C500-CFG: A Novel Algorithm to Extract Control Flow-based Features for IoT Malware Detection

Submitted by grigby1 on Fri, 12/11/2020 - 2:34pm

Title	C500-CFG: A Novel Algorithm to Extract Control Flow-based Features for IoT Malware Detection
Publication Type	Conference Paper
Year of Publication	2019
Authors	Phu, T. N., Hoang, L., Toan, N. N., Tho, N. Dai, Binh, N. N.
Conference Name	2019 19th International Symposium on Communications and Information Technologies (ISCIT)
Date Published	Sept. 2019
Publisher	IEEE
ISBN Number	978-1-7281-5009-3
Keywords	C500-CFG, C500-CFG algorithm, computational complexity, computer network security, control flow graph, control flow-based features, decom-piled executable codes, Ding's NP-hard problem, dynamic programming, feature extraction, feature information, graph theory, high-complexity programs, Human Behavior, Internet of Things, invasive software, IoT, IoT malware detection, malicious code, malware analysis, malware detection, Metrics, privacy, pubcrawl, resilience, Resiliency, static characteristic extraction method , text analysis, text-based methods

Abstract

{Static characteristic extraction method Control flow-based features proposed by Ding has the ability to detect malicious code with higher accuracy than traditional Text-based methods. However, this method resolved NP-hard problem in a graph, therefore it is not feasible with the large-size and high-complexity programs. So, we propose the C500-CFG algorithm in Control flow-based features based on the idea of dynamic programming, solving Ding's NP-hard problem in O(N2) time complexity, where N is the number of basic blocks in decom-piled executable codes. Our algorithm is more efficient and more outstanding in detecting malware than Ding's algorithm: fast processing time, allowing processing large files, using less memory and extracting more feature information. Applying our algorithms with IoT data sets gives outstanding results on 2 measures: Accuracy = 99.34%

URL	https://ieeexplore.ieee.org/document/8905120
DOI	10.1109/ISCIT.2019.8905120
Citation Key	phu_c500-cfg_2019

C500-CFG C500-CFG algorithm computational complexity computer network security control flow graph control flow-based features decom-piled executable codes Ding's NP-hard problem dynamic programming feature extraction feature information graph theory high-complexity programs Human behavior Internet of Things invasive software IoT IoT malware detection malicious code Malware Analysis malware detection Metrics privacy pubcrawl resilience Resiliency static characteristic extraction method text analysis text-based methods