

Analise Estática de Programas para a Segurança

Proposta de Mestrado

Orientador: Simão Melo de Sousa

1 Objetivos

O objectivo deste projecto é a implementação de analisadores estáticos de programas para a linguagem CAO de domínio específico para a criptografia.

Estes analisadores permitam analisar e destacar certos comportamentos de programas sem sequer necessitar a execução dos programas visados.

Estas técnicas permitam descobrir *bugs*, falhas (e.g. de segurança) muito subtis.

O corpo de conhecimentos necessário à definição de tais algoritmos de análises pertence a área das linguagens de programação, em particular à análise semântica, à semântica das linguagens de programação e aos fundamentos algébricos da programação.

Estas análises tem sido usadas intensivamente pela industria aeroespacial, aeronáutica, segurança (e.g. Trus-in-Soft, Core Infrastructure Initiative) e mais recentemente por empresas como Facebook, Apple e Microsoft, no contexto das *apps* (e.g. o *infer* (link) da Facebook, entre muitos...)

Neste projecto propomos a implementação duma framework que sustente a cooperação de varios algoritmos *state-of-the-art* de análise estática de programas para a linguagem CAO.

2 Tarefas a Realizar

T1 Estudo do estado da arte em análise estática de programas, CAO

T2 Estudo dos algoritmos e das tecnologias de compilação por utilizar

T3 Implementação dos algoritmos

T4 Análises dos resultados

T5 Escrita do relatório de projeto

3 Cronograma

T1 2 mês

T2 2 mês

T3 2 mês

T4 1,5 mês

T5 1,5 mês

4 Requisitos Técnicos

Gosto em programar e em resolver com rigor problemas de natureza informática. Gosto em desenvolver capacidade em programação, algoritmos e estruturas de dados. Vontade de aprender novas conceitos e novas tecnologias.

5 Resultados esperados

- 1 protótipo do compilador.
- 1 relatório de projeto.

6 Contactos

Simão Melo de Sousa (desousa@di.ubi.pt)