CerCo

INFORMATION AND COMMUNICATION
TECHNOLOGIES
(ICT)
PROGRAMME

Project FP7-ICT-2009-C-243881 CerCo

Report n. D6.6
Packages for Linux distributions and Live CD

Version 1.0

Main Authors:
Claudio Sacerdoti Coen

Project Acronym: CerCo
Project full title: Certified Complexity
Proposal/Contract no.: FP7-ICT-2009-C-243881 CerCo

Abstract We provide Debian packages for all the software developed in CerCo and for all its software dependencies. The Debian packages are for the forthcoming stable Debian distribution. Moreover, we provide a Live CD, also based on Debian, that contains a pre-installed version of all the packages and a copy of the formalization.

Contents

1 Task

The Grant Agreement describes deliverable D6.6 as follows:

> **Packages for Linux distributions and Live CD**: In order to foster adoption of the CerCo compiler in a wider community, we will provide packages for selected Linux distributions and a Live CD with the software developed in the project. We will also consider and discuss the integration of our software in an extensible platform dedicated to source-code analysis of C software, like Frama-C. However, at the moment it is unclear how these rapidly changing platforms will evolve in the next two years, if integration would provide an added value and if it would be possible to practically achieve the integration in the project timeframe without an actual involvement of the platform developers (that would need to contribute man-power to the task).

Integration with Frama-C has been done in D5.1-D5.3. This report overviews the packages that have been provided and the contents of the Live CD.

2 Debian packages

We show here the description of every Debian package made for the software developed in CerCo, as reported by `apt-cache show`. Only the relevant fields are shown.

1. Package name: `acc`, Version: 0.2-1
   CerCo's Annotating C Compiler
   CerCo's Annotating C Compiler is a C compiler for the 8051 microprocessor. It produces both an Intel HEX code memory representation and an instrumented version of the source code. The instrumented source code is a copy of the original source code augmented with additional instructions to keep track of the exact number of clock cycles spent by the microprocessor to execute the program basic blocks. Combined with CerCo's Frama-C Cost Plugin it allows to certify exact parametric time and stack bounds for the source code. Limitations: the source code must all be in one .c file and it must not contain external calls.

2. Package name: `acc-trusted`, Version: 0.2-1
   CerCo's Trusted Annotating C Compiler
   CerCo's Annotating C Compiler is a C compiler for the 8051 microprocessor. It produces both an Intel HEX code memory representation and an instrumented version of the source code. The instrumented source code is a copy of the original source code augmented with additional instructions to keep track of the exact number of clock cycles spent by the microprocessor to execute the program basic blocks. Combined with CerCo's Frama-C Cost Plugin it allows to certify exact parametric time and stack bounds for the source code. Limitations: the source code must all be in one .c file and it must not contain external calls. This version of the compiler has been certified for preservation of the inferred costs using the interactive theorem prover Matita.

3. Package name: `frama-c-cost-plugin`, Version: 0.2-1
   Depends: `acc | acc-trusted`, Recommends: `why, why3, cvc3`
   CerCo's Frama-C Cost Plugin

The CerCo's Frama-C Cost Plugin has been developed by the CerCo project http://cerco.cs.unibo.it. It compiles a C source file to an 8051 Intel HEX using either the acc or the acc-trusted compilers. The compilation also produces an instrumented copy of the source code obtained inserting instractions to keep track of the number of clock cycles spent by the program on the real hardware. The plugin implements an invariant generator that computes parametric bounds for the total program execution time and stack usage. Moreover, the plugin can invoke the Jessie condition generators to generate proof obligations to certify the produced bound. The proof generators may be automatically closed using the why3 tool that invokes automated theorem provers. The cvc3 prover works particularly well with the proof obligations generated from the cost plugin.

The following additional Debian packages are required by the CerCo's Frama-C Cost Plugin. They do not install software developed in CerCo, but their Debian packages themselves have been made by CerCo. Among all the theorem provers that can be used in combination with Why3 (and the CerCo Cost Plugin), we have decided to package cvc3 because its licence allows free redistribution and because it is powerful enough to close most proof obligations generated by CerCo on common examples. The user can still manually install and try other provers that will be automatically recognized by why3 just by running `why3config`. We do not provide any Debian packages for them.

