Extraction of typing information from binary code

The Insight project is offering a Master's internship on the extraction of typing information from binary code.

The internship should start in February 2013 and end in June 2013, and the monthly wage is a bit above 400 euros.

Goal

The Insight project is interested in the analysis of binary executables, and we have developed a library which allows loading a binary executable and disassembling it using various techniques, the most advanced of which interfaces with an SMT solver.

During this internship we would like the student to get acquainted with our C++ framework, to study the ideas behind the paper [Mycroft] and come up with an implementation transforming a fragment of microcode into SSA (Single Static Assignment) form and inferring from it possible datatypes of the various variables and memory locations manipulated by this fragment.

The Insight framework does not take as given the control flow graph of the program under study, and it is reconstructed on the fly while analyses are being performed. We would like the intern to explore how algorithms can be designed to make the general idea of [Mycroft] work in the case of an evolving control flow graph.

The expected contribution is twofold:

- a good understanding of the whole inferrence chain and a proposed extension to the evolving control flow graph case
- an implementation based on the Insight framework and working at least on a small example

Bibliography

[Mycroft] Alan Mycroft, *Type-Based Decompilation*, Lecture Notes in Computer Science: Proc. ESOP'99, vol. 1576. Springer-Verlag, 1999.

```
http://insight.labri.fr/
http://insight.labri.fr/trac/wiki/Proposals
```

Advisors

- Emmanuel Fleury **<fleuryàlabri.fr>**, office 261, +33 5 4000 6934
- Aymeric Vincent **<vincentàlabri.fr>**, office 264, +33 5 4000 3509

Snail mail address:
Batiment A30
351 cours de la Libération
33405 Talence Cedex
France