The Fox Project: Advanced Development of Systems Software

R&D Status Report
July 1 to September 30, 1999

School of Computer Science
Carnegie Mellon University
Pittsburgh, PA 15213

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.

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 third calendar quarter of 1999, and the research objectives for the fourth quarter of 1999.

Accomplishments (July-September):

- Achieved the first complete bootstrap of the TILT compiler for Standard ML. The compiler now compiles itself, and the compiled compiler compiles itself. This is our first full-scale demonstration of the use of typed intermediate languages and type-directed translation for a full-scale programming language.

- Completed the proof of decidability of type checking for the TILT intermediate language. This is a critical result for achieving safety certification by type checking.

- Completed a stop-and-copy parallel copying garbage collector.

- Developed a specification for a security policy language for self-certified code (PCC, TAL).

- Designed and implemented a dialect of TAL capable of specifying and enforcing bounds on resource consumption.

- Implemented prototype certifying compiler for C generating resource-bound TAL.

- Proved correctness of a translation for eliminating ML type-sharing constraints.

- Made a new implementation of the logical framework (Twelf 1.2R5) with constraints available to a Darpa-sponsored project at Princeton University under the direction of Andrew Appel and Ed Felton. It is now actively in use at Stanford and Princeton for experiment in proof-generating decision procedures and proof-carrying code.

Objectives (October-December):

- Complete the first public release of the TILT compiler.

- Formulate a coercion calculus to handle datatype matching in TILT.

- Investigate how to implement a certifying back-end for TILT.

- Implement and benchmark concurrent and parallel copying garbage collectors.

- Begin augmentation of the TILT compiler to generate TAL.

- Design and begin implementation of a release-quality certifying compiler for certifying resource-bounded computations.

- Release a new, fully documented version of Twelf based on the pre-release 1.2R5.

- Finish an implementation of a refinement type checker for ML.

2 Noteworthy Publications

- *Decidable Type Equivalence for a Language with Singleton Kinds.* Robert Harper and Christopher A. Stone. Submitted for publication to the 2000 ACM Symposium on Principles of Programming Languages. Also published as technical report CMU-CS-99-155.

- *On Equivalence and Canonical Forms in the LF Type Theory.* Robert Harper and Frank Pfenning. Workshop on Logical Frameworks and Metalanguages, Paris, France, October, 1999.

- *Resource Bound Certification.* Karl Crary and Stephanie Weirich. Accepted for publication in the Symposium on Principles of Programming Languages, 2000.

- *A Modal Analysis of Staged Computation.* Rowan Davies and Frank Pfenning. Submitted for publication. Also published as technical report CMU-CS-99-153, August, 1999.

- *Logical and Meta-Logical Frameworks.* Frank Pfenning. In G. Nadathur, editor, Proceedings of the International Conference on Principles and Practice of Declarative Programming (PPDP'99), Paris France, September, 1999. Springer-Verlag LNCS. Abstract of invited talk.

- System Description: *Twelf --- A Meta-Logical Framework for Deductive Systems.* Frank Pfenning and Carsten Schuermann. In H. Ganzinger, editor, Proceedings of the 16th International Conference on Automated Deduction (CADE-16), pages 202-206, Trento, Italy, July, 1999. Springer-Verlag LNAI 1632.

- *A Formalization of the Proof-Carrying Code Architecture in a Linear Logical Framework.* Mark Plesko and Frank Pfenning. In A. Pnueli and P. Traverso, editors, Proceedings of the Workshop on Run-Time Result Verification, Trento, Italy, July, 1999.

3 Capital Equipment Purchases

- 1 IBM ThinkPad System Board and Keyboard Replacement, $1,054.00

- 1 Sharp Actius Notebook Computer, $2,888.06

- 1 Pentium III 500MHz Workstation and accessories, $2,947.00

- 1 Pentium III 600MHz Workstation and accessories, $2,484.30

- 1 NEC Z-1 Workstation, $2,422.87

4 Key Personnel Changes

- Frank Pfenning switched from a position as Senior Research Scientist to Associate Professor at Carnegie Mellon University.

5 Noteworthy Meetings

- 1999 INRIA Types Summer School: Theory and Practice of Formal Proofs (Giens, France, August 30 to September 10, 1999).
- IFIP 2.8 Working Group Meeting on Functional Programming (Saint-Malo, France, September 19-24, 1999).
- 1999 International Conference on Functional Programming (Paris, France, September 27 to October 1, 1999).

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): 3,817,952
Total Funding UNExpended: 358,005

Date Current Funding will be Expended: 28 FEB 2000

Funding Expended in Most Recent Quarter: 190,291

Incremental Funding required for FY 2000: 850,000

Date of Financial Data: 30 SEP 1999