July 4, 2020

Search Committee
Programming Languages Group, TUDelft
Delft, The Netherlands

Dear Search Committee,

I am writing to apply for the Assistant Professor position advertised by the Programming Language Group, TUDelft (TUD00153). I am currently working as a Research Fellow with Toby Murray in the School of Computing and Information Systems, University of Melbourne, Melbourne. My research area is primarily focussed on formal verification of software programs. However, I am willing to explore the areas to make the formal verification accessible to everyone by means of designing new programming language .

As a Research Fellow at the University of Melbourne, I am investigating the information flow security in weak memory model in the presence of concurrency with Toby Murray. Verifying the correctness of functional programs without any side effect in a theorem prover is not very difficult. Moreover, in most of cases, the proofs are simple pen-and-paper proof. However, in case of side effects, the reasoning about the correctness of program is difficult, mainly in the context of heap manipulating programs, and this situation gets more complicated in the presence of concurrency in weak-memory. Our project is geared towards a formal reasoning the information flow security in weak memory model and the method we will develop will be applied to verify the security of seL4-based software for critical embedded devices. The project is still in nascent phase; however, Toby and his team has developed a software tool, SecC, to formally reason about information flow in concurrent C programs. I have used this tool to develop a formally verified email server, which does not leak any information classified as a secret, but the goal was to identify the further challenges while using the SecC tool and further investigation on those findings. The ultimate goal is to add the information flow reasoning logic for C/C++11, formally prove that logic is sound in Coq theorem prover, and develop a tool to automate it (more likely feature addition in SecC).

Other than research, I am also exploring the horizons for my own research agenda. Therefore, I have recently participated in a program, organised by the University of Melbourne, to pitch the idea for research agencies and collaboration with industry. I found it very pleasant to know that my research is a must requirement for any setting where they care about security/confidentiality/correctness properties. More importantly, to establish myself as a security researcher, I am applying for various research grants, including ECR (Early Career Research), a scheme of University of Melbourne which promotes promising research, ARC (Australian Research Council) future fellowship, and DECRA (Discovery Early Career Researcher Award). I intended to use these funds to visit the research group, Max Planck Institute for Security and Privacy (Giles Barthe), Princeton University (Andrew Appel), and INRIA (Xavier Leroy). Gilles Barthe is a security researcher and one of the developer of easycrypt and certicrypt, a tool to automate the proofs of cryptographic construction, Andrew Appel is professor at the Princeton University, and his group has developed a tool VST (Verified Software Toolchain) to reason about C programs, and Xavior Leroy is a researcher at the INRIA and developer of CompCert, a formally verified C compiler. I believe visiting all these three researcher would give me a unique perspective on developing a language like C for writing cryptographic programs with correctness guarantee. Moreover, if we can these programs to assembly code using formally verified compiler, then we have correctness guarantee upto machine code. Locally, at the DelftPL group, I can use the expertise of Robbert Krebbers (I see he is moving to Radboud University Nijmegen) for separation logic, Eelco Visser in designing the domain specific language, Jesper Cockx in developing the type system, and Casper Bach Poulsen in designing the type safe language.

On the academic note, I am involved in evaluating the master thesis of students' working under

Toby Murray. In addition, I am going to head tutor the Algorithm course this semester with Toby Murray.

Below is my response for every point in the job advertisement:

1. *Conducting high impact research in the area of programming languages:* since my PhD, I have published paper in conferences like ACM Conference on Computer and Communications Security (CCS), Interactive Theorem Proving (ITP), etc. I intended to continue do so, but now focussing to a broader community of security and programming languages.
2. *Supervising PhD students and helping them to become top researchers in programming languages:* given that my research agenda involves intersection of many fields, it is impossible that I can do it all alone. I certainly need to collaborate, supervise PhD, master's and bachelor students. Besides, it's the joy of being academic, and my goal is to be a researcher like Dirk Pattinson, who was never afraid of saying that he does not know the solution, but together we will figure out.
3. *Teaching courses on programming and programming languages topics at the bachelor and master's level in the TU Delft Computer Science curriculum:* I have already addressed this in my teaching statement.
4. *Supervising bachelor and master's students in their graduation projects:* addressed in the second point.
5. *Acquiring and managing externally funded research projects in programming languages:* addressed above that I am already applying for various agencies for funding to establish my independent research agenda.
6. *Collaborating with industry to ensure that the group's research results have a lasting impact in software development practice:* addressed above that I am pitching my idea to industry and applying for industry funds.
7. *Strengthening the contacts between the group and industry as well as other international academic institutions:* I would continue my research with Toby Murray at the University of Melbourne, and Dirk Pattinson at the Australian National University. In addition, I would like to explore groups who are doing research in Cryptography, groups doing research in formal verification, and groups doing research in separation logic.
8. *Taking responsibility for management and committee work within the section and the department:* I understand that these obligations are also a part of being academic, and I would be more than happy to do it.

Finally, I feel that I am perfect fit for this role as my experience and skill set would make me a invaluable candidate for this position and to your research group. I appreciate your consideration and look forward to hearing for you. Please contact me if you need any further information.

Mukesh Tiwari
Research Fellow
School of Computing and Information Systems
University of Melbourne
Melbourne, Victoria
https://findanexpert.unimelb.edu.au/profile/860472-mukesh-tiwari