1. FraudDroid: Automated ad fraud detection for android apps (*Open Access*)

Dong, Feng (1); Wang, Haoyu (1); Li, Li (2); Guo, Yao (3); Bissyandé, Tegawendé F. (4); Liu, Tianming (1); Xu, Guoai (1); Klein, Jacques (4)

Source: *ESEC/FSE 2018 - Proceedings of the 2018 26th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering*, p 257-268, October 26, 2018, *ESEC/FSE 2018 - Proceedings of the 2018 26th ACM Joint Meeting on European So ftware Engineering Conference and Symposium on the Foundations of So ftware Engineering*; **ISBN-13:** 9781450355735; **DOI:** 10.1145/3236024.3236045;
Conference: 26th ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering, ESEC/FSE 2018, November 4, 2018 - November 9, 2018; **Sponsor:** ACM SIGSOFT;
Publisher: Association for Computing Machinery

Author affiliation: (1) Beijing University of Posts and Telecommunications, China (2) Faculty of Information Technology, Monash University, Australia (3) Key Laboratory of High-Confidence Software Technologies (MOE), Peking University, China (4) University of Luxembourg, Luxembourg, Luxembourg

Abstract: Although mobile ad frauds have been widespread, state-of-the-art approaches in the literature have mainly focused on detecting the so-called static placement frauds, where only a single UI state is involved and can be identified based on static information such as the size or location of ad views. Other types of fraud exist that involve multiple UI states and are performed dynamically while users interact with the app. Such dynamic interaction frauds, although now widely spread in apps, have not yet been explored nor addressed in the literature. In this work, we investigate a wide range of mobile ad frauds to provide a comprehensive taxonomy to the research community. We then propose, FraudDroid, a novel hybrid approach to detect ad frauds in mobile Android apps. Fraud- Droid analyses apps dynamically to build UI state transition graphs and collects their associated runtime network traffics, which are then leveraged to check against a set of heuristic-based rules for identifying ad fraudulent behaviours. We show empirically that FraudDroid detects ad frauds with a high precision $(\sim 93\%)$ and recall $(\sim 92\%)$. Experimental results further show that FraudDroid is capable of detecting ad frauds across the spectrum of fraud types. By analysing 12,000 ad-supported Android apps, FraudDroid identified 335 cases of fraud associated with 20 ad networks that are further confirmed to be true positive results and are shared with our fellow researchers to promote advanced ad fraud detection. © 2018 Association for Computing Machinery. (82 refs)

Main heading: Android (operating system)
Controlled terms: Automation - Crime - Engineering research - User interfaces
Uncontrolled terms: ad fraud - Android - Dynamic interaction - Mobile app - Research communities - State transition graphs - State-of-the-art approach - Static information
Classification Code: 722.2 Computer Peripheral Equipment - 723 Computer Software, Data Handling and Applications - 731 Automatic Control Principles and Applications - 901.3 Engineering Research - 971 Social Sciences
Open Access type(s): All Open Access, Green
Database: Compendex
Data Provider: Engineering Village