Software Component Technology Group

Semester Project

A Case Study for the Boogie Methodology

System.IO

Olivier Girard

12.April 2006

Introduction *Spec#* is a new programming system for specification and verification of object-oriented software. The Spec# language is a superset of the programming language C# extending C# by non-null types, method contracts, object invariants and an ownership type system. The behavior of a Spec# program is *checked at runtime* and *statically verified* by *Boogie*, the Spec# static program verifier.

The Boogie methodology for static verification is described in many papers and proven to be sound. Small sample Spec# programs exist, but until now, no real-life projects have been verified using the Boogie methodology.

The goal of this semester project is to make a case study for the Spec# system from a *practitioner's point of view*. A part of a *real-life* C# application should be transformed to the Spec# programming language in order to test the capabilities of the Spec# system. This will be a subset of the Mono[1] System.IO core component. This case study should point out advantages and disadvantages of the current system. The implementation and the results of the case study will be documented. We are hoping that this documentation will support Spec# practitioners and programmers and that it will be used and extended by the community in future.

Contact Information

	Prof. Peter Müller	Joseph N. Ruskiewicz
Room:	RZ F2	RZ F3
Phone:	(01) 63-22868	(01) 63-26761
Email:	Peter.Mueller@inf.ethz.ch	joseph.ruskiewicz@inf.ethz.ch
WWW:	http://sct.inf.ethz.ch/projects/index.html	

[1] http://www.mono-project.com