CODE-CARRYING THEORY

By

Aytekin Vargun

An Abstract of a Thesis Submitted to the Graduate

Faculty of Rensselaer Polytechnic Institute

in Partial Fulfillment of the

Requirements for the Degree of

DOCTOR OF PHILOSOPHY

Major Subject: Computer Science

The original of the complete thesis is on file
in the Rensselaer Polytechnic Institute Library

Examining Committee:

David R. Musser, Thesis Adviser
Selmer Bringsjord, Member
Mukkai Krishnamoorthy, Member
Paliath Narendran, Member
Carlos Varela, Member

Rensselaer Polytechnic Institute
Troy, New York

December 2006
(For Graduation December 2006)

ABSTRACT

Code-Carrying Theory (CCT) is an alternative to the proof-carrying Code (PCC) approach to secure delivery of code. With PCC, code is accompanied by assertions and a proof of its correctness or of other required properties. The code consumer does not accept delivery unless it first succeeds in generating theorems, called verification conditions, from the code and assertions and checking that the supplied proof proves these theorems. With CCT, instead of transmitting both code and proof explicitly, only assertions and proofs are transmitted to the consumer. If proof checking succeeds, code is then obtained by applying a simple tool called CodeGen to the resulting theory. This thesis first explains the design and implementation of CCT steps and shows how it can be used to achieve secure delivery of code with required correctness or safety properties. All the tools used in the verification steps are implemented in Athena, which is both a traditional programming language and a deduction language. In addition, we present examples of generic and non-generic proofs which play an important role in our design. We show how critical it is to organize theories and proofs to reduce the amount of information transmitted between the producer and consumer and to ease the development of code-carrying code theories.