A Reverse Engineering Approach of Obfuscated Array

Wei Ding[12], ZhiMin Gu[1]

1 School of Computer Science Technology, Beijing Institute of Technology ,Beijing,China

2 College of Information Science and Engineering, Henan University of Technology, Zhengzhou,china

orangeding@163.com, dingwei@haut.edu.cn

***Abstract*—Recently, research community has advanced in type reconstruction technology for reverse engineering. However, emerging with obfuscated technology, data type reconstruction grows more and more difficult, and obfuscated code is easier to be monitored and analyzed by attacker or hacker. Therefore, it's essential to develop a novel approach to reverse engineering obfuscated array type based on refined CFG. We take split array for example and analyze feature in CFG and take advantage of compiler algorithm to identify obfuscated array.**

***Keywords*—Obuscated array, Reverse Engineering, Array Splitting, Array Folding, Array Flattening**

Wei Ding was born in Anhui province, china. After graduated from Henan Institute of Technology in 2002, she entered into Zhengzhou University, and gained Master Degree. Then she worked into Henan Universality of Technology and became a doctorial student of Beijing Institute of Technology in 2009. Her research area of interest is binary analysis and software security.