Engineering Village™

1. **Difuzer: Uncovering Suspicious Hidden Sensitive Operations in Android Apps**
Samhi, J.; Li, L.; Bissyande, T.F.; Klein, J. **Source:** *2022 IEEE/ACM 44th International Conference on Software Engineering (ICSE)*, 723-35, 2022; **ISBN-13:** 978-1-4503-9221-1; **DOI:** 10.1145/3510003.3510135; **Conference:** 2022 IEEE/ACM 44th International Conference on Software Engineering (ICSE), 25-27 May 2022, Pittsburgh, PA, USA; **Sponsor:** IEEE Computer Society;ACM SIGSOFT;IEEE Technical Council in Software Engineering; **Publisher:** IEEE, Piscataway, NJ, USA

Author affiliation:
University of Luxembourg, SnT, Luxembourg
Monash University, Australia

Abstract: One prominent tactic used to keep malicious behavior from being detected during dynamic test campaigns is logic bombs, where malicious operations are triggered only when specific conditions are satisfied. Defusing logic bombs remains an unsolved problem in the literature. In this work, we propose to investigate Suspicious Hidden Sensitive Operations (SHSOs) as a step towards triaging logic bombs. To that end, we develop a novel hybrid approach that combines static analysis and anomaly detection techniques to un-cover SHSOs, which we predict as likely implementations of logic bombs. Concretely, Difuzer identifies SHSO entry-points using an instrumentation engine and an inter-procedural data-flow analysis. Then, it extracts trigger-specific features to characterize SHSOs and leverages One-Class SVM to implement an unsupervised learning model for detecting abnormal triggers. We evaluate our prototype and show that it yields a precision of 99.02% to detect SHSOs among which 29.7% are logic bombs. Difuzer outperforms the state-of-the-art in revealing more logic bombs while yielding less false positives in about one order of magnitude less time. All our artifacts are released to the community. (0 refs.) **Inspec controlled terms:** Android (operating system) - data flow analysis - feature extraction - program testing - security of data - support vector machines - unsupervised learning

Uncontrolled terms: Difuzer - logic bombs - malicious behavior - SHSOs - suspicious hidden sensitive operations - Android apps - dynamic test campaigns - malicious operations - static analysis - anomaly detection - instrumentation engine - inter-procedural data-flow analysis - trigger-specific feature extraction - one-class SVM - unsupervised learning - abnormal trigger detection

Classification Code: C6190V Mobile, ubiquitous and pervasive computing - C6262 - C6265 - C6150G Diagnostic, testing, debugging and evaluating systems - C6130S Data security

IPC Code: G06F9/44 - G06F9/46 - G06F11/36 - G06F21/00 - G06N20/00

Treatment: Bibliography (BIB); Practical (PRA)

Database: Inspec