1. Beyond Google play: A large-scale comparative study of Chinese android app markets

Wang, Haoyu (1); Liu, Zhe (2); Liang, Jingyue (2); Vallina-Rodriguez, Narseo (5); Guo, Yao (5); Li, Li (3); Tapiador, Juan (4); Cao, Jingcun (5); Xu, Guoai (1)

Source: *Proceedings of the ACM SIGCOMM Internet Measurement Conference, IMC*, p 293-307, October 31, 2018, *IMC 2018 - Proceedings of the Internet Measurement Conference*; **ISBN-13:** 9781450356190; **DOI:** 10.1145/3278532.3278558; **Conference:** 2018 Internet Measurement Conference, IMC 2018, October 31, 2018 - November 2, 2018; **Sponsor:** ACM SIGCOMM; **Publisher:** Association for Computing Machinery

Author affiliation: (1) Beijing University of Posts and Telecommunications, China (2) Key Laboratory of High-Confidence Software Technologies (MOE), Peking University, 3 IMDEA Networks, 4 ICSI, China (3) Monash University, Australia (4) Universidad Carlos III de Madrid, Spain (5) Indiana University, Bloomington, United States

Abstract: China is one of the largest Android markets in the world. As Chinese users cannot access Google Play to buy and install Android apps, a number of independent app stores have emerged and compete in the Chinese app market. Some of the Chinese app stores are pre-installed vendor-specific app markets (e.g., Huawei, Xiaomi and OPPO), whereas others are maintained by large tech companies (e.g., Baidu, Qihoo 360 and Tencent). The nature of these app stores and the content available through them vary greatly, including their trustworthiness and security guarantees. As of today, the research community has not studied the Chinese Android ecosystem in depth. To fill this gap, we present the first large-scale comparative study that covers more than 6 million Android apps downloaded from 16 Chinese app markets and Google Play. We focus our study on catalog similarity across app stores, their features, publishing dynamics, and the prevalence of various forms of misbehavior (including the presence of fake, cloned and malicious apps). Our findings also suggest heterogeneous developer behavior across app stores, in terms of code maintenance, use of third-party services, and so forth. Overall, Chinese app markets perform substantially worse when taking active measures to protect mobile users and legit developers from deceptive and abusive actors, showing a significantly higher prevalence of malware, fake, and cloned apps than Google Play. © 2018 Association for Computing Machinery. (103 refs)

Main heading: Mobile security
Controlled terms: Android (operating system) - Cloning - Commerce - Ecosystems - FORTH (programming language) - Malware - Network security
Uncontrolled terms: Android markets - Comparative studies - Developer behavior - Google plays - Permission - Research communities - Third parties - Third party services
Classification Code: 454.3 Ecology and Ecosystems - 461.8.1 Genetic Engineering - 723 Computer Software, Data Handling and Applications
Funding Details: Number: -, Acronym: -, Sponsor: Vehicle Technologies Program; Number: -, Acronym: -, Sponsor: Research and Development; Number: 786741, Acronym: H2020, Sponsor: Horizon 2020 Framework Programme; Number: 61702045,61772042, Acronym: NSFC, Sponsor: National Natural Science Foundation of China; Number: S2013/ICE3095,TIN2016-79095-C2-2-R, Acronym: MINECO, Sponsor: Ministerio de Econom&iacute;a y Competitividad; Number: 2017RC40, Acronym: -, Sponsor: Horizon 2020; Number: CNS-1564329, Acronym: NSF, Sponsor: National Science Foundation; Number: 2018YFB0803603, Acronym: NKRDPC, Sponsor: National Key Research and Development Program of China;
Funding text: We sincerely thank our shepherd Prof. Zhenhua Li (Tsinghua University), and all the anonymous reviewers for their valuable suggestions and comments to improve this paper. This work is supported by the National Key Research and Development Program of China (grant No.2018YFB0803603), the National Natural Science Foundation of China (grants No.61702045, and No.61772042); the BUPT Youth Research and Innovation Program (No.2017RC40); Spain’s Ministry of Economy and Competitiveness (grant TIN2016-79095-C2-2-R); the Madrid Region’s Technologies 2014 Research Program (grant S2013/ICE3095); the US National Science Foundation (grant CNS-1564329); and the European Union’s Horizon 2020 Innovation Action programme (grant Agreement No. 786741, SMOOTH Project).We sincerely thank our shepherd Prof. Zhenhua Li (Tsinghua University), and all the anonymous reviewers for their valuable suggestions and comments to improve this paper. This work is supported by the National Key Research and Development Program of China (grant No.2018YFB0803603), the National Natural Science Foundation of China (grants No.61702045, and No.61772042); the BUPT Youth Research and Innovation Program (No.2017RC40); Spain's Ministry of Economy and Competitiveness (grant TIN2016-79095-C2-2-R); the Madrid Region's Technologies 2014 Research Program (grant S2013/ICE3095); the US National Science Foundation (grant CNS-1564329); and the European Union's Horizon 2020 Innovation Action programme (grant Agreement No. 786741, SMOOTH Project).
Database: Compendex
Data Provider: Engineering Village