Program verification and programming methodology

K. Rustan M. Leino

Microsoft Research, Redmond, WA, USA
leino@microsoft.com

Abstract. With appropriate tool support, specifications and verification may help reduce the cost of software engineering. In this talk, I will describe some of the basic pieces that go into building a program verification system. I will point out which pieces of the technology I think have reached a higher degree of maturity and which pieces require more research. Programming methodology plays a central role, because it guides both the programmer—by suggesting ways to structure the program—and the design of the verification system—by limiting the possible behaviors of programs. I will include a demo of the experimental Spec# programming system, which features an object-oriented language with contracts (like preconditions and object invariants) along with various degrees of dynamic and static checking (including a program verifier).
Joint work with Mike Barnett, Robert DeLine, Manuel Fähndrich, Peter Müller, David A. Naumann, Wolfram Schulte, and Herman Venter.