23rd October 2019

Department of Home Affairs
Australia

Submission to Australia's 2020 Cyber Security Strategy

To whom it may concern,

Oracle Labs is the R&D organisation for Oracle, a multi-national company. I am the Director for Oracle Labs in Australia, based in Brisbane. The focus of our work is centered around vulnerability detection to improve the quality of software before it gets deployed worldwide. We invest in research to develop new techniques that can automatically help with vulnerability detection in enterprise software, as well as in advanced development, to bring successful research techniques to life and deploy them throughout Oracle. We are the only organisation at Oracle who focuses on development of techniques and tools that prevent vulnerabilities. Today, our tools are being used by thousands of developers worldwide on a day-to-day basis. These tools are fully developed in Brisbane.

My team comprises research staff that have PhDs in Computer Science in the areas of Program Analysis and/or Machine Learning, and engineering staff that have either a Masters or Bachelors degree in Computer Science or Software Engineering. We also hire interns at the PhD, Masters and undergraduate level throughout the year.

Growing and scaling a highly technical team in Australia is hampered by the fact that there is a skills shortage in Australia. For example, for internships, our most highly qualified students are all doing a PhD degree and they come from countries like Germany, France, Greece, Korea, New Zealand, and USA, to name a few, because we cannot fill these vacancies with Australian PhD students. For permanent positions, in recent years, our new research staff are non Australians who have obtained their PhDs in Canada, Austria and Singapore. We train in-house our engineering staff when they join our team, as the undergraduate Computer Science and Software Engineering degrees do not provide them with relevant subjects to work with us. We are consumers of university graduates. Today's Australian Computer Science and Software Engineering degrees do not cover areas such as Program Analysis, a branch of Programming Languages. This subject is taught overseas at some universities where we recruit students and researchers from.

Not only do we spend time and effort in training our new engineering staff, hiring of highly qualified overseas PhD research staff is expensive (visas for candidate to be hired and dependents, relocation costs to Australia, and temporary housing when they first arrive in Australia). I would like to grow my team with Australian talent, however, there is a shortage of it, which prevents scaling up my organisation in Australia, as well as limits the type of security issues that we can investigate in Australia.

We collaborate with academics throughout the world by providing grants to support their research in areas of interest to us. In order to address the skills shortage, we are providing a grant to The University of Queensland, School of Information Technology and Electrical Engineering, to support research in the area of Program Verification, a branch of Programming Languages, and teaching in the area of Program Analysis. Clearly, one university is not enough to provide a pipeline of students who have the skills to work in a highly technical team. One university cannot do it alone. It is important to ensure Australian universities update their Computer Science and Software Engineering degrees to cater for more technical areas that are relevant to Cyber Security.

Program Analysis is not the only area that is lacking in the Australian Computer Science and Software Engineering degree. There is a need for students:

- To become aware of vulnerabilities they can write in code they develop (e.g., buffer overflows in the C and C++ language, SQL injections in the Java, Python and other languages, cross-site scripting in most languages, etc);
- To become aware of how attackers exploit such vulnerabilities, including techniques such as fuzzing and penetration testing;
- To learn to write secure code by design, taking into account secure architecture design, architecture review, and design review from a security standpoint;
- To learn to test software from a security point of view;
- To become aware of tools that can be used during the software development process to aid in detecting vulnerabilities early in the process; tools in the Application Security Testing (AST) domain such as SAST (static), DAST (dynamic), IAST (interactive), SCA (software composition analysis), WAF (web application firewall), or the more recent RASP (runtime application self-protection);
- To develop skills to implement AST tools.

By developing the above skills, Australia would have a more skilled developer workforce that can address development of secure code, development of tools to aid with securing code, and development of new IP (intellectual property) that can compete with that of overseas countries. Research in this space would also benefit from a more highly skilled workforce. Scaling highly technical organisations in Australia is a dream that we should all strive for.

Regards,

[redacted]

Dr Cristina Cifuentes
Senior Director R&D, Oracle
Director, Oracle Labs Australia
Adjunct Professor The University of Queensland
Adjunct Professor Queensland University of Technology
2001 QUT Chancellor’s Outstanding Alumnus of the Year