Towards Practical Selection of Source Code Obfuscation Methods against Man-At-The-End Attacks

氏　　名

北岡　哲哉

研 究 室 名

ソフトウェア工学研究室

主指導教員名（論文博士の場合は推薦教員名）

松本　健一

内 容 梗 概（１ページ目に収めること）

This thesis focuses on code obfuscation, a widely used countermeasure against Man-At-The-End (MATE) attacks, with the primary goal of supporting the selection of practical code obfuscation methods. For commercial software and sensitive applications, protecting intellectual property such as program logic, authentication credentials, and unpublished content is essential for maximizing business value. A critical challenge to this protection arises due to MATE attacks, which involve reverse engineering executable code to analyze and tamper with program logic. This threat is further intensified by recent advances in binary analysis technology and Large Language Models (LLMs), which have reduced the difficulty of reverse engineering. The thesis evaluates well-known obfuscation methods, assessing their reliability, defined as the ability to preserve original functionality during code transformation, especially when combined with other methods or code optimization. Furthermore, it assesses resilience against LLM-based MATE attacks, specifically focusing on inferring function names from pseudocode obtained by decompiling obfuscated code. The evaluation demonstrates that obfuscation methods based on code virtualization achieve relatively high code transformation rate while preserving functionality. Additionally, code optimization reveals that programs obfuscated using complex arithmetic expressions are prone to incorrect results and runtime errors. Regarding resilience, code virtualization indicates the highest resilience among the tested LLMs in the experiments.