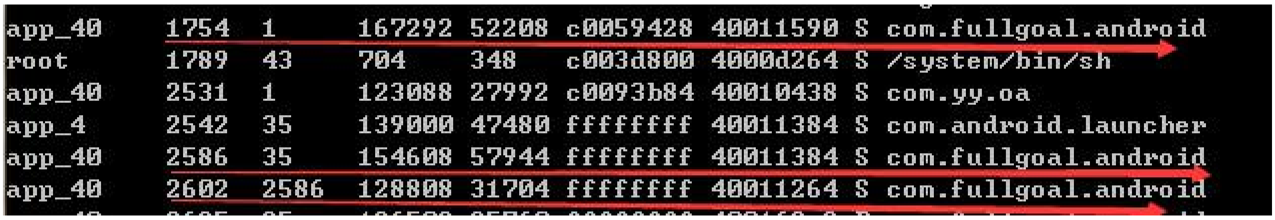
修改 fork.c 文件，实现不让 app fork 多个相同的进程，相互 ptrace

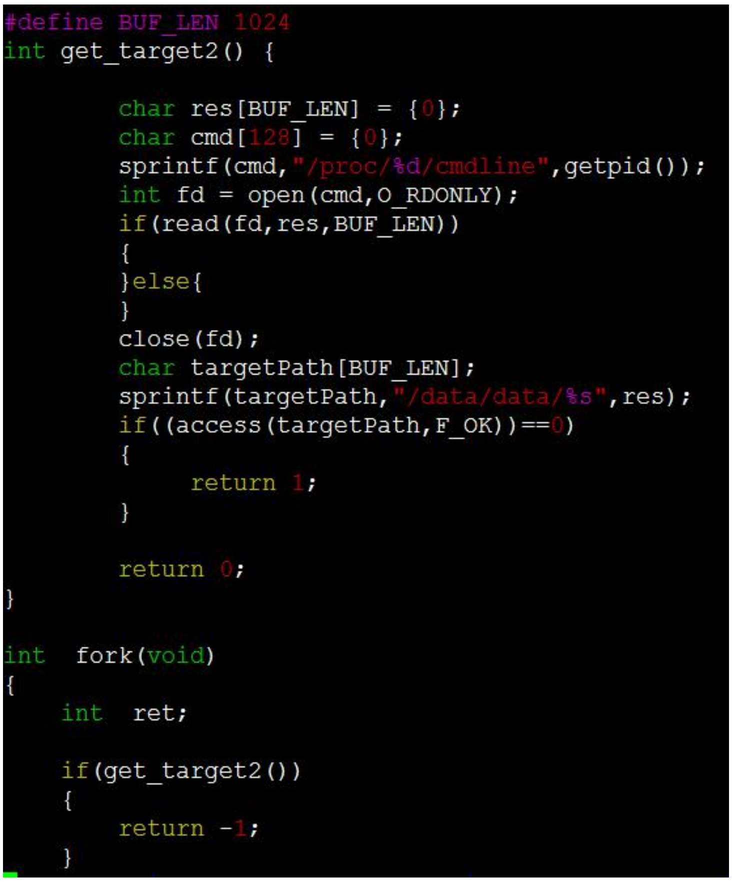
原理：多进程都是通过 fork 出来的，因此我们修改/bionic/libc/bionic/fork.c 里面的 fork 函数来使得目标进程 fork 失败

很多加固都采用多进程 ptrace 的方式来反调试：



```
app_40    1754  1     167292 52208 c0059428 40011590 S com.fullgoal.android
root      1789  43    704    348   c003d800 4000d264 S /system/bin/sh
app_40    2531  1     123088 27992 c0093b84 40010438 S com.yy.oa
app_4     2542  35    139000 47480 ffffffff 40011384 S com.android.launcher
app_40    2586  35    154608 57944 ffffffff 40011384 S com.fullgoal.android
app_40    2602  2586  128808 31704 ffffffff 40011264 S com.fullgoal.android
```

https://bbs.pediy.com/thread-211548.htm 中的基本思路



```
#define BUF_LEN 1024
int get_target2() {

        char res[BUF_LEN] = {0};
        char cmd[128] = {0};
        sprintf(cmd,"/proc/%d/cmdline",getpid());
        int fd = open(cmd,O_RDONLY);
        if(read(fd,res,BUF_LEN))
        {
        }else{
        }
        close(fd);
        char targetPath[BUF_LEN];
        sprintf(targetPath,"/data/data/%s",res);
        if((access(targetPath,F_OK))==0)
        {
             return 1;
        }

        return 0;
}

int  fork(void)
{
    int  ret;

    if(get_target2())
    {
        return -1;
    }
```

