INDIAN INSTITUTE OF TECHNOLOGY GUWAHATI
SHORT ABSTRACT OF THESIS

Name of the Student	:	Priyanka Panigrahi
Roll Number	:	176101006
Programme of Study	:	Ph.D.

Thesis Title: Security Verification of Compiler Optimizations: An Information Flow Perspective

Name of Thesis Supervisor(s)	:	Dr. Chandan Karfa
Thesis Submitted to the Department/ Center	:	Yes
Date of completion of Thesis Viva-Voce Exam	:	24th April 2024
Key words for description of Thesis Work	:	Compiler, Security, Information Flow, Information Leakage, Register Allocation, LLVM, Taint Analysis, Model Checking, Formal Verification, CBMC, Scan Chain, Side Channel, Register Transfer Level.

SHORT ABSTRACT

Modern compilers like GCC, LLVM apply various optimizations on the source program to improve the performance of the target code for execution time, code size, resource usage, memory usage, etc. One of its critical requirements is to generate a functional equivalent target code. A target code generated after application of compiler optimization may be functionally equivalent to the source program but it may not be as secure as the source program (i.e., relatively secure). Therefore, it is essential to ensure that the optimized code does not introduce any security vulnerability during the optimization phase. This thesis aims to verify the relative security between the source and optimized programs, irrespective of the optimizations applied by a compiler. Specifically, the information flow is considered as the security property in a program in this thesis. To achieve relative security, we first aim to quantify the information leakage in a program using static taint analysis. Then, we propose a bisimulation method for translation validation of information leakage for relative security verification between a source and an optimized program. The next work explores how a model checker can be utilized to quantify the information leakage in a program. The model checking based security analysis method can further be applied to translation validation of information leakage for relative security verification between the source and optimized programs. With our notion of relative security, we have shown that the register allocation step in a compiler is not secure in the presence of spilling. We then propose a secure register allocation approach for the LLVM compiler framework. Finally, this thesis aims to protect these registers from information leakage, specifically from scan-based attacks.