MOSDEF 2.0 Release Notes
January 2008
www.immunityinc.com
(http://www.immunityinc.com/resources-freesoftware.shtml)

Introduction

MOSDEF is an LGPL C-like compiler suite originally built and designed for Immunity's CANVAS attack framework. It's written completely in Python (requires Python 2.5) and is portable in that sense, but is also portable in the sense of generating binaries which will run on multiple platforms. MOSDEF can currently target Windows, Linux, BSD, AIX, OS X and Solaris. MOSDEF's assemblers can target X86, SPARC, and PPC. MOSDEF's object file creator can create PE, COFF, and ELF.

MOSDEF's parser uses the Ply (http://www.dabeaz.com/ply/ply.html). The assemblers often parse code that is similar but not identical to their GCC counterparts. For example, they may use "//" as a comment indicator instead of ";" as Gnu Assembler would.

Immunity has released MOSDEF in the hopes that it is a useful learning tool for learning how to write a parser, but please keep in mind none of the people involved in the project had ever written a compiler of any kind before this one.

MOSDEF was named after a common expression in "The Wire" ("Most Definitely").

MOSDEF has been released under the LGPL license. Ply was also originally under the LGPL license. There's also quite a lot of useful libraries included in MOSDEF, such as the integer handling API's or the PE file outputter. You may find these handy even if you don't need to compile binaries.

Generally MOSDEF is a great way to answer the questions:

1. How does a real compiler work?
2. How does a real assembler work?
3. What are the decisions you make when building a compiler, and how would I have done it better than Immunity did?

History of MOSDEF

The first public version of MOSDEF was released in 2003 and was based on spark.py, which is a slow parser, but very easy to learn and use. This parser is still included today in the package and can be turned on for comparison purposes. At the time CANVAS did not support AIX, BSD, or many other platforms. For those reasons the original parser was quite incomplete. Since then the entire tree has been arranged to include a mini-libc. This is quite useful as many platforms are quite similar and adding a new platform can take less than a week now.

When MOSDEF switched to using Ply, we found that Ply was originally written for programs that did parsing in a single-threaded manner and was only useful on Modules. Immunity ported Ply to a threaded, Class-based system, and released that result as PlyC v1.4. Immunity has redone this effort to in this MOSDEF release with the much more modern Ply 2.5. Ply, in addition to not requiring large stack sizes as spark.py did, is much faster. We have not benchmarked MOSDEF against other compilers. See the “PLY” section for more information on our modified PLY.

Because MOSDEF is typically used as part of a computer attack known as a buffer overflow, all code it generates is Position Independent Code. The assembly output is not heavily optimized, although the x86 assembler will attempt to make it small by avoiding long jumps where possible.

Using MOSDEF

First you should generate a test.c program such as the one below.

```
#import "local", "write" as "write"
#import "local", "exit" as "exit"

int main(void)
{
  int i;
  i=8;
  write(1,"HITHERE\n",8);
  exit(1);
}
```

Now you can compile it with python *python cc.py -o test test.c*. The default is X86 Linux. Running ./test will now print out HITHERE and exit. See the “Implementation” section to see how that happened.

You'll notice that if you strace this program, it doesn't do anything other than call write and exit. This is because it's not linked to libc at all. It's also tiny, around 1500 bytes total. Getting used to importing every library call you want to use takes some getting used to. You'll notice MOSDEF is also quite strict about how you deal with structures (I.e. struct1.struct2.struct3.thing does not work, sorry).

If you just want to play with the assemblers, you should use *mosdef.py*. MOSDEF can be configured to output its intermediary assembly and IL files, if you so wish. A quick way of achieving this is by calling *cparse2.py* directly and passing it a C file: *python cparse2.py test.c* will output the intermediate language, assembly and bytecode for both the X86 and PPC architectures for the Linux OS. In the MOSDEF version that ships with CANVAS the following OS and CPU architectures are supported: Windows, Linux, BSD, OSX, AIX, Solaris, X86, PPC & SPARC though it is expected more will be added over time.

Design and Implementation

MOSDEF is built much like GCC, with the major exception that its design goal was for post-exploitation control over a target.

You will see a chain that looks like this:

cc.py -> cpp.py -> cparse2.py -> il2x86.py -> x86parse.py -> makeexe.py

The C pre-processor is responsible for #ifdef and comments and such things. *cparse2.py* will generate an IL, this will then get turned into assembly language for whatever processor you choose, and that will be written to disk in a binary format by *makeexe.py*. In normal CANVAS use things compiled by MOSDEF are sent over the wire in some way to interact with a live target, rather than written to disk.

More information on MOSDEF as it is used in CANVAS and general concepts is available here: http://www.immunityinc.com/downloads/MOSDEF_Exploitation.sxi

Windows programs compiled by MOSDEF are designed to be hooked into by a shellserver. A shellserver in normal CANVAS usage would remotely resolve all external symbols the Windows programmer wanted to use and link those into the program as function pointers. Shellservers were not included in this release of MOSDEF.

Parts of MOSDEF (for example OS X) have not been used nearly as much as other parts – so let us know if you find something broken and we will try to fix it with you. The initial MOSDEF 2.0 release includes tested functionality for x86 and PPC Linux only.

PLY

MOSDEF uses the Python Lex Yacc (PLY) modules originally written by David M. Beazley of the University of Chicago. These modules create the parser and lexer by reading the documentation fields of various functions in individual parser and lexer modules.

