World Academy of Science, Engineering and Technology
International Journal of Information and Communication Engineering
Vol:16, No:05, 2022

# BodeACD: Buffer Overflow Vulnerabilities Detecting Based on Abstract Syntax Tree, Control Flow Graph, and Data Dependency Graph

**Authors :** Xinghang Lv, Tao Peng, Jia Chen, Junping Liu, Xinrong Hu, Ruhan He, Minghua Jiang, Wenli Cao

**Abstract :** As one of the most dangerous vulnerabilities, effective detection of buffer overflow vulnerabilities is extremely necessary. Traditional detection methods are not accurate enough and consume more resources to meet complex and enormous code environment at present. In order to resolve the above problems, we propose the method for Buffer overflow detection based on Abstract syntax tree, Control flow graph, and Data dependency graph (BodeACD) in C/C++ programs with source code. Firstly, BodeACD constructs the function samples of buffer overflow that are available on Github, then represents them as code representation sequences, which fuse control flow, data dependency, and syntax structure of source code to reduce information loss during code representation. Finally, BodeACD learns vulnerability patterns for vulnerability detection through deep learning. The results of the experiments show that BodeACD has increased the precision and recall by 6.3% and 8.5% respectively compared with the latest methods, which can effectively improve vulnerability detection and reduce False-positive rate and False-negative rate.

**Keywords :** vulnerability detection, abstract syntax tree, control flow graph, data dependency graph, code representation, deep learning
**Conference Title :** ICSOC 2022 : International Conference on Service Oriented Computing
**Conference Location :** Barcelona, Spain
**Conference Dates :** May 26-27, 2022