ESC/Java project review

10 March 1998

CormacFlanagar	75%
K. Rustan M. Leino	(project leader) 100%
Mark Lillibridge	100%
Greg Nelson	100%
James B. Saxe	80%
Raymie Stata	80%

What is Extended Static Checking?

ESC/Java > "null-dereference" > error on line 218" Annotated program

Checks for:

- · null-dereference errors
- · array bounds errors
- · type cast errors · race conditions
- · dead locks

ESC/Java Goal

Deploy ESC technology in checher that lay programmers are eager to use.

Research required

- · Formalize Java semantics
- · Tool should be easy to use, reliable
- · Simple annotations, new checks
- · Performance (space, time, variability)
- · Where to give up on soundness and completeness
- · Enhanced error reporting

How the checker works Annotated Java Parser and typechecker Java AST Java-to-Guardedcommand compiler Type system formalizer Guarded command Weakest-precondition generator Verification condition Theorem prover Counterexample Post processor Error message

Achievements

- · Java parser and type checker implemented
- · Logic of ESC/Java defined
- · Java-to-guarded command translation defined
- (. Theorem prover, from ESC/Modula-3)

In progress

- · Parse and type check annotations
- · Definition of annotation translation
- · Implementation of Java-to-verification condition

Upcoming targets

- · April 1: checker we can use
- · May 31: checker SRC can use