Faculty Exchange Fellowship at Carnegie Mellon University - Final Report

João Costa Seco – Universidade Nova de Lisboa

This document summarizes the results of my faculty exchange fellowship at the Carnegie Mellon University sponsored by the Carnegie Mellon Portugal Program. The visit took place from August 21 to December 21, 2012, and was hosted by Prof. Frank Pfenning, of the Computer Science Department.

While at the Computer Science Department (CSD), I was able to interact with several faculty members, other visitors and post-docs in fruitful research discussions; to attend many seminars and thesis defenses occurring in the campus, especially in the POP seminar series; to participate in reading group sessions; to observe teaching activities at different levels; and to take the necessary time to develop promising research work.

Research The main focus of my visit was the continuation of an active research collaboration between Prof. Frank Pfenning and members of the CITI research team under the Interfaces research project. This work started during a previous visit of Prof. Carla Ferreira, and its general goal is to extend the foundations of existing work on type based security. In [1], we focused on access control for data-centric applications, and applied a technique based on refinement types and data manipulation abstractions, to allow the static verification of access control policies that depend on the actual data being protected. However, this is not expressive enough to prevent general information leaks. In our current approach we explore the more expressive technique of information flow analysis to track and ensure confidentiality of data. We take a store oriented approach to defining data security levels, which we believe is best suited to the particular context motivating this work, that of data-centric applications. We extend the current literature by allowing security policies to be shaped by the data itself, and express our model on monadic imperative language extending [2]. This demands a special approach based on dependent type theory, using techniques such as logical relations to prove the soundness of our system. This visit contributed with significant advances towards a relevant research result in this topic: we have developed a type discipline for a monadic imperative language where security policies are expressed using logic propositions over runtime values; and were able to provide (for a non-dependent fragment) an explicit and clear semantic definition of confidentiality. We continue by extending the results to the complete dependent type system.

At the CSD I also interacted in research related discussions with several faculty members like Umut Acar, Jonathan Aldrich, and Stephen Brookes. These discussions were crucial not only to disseminate recent research results and receive feedback, but also to explore new ideas. Furthermore, I met and discussed with visitors like Dr. Rustan Leino, from Microsoft Research. We discussed about the features of his current project, the Dafny programming

language. I also met with Tucker Taft from AdaCore and designer of the Parasail programming language, also visiting CMU, with whom I discussed our type based approach to disciplining aliasing and controlling concurrency. I also participated on a project meeting of the Certified Interfaces research project, with other CITI members, in a short visit to Carnegie Mellon. All these discussions will certainly have direct impact on my future teaching activities at the Universidade Nova de Lisboa, and on future research directions.

Teaching activities I observed two undergraduate courses while at the CSD: Principles of Imperative Programming (15-122) offered at freshmen level, and Compiler Design (15-411) offered to more advanced levels of the CS major.

The syllabus of Principles of Imperative Programming, designed and taught by Prof. Frank Pfenning, is strongly supported on reasoning principles about programming correctness. The course draws a path from a scenario with a strong type discipline and managed memory, of the customly designed language C0, to the full-fledged C programming language. On the Compiler Design course, designed by Prof. Frank Pfenning and extended and currently taught by Prof. André Platzer, I observed a significant part of the lectures. This course comprises a comprehensive selection of topics from code generation, register allocation, to code optimization. Both courses are directly related to my teaching activities, and the level of detail that I observed is certainly inspiring.

Conclusions This visit was a very fruitful and enriching experience, both at the personal and at the professional level. I experienced the rich and dynamic environment at Carnegie Mellon, both at the teaching and research levels, which will certainly influence my future activities.

Acknowledgments I would like to thank in the first place to Prof. Frank Pfenning and the Carnegie Mellon Portugal program, to its direction and staff. I would like to also thank the fellow visitors, Beniamino Accattoli, Ioannis Caragiannis, and Shuai Cui, for such a pleasant company.

December 21, 2012
João Costa Seco

References

[1] Luís Caires, Jorge A. Pérez, João C. Seco, Hugo T. Vieira, Lúcio Ferrão. Type-Based Access Control in Data-Centric Systems. In *Proceedings of the European Symposium on Programming (ESOP)*, 2011

[2] Karl Crary, Aleksey Kliger, and Frank Pfenning. A Monadic Analysis of Information Flow Security with Mutable State. *Journal of Functional Programming*, **15**(2), pages 249–291, 2005.