

Public Abstract

First Name:Jia

Middle Name:

Last Name:Chen

Adviser's First Name:Rohit

Adviser's Last Name:Chadha

Co-Adviser's First Name:

Co-Adviser's Last Name:

Graduation Term:SS 2014

Department:Computer Science

Degree:MS

Title:CALCULATING INFORMATION LEAKAGE USING MODEL CHECKING TOOLS

A confidential program should not allow any information about its secret inputs to be inferred from its public outputs. As such confidentiality is difficult to achieve in practice, it has been proposed in literature to evaluate security of programs by computing the amount of information it leaks. In this thesis, we consider the problem of computing information leaked by a deterministic program and use the information-theoretic measure of min-entropy to quantify the amount of information.

The main challenge in computing information leakage by a program using min-entropy is that one has to count the number of distinct outputs by that program. We find a polynomial-time reduction from the problem of counting outputs to the problem of checking reachability in programs. Thus we propose a hypothesis that we can estimate leakage using model checking tools which are originally developed for checking reachability.

We test the above hypothesis using two popular model checking tools, jMoped and Getafix. Our tests indicate that they do not scale as the number of bits in the input increases. However, we find that if the program enjoys the additional property of semi-monotonicity then we can use a different reduction to the problem of checking reachability. We observe a dramatic improvement in performance with this new reduction.