# The Design and Implementation of a Certifying Compiler [Necula, Lee]

# A Certifying Compiler for Java [Necula, Lee et al]

David W. Hill
CSCI 297
5.31.2005

# How to deal with Untrusted Code?

- How can the host system ensure that the untrusted code will not damage it, for example, by corrupting internal data structures?
- How can the host ensure that the untrusted code will not use too many resources (such as CPU, memory, and so forth) or use them for too long a time period?
- How can the host make these assurances without undue effort and negative effect on overall system performance?

# Proof Carrying Code

- Proof-Carrying Code is a technique by which the host establishes a set of safety rules that guarantee safe behavior of programs.
- The code producer creates a formal *safety proof* that proves, for the untrusted code, adherence to the safety rules.
- Then, the host is able to use a simple and fast *proof validator* to check, with certainty, that the proof is valid and hence the foreign code is safe to execute.