ITCS 6144/8144 Course Project (Midterm Report)

Project Title: Understand Linux OS via Modern Tool (Systemtap)
Prepared by: Abdullah Al Raqibul Islam (UNCC ID # 801151189)

Project Overview: The main purpose of this project is to understand and observe the internal behaviors and performance characteristics of Linux operating system using systemtap tool.

Background Study: I have spent quality time for the background study which includes learning to write systemtap script to trace, study, and monitor the activities of the Linux operating system.

Platform: I have used centos7 to perform the necessary experiments. I have installed centos7 on a virtual machine (VirtualBox).

Work Done: So far, I have prepared several scripts to understand the behavior of system calls and process. Here I am giving the brief descriptions of the scripts

1. /scripts/systemcall/process_tracing.stp
    a. This script is prepared to gather in-depth knowledge about process. It includes log for tracking parent-child tree of a process. Detailed current process information (including executable files, command line arguments, environment variables, uid, gid, cpuid, etc.) also been included. Besides these I have also traced the time duration a process takes before the process actually starts to execute. Here is the sample output,

```
2029[    bash]/  5394[gnome-terminal-] kprocess.create
 2029[    bash]/  5394[gnome-terminal-] scheduler.process_fork
Parent ID: [2029] -> Child ID: [2053]
 2029[    bash]/  5394[gnome-terminal-] scheduler.wakeup_new
process_id [2029] took 221233 microseconds to be dispatched onto CPU first time
 2053[    bash]/  2029[    bash] kprocess.start
 2053[    bash]/  2029[    bash] kprocess.create
 2053[    bash]/  2029[    bash] scheduler.process_fork
Parent ID: [2053] -> Child ID: [2054]
 2053[    bash]/  2029[    bash] scheduler.wakeup_new
process_id [2053] took 421 microseconds to be dispatched onto CPU first time
 2053[    bash]/  2029[    bash] syscall.wait4
 2053[    bash]/  2029[    bash] scheduler.process_wait
 2054[    bash]/  2053[    bash] kprocess.start
 2054[    bash]/  2053[    bash] syscall.execve
 2054[    bash]/  2053[    bash] kprocess.exec
filename: "/usr/bin/uname"
 2054[   uname]/  2053[    bash] kprocess.exec_complete
 2054[   uname]/  2053[    bash] kprocess.exit
return code: 0
 2054[   uname]/  2053[    bash] scheduler.process_exit
 2053[    bash]/  2029[    bash] kprocess.release
```

2. /scripts/systemcall/syscall_count.stp
    a. This script is intended to collect system-call data for the whole system. It will show the top 20 <process, syscall> pair in every 10 seconds. Here is the sample output,

```
Collecting system-call data for the whole system
Top 20 <processes, syscall> pair will be displayed for the interval of 10 seconds
Type Ctrl+c to exit the program


            Process Name             Syscall Name  #Syscalls
                 polkitd                     poll      44075
                   crond                    close       4183
              gnome-shell                  recvmsg       3746
                    bash            rt_sigprocmask       2526
           gnome-terminal-                 recvmsg       2122
                       X                   recvmsg       1624
                       X                    writev       1502
                       X                 setitimer       1406
              gnome-shell                     poll       1394
           gnome-terminal-                    poll       1177
                       X                epoll_wait       1176
                   pidof                      read        797
                    bash             rt_sigaction        767
              gnome-shell                   writev        629
              gnome-shell                    write        526
                    gdbus                     poll        508
             InputThread                      read        503
                   pidof                     mmap2        427
                   gdbus                     write        425
                   pidof                     close        418
                         ***************<>***************
            Process Name             Syscall Name  #Syscalls
              gnome-shell                  recvmsg       1808
                       X                   recvmsg        912
           gnome-terminal-                 recvmsg        823
                       X                    writev        783
                       X                 setitimer        738
              gnome-shell                     poll        679
                       X                epoll_wait        600
           gnome-terminal-                    poll        476
           at-spi2-registr                 recvmsg        385
              gnome-shell                   writev        338
              gnome-shell                    write        207
             InputThread                      read        198
           at-spi2-registr                    poll        187
           accounts-daemon                   alarm        165
           accounts-daemon                    read        136
           accounts-daemon                   fcntl        110
           accounts-daemon             rt_sigaction        110
           gnome-terminal-                   writev         98
              gnome-shell                      read         85
           at-spi2-registr                   writev         84
                         ***************<>***************

Total Result:
            Process Name             Syscall Name  #Syscalls
                 polkitd                     poll      44076
              gnome-shell                  recvmsg       6036
                   crond                    close       4183
```

```
gnome-terminal-                  recvmsg       3163
             X                   recvmsg       2740
          bash            rt_sigprocmask       2528
             X                    writev       2494
             X                 setitimer       2316
    gnome-shell                      poll       2249
             X                 epoll_wait       1919
gnome-terminal-                      poll       1769
    gnome-shell                     writev       1052
          pidof                       read        797
    gnome-shell                      write        784
           bash                rt_sigaction        768
    InputThread                       read        757
          gdbus                       poll        587
          gdbus                      write        484
at-spi2-registr                   recvmsg        477
          pgrep                       open        445
```

