Two fully funded PhD positions in obfuscation and cryptography
Computer Science/Mathematics
University of Auckland, New Zealand

Two, three-year PhD scholarships, covering international tuition fees and a stipend of $27,500 per year.

Application deadline: March 12, 2017.

Introduction
Malware and software piracy are major security issues that are increasingly prominent in modern computing. They are particularly relevant in the domain of mobile apps (in the following we will use the term app to refer to both mobile and PC applications): a major software domain, with both Apple and Google reporting more than 50 billion downloads from their respective stores.

The main technique to inject malware into a legitimate app is by means of reverse engineering the app to recover its source code. To protect the app from such an attack, app developers use obfuscation tools such that the resulting program is functionally equivalent to the original app but its code will be more complicated to reverse engineer.

Background
There have been a number of methods suggested in the literature to hide control flow, such as opaque predicates (i.e., dummy branches), function splitting and recombination, and control flow flattening. Most of these methods only protect against a static analysis. A powerful class of attacks is to execute a program in a symbolic or concolic execution tool. Hence, there is a need to develop dynamic protections to hide control flow.

Project Aim

The aim of the project is to develop new theoretical foundations for practical obfuscation. The project has two main components: theoretical and practical.

The theoretical component will focus on designing and evaluating new security definitions for practical obfuscation solutions. One important objective is to be able to support verifiable obfuscation where a third-party is able verify properties of the code without the need to access its original non-obfuscated version.

The practical component will focus on creating practical obfuscation tools inspired by the results obtained in the theoretical component.

The theoretical work will be led by Prof Steven Galbraith while Dr. Giovanni Russello will lead the practical aspects. There are two fully-funded PhD scholarships for this project. We expect a close collaboration between the two PhD students involved in this project.

Experience

The ideal candidate will have an undergraduate degree in computer science, engineering or mathematics and have written a master thesis in some topic related to security, cryptography, or the underlying mathematics. We are looking for candidates with experience in some or all of the following:

- Hands-on experience with standard obfuscators and de-obfuscator tools
- Understanding of cryptography and its applications
- Understanding of ARM and/or X86 architecture and respective instruction set
- Experience in coding in C/C++ and assembly
- Understanding of compilers and run-time code optimisations

Application Process:

Please send an email to aucklandobfuscationphd@gmail.com with a short CV and an unofficial transcript of grades in your degree.

Successful applicants will be asked to provide further information (such as an IELTS English language test and official transcripts of their degrees) at a later stage of the application process.

The University of Auckland

The University of Auckland's main City Campus is located in the heart of Auckland, which is ranked fourth out of 215 world cities for quality of living in the 2009 Mercer Quality of Living Survey (see www.mercer.com/qualityofliving).

The University of Auckland is New Zealand's leading research-led university. We're ranked among the top 100 universities in the world by the QS World University Rankings (2016/2017). We offer PhD studies in nearly 100 subjects. We have a global reputation for academic excellence and a supportive student environment.