

The Fox Project: Advanced Development of Systems Software

R&D Status Report
January 1 to March 31, 2000

School of Computer Science
Carnegie Mellon University
Pittsburgh, PA 15213

DISTRIBUTION STATEMENT A
Approved for Public Release
Distribution Unlimited

20000417 145

This research is sponsored by the Defense Advanced Research Projects Agency, DoD, through ARPA Order 8313, and monitored by ESD/AVS under contract F19628-95-C-0050. Views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the Defense Advanced Research Projects Agency or the United States Government.

DTIC QUALITY INSPECTED 3

The long-term objectives of the Carnegie Mellon Fox Project are to improve the design and construction of systems software and to further the development of advanced programming language technology. We use principles and techniques from the mathematical foundations of programming languages, including semantics, type theory, and logic, to design and implement systems software, including operating systems, network protocols, and distributed systems. Much of the implementation work is conducted in the Standard ML (SML) language, a modern functional programming language that provides polymorphism, first-class functions, exception handling, garbage collection, a parameterized module system, static typing, and a formal semantics. This Project involves several faculty members and spans a wide range of research areas, from (1) advanced compiler development to (2) language design to (3) software system safety infrastructure.

1 Research Progress

We report on the research accomplishments during the first calendar quarter of 2000, and the research objectives for the second quarter of 2000.

Accomplishments (January-March):

- Developed VCGen for security-property language.
- Finished implementation and debugging of all garbage collectors and have begun some preliminary benchmarking and optimizations.
- Completed work establishing a sound version of intersection types in the presence of computational effects and submitted a paper on this topic.
- Formalization of the type-theoretic semantics of a fragment of ML in Twelf and mechanization of its soundness proof.
- Developed a strategy for compiling languages supporting inclusive subtyping without introducing run-time costs, while preserving type information.
- Proved key facts critical to the use of logical relations proof techniques in the presence of recursive types.

Objectives (April-June):

- Publish a technical report based on VCGen, soundness proof, and thesis proposal.
- Begin implementation of VCGen for security-property language.
- Complete the first public release of TILT compiler.
- Continue benchmarking and extending the garbage collectors to handle deep stacks and large objects.
- Publish technical report on the implementation of the TILT typechecker.
- Release of Twelf version 1.3, an implementation of a logical framework used for proof-carrying code and certified compilation.
- Extend TILT compiler to support recursive modules.
- Complete development of technology (logical relations proof techniques) for proving the correctness of program transformations in the presence of recursive types.

2 Noteworthy Publications

- *Typed Compilation of Inclusive Subtyping*. Karl Crary. Submitted for publication.

3 Capital Equipment Purchases

- None.

4 Key Personnel Changes

- None.

5 Noteworthy Meetings

- ACM SIGPLAN/SIGACT Symposium on Principles of Programming Languages (POPL) 2000. (Boston, MA, January 19-21, 2000).
- DISCEX 2000 (Hilton Head, SC, January 25-27, 2000).

6 Administrative Data

Base Funding (excludes options): 5,630,798

Funded Options:

UNFunded Options: 648,704

Total Funding Provided to Date (both base and options): 4,175,957

Total Funding Expended to Date (both base and options): 4,008,418

Total Funding UNExpended: 167,541

Date Current Funding will be Expended: 28 FEB 2000

Funding Expended in Most Recent Quarter: 190,466

Incremental Funding required for FY 2000: 850,000

Date of Financial Data: 31 DEC 1999