Abstract:

This talk introduces a method of programming from specifications so that each programming step can be checked by a verifier. Logic errors can be reported the way syntax errors are reported now. Program verification is easier than you think. Invariants and variants are not explicitly needed. The kinds of comments that programmers write, when formalized, are sufficient. And the proofs are well within the abilities of existing provers.