Immunity has heavily modified the public versions of PLY to include in CANVAS. The focus has been thread safety, speed, and modularity for use within a commercial product that may have fifteen or more parsing operations happening at the same time in various stages of operation.

For this reason you will see the very old *spark.py* parser (for the original *cparse.py*), the modified *lex.py*/*yacc.py* based off of the PLYv1.4 (used for the first version of cparse2 and the assemblers in the original cparse) and the even newer *lex2.py* and *yacc2.py* based off of PLYv2.5 (used for the *cparse2.py* and all assemblers in modern MOSDEF2.0). These include the following changes (to PLY 2.5, the latest release):

- Speed improvements
  - PLY now dumps its parse/lex tables as pickles, rather than python modules. This saves time and effort on both the writing and more importantly the reading of the tables, as well as just generally making more sense
    [NOTE: Obviously all the normal warnings about untrusted pickles apply, don't use parse/lextables generated by somebody else because you will get 0wned – generate your own parse/lextables and stay safe kids!]
  - Parse/lextables can now also be written to a specified directory path not just the CWD

    - The original PLY code had a bug where it did MD5 table signature generation over a different data set on writing than on the reading which meant you always got a hash mismatch causing table regeneration. The obviously slowed things down, the hashing now functions correctly (albeit over a slightly smaller data set) and tables are read in once on initialization and cached for future use.
      [NOTE: The normal caveats about very little error checking taking place to ensure parse/lextables match the parsed grammar still apply, if you change the grammar regenerate your parse/lextables!!]
- Modularity
    - Global variables have been removed. This is required for multi-threaded parser programs, and recursive parsing such as MOSDEF *#import* construct where a new parser namespace is required at each code level
    - PLY is able to now use classes rather than modules to generate the parsers

If you are interested in seeing the differences between MOSDEF 1.0/*cparse.py* and MOSDEF2.0/*cparse2.py* we have included a utility used in the development of MOSDEF which shows you some interesting metrics of the two generation processes. *cparse_to_cparse2_diff.py* has a number of parameters that can be passed in, in its simplest form the following will produce some timing data and a diff of the generated IL: *python cparse_to_cparse2.py -m test.c*. Further options such as dumping the entire IL (-d) using python profile modules to look for slow steps and hotspots (-p) can be added to the command line to get more information.
[NOTE: as label names are essentially randomly generated for the IL the diff will sometimes show that the IL generated by cparse1 and the IL generated by cparse2 are different, when you actually check the diff data you will see it is (hopefully!) only the LABEL identifiers that differ not the actual logic of the IL itself.]

Future Work

You could build a packer or program obfuscation tool that worked with MOSDEF and was polymorphic based around its parse tree, rather than on low level assembly. Having complete control over a parser can be quite useful for this sort of thing.

You could output Java IL or another IL rather than the IL we use. You could output Python IL or just Python code to emulate some process you're interested in.

You could add error checking or optimizations to the MOSDEF IL generator in *cparse2.py*.

There's really no end of little fun projects to do with something like this. Of course, if you're into security, we recommend you get CANVAS and use the ShellServer capability to do your next amazing project. We also have an entire shellcode library which comes in handy when doing exploitation work. If you're interested in this sort of thing, we recommend you log onto http://forum.immunityinc.com and start a thread about it.

Thanks for using MOSDEF!

The Immunity CANVAS Team

Some example outputs:

Example: test.c for Linux ppc (cc.py -t 4 test.c -o test)

```
immunity@macminippc:~$ uname -a
Linux macminippc 2.6.25-2-powerpc #1 Tue Sep 30 14:49:00 UTC 2008 ppc GNU/Linux
immunity@macminippc:~$ strace ./test
execve("./test", ["./test"], [/* 18 vars */]) = 0
write(1, "HITHERE\n", 8HITHERE
)               = 8
exit(1)                                 = ?
Process 6170 detached
immunity@macminippc:~$ ./test
HITHERE
immunity@macminippc:~$
```

Example: test.c for Linux ppc (cc.py -t 2 test.c -o test)

```
evil@ubuntu:~/new/CANVAS$ uname -a
Linux ubuntu 2.6.25.4-grsec #2 SMP Tue Jun 10 13:55:53 EDT 2008 i686 GNU/Linux
evil@ubuntu:~/new/CANVAS$ strace ./test
execve("./test", ["./test"], [/* 37 vars */]) = 0
write(1, "HITHERE\n", 8HITHERE
)               = 8
_exit(1)                                = ?
Process 9247 detached
evil@ubuntu:~/new/CANVAS$ ./test
HITHERE
evil@ubuntu:~/new/CANVAS$
```

