Factsheet

Valex for PPC

Release 23.10i, b13994404

October 24, 2023

AbsInt

Valex is a tool for the postpass validation of binaries produced by the formally verified CompCert C compiler. Valex checks the correctness of the assembling and linking steps of a statically and fully linked executable. Valex works on the assembly level and compares the abstract assembly representation produced by CompCert with the disassembled code of the executable.

Checked properties

- Checks per function for equivalence between abstract assembly and the actual assembly code contained in executable. Checked properties are assembly mnemonics, operand types and values of instructions as well as referenced labels and symbols.
- Checks that referenced to labels and symbolic names are used consistently. All references to the same item always must resolve to the same memory address.
- Checks correspondence of global variables. Symbols must be contained in the symbol table, have the correct size, alignment, and initialization data.
- Checks that functions and variables are mapped to the correct sections in the executable.

Key benefits

Valex extends the verified toolchain of CompCert to the binary level. All safety properties verified on the source code (e.g. by static analyzers or model checking) now automatically hold for the generated final binary.

Supported compilers

- CompCert C Compiler

Current limitations

- Return addresses must not be modified.
- The instruction *dcread* is only supported in alternative encoding.
- The *mbar* instruction from the category Embedded of the PowerPC ISA uses the same encoding as the *eieio* instruction from the category Server.
  Valex will silently ignore the *MO* field of an *mbar* instruction and treat *mbar* and *eieio* as equivalent.
- The linker should not perform any link time optimizations or other modifications of the code structure.
- Inline assembly is supported, but each snippet needs an additional annotation for the number of contained instructions. Annotated inline assembly snippets of the executable are skipped by Valex and not checked for correct translation.
- Unreachable code in the executable (e.g. additional code after a return at the end of a routine) is not matched with the CompCert output and does not cause a warning.
- Use of the CompCert commandline-options *-falign-branch-targets* ot *-falign-cond-branches* may introduce additional code to satisfy the alignment constraints (e.g. *NOP* or branch instructions).
  These instructions are not part of the internal abstract assembly representation of CompCert.
  Valex will therefore issue error messages and fail to match the executable.

System requirements

- Windows: 64-bit Windows 10 or newer
- Linux: 64-bit CentOS/RHEL 7 or compatible
- 4 GB of RAM (16 GB recommended)
- 4 GB of disk space

Also available

The following AbsInt products are also available for this target:

- StackAnalyzer
- TimingProfiler
- ValueAnalyzer
- TimeWeaver
- Qualification Support Kit

More information

- Visit our website: www.absint.com
- Speak with a product specialist: call +49 681 383 600

About AbsInt

AbsInt provides advanced development tools for embedded systems, and tools for analysis, optimization and verification of safety-critical software. Our customers are located in more than 40 countries worldwide. We have distribution agreements with major software distributors in Asia, North America, Middle East, and throughout Europe.

Our headquarters

Science Park 1
66123 Saarbrücken, Germany
Phone: +49 681 383 600
Fax: +49 681 383 60 20
Email: info@absint.com
Web: www.absint.com