SCIENCE AND ENGINEERING RESEARCH COUNCIL
RUTHERFORD APPLETON LABORATORY

INFORMATICS DEPARTMENT

SOFTWARE AND KNOWLEDGE ENGINEERING GROUP NOTE 203

issued by
R W Witty
28 March 1988

COMMERCIAL IN CONFIDENCE
A Visit to Computational Logic Incorporated
March 1988

DISTRIBUTION: Tim Walker, Alvey
David Morgan, Alvey
Robert Foster, DTI IT
John Thynne, DTI IT
F R A Hopgood
Dr R Horton, British Embassy

(As received by e-mail)

(see next page)

Subject: visit report II

Commercial in Confidence
A Visit to Computational Logic Incorporated
March 1988

Computational Logic Incorporated (CLINC) has been formed by Dr. Don Good who was formally at the University at Texas at Austin. Good has founded "CLINC" to continue similar research objectives as pursued at the University of Texas but in a commercial environment so that he may pay his researchers competitive salaries. CLINC currently occupies commercial premises in Austin and employs in total some 25 to 30 people. This number includes John McQ and Dan Craigen who work in North Carolina and Canada. CLINC's main source of revenue is DOD research contracts although they are teaching some courses to generate short term revenue.

A major objective of CLINC is to build verified systems. A verified system for CLINC means a verified applications code running on a verified operating system on top of the security kernel on top of a verified assembler, on top of verified hardware. To this end CLINC has money from Darpa through the testbed systems route which is an SDI initiative. Warren Hunt is working on verified hardware design. He did his PHD on this topic at the University of Texas using the Boyer-Moore Theorem Prover to prove functional equivalence between an interpreter for machine code instructions and an interpreter for machine simulator at the gate level. Hunt is now looking at using the same technique of proving functional equivalence between the instruction and gate levels for CORE-MIPS.

Bill Revere is working on a verified separation kernel. He is trying to build a kernel which will guarantee process separation in the presence of clock interrupts.

J Moore is working on building a verified assembler, linker and loader.

Bill Young is doing a PhD project associated with CLINC and the University of Texas which is to build a verified compiler which compiles down to J Moore's verified assembler language which is called Piton. The language which Young is compiling is a subset of Gypsy which is called Micro-Gypsy.

CLINC are also working on the AVA project to produce A Verifiable ADA. This work is being done by Mike Smith, by Dan Craigen half time and with some input by Dave Musser. The general approach is to build an interpreter for a verifiable subset of ADA so that the Boyer-Moore Theorem Prover can be used to prove a functional equivalence between the interpreter and other components.

As of today CLINC can verify an ADA program which can swap two integers contained in variables.

Darpa are also funding the ROSE project. This is trying to build a functional language which can be used to build verified software. It is aimed again at functional equivalence being proved between programs in the language and verified hardware using the Boyer-Moore Theorem Prover. CLINC have been talking to David Turner of Kent about the design of this language and have employeed Martin Kaufman who was perviously with the Burroughs project in Austin, Texas for which Turner was a consultant and which was recently shut down.

CLINC are also funded to give GYPSY support to Al defence contractors. GYPSY is being used to build some of the secure parts of the data network, the army secure operating system and LOGK which is a Honeywell Security Co-Processor. It also being used by Ford Aero Space to build a secure multi-net gateway. My impression of CLINC was that they were a thriving organization, seem to be well set up and well equipped with a established line of funding which they had managed to move almost intact from the University of Texas. Larry Hatch from the National Security Agency had resently spent three months at CLINC learning to use the Boyer-Moore Theorem Prover. This shows that NSA is continuing its support of Don Good and Boyer and Moore.

seg6/seg 203