Example: Profiling comparison cparse1 to cparse2 (cparse_to_cparse2_diff.py -m test.c -p)

```
evil@evil-desktop ~/MOSDEF2 $ python cparse_to_cparse2_diff.py -m test.c -p

cparse 1 profile:
         105050 function calls (97352 primitive calls) in 0.538 CPU seconds

   Ordered by: internal time
   List reduced from 389 to 25 due to restriction <25>

   ncalls  tottime  percall  cumtime  percall filename:lineno(function)
     1560    0.117    0.000    0.123    0.000 /home/evil/MOSDEF2/spark.py:260(buildState)
       35    0.055    0.002    0.107    0.003 /home/evil/MOSDEF2/cpp.py:65(preprocess)
   3787/1    0.038    0.000    0.439    0.439 /home/evil/MOSDEF2/spark.py:551(postorder)
       34    0.038    0.001    0.045    0.001 /home/evil/MOSDEF2/spark.py:96(tokenize)
       34    0.020    0.001    0.028    0.001 /home/evil/MOSDEF2/spark.py:133(addRule)
  2295/34    0.017    0.000    0.046    0.001 /home/evil/MOSDEF2/spark.py:395(buildTree_r)
       34    0.017    0.000    0.017    0.000 /home/evil/MOSDEF2/spark.py:176(makeFIRST)
        1    0.015    0.015    0.024    0.024 /home/evil/MOSDEF2/x86opcodes.py:14(<module>)
     4995    0.012    0.000    0.053    0.000 /usr/lib64/python2.5/re.py:134(match)
     2261    0.009    0.000    0.023    0.000 /home/evil/MOSDEF2/spark.py:490(buildASTNode)
     5080    0.009    0.000    0.054    0.000 /usr/lib64/python2.5/re.py:227(_compile)
     2261    0.008    0.000    0.013    0.000 /home/evil/MOSDEF2/spark.py:501(nonterminal)
      107    0.008    0.000    0.008    0.000 /usr/lib64/python2.5/sre_compile.py:264(_mk_bitmap)
   223/88    0.008    0.000    0.017    0.000 /usr/lib64/python2.5/sre_parse.py:385(_parse)
     3066    0.006    0.000    0.006    0.000 /home/evil/MOSDEF2/x86opcodes.py:118(__init__)
      124    0.006    0.000    0.014    0.000 /usr/lib64/python2.5/sre_compile.py:213(_optimize_charset)
     1526    0.006    0.000    0.006    0.000 /home/evil/MOSDEF2/cparse.py:57(__getitem__)
     5398    0.005    0.000    0.005    0.000 /home/evil/MOSDEF2/cparse.py:51(__cmp__)
      693    0.005    0.000    0.005    0.000 /home/evil/MOSDEF2/mosdefutils.py:505(dInt)
      519    0.005    0.000    0.015    0.000 MOSDEF/MOSDEFlibc/MLCutils.py:149(setdefine)
     3638    0.004    0.000    0.006    0.000 /home/evil/MOSDEF2/spark.py:483(preprocess)
       68    0.004    0.000    0.004    0.000 /home/evil/MOSDEF2/spark.py:45(_namelist)
       34    0.004    0.000    0.190    0.006 /home/evil/MOSDEF2/spark.py:219(parse)
   363/41    0.004    0.000    0.020    0.000 /usr/lib64/python2.5/sre_compile.py:38(_compile)
    10590    0.004    0.000    0.004    0.000 /home/evil/MOSDEF2/ast.py:40(__getitem__)


================================================================================
cparse 2 profile:
         52513 function calls (51341 primitive calls) in 0.363 CPU seconds

   Ordered by: internal time
   List reduced from 224 to 25 due to restriction <25>
```

```
   ncalls  tottime  percall  cumtime  percall filename:lineno(function)
     3277    0.093    0.000    0.106    0.000 /home/evil/MOSDEF2/yacc2.py:2302(add_production)
       34    0.049    0.001    0.068    0.002 /home/evil/MOSDEF2/cpp.py:65(preprocess)
     1073    0.024    0.000    0.130    0.000 /home/evil/MOSDEF2/yacc2.py:2422(add_function)
     30/1    0.018    0.001    0.322    0.322 /home/evil/MOSDEF2/yacc2.py:1827(parseopt_notrack)
     1174    0.018    0.000    0.025    0.000 /home/evil/MOSDEF2/lex2.py:373(token)
       30    0.016    0.001    0.153    0.005 /home/evil/MOSDEF2/yacc2.py:2912(yacc)
     3277    0.013    0.000    0.013    0.000 /home/evil/MOSDEF2/yacc2.py:2231(__init__)
     4842    0.012    0.000    0.019    0.000 /usr/lib64/python2.5/re.py:134(match)
     4922    0.008    0.000    0.018    0.000 /usr/lib64/python2.5/re.py:227(_compile)
      850    0.006    0.000    0.006    0.000 /home/evil/MOSDEF2/mosdefutils.py:505(dInt)
      499    0.004    0.000    0.014    0.000 MOSDEF/MOSDEFlibc/MLCutils.py:149(setdefine)
     4176    0.004    0.000    0.004    0.000 /home/evil/MOSDEF2/yacc2.py:3081(<lambda>)
      153    0.004    0.000    0.009    0.000 MOSDEF/cparse2.py:1276(p_rightvalue)
       88    0.004    0.000    0.004    0.000 MOSDEF/cparse2.py:570(p_statementlist)
     29/2    0.003    0.000    0.312    0.156 /home/evil/MOSDEF2/mosdef.py:98(compile_to_IL)
       30    0.003    0.000    0.015    0.000 /home/evil/MOSDEF2/lex2.py:615(lex)
     58/2    0.003    0.000    0.318    0.159 MOSDEF/cparse2.py:953(p_importdirective)
     5949    0.003    0.000    0.003    0.000 /home/evil/MOSDEF2/yacc2.py:143(__getitem__)
      947    0.003    0.000    0.004    0.000 MOSDEF/cparse2.py:349(get_cthing)
       30    0.003    0.000    0.003    0.000 /home/evil/MOSDEF2/yacc2.py:1355(lr_read_tables)
     1597    0.003    0.000    0.003    0.000 /home/rich/Devel/CANVAS/internal/debug.py:130(devlog)
      147    0.003    0.000    0.003    0.000 MOSDEF/MOSDEFlibc/UNIX.py:166(add_generic_syscall)
       88    0.002    0.000    0.003    0.000 MOSDEF/cparse2.py:596(p_statement)
       31    0.002    0.000    0.004    0.000 MOSDEF/cparse2.py:884(p_functioncall)
   112/46    0.002    0.000    0.006    0.000 /usr/lib64/python2.5/sre_parse.py:385(_parse)

evil@evil-desktop ~/Devel/CANVAS $
```