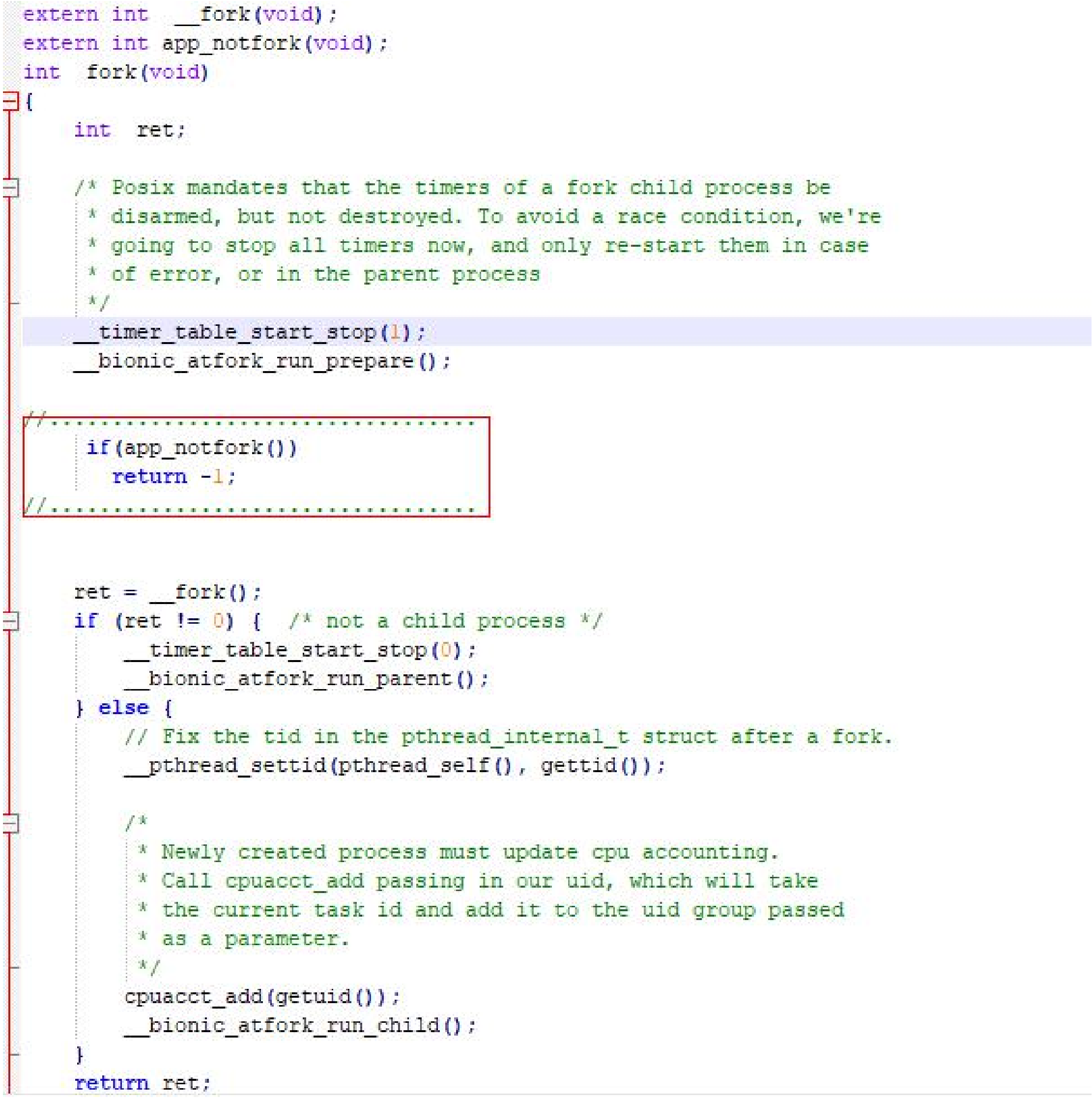
实现如下：

config.txt 中内容：target=0;fork=0;

