# DroidExec: Root Exploit Malware Recognition Against Wide Variability via Folding Redundant Function-relation Graph

Te-En Wei*, Hahn-Ming Lee*, Hsiao-Rong Tyan**, Hong-Yuan Mark Liao***, Albert B. Jeng*, Jiunn-Chin Wang*

**Department of Computer Science and Information Engineering, National Taiwan University of Science and Technology, Taipei 106, Taiwan*

***Department of Information and Computer Engineering, Chung Yuan Christian University, Chung Li 32023, Taiwan*

**** Institute of Information Science, Academia Sinica, Nankang 11529, Taiwan*

**d9807501@mail.ntust.edu.tw, hmlee@mail.ntust.edu.tw, tyan@ice.cycu.edu.tw, liao@iis.sinica.edu.tw, albertjeng@hotmail.com, jcwang@just.edu.tw**

***Abstract*—DroidExec is a novel root exploit recognition to reduce the influence of wide variability, which usually affects the Android malware detection rate, because of Android applica- tions's various properties. In Android, a specific malware family (e.g., root exploit malware), and thus its implementation may be influenced by the campaign it is serving, and thus producing wide variability, leading its samples to appear to match a wider range of potential families. In this paper, we propose a similarity recognition named as DroidExec, reducing wide variability via folding redundant function-relation graph based on Bipartite Graph Conceptual Matching of graph edit distance. We compute the multiple square roots for each 2 × 2 block in the cost matrix to conceptually cripple the wide variability. In the experiments, we measure the applications's opcode structural similarity for clustering Android malware. Empirical validation shows that DroidExec can effectively filter surplus and various behaviors, which can improve the precision/recall rate from 82%/95% to 83%/97%, respectively.**

***Keyword*—Root Exploit, Android Malware, Graph Edit Distance, Function-relation Graph, Bipartite Graph Conceptual Matching, Bipartite Graph Matching**

**Te-En Wei** received Master degree in the Department of Electrical Engineering of National Taiwan University of Science and Technology at Taipei, Taiwan in 2009. Currently, he is not only a researcher at the Institute for Information Industry (III), Taipei, Taiwan but also studies the Ph.D. degree in the Department of Computer Science and Information Engineering at National Taiwan University of Science and Technology. His research interests include Application security (i.e., Mobile device applications, computer software and dynamic application testing and monitoring), Cloud security (Authentication, Key Exchange and CAPTCHA) and Network security (i.e., static web testing and dynamic web testing).

**Hahn-Ming Lee** received the B.S. degrees from the Department of Computer Science and Information Engineering, National Taiwan University, Taipei, Taiwan, in 1984 and 1991, respectively. He is currently a Professor in the Department of Computer Science and Information Engineering at National Taiwan University of Science and Technology, Taipei. His research interests include neural networks, information security, intelligence on the web and science and technology policy research.

**Hsiao-Rong Tyan** received the PhD. degree from the Department of Electrical Engineering and Computer Science, Northwestern University, USA. She is currently a Professor in the Department of Information and Computer Engineering at Chung Yuan Chri stian University, Chung Li. His research interests include information security and intelligence on the web and malware analysis.

**Hong-Yuan Mark Liao** received the MS. and PhD. degree from the Department of Electrical Engineering and Computer Scienc e, Northwestern University, USA, in 1985 and 1990, respectively. He is currently a Professor in the Institute of Information Sci ence, Academia Sinica, Nankang. His research interests include Content-based Multimedia Retrieval, Video-based Human Behavio ur Analysis, Multimedia Protection, 3D Mesh Decomposition and Recognition and Multimedia Signal Processing.

**Albert B. Jeng** has more than 30 years of industrial and academic experience primarily in the areas of Cloud Computing, Internet of Things, RFID and Wireless Commu- nications Security, Computer Networking, Secure protocols, Applied Cryptography, and Information System Security (INFOSEC). His experience includes system architect, system engineering, system design, strategic planning, and sys- tem/product specification and acquisition. He has been an in- formation security consultant for more than 30 years. His ma- jor clients include US and other Asia Pacific companies, large multinational companies, and IT and networking solution pro- vider companies. He is currently a Professor in the Department of Computer Science and Information Engineering at National Taiwan University of Science and Technology and Jinwen University of Science and Technology, Taipei.

**Jiunn-Chin Wang** received the MS degree from EE. National Cheng Kung University, Tainan, Taiwan. He is currently a Lectur er in the Department of Computer Science and Information Engineering at Jinwen University of Science and Technology, Taipei. His research interests include Optimized algorithms, computer network technology, virtualization and operating system.