Example: Comparing cparse1 to cparse2 (cparse_to_cparse2_diff.py -m test.c)

[Note: the diff output identifies differences in labeldefines and comments (rem) in the IL but the actual IL logic is the same]

```
evil@evil-desktop ~/MOSDEF2 $ python cparse_to_cparse2_diff.py -m test.c
------------------
IL Code diff:

cparse1                                                                 |       cparse2
*** 3,12 ****                                                           |       --- 3,12 ----
  rem <SHOULD NOT BE REACHED>                                           |         rem <SHOULD NOT BE REACHED>
  ret 0                                                                 |         ret 0
  rem </SHOULD NOT BE REACHED>                                          |         rem </SHOULD NOT BE REACHED>
! rem Import directive found local:write:write:LABEL1_636759            |       ! rem Import directive found
local:write:write:LABEL1_382293
! labeldefine LABEL1_636759                                            |       ! labeldefine LABEL1_382293
! rem Import directive found local:syscall3:syscall3:LABEL1_1155859     |       ! rem Import directive found
local:syscall3:syscall3:LABEL1_835477
! labeldefine LABEL1_1155859                                           |       ! labeldefine LABEL1_835477
  asm                                                                   |         asm
  asm             syscall3:                                             |         asm             syscall3:
  asm             push %ebp                                             |         asm             push %ebp

*** 59,70 ****                                                         |       --- 59,70 ----
  functionpostlude 12                                                   |         functionpostlude 12
  ret 12                                                                |         ret 12
  rem <end of write> (end of epilog)                                    |         rem <end of write> (end of epilog)
! rem Import directive found local:exit:exit:LABEL2_636759              |       ! rem Import directive found local:exit:exit:LABEL2_382293
! labeldefine LABEL2_636759                                            |       ! labeldefine LABEL2_382293
! rem Import directive found local:close:close:LABEL1_684003           |       ! rem Import directive found
local:close:close:LABEL1_1046340
! labeldefine LABEL1_684003                                            |       ! labeldefine LABEL1_1046340
! rem Import directive found local:syscall1:syscall1:LABEL1_402030     |       ! rem Import directive found
local:syscall1:syscall1:LABEL1_1071298
! labeldefine LABEL1_402030                                            |       ! labeldefine LABEL1_1071298
  asm                                                                   |         asm
  asm             syscall1:                                             |         asm             syscall1:
  asm             push %ebp                                             |         asm             push %ebp

*** 105,114 ****                                                       |       --- 105,114 ----
  functionpostlude 4                                                    |         functionpostlude 4
  ret 4                                                                 |         ret 4
  rem <end of close> (end of epilog)                                    |         rem <end of close> (end of epilog)
! rem Import directive found local:read:read:LABEL2_684003             |       ! rem Import directive found local:read:read:LABEL2_1046340
! labeldefine LABEL2_684003                                            |       ! labeldefine LABEL2_1046340
! rem Import directive found local:syscall3:syscall3:LABEL1_983082     |       ! rem Import directive found
local:syscall3:syscall3:LABEL1_723895
! labeldefine LABEL1_983082                                            |       ! labeldefine LABEL1_723895
  rem                                                                   |         rem
  rem Found function declare read (stack = 4)                           |         rem Found function declare read (stack = 4)
  rem                                                                   |         rem

*** 141,152 ****                                                       |       --- 141,152 ----
  functionpostlude 12                                                   |         functionpostlude 12
  ret 12                                                                |         ret 12
  rem <end of read> (end of epilog)                                     |         rem <end of read> (end of epilog)
! rem Import directive found local:write:write:LABEL3_684003           |       ! rem Import directive found
local:write:write:LABEL3_1046340
! labeldefine LABEL3_684003                                            |       ! labeldefine LABEL3_1046340
! rem Import directive found local:pipe:pipe:LABEL4_684003             |       ! rem Import directive found local:pipe:pipe:LABEL4_1046340
```

```
! labeldefine LABEL4_684003                                          |        ! labeldefine LABEL4_1046340
! rem Import directive found local:syscall1:syscall1:LABEL1_681189    |        ! rem Import directive found
local:syscall1:syscall1:LABEL1_788915
! labeldefine LABEL1_681189                                          |        ! labeldefine LABEL1_788915
  rem                                                                |          rem
  rem Found function declare pipe (stack = 4)                        |          rem Found function declare pipe (stack = 4)
  rem                                                                |          rem

*** 173,182 ****                                                     |        --- 173,182 ----
  functionpostlude 4                                                 |          functionpostlude 4
  ret 4                                                              |          ret 4
  rem <end of pipe> (end of epilog)                                  |          rem <end of pipe> (end of epilog)
! rem Import directive found local:chown:chown:LABEL5_684003         |        ! rem Import directive found
local:chown:chown:LABEL5_1046340
! labeldefine LABEL5_684003                                          |        ! labeldefine LABEL5_1046340
! rem Import directive found local:syscall3:syscall3:LABEL1_758141    |        ! rem Import directive found
local:syscall3:syscall3:LABEL1_643291
! labeldefine LABEL1_758141                                          |        ! labeldefine LABEL1_643291
  rem                                                                |          rem
  rem Found function declare chown (stack = 4)                       |          rem Found function declare chown (stack = 4)
  rem                                                                |          rem

*** 209,218 ****                                                     |        --- 209,218 ----
  functionpostlude 12                                                |          functionpostlude 12
  ret 12                                                             |          ret 12
