Hybrid obfuscation technique to protect source code from prohibited software reverse engineering

ABSTRACT

In this research, a new Hybrid Obfuscation Technique was proposed to prevent prohibited Reverse Engineering. The proposed hybrid technique contains three approaches; first approach is string encryption. The string encryption is about adding a mathematical equation with arrays and loops to the strings in the code to hide the meaning. Second approach is renaming system keywords to Unicode to increase the difficulty and complexity of the code. Third approach is transforming identifiers to junk code to hide the meaning and increase the complexity of the code. An experiment was conducted to evaluate the proposed Hybrid Obfuscation Technique. The experiment contains two phases; the first phase was conducting reverse engineering against java applications that do not use any protection to determine the ability of reversing tools to read the compiled code. The second phase was conducting reverse engineering against the proposed technique to evaluate the effectiveness of it. The experiment of the hybrid obfuscation technique was to test output correctness, syntax, reversed code errors, flow test, identifiers names test, methods, and classes correctness test. With these parameters, it was possible to determine the ability of the proposed technique to defend the attack. The experiment has presented good and promising results, where it was nearly impossible for the reversing tool to read the obfuscated code. Even the revealed code did not perform as well as original and obfuscated code.

Keyword: Obfuscation techniques; Reverse engineering (RE); Anti reverse engineering; Intellectual property; Software security; Piracy