The Fox Project: Advanced Development of Systems Software

R&D Status Report
October 1 to December 31, 1997

School of Computer Science
Carnegie Mellon University
Pittsburgh, PA 15213

DISTRIBUTION STATEMENT A
Approved for public release
Distribution Unlimited

19980122 058

DTIC QUALITY INSPECTED 3

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) experimental development of systems software to (2) advanced compiler development to (3) language design.

1 Research Progress

For each of the three areas listed above, we report on the research accomplishments during the fourth calendar quarter of 1997, and the research objectives for the first quarter of 1998.

1.1 Experimental Development of Systems Software

Accomplishments (October-December):

- Completed the implementation of a prototype certifying compiler that automatically generates Proof-Carrying Code for a type-safe subset of the C language.

Objectives (January-March):

- Design the necessary extensions and modifications to the Proof-Carrying Code system to support the Intel x86 architecture.

1.2 Language Design

Accomplishments (October-December):

- Evaluated the initial design and implementation of the middle internal language of the TILT compiler.
- Completed a prototype implementation and technical report describing a meta-theorem prover for a logical framework.
- Completed a prototype implementation of a linear logical framework for experimentation with verification condition generators for proof-carrying code.

Carnegie Mellon

Carnegie Mellon University
Computer Science Department
5000 Forbes Avenue
Pittsburgh, PA 15213-3891 USA

January 14, 1998

ESC/AXS Harry Koch
ARPA Agent
5 Eglin Street
Building 1704, Room 205
Hanscom AFB, MA 01731-2116

Dear Harry:

RE: Contract F19628-95-C-0050
"The Fox Project: Advanced Languages for Systems Software"
#1-52220

Enclosed is the quarterly R&D Status Report covering our research progress during the period October 1 through December 31, 1997. Should you have any questions, please do not hesitate to contact me at 412/268-3853.

Have a wonderful day and a happy, healthy, and prosperous 1998!

Best regards,

Rosie

Rosie Hornyak

/rmh
Enclosures

Copy to: G. Koob, DARPA/ITO
C. Stephan, ESC/AXK
DARPA Technical Library
Office of Naval Research
Defense Technical Information Center/OCC

P. Lee, CMU
R. Harper, CMU
M. Brendel, CMU
A. Stoltzfus, CMU

DTIC QUALITY INSPECTED 3

Objectives (January-March):

- Complete the first release of TILT compiler for Standard ML.
- Complete a paper on the design and implementation of TILT and continue working on and evaluating the compiler

1.3 SML Compiler and System Development

Accomplishments (October-December):

- Continued development and debugging of the TILT compiler. TILT can now compile all of the old TILT benchmarks and can perform separate and cutoff compilation.
- Developed a GC idea that allows fast allocation and reclamation of tenured (garbage) data asymptotic to the amount of reclaimed space.
- Ported the ML-RISC back-end for TILT to x86 architecture.
- Completed and evaluated first prototype implementation of dependent type system for static array bound checking for a fragment of ML.

Objectives (January-March):

- Improve the performance of TILT to the point where large programs (thousands to tens of thousands of lines) can be compiled. Then, bootstrap TILT by self-compiling.
- Wrap up ML-RISC back-end for TILT.
- Begin development of techniques for a cross-module optimization in TILT.

2 Noteworthy Publications

- A Linear Logical Framework by Iliano Cervesato and Frank Pfenning. Information and Computation, 1998. Accepted to the special issue with invited papers from LICS'96, E. Clarke, editor.
- A Schema for Adding Dependent Types to ML by Hongwei Xi and Frank Pfenning. Submitted to LICS'98, December 1997.
- Eliminating Array Bound Checking through Dependent Types by Hongwei Xi and Frank Pfenning. Submitted to PLDI'98, November 1997.
- Relational Interpretation of Recursive Types in an Operational Setting by Lars Birkedal and Robert Harper, Theoretical Aspects of Computer Science, Sendai, Japan, September, 1997.