  rem <end of chown> (end of epilog)                                 |          rem <end of chown> (end of epilog)
! rem Import directive found local:fchown:fchown:LABEL6_684003       |        ! rem Import directive found
local:fchown:fchown:LABEL6_1046340
! labeldefine LABEL6_684003                                          |        ! labeldefine LABEL6_1046340
! rem Import directive found local:syscall3:syscall3:LABEL1_722578    |        ! rem Import directive found
local:syscall3:syscall3:LABEL1_462328
! labeldefine LABEL1_722578                                          |        ! labeldefine LABEL1_462328
  rem                                                                |          rem
  rem Found function declare fchown (stack = 4)                      |          rem Found function declare fchown (stack = 4)
  rem                                                                |          rem

*** 245,254 ****                                                     |        --- 245,254 ----
  functionpostlude 12                                                |          functionpostlude 12
  ret 12                                                             |          ret 12
  rem <end of fchown> (end of epilog)                                |          rem <end of fchown> (end of epilog)
! rem Import directive found local:lchown:lchown:LABEL7_684003       |        ! rem Import directive found
local:lchown:lchown:LABEL7_1046340
! labeldefine LABEL7_684003                                          |        ! labeldefine LABEL7_1046340
! rem Import directive found local:syscall3:syscall3:LABEL1_350502    |        ! rem Import directive found
local:syscall3:syscall3:LABEL1_732195
! labeldefine LABEL1_350502                                          |        ! labeldefine LABEL1_732195
  rem                                                                |          rem
  rem Found function declare lchown (stack = 4)                      |          rem Found function declare lchown (stack = 4)
  rem                                                                |          rem

*** 281,290 ****                                                     |        --- 281,290 ----
  functionpostlude 12                                                |          functionpostlude 12
  ret 12                                                             |          ret 12
  rem <end of lchown> (end of epilog)                                |          rem <end of lchown> (end of epilog)
! rem Import directive found local:chdir:chdir:LABEL8_684003         |        ! rem Import directive found
local:chdir:chdir:LABEL8_1046340
! labeldefine LABEL8_684003                                          |        ! labeldefine LABEL8_1046340
! rem Import directive found local:syscall1:syscall1:LABEL1_1096645   |        ! rem Import directive found
local:syscall1:syscall1:LABEL1_998930
! labeldefine LABEL1_1096645                                         |        ! labeldefine LABEL1_998930
  rem                                                                |          rem
  rem Found function declare chdir (stack = 4)                       |          rem Found function declare chdir (stack = 4)
  rem                                                                |          rem

*** 311,320 ****                                                     |        --- 311,320 ----
  functionpostlude 4                                                 |          functionpostlude 4
  ret 4                                                              |          ret 4
  rem <end of chdir> (end of epilog)                                 |          rem <end of chdir> (end of epilog)
! rem Import directive found local:fchdir:fchdir:LABEL9_684003       |        ! rem Import directive found
local:fchdir:fchdir:LABEL9_1046340
! labeldefine LABEL9_684003                                          |        ! labeldefine LABEL9_1046340
! rem Import directive found local:syscall1:syscall1:LABEL1_999240    |        ! rem Import directive found
local:syscall1:syscall1:LABEL1_1149174
! labeldefine LABEL1_999240                                          |        ! labeldefine LABEL1_1149174
  rem                                                                |          rem
  rem Found function declare fchdir (stack = 4)                      |          rem Found function declare fchdir (stack = 4)
  rem                                                                |          rem

*** 341,350 ****                                                     |        --- 341,350 ----
  functionpostlude 4                                                 |          functionpostlude 4
  ret 4                                                              |          ret 4
  rem <end of fchdir> (end of epilog)                                |          rem <end of fchdir> (end of epilog)
! rem Import directive found local:getcwd:getcwd:LABEL10_684003       |        ! rem Import directive found
local:getcwd:getcwd:LABEL10_1046340
! labeldefine LABEL10_684003                                         |        ! labeldefine LABEL10_1046340
! rem Import directive found local:syscall2:syscall2:LABEL1_1421161   |        ! rem Import directive found
local:syscall2:syscall2:LABEL1_871234
! labeldefine LABEL1_1421161                                         |        ! labeldefine LABEL1_871234
  asm                                                                |          asm
  asm             syscall2:                                          |          asm             syscall2:
  asm             push %ebp                                          |          asm             push %ebp

*** 391,400 ****                                                     |        --- 391,400 ----
  functionpostlude 8                                                 |          functionpostlude 8
  ret 8                                                              |          ret 8
  rem <end of getcwd> (end of epilog)                                |          rem <end of getcwd> (end of epilog)
! rem Import directive found local:dup:dup:LABEL11_684003            |        ! rem Import directive found local:dup:dup:LABEL11_1046340
! labeldefine LABEL11_684003                                         |        ! labeldefine LABEL11_1046340
! rem Import directive found local:syscall1:syscall1:LABEL1_369739   |        ! rem Import directive found
```

```
local:syscall1:syscall1:LABEL1_233082
! labeldefine LABEL1_369739                                          |        ! labeldefine LABEL1_233082
  rem                                                                |          rem
  rem Found function declare dup (stack = 4)                         |          rem Found function declare dup (stack = 4)
  rem                                                                |          rem

*** 421,430 ****                                                     |        --- 421,430 ----
  functionpostlude 4                                                 |          functionpostlude 4
  ret 4                                                              |          ret 4
