SPEC CPU 2006 Benchmark Compilation and Runtime Errors

As mentioned in our submitted manuscript, we use Clang (version 9.0.0) with C++11 support to compile SPEC CPU2006 programs with sanitization. From in total 19 C/C++ programs provided by SPEC CPU2006, 11 programs can be successfully compiled and executed. We list the encountered errors for the other eight cases. As shown in Table 1, Clang/LLVM was trapped in the compiling seven SPEC programs when enabling sanitizer checks. In addition, some memory access errors were (unexpectedly) triggered when executing the other two programs. Overall, these eight test cases cannot be smoothly benchmarked.

We list all the compilation errors and runtime exceptions we encountered to present a complete picture of our study. We note that such issue has also been reported by the closely related research, ASAP [1], which can run 14 SPEC benchmarks for ASan and 12 for UBSan. Although the specific version of Clang/LLVM compiler used in the ASAP paper is not disclosed, more compilation errors and runtime exceptions are presumably due to updates in the compiler framework (ASAP was published in 2015). Nevertheless, to provide an up-to-date understanding of de facto ASan/UBSan and its potential of reduction, we decide to use the more recent version 9.0.0 of Clang/LLVM.

References

[1] Jonas Wagner, Volodymyr Kuznetsov, George Candea, and Johannes Kinder. High system-code security with low overhead. In *2015 IEEE Symposium on Security and Privacy*, pages 866–879. IEEE, 2015.

Table 1: Compilation and execution errors of eight SPEC CPU2006 C/C++ programs.

Test Case	Error Type	Simplified Error Message
400.perlbench	Compilation Error	1. util.c:3641: error: conflicting types for 'Perl_init_tm' Perl_init_tm(pTHX_ struct tm *ptm) 2. pp_sys.c:4489: error: incomplete definition of type 'struct tm' dayname[tmbuf-¿tm_wday]
447.dealII	Compilation Error	1. dof_renumbering.cc:63: error: ISO C++11 does not allow access declarations 2. tria.all_dimensions.cc:107: error: non-const-expression cannot be narrowed from 'int' to 'unsigned int' 3. tria.cc:5539: error: non-constant-expression cannot be narrowed from type 'int' to 'unsigned int' 4. include/lac/vector.templates.h:750: error: no member named 'strcat' in namespace 'std'
450.soplex	Compilation Error	1. mpsinput.cc:75: error: invalid operands to binary expression
473.astar	Compilation Error	1. Library.cpp:80: error: invalid suffix on literal
483.xalancbmk	Compilation Error	1. ParserForXMLSchema.cpp:303: error: non-const-expression cannot be narrowed from 'XMLInt32' to 'XMLCh' 2. FormatterToHTML.cpp:139: error: use of undeclared identifier 'memset' 3. ElemNumber.cpp:1401: error: use of undeclared identifier 'memset'
471.omnetpp	Compilation Error	1. heap.cc: multiple definition of 'operator delete(void*)'. asan_new_delete.cc:166: first defined here 2. heap.cc: multiple definition of 'operator new(unsigned long)'. asan_new_delete.cc:105: first defined here
403.gcc	Runtime Error	We provide a 42KB error message file at https://www.dropbox.com/s/m3sy1j4mjt1jrrj/gcc-error.txt?dl=0.
464.h264ref	Runtime Error	global-buffer-overflow biariencode.cc:334:14 in biari_init_context