.-H. Mao, T.-E. Wei, H.-M. Lee, and K.-P. Wu. Droidmat: Android malware detection through manifest and api calls tracing. In *Information Security (Asia JCIS), 2012 Seventh Asia Joint Conference on*, pages 62–69, Aug 2012.
- [30] S. Yerima, S. Sezer, and G. McWilliams. Analysis of bayesian classification-based approaches for android malware detection. *Information Security, IET*, 8(1):25–36, Jan 2014.
- [31] Y. Zhou and X. Jiang. Dissecting android malware: Characterization and evolution. In *Proceedings of the 2012 IEEE Symposium on Security and Privacy, SP '12*, pages 95–109, Washington, DC, USA, 2012. IEEE Computer Society.
- [32] Y. Zhou and X. Jiang. Dissecting android malware: Characterization and evolution. In *Security and Privacy (SP), 2012 IEEE Symposium on*, pages 95–109. IEEE, 2012.