  rem <end of dup> (end of epilog)                                   |          rem <end of dup> (end of epilog)
! rem Import directive found local:dup2:dup2:LABEL12_684003          |        ! rem Import directive found
local:dup2:dup2:LABEL12_1046340
! labeldefine LABEL12_684003                                         |        ! labeldefine LABEL12_1046340
! rem Import directive found local:syscall2:syscall2:LABEL1_468266   |        ! rem Import directive found
local:syscall2:syscall2:LABEL1_1046549
! labeldefine LABEL1_468266                                          |        ! labeldefine LABEL1_1046549
  rem                                                                |          rem
  rem Found function declare dup2 (stack = 4)                        |          rem Found function declare dup2 (stack = 4)
  rem                                                                |          rem

*** 454,463 ****                                                     |        --- 454,463 ----
  functionpostlude 8                                                 |          functionpostlude 8
  ret 8                                                              |          ret 8
  rem <end of dup2> (end of epilog)                                  |          rem <end of dup2> (end of epilog)
! rem Import directive found local:execve:execve:LABEL13_684003      |        ! rem Import directive found
local:execve:execve:LABEL13_1046340
! labeldefine LABEL13_684003                                         |        ! labeldefine LABEL13_1046340
! rem Import directive found local:syscall3:syscall3:LABEL1_844774   |        ! rem Import directive found
local:syscall3:syscall3:LABEL1_689319
! labeldefine LABEL1_844774                                          |        ! labeldefine LABEL1_689319
  rem                                                                |          rem
  rem Found function declare execve (stack = 4)                      |          rem Found function declare execve (stack = 4)
  rem                                                                |          rem

*** 490,499 ****                                                     |        --- 490,499 ----
  functionpostlude 12                                                |          functionpostlude 12
  ret 12                                                             |          ret 12
  rem <end of execve> (end of epilog)                                |          rem <end of execve> (end of epilog)
! rem Import directive found local:_exit:_exit:LABEL14_684003        |        ! rem Import directive found
local:_exit:_exit:LABEL14_1046340
! labeldefine LABEL14_684003                                         |        ! labeldefine LABEL14_1046340
! rem Import directive found local:syscall1:syscall1:LABEL1_151642   |        ! rem Import directive found
local:syscall1:syscall1:LABEL1_634952
! labeldefine LABEL1_151642                                          |        ! labeldefine LABEL1_634952
  rem                                                                |          rem
  rem Found function declare _exit (stack = 0)                       |          rem Found function declare _exit (stack = 0)
  rem                                                                |          rem

*** 509,518 ****                                                     |        --- 509,518 ----
  functionpostlude 4                                                 |          functionpostlude 4
  ret 4                                                              |          ret 4
  rem <end of _exit> (end of epilog)                                 |          rem <end of _exit> (end of epilog)
! rem Import directive found local:getpid:getpid:LABEL15_684003      |        ! rem Import directive found
local:getpid:getpid:LABEL15_1046340
! labeldefine LABEL15_684003                                         |        ! labeldefine LABEL15_1046340
! rem Import directive found local:syscall0:syscall0:LABEL1_846019   |        ! rem Import directive found
local:syscall0:syscall0:LABEL1_323322
! labeldefine LABEL1_846019                                          |        ! labeldefine LABEL1_323322
  asm                                                                |          asm
  asm             syscall0:                                          |          asm             syscall0:
  asm             push %ebp                                          |          asm             push %ebp

*** 547,556 ****                                                     |        --- 547,556 ----
  functionpostlude 0                                                 |          functionpostlude 0
  ret 0                                                              |          ret 0
  rem <end of getpid> (end of epilog)                                |          rem <end of getpid> (end of epilog)
! rem Import directive found local:getppid:getppid:LABEL16_684003    |        ! rem Import directive found
local:getppid:getppid:LABEL16_1046340
! labeldefine LABEL16_684003                                         |        ! labeldefine LABEL16_1046340
! rem Import directive found local:syscall0:syscall0:LABEL1_954782   |        ! rem Import directive found
local:syscall0:syscall0:LABEL1_784356
! labeldefine LABEL1_954782                                          |        ! labeldefine LABEL1_784356
  rem                                                                |          rem
  rem Found function declare getppid (stack = 4)                     |          rem Found function declare getppid (stack = 4)
  rem                                                                |          rem

*** 574,583 ****                                                     |        --- 574,583 ----
  functionpostlude 0                                                 |          functionpostlude 0
  ret 0                                                              |          ret 0
  rem <end of getppid> (end of epilog)                               |          rem <end of getppid> (end of epilog)
! rem Import directive found local:getpgrp:getpgrp:LABEL17_684003    |        ! rem Import directive found
local:getpgrp:getpgrp:LABEL17_1046340
! labeldefine LABEL17_684003                                         |        ! labeldefine LABEL17_1046340
! rem Import directive found local:syscall0:syscall0:LABEL1_1236858  |        ! rem Import directive found
local:syscall0:syscall0:LABEL1_459145
! labeldefine LABEL1_1236858                                         |        ! labeldefine LABEL1_459145
  rem                                                                |          rem
  rem Found function declare getpgrp (stack = 4)                     |          rem Found function declare getpgrp (stack = 4)
  rem                                                                |          rem

*** 601,610 ****                                                     |        --- 601,610 ----
  functionpostlude 0                                                 |          functionpostlude 0
  ret 0                                                              |          ret 0
  rem <end of getpgrp> (end of epilog)                               |          rem <end of getpgrp> (end of epilog)