3. /scripts/systemcall/syscall_count_arg.stp
    a. This script is intended to collect system-call data for the process passed by argument. It will show the top 20 syscalls by the corresponding process in every 10 seconds. Here is the sample output,

```
Collecting system-call data for the process: gnome-shell
Top 20 syscall by process [gnome-shell] will be displayed for the interval of 10 seconds
Type Ctrl+c to exit the program


        Process Name             Syscall Name  #Syscalls
         gnome-shell                  recvmsg       2804
         gnome-shell                     poll       1065
         gnome-shell                    writev        532
         gnome-shell                     write        316
         gnome-shell                      read        127
         gnome-shell                      stat         40
         gnome-shell                     fstat         14
         gnome-shell                    access          8
         gnome-shell                     mmap2          7
         gnome-shell                    munmap          7
         gnome-shell                     fcntl          7
         gnome-shell                      open          7
         gnome-shell                     close          7
                    ***************<>***************
        Process Name             Syscall Name  #Syscalls
         gnome-shell                  recvmsg       3436
         gnome-shell                     poll       1310
         gnome-shell                    writev        639
         gnome-shell                     write        415
         gnome-shell                      read        174
         gnome-shell                      stat         40
         gnome-shell                     fstat         28
         gnome-shell                    access         16
         gnome-shell                      open         15
         gnome-shell                     mmap2         14
         gnome-shell                    munmap         14
         gnome-shell                     fcntl         14
         gnome-shell                     close         14
         gnome-shell                    shmget          1
         gnome-shell                     shmat          1
         gnome-shell                    shmctl          1
         gnome-shell                     uname          1
```

```
                          ***************<>***************

Total Syscall Result for Process [gnome-shell]:
             Process Name              Syscall Name  #Syscalls
              gnome-shell                   recvmsg       7550
              gnome-shell                      poll       2858
              gnome-shell                     writev       1401
              gnome-shell                      write        862
              gnome-shell                       read        362
              gnome-shell                       stat        120
              gnome-shell                      fstat         52
              gnome-shell                       open         27
              gnome-shell                      mmap2         26
              gnome-shell                     munmap         26
              gnome-shell                      fcntl         26
              gnome-shell                      close         26
              gnome-shell                     access         24
              gnome-shell                     shmctl          2
              gnome-shell                     shmget          1
              gnome-shell                      shmat          1
              gnome-shell                      shmdt          1
              gnome-shell                      uname          1
```

