Abstract:

Software systems may contain sensitive data that should be protected. In a scenario, where an analyst has full access to the system, it may be desirable to transform the program to become harder to understand and reverse-engineer, while preserving the original functionality of the program.

Machine code obfuscation tackles this problem by adding complexity to the program’s control flow, a programming idiom removal, and various abstractions. Specifically, WProtect is an obfuscation engine that utilises a stack virtual machine and its own instruction set to achieve these properties.

In this thesis, I will analyse WProtect obfuscation engine, its obfuscation algorithms and present a generic approach to an extraction of a code protected by WProtect. Furthermore, I will design a generic framework for a static code extraction that is tweakable in order to support different WProtect configurations.

Several improvements to WProtect, both in terms of configuration and design, will also be proposed. These proposals mostly intend to mitigate vulnerabilities that are exploited in the code extraction, however, several proposals shall also include improvements specifically targeting static analysis prevention.