! rem Import directive found local:setsid:setsid:LABEL18_684003      |        ! rem Import directive found
local:setsid:setsid:LABEL18_1046340
! labeldefine LABEL18_684003                                         |        ! labeldefine LABEL18_1046340
! rem Import directive found local:syscall0:syscall0:LABEL1_618633   |        ! rem Import directive found
local:syscall0:syscall0:LABEL1_830786
```

```
! labeldefine LABEL1_618633                                          |        ! labeldefine LABEL1_830786
  rem                                                                |          rem
  rem Found function declare setsid (stack = 4)                      |          rem Found function declare setsid (stack = 4)
  rem                                                                |          rem

*** 628,637 ****                                                     |        --- 628,637 ----
  functionpostlude 0                                                 |          functionpostlude 0
  ret 0                                                              |          ret 0
  rem <end of setsid> (end of epilog)                                |          rem <end of setsid> (end of epilog)
! rem Import directive found local:getuid:getuid:LABEL19_684003      |        ! rem Import directive found
local:getuid:getuid:LABEL19_1046340
! labeldefine LABEL19_684003                                        |        ! labeldefine LABEL19_1046340
! rem Import directive found local:syscall0:syscall0:LABEL1_436755  |        ! rem Import directive found
local:syscall0:syscall0:LABEL1_918749
! labeldefine LABEL1_436755                                         |        ! labeldefine LABEL1_918749
  rem                                                                |          rem
  rem Found function declare getuid (stack = 4)                      |          rem Found function declare getuid (stack = 4)
  rem                                                                |          rem

*** 655,664 ****                                                     |        --- 655,664 ----
  functionpostlude 0                                                 |          functionpostlude 0
  ret 0                                                              |          ret 0
  rem <end of getuid> (end of epilog)                                |          rem <end of getuid> (end of epilog)
! rem Import directive found local:geteuid:geteuid:LABEL20_684003    |        ! rem Import directive found
local:geteuid:geteuid:LABEL20_1046340
! labeldefine LABEL20_684003                                        |        ! labeldefine LABEL20_1046340
! rem Import directive found local:syscall0:syscall0:LABEL1_689170  |        ! rem Import directive found
local:syscall0:syscall0:LABEL1_644144
! labeldefine LABEL1_689170                                         |        ! labeldefine LABEL1_644144
  rem                                                                |          rem
  rem Found function declare geteuid (stack = 4)                     |          rem Found function declare geteuid (stack = 4)
  rem                                                                |          rem

*** 682,691 ****                                                     |        --- 682,691 ----
  functionpostlude 0                                                 |          functionpostlude 0
  ret 0                                                              |          ret 0
  rem <end of geteuid> (end of epilog)                               |          rem <end of geteuid> (end of epilog)
! rem Import directive found local:getgid:getgid:LABEL21_684003      |        ! rem Import directive found
local:getgid:getgid:LABEL21_1046340
! labeldefine LABEL21_684003                                        |        ! labeldefine LABEL21_1046340
! rem Import directive found local:syscall0:syscall0:LABEL1_815707  |        ! rem Import directive found
local:syscall0:syscall0:LABEL1_530473
! labeldefine LABEL1_815707                                         |        ! labeldefine LABEL1_530473
  rem                                                                |          rem
  rem Found function declare getgid (stack = 4)                      |          rem Found function declare getgid (stack = 4)
  rem                                                                |          rem

*** 709,718 ****                                                     |        --- 709,718 ----
  functionpostlude 0                                                 |          functionpostlude 0
  ret 0                                                              |          ret 0
  rem <end of getgid> (end of epilog)                                |          rem <end of getgid> (end of epilog)
! rem Import directive found local:getegid:getegid:LABEL22_684003    |        ! rem Import directive found
local:getegid:getegid:LABEL22_1046340
! labeldefine LABEL22_684003                                        |        ! labeldefine LABEL22_1046340
! rem Import directive found local:syscall0:syscall0:LABEL1_756882  |        ! rem Import directive found
local:syscall0:syscall0:LABEL1_909771
! labeldefine LABEL1_756882                                         |        ! labeldefine LABEL1_909771
  rem                                                                |          rem
  rem Found function declare getegid (stack = 4)                     |          rem Found function declare getegid (stack = 4)
  rem                                                                |          rem

*** 736,745 ****                                                     |        --- 736,745 ----
  functionpostlude 0                                                 |          functionpostlude 0
  ret 0                                                              |          ret 0
  rem <end of getegid> (end of epilog)                               |          rem <end of getegid> (end of epilog)
! rem Import directive found local:setuid:setuid:LABEL23_684003      |        ! rem Import directive found
local:setuid:setuid:LABEL23_1046340
! labeldefine LABEL23_684003                                        |        ! labeldefine LABEL23_1046340
! rem Import directive found local:syscall1:syscall1:LABEL1_998957  |        ! rem Import directive found
local:syscall1:syscall1:LABEL1_632867
! labeldefine LABEL1_998957                                         |        ! labeldefine LABEL1_632867
  rem                                                                |          rem
  rem Found function declare setuid (stack = 4)                      |          rem Found function declare setuid (stack = 4)
  rem                                                                |          rem

*** 766,775 ****                                                     |        --- 766,775 ----
  functionpostlude 4                                                 |          functionpostlude 4
  ret 4                                                              |          ret 4
  rem <end of setuid> (end of epilog)                                |          rem <end of setuid> (end of epilog)
