ESCJ 14:
ESC/Java Project Review Slides

March 6th, 1997

What

- Extended static checker for Java
  - Array-bounds errors
  - Null dereference errors
  - Downcast errors
  - Concurrency errors

Goals

- Deploy ESC technology in useful form
  - Want eager users
- Research required
  - Adopt to Java (interfaces)
  - New kinds of checks (object invariants)
  - Performance (space, time, variability)
  - Where to give up soundness and completeness

Why: big picture

- Reliable software is expensive to develop
- Java is the future of programming
- Leverage SRC strengths
  - Past ESC work
  - Java is like Modula-3

Why: benefits to Digital

- Build Java expertise
- Support Java programmers in RAD, DEC
- PR: Digital as a center of Java excellence
- Build prover technology, expertise
- Product?

How

- Interview RAD Java users
- Design, test, document annotation language
- Build checker
  - New code in Java
    - Front end
    - Verification-condition generator
  - Reuse theorem prover from ESC/Modula-3

When

- About a year
  - Release first version of tool
- Following months
  - Build user community
  - Fold feedback into tool

Who

- Rustan Leino
- Greg Nelson
- Jim Saxe
- Raymie Stata
- …others