- How Generic is a Generic Back-End? by Andrew Bernard, Robert Harper, and Peter Lee. Submitted for publication Types in Compilation Workshop, Kyoto, Japan, March, 1998.
- A Comprehensive Account of Typed Closure Conversion (Extended Abstract) by Greg Morrisett and Robert Harper. Submitted to the Workshop on Higher-Order Operational Techniques in Semantics.
- Efficient Representation and Validation of Logical Proofs by George Necula, CMU Technical Report, CMU-CS-97-172.
- Efficient Representation and Validation of Proofs by George Necula and Peter Lee. Submitted for publication to the IEEE Symposium on Logic in Computer Science (LICS98).
- The Design and Implementation of a Certifying Compiler by George Necula and Peter Lee. Submitted for publication to the Symposium on Programming Language Design and Implementation (PLDI98).
- Safe, Untrusted Agents using Proof-Carrying Code by George Necula and Peter Lee. Submitted for publication to a LNCS Special Issue on Mobile Code Security.
- Modal Types as Staging Specifications for Run-time Code Generation by Philip Wickline, Peter Lee, Frank Pfenning, and Rowan Davies. To appear in 1998 Symposium on Partial Evaluation, a special issue of ACM computing surveys.
- Run-time Code Generation and Modal-ML by Philip Wickline, Peter Lee, and Frank Pfenning. Submitted for publication to the Symposium on Programming Language Design and Implementation (PLDI98).

3 Capital Equipment Purchases

- 2 CISC0766 Cisco 766 Ethernet/ISDN/NI1/IP, $1,118.60.

4 Key Personnel Changes

- None.

5 Noteworthy Meetings

- Workshop on Higher-Order Operational Techniques in Semantics (Stanford, CA, December, 1997) attended by Robert Harper.

6 Administrative Data

<ADMINISTRATIVE_AND_FINANCIAL_DATA>
<DATE_PREPARED>
09 JAN 1998
</DATE_PREPARED>
<AWARD_NUMBER>
F19628-95-C-0050
</AWARD_NUMBER>
<AWARD_AGENT>
Hanscom Air Force Base
</AWARD_AGENT>
<AWARD_TITLE>
The Fox Project: Advanced Languages for Systems Software
</AWARD_TITLE>
<ACTUAL_START_DATE>
08 JUN 1995
</ACTUAL_START_DATE>
<ACTUAL_START_DATE_COMMENT>
</ACTUAL_START_DATE_COMMENT>
<OFFICIAL_AWARD_END_DATE>
30 JUN 1998
</OFFICIAL_AWARD_END_DATE>
<CURRENT_AWARD_PROFILE_BY_FISCAL_YEAR>
<FY>95</FY><BASE>922,250</BASE>
<FY>96</FY><BASE></BASE>
<OPT_NAME>Option1</OPT_NAME><OPT_AMT>964,201</OPT_AMT>
<FY>97</FY><BASE></BASE>
<OPT_NAME>Option1</OPT_NAME><OPT_AMT></OPT_AMT>
<OPT_NAME>Option2</OPT_NAME><OPT_AMT>1,008,341</OPT_AMT>
<OPT_NAME>Option4</OPT_NAME><OPT_AMT>275,005</OPT_AMT>
<FY>98</FY><BASE></BASE>
<OPT_NAME>Option1</OPT_NAME><OPT_AMT></OPT_AMT>
<OPT_NAME>Option2</OPT_NAME><OPT_AMT></OPT_AMT>
<OPT_NAME>Option4</OPT_NAME><OPT_AMT></OPT_AMT>

</CURRENT_AWARD_PROFILE_BY_FISCAL_YEAR>
<OPTIONS_UNFUNDED_BY_FISCAL_YEAR>
<FY>98</FY><OPT_NAME>Option
4</OPT_NAME><OPT_AMT></OPT_AMT>
</OPTIONS_UNFUNDED_BY_FISCAL_YEAR>

<TOTAL_FUNDS_PROVIDED_TO_DATE>
3,169,797
</TOTAL_FUNDS_PROVIDED_TO_DATE>
<ACTUAL_FUNDS_EXPENDED_TO_DATE>
2,238,152
</ACTUAL_FUNDS_EXPENDED_TO_DATE>
<ACTUAL_FUNDS_UNEXPENDED_TO_DATE>
931,645
</ACTUAL_FUNDS_UNEXPENDED_TO_DATE>
<DATE_CURRENT_FUNDING_EXPENDED>

30 JUN 1998
</DATE_CURRENT_FUNDING_EXPENDED>

<FUNDING_FOR_NEXT_FY>

</FUNDING_FOR_NEXT_FY>
<DATE_OF_FINANCIAL_DATA>
31 DEC 1997
</DATE_OF_FINANCIAL_DATA>

<ANYTHING_ELSE_YOU_NEED>

</ANYTHING_ELSE_YOU_NEED>

</ADMINISTRATIVE_AND_FINANCIAL_DATA>