! rem Import directive found local:seteuid:seteuid:LABEL24_684003    |        ! rem Import directive found
local:seteuid:seteuid:LABEL24_1046340
! labeldefine LABEL24_684003                                        |        ! labeldefine LABEL24_1046340
! rem Import directive found local:syscall3:syscall3:LABEL1_397134  |        ! rem Import directive found
local:syscall3:syscall3:LABEL1_507838
! labeldefine LABEL1_397134                                         |        ! labeldefine LABEL1_507838
  rem                                                                |          rem
  rem Found function declare seteuid (stack = 4)                     |          rem Found function declare seteuid (stack = 4)
  rem                                                                |          rem

*** 800,809 ****                                                     |        --- 800,809 ----
  functionpostlude 4                                                 |          functionpostlude 4
  ret 4                                                              |          ret 4
  rem <end of seteuid> (end of epilog)                               |          rem <end of seteuid> (end of epilog)
! rem Import directive found local:setgid:setgid:LABEL25_684003      |        ! rem Import directive found
local:setgid:setgid:LABEL25_1046340
! labeldefine LABEL25_684003                                        |        ! labeldefine LABEL25_1046340
! rem Import directive found local:syscall1:syscall1:LABEL1_799825  |        ! rem Import directive found
local:syscall1:syscall1:LABEL1_977252
! labeldefine LABEL1_799825                                         |        ! labeldefine LABEL1_977252
```

```
  rem                                                                 |          rem
  rem Found function declare setgid (stack = 4)                       |          rem Found function declare setgid (stack = 4)
  rem                                                                 |          rem

*** 830,839 ****                                                      |        --- 830,839 ----
  functionpostlude 4                                                  |          functionpostlude 4
  ret 4                                                               |          ret 4
  rem <end of setgid> (end of epilog)                                 |          rem <end of setgid> (end of epilog)
! rem Import directive found local:setegid:setegid:LABEL26_684003     |        ! rem Import directive found
local:setegid:setegid:LABEL26_1046340
! labeldefine LABEL26_684003                                         |        ! labeldefine LABEL26_1046340
! rem Import directive found local:syscall3:syscall3:LABEL1_450553    |        ! rem Import directive found
local:syscall3:syscall3:LABEL1_880622
! labeldefine LABEL1_450553                                          |        ! labeldefine LABEL1_880622
  rem                                                                 |          rem
  rem Found function declare setegid (stack = 4)                      |          rem Found function declare setegid (stack = 4)
  rem                                                                 |          rem

*** 864,873 ****                                                      |        --- 864,873 ----
  functionpostlude 4                                                  |          functionpostlude 4
  ret 4                                                               |          ret 4
  rem <end of setegid> (end of epilog)                                |          rem <end of setegid> (end of epilog)
! rem Import directive found local:fork:fork:LABEL27_684003           |        ! rem Import directive found
local:fork:fork:LABEL27_1046340
! labeldefine LABEL27_684003                                         |        ! labeldefine LABEL27_1046340
! rem Import directive found local:syscall0:syscall0:LABEL1_1054372   |        ! rem Import directive found
local:syscall0:syscall0:LABEL1_1167266
! labeldefine LABEL1_1054372                                         |        ! labeldefine LABEL1_1167266
  rem                                                                 |          rem
  rem Found function declare fork (stack = 4)                         |          rem Found function declare fork (stack = 4)
  rem                                                                 |          rem

*** 891,900 ****                                                      |        --- 891,900 ----
  functionpostlude 0                                                  |          functionpostlude 0
  ret 0                                                               |          ret 0
  rem <end of fork> (end of epilog)                                   |          rem <end of fork> (end of epilog)
! rem Import directive found local:unlink:unlink:LABEL28_684003       |        ! rem Import directive found
local:unlink:unlink:LABEL28_1046340
! labeldefine LABEL28_684003                                         |        ! labeldefine LABEL28_1046340
! rem Import directive found local:syscall1:syscall1:LABEL1_1270972   |        ! rem Import directive found
local:syscall1:syscall1:LABEL1_850868
! labeldefine LABEL1_1270972                                         |        ! labeldefine LABEL1_850868
  rem                                                                 |          rem
  rem Found function declare unlink (stack = 4)                       |          rem Found function declare unlink (stack = 4)
  rem                                                                 |          rem

*** 945,957 ****                                                      |        --- 945,957 ----
  accumulator2memorylocal 4 4                                         |          accumulator2memorylocal 4 4
  loadint 8                                                           |          loadint 8
  arg 2                                                               |          arg 2
! jump LABEL5_636759                                                 |        ! jump LABEL5_382293
! labeldefine LABEL4_636759                                          |        ! labeldefine LABEL4_382293
  urlencoded HITHERE%0A                                               |          urlencoded HITHERE%0A
  databytes 0                                                         |          databytes 0
  archalign                                                           |          archalign
! labeldefine LABEL5_636759                                          |        ! labeldefine LABEL5_382293
! loadglobaladdress LABEL4_636759                                    |        ! loadglobaladdress LABEL4_382293
  arg 1                                                               |          arg 1
  loadint 1                                                           |          loadint 1
  arg 0                                                               |          arg 0


IL Metrics:                  cparse1           cparse2
Number of lines of IL:       966               966
Mean time to generate IL:    0.380026 secs     0.293140 secs      delta: 0.086886 secs
Percentage time differences: 129.64 %          77.14 %
```