Karl Crary

Assistant Professor
Computer Science Department, SCS
4 September 2007

Research Topic
Computer Security

Research Problem
What is an efficient certified code?

Problem Statement
Given an operating system and code, construct a certified code that is safe, unrestrictive, and efficient.

Problem Description
Operating systems can be protected using static checking as opposed to more traditional hardware methods. This is done using certified code. Certified code demonstrates to a prospective user that the code is safe. Perhaps the most famous example of certified code is JAVA. JAVA is a proof carrying code, unfortunately however, the imbedded proofs are restrictive and make the code inefficient. An improvement on JAVA is to couple a binary code with a proof, and once the proof is verified, it can be discarded and the binary code can be run efficiently. There are many methods to develop certified code and this is the focus of research.

Computer Science Perspective
Four key computer science issues were identified. First, static checking improves performance. Second, it allows for simpler hardware. Third, it is good for software to work correctly. Finally, it is more secure, considering that some networks do not contain firewalls and other security measures.

Disciplines Actively Involved
Mathematics

Other Discipline Involved
Cryptography is widely used in this research. Cryptography is an application of abstract algebra (mathematics) that studies message secrecy.

Actively Involved Discipline is defined as a discipline associated with an investigator working on the research problem.

References

- Karl Crary and Susmit Sarkar. **Foundational Certified Code in a Metalogical Framework.** *ACM Transactions on Computational Logic,* to appear.
  (pdf)

By imccullo
Updated imccullo