A proof-producing machine-code analyzer for secure information flow

ABSTRACT

An approach enabling end-users to verify that a downloaded untrusted code will not leak confidential data to unauthorized parties is presented. The approach certifies RISC-style assembly programs for secure information flow by statically analyzing the code based on the idea of Proof Carrying Code (PCC). The proofs that untrusted code does not leak sensitive information are generated and checked on the host machine and if they are valid, then the untrusted code can be installed and executed safely. The proposed security analyzer operates directly on the machinecode requiring only the inputs and outputs of the code be annotated with security levels. The generated proofs serve as evidence that give end-users a guarantee about the security of the untrusted code.