1. Package name: `why`, Version: 2.31+cerco-1
   Software verification tool
   Why aims at being a verification conditions generator (VCG) back-end for other verification tools. It provides a powerful input language including higher-order functions, polymorphism, references, arrays and exceptions. It generates proof obligations for many systems: the proof assistants Coq, PVS, Isabelle/HOL, HOL 4, HOL Light, Mizar and the decision procedures Simplify, Alt-Ergo, Yices, CVC Lite and haRVey.

2. Package name: `why3`, Version: 0.73+cerco-1
   Software verification tool
   Why aims at being a verification conditions generator (VCG) back-end for other verification tools. It provides a powerful input language including higher-order functions, polymorphism, references, arrays and exceptions. It generates proof obligations for many systems: the proof assistants Coq, PVS, Isabelle/HOL, HOL 4, HOL Light, Mizar and the decision procedures Simplify, Alt-Ergo, Yices, CVC Lite and haRVey.

3. Package name: `cvc3`, Version: 2.4.1-1
   CVC3 is an automatic theorem prover for Satisfiability Module Theories
   CVC3 is an automatic theorem prover for Satisfiability Modulo Theories (SMT) problems. It can be used to prove the validity (or, dually, the satisfiability) of first-order formulas in a large number of built-in logical theories and their combination. CVC3 is the last offspring of a series of popular SMT provers, which originated at Stanford University with the SVC system. In particular, it builds on the code base of CVC Lite, its most recent predecessor. Its high level design follows that of the Sammy prover. CVC3 works with a version of first-order logic with polymorphic types and has a wide variety of features including: * several built-in base theories: rational and integer linear arithmetic, arrays, tuples, records, inductive data types, bit vectors, and equality over

uninterpreted function symbols; * support for quantifiers; * an interactive text-based interface; * a rich C and C++ API for embedding in other systems; * proof and model generation abilities; * predicate subtyping; * essentially no limit on its use for research or commercial purposes (see license).

Finally, we have released and packaged a new version of Matita that contains several improvements driven by CerCo, like code extraction.

1. Package name: `matita`, Version: 0.99.2-1
   Interactive theorem prover
   Matita is a graphical interactive theorem prover based on the Calculus of (Co)Inductive Constructions.

All Debian packages mentioned above can be downloaded from the CerCo's website `http://cerco.cs.unibo.` and are compatible with the *testing* release of Debian, soon to be freezed and become the forthcoming *stable* release. The source code to recompile the Debian packages from scratch is part of the CerCo repository and can be also downloaded from the website.

3 Live CD

We also provide a Live CD to easily test all the software implemented in CerCo without having to recompile the software by hand or install a Debian distribution. The Live CD can be downloaded from the CerCo's website `http://cerco.cs.unibo.it`. It is a Live Debian CD that can be either burnt on a physical disk used to boot a real machine, or it can be used to bootstrap a virtual machine using any virtualizer like `virtualbox, qemu` or similar ones.

The Live CD contains an xserver and a standard gnome environment and it connects automatically to any available network. The virtualbox guest tools have also been installed to facilitate communication between the host and the virtual machine, e.g. for file transfer.

The Live CD also has pre-installed all the Debian packages described in the previous section. The user can simply boot the system and invoke the `cerco` executable to compile any compatible C file to the Intel HEX format for the 8051. The executable also computes the cost model for the source program, its cost invariants and tries to certify them using the cvc3 theorem prover. In case of failure, the flag `-ide` can be used to open an interactive why3 session to experiment with different theorem prover flags (e.g. increasing the prover timeout).

Further informations on the `cerco` executable can be found in Deliverable D5.2.

Finally, the Live CD also has a preinstalled copy of the interactive theorem prover Matita and a snapshot of the compiler certification. The snapshot can be found in the user's home directory, under `cerco/src`. Matita files can be opened running `matita`. The other directory `cerco/driver` contains the extracted code together with the untrusted code that forms the CerCo Trusted Compiler.