4. /scripts/systemcall/syscall_count_by_pid.stp
5. /scripts/systemcall/syscall_count_by_proc.stp
6. /scripts/systemcall/syscall_count_by_name.stp
    a. These scripts are intended to collect system-call data by pid, process and syscall name respectively for the whole system. It will show the top 20 syscalls by the corresponding process in every 10 seconds. Here is a sample output,

```
Collecting system-call data for the whole system
Top 20 system-calls will be displayed for the interval of 10 seconds
Type Ctrl+c to exit the program


     Process ID  #Syscalls
           3401      10720
           4729       9701
           5394       5174
           3337       3153
           4703        372
              1        268
           2729        183
           4999        120
           1506         82
           2735         80
           1540         79
           2738         55
           4697         48
           4785         39
           5024         30
           3325         30
           4855         26
           2878         25
           4492         24
           3801         23
***************<>***************
     Process ID  #Syscalls
```

```
           3401       7299
           4729       5539
           5394       3634
           4703        452
           2729        182
           4697         54
           5024         32
           4492         28
           5353         27
           4855         26
           4936         26
           4999         23
           3325         22
           5465         12
           5038         12
           5040         12
           6894         12
           4894         12
           5325         11
           3323         10
***************<>***************
     Process ID  #Syscalls
           3401       8988
           4729       7066
           5394       4061
           4703        440
           4999        290
           1506        206
           5353        186
           2729        180
           5024         66
           4936         42
           3325         42
           2836         42
           4697         42
           2843         41
           5465         36
           5038         36
           5040         36
           6894         36
           4894         36
           4492         28
***************<>***************
     Process ID  #Syscalls
           4729       3036
           3401       3024
           5394        882
           2729        182
           4703        126
           5024         44
           4936         34
           4855         26
           5465         24
           5038         24
           5040         24
           6894         24
           4894         24
           3325         22
           4934         16
           4955         16
           4999         16
           4762         16
           4476         16
           4950         16
```

```
***************<>***************

Total Result:
     Process ID  #Syscalls
           3401      31418
           4729      26821
           5394      14394
           3337       3153
           4703       1454
           2729        770
           4999        453
           1506        288
              1        268
           5353        256
           5024        188
           4697        159
           4936        130
           3325        122
           4855        104
           4492         89
           4894         87
           5040         81
           2735         80
           1540         79
```

7. /scripts/systemcall/syscall_timetrace_by_proc.stp
    a. This script is intended to trace time spent in all system calls in a per-process way. It will show the top 20 results in every 10 seconds. Here is the sample output,

```
Trace time spent in all system calls in a per-process way
Top 20 processes will be displayed for the interval of 10 seconds
Type Ctrl+c to exit the program


            Process Name Duration spend on syscalls
            in:imjournal 9921023
                  stapio 9812568
             InputThread 9388594
                       X 9140344
          at-spi2-registr 9099752
                gsd-color 9024482
                    tuned 9020770
             dbus-daemon 8986363
                   gmain 7445831
                    pool 7204506
          gnome-terminal- 5877977
                      id 5153166
                     tty 5141856
                   fwupd 5013806
          goa-identity-se 5005354
          accounts-daemon 5005085
                   uname 4983496
                     sed 4974000
               dircolors 4970954
                    tput 4969359
                    grep 4966021
             grepconf.sh 4963662
                 systemd 4954934
                 timeout 4954402
           systemd-logind 4954076
```

```
              pkg-config 4950625
                      ls 4943581
                   pidof 4937188
                  mktemp 4935465
                   mkdir 4932854
   ****************<>****************

Total Result:
             Process Name Duration spend on syscalls
                   stapio 15019357
                gsd-color 14662398
             in:imjournal 14440552
              InputThread 14355048
          at-spi2-registr 14344276
                   tuned 14024956
                       X 13918862
              dbus-daemon 12175339
                   gmain 12101044
                   fwupd 10018168
                ssh-agent 10010540
           wpa_supplicant 10004632
          goa-identity-se 9998548
                    pool 9933708
                   gdbus 6846456
          gnome-terminal- 6277367
          accounts-daemon 6176405
          gnome-pty-helpe 5842846
                    bash 5358591
                      id 5153166
                     tty 5141856
                   uname 4983496
                     sed 4974000
                dircolors 4970954
                    tput 4969359
                    grep 4966021
             grepconf.sh 4963662
                 systemd 4954934
                 timeout 4954402
           systemd-logind 4954076
```