target :appname ,

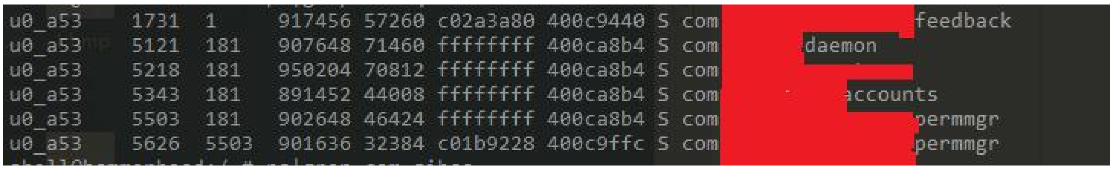
fork:fork=0 按系统原本运行;fork=1，并且 target=com.xx.xx ，则 fork 失败

```
#define bufflen 128
char* getcmdline()
{
    char res[bufflen]={0};
    char cmd[bufflen]={0};
    sprintf(cmd,"/proc/%d/cmdline",getpid());
    int fd=open(cmd,O_RDONLY);
    if(fd){
        read(fd,res,bufflen);
    }
    close(fd);
    return res;
}
int gettarget()
{

    char targetPath[bufflen]={0};
    sprintf(targetPath,"/data/data/%s",getcmdline());
    if(access(targetPath,F_OK)==0){
        //the main process
        return 1;
    }
    return 0;
}
int app_notfork()
{

if(gettarget()==1){//is app com.xx.apk
    initconfigdata();

if(userdefineFork&&strlen(userdefineTarget)>=1&&strcmp(userdefineTarg
et,"0")!=0&&strncmp(getcmdline(),userdefineTarget,
strlen(userdefineTarget))==0) {
       return 1;
    }
  }
return 0;
}
```

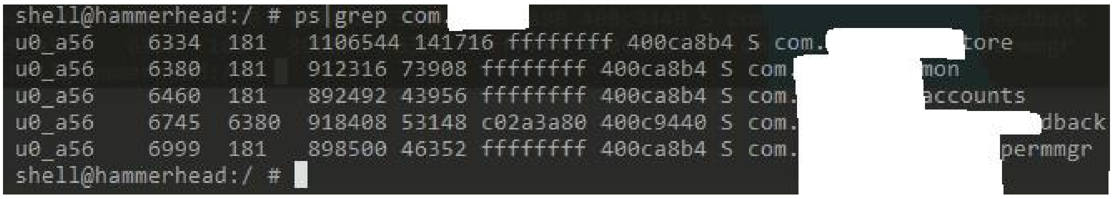


```
extern int  __fork(void);
extern int app_notfork(void);
int  fork(void)
{
    int  ret;

    /* Posix mandates that the timers of a fork child process be
     * disarmed, but not destroyed. To avoid a race condition, we're
     * going to stop all timers now, and only re-start them in case
     * of error, or in the parent process
     */
    __timer_table_start_stop(1);
    __bionic_atfork_run_prepare();

//..................................
     if(app_notfork())
       return -1;
//..................................


    ret = __fork();
    if (ret != 0) {  /* not a child process */
        __timer_table_start_stop(0);
        __bionic_atfork_run_parent();
    } else {
        // Fix the tid in the pthread_internal_t struct after a fork.
        __pthread_settid(pthread_self(), gettid());

        /*
         * Newly created process must update cpu accounting.
         * Call cpuacct_add passing in our uid, which will take
         * the current task id and add it to the uid group passed
         * as a parameter.
         */
        cpuacct_add(getuid());
        __bionic_atfork_run_child();
    }
    return ret;
```

实现效果如下：



```
u0_a53    1731  1     917456 57260 c02a3a80 400c9440 S com[redacted]feedback
u0_a53    5121  181   907648 71460 ffffffff 400ca8b4 S com[redacted]daemon
u0_a53    5218  181   950204 70812 ffffffff 400ca8b4 S com[redacted]
u0_a53    5343  181   891452 44008 ffffffff 400ca8b4 S com[redacted]accounts
u0_a53    5503  181   902648 46424 ffffffff 400ca8b4 S com[redacted]permmgr
u0_a53    5626  5503  901636 32384 c01b9228 400c9ffc S com[redacted]permmgr
```



```
shell@hammerhead:/ # ps|grep com[redacted]
u0_a56    6334  181   1106544 141716 ffffffff 400ca8b4 S com.[redacted]tore
u0_a56    6380  181   912316 73908 ffffffff 400ca8b4 S com.[redacted]mon
u0_a56    6460  181   892492 43956 ffffffff 400ca8b4 S com.[redacted]accounts
u0_a56    6745  6380  918408 53148 c02a3a80 400c9440 S com.[redacted]dback
u0_a56    6999  181   898500 46352 ffffffff 400ca8b4 S com.[redacted]permmgr
shell@hammerhead:/ #
```

参见：https://bbs.pediy.com/thread-211548.htm

附件：修改的文件

userconfig.h　fork.c　userconfig.c