原 Linux 获取随机数

2014年01月12日 10:54:04 阅读数：5968

- 伪随机法

伪随机法就是通过一个确定性的算法来获取看似随机或者乱序，在计算伪随机序列时，如果使用的开始值不变化的，实际上获取到的随机序列的值顺序是保持不变。例如在C中比较常用的随机函数rand()，是比较典型的伪随机法。

在调用rand()函数时，没有显示的调用srand()函数来设置随机序列开始种子的话，默认随机序列的种子即为1，此时的随机序列为：1804289383

846930886、1681692777、1714636915、1957747793、424238335、719885386、1649760492。

rand()函数是实现在glibc库中，运行于用户态，运行效率比较高效；

- 真随机法

真随机法，在在计算机环境中，主要是依赖于计算机环境中的背景操作，例如来自驱动程序或者其他来源的背景噪声。真随即法具有不可预测和再现性，原因在于产生随机数的操作系统所处的环境充满了未知性。在Linux中，/dev/random产生的是真正的随机数序列。

随机函数发生器通过驱动程序或者其他来源来获取环境噪声来计算出一个随机数，同时将产生的随机数放入到随机数池中，每次需要随机数时，从池中获取一个数据数即可，如果随机池已空，从/dev/random读取数据时，将会被阻塞，直到新的随机数被放入到池中才会返回，这个地方无疑是个巨大的坑，当面对大量的请求需要随机数时。

/dev/unrandom，也是从随机池中获取一个随机数，与/dev/random的区别点在于随机池为空时，随机数的程度不够高。

调用/dev/(u)random获取随机数的方法，相比rand()方法效率会低很多，每获取一次random值，均需要发起一次系统调用，来调用该值。

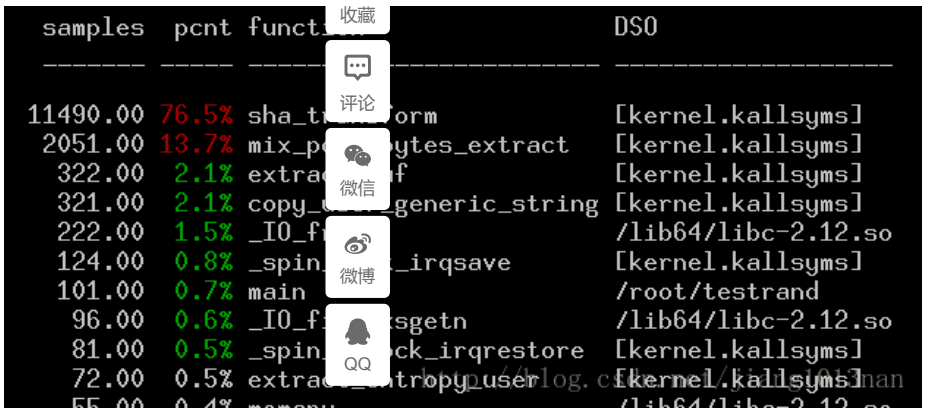
示例代码为：

```
FILE *fs_p = NULL;

fs_p = fopen ("/dev/urandom", "r");

    fread(&seed, sizeof(int), 1, fs_p);  //obtain oneunsigned int data
     fclose(fs_p);
```

针对这段代码计算分析，会大量大量的计算性能消耗于内核态：



个人分类： Linux

查看更多>>

想对作者说点什么？ 我来说一句

linux下 C语言随机数生成方法rand（产生随机数）

#include #include #include main() { int i,j; srand((int)time(0)); for(i=0;i

zhanweizhao_111 2014-07-16 16:32:13 阅读数：5686

linux产生随机数

//---------- rand函数 函数rand()是真正的随机数生成器，而s...

imxiangzi 2012-07-03 10:15:56 阅读数：32659

C/C++中产生随机数(rand,srand用法)

计算机的随机数都是由伪随机数，即是由小M多项式序列生成的，其中产生每个小序列都有一个初始值，即随机种子。（注意： 小M多项式序列的周期是65535，即每次利用一个随机种子生成的随机数的周期...

zxh2075 2016-09-09 16:37:22 阅读数：3097

linux C语言获取随机数rand()和srand(time(NULL))介绍

linux C语言获取随机数rand()和srand(time(NULL))介绍 一、在使用rand()产生随机数时，产生的是0~RAND_MAX（该值与平台有关，至少为3276 7，我下...

qq_37858386 2017-12-05 17:10:22 阅读数：360

从Linux内核中获取真随机数

内核随机数产生器 Linux内核实现了一个随机数产生器，从理论上说这个随机数产生器产生的是真随机数。与标准C库中的rand(),srand()产生的伪随机数不同，尽管伪随机数带有一定的随机特...

adamska0104 2015-05-15 12:23:00 阅读数：1068

Linux下随机数生成的常见方法

众所周知，利用Linux下的rand函数可以生成范围在0到RAND_MAX（在stdlib.h中定义，值为2147483647）的数值，但是一般来讲，为了达到更好的随机效果，需要利用srand函数设置...

chenlilong84 2013-10-15 11:46:25 阅读数：7554

Linux产生随机数

原转载地址：http://jimmyleeee.blog.163.com/blog/static/930961820071135224556 3/ 一、rand函数 函数rand()是真正的...

hongwazi_2010 2015-01-14 15:41:05 阅读数：1269

shell实例浅谈之三产生随机数七种方法

shell随机数

taiyang1987912 2014-10-11 19:53:01 阅读数：24890

在linux下如何较好的生成随机数

#include #include #include #include using namespace std; int main() { int iRandNum = -1; ...

tenfyguo 2012-11-05 19:12:14 阅读数：4329

关于linux下的随机数

在linux下取随机数，当然可以简单的用rand函数，不过要注意的是一定要设置好种子，否则伪随机数就会变成非常伪的随机数。设置种子，一般就用time函数返回当前时间即可。一般来讲，这样的做法基本上就可...

x86 2008-04-07 15:24:00 阅读数：11724

linux随机数原理

http://www.mutepig.club/index.php/archives/61/ 这里是原理的推导，下面根据dalao的writeup，贴出py代码 看雪CTF秋季赛第四题Ne...

kevin66654 2017-11-18 15:32:40 阅读数：131

Linux 生成随机数

在bash下，有时需要用到随机数，但是我们怎么获取呢？有如下方法可以使用： 1、通过bash变量获取 [root@vm3 ~]# echo $RANDOM 2417 [roo t...

m0_38020436 2017-08-22 10:27:47 阅读数：113

Linux命令学习：随机数

在日常生活中，随机数实际上经常遇到，想丢骰子，抓阄，还有抽签。呵呵，非常简单就可以实现。那么在做程序设计，真的要通过自己程序设计出随机数那还真的不简单了。现在很多都是操作系统内核会提供相应的api，这...

qdx411324962 2015-02-12 12:30:28 阅读数：1018

如何获取大量随机数

获取大量随机数给程序做测试

Code_star_one 2017-04-05 22:25:33 阅读数：201

关于“使用rand()产生的随机数每次得到的结果相同”的问题

之前使用rand()产生随机数出现了一个怪问题，一直没能理解 初次出现的随机数数列是1111 5556 3543 6434 3245 再次运行，产生的结果仍然是1111 5556 3543 643...

qq_28301007 2016-01-22 18:03:52 阅读数：2079

shell 生成指定范围随机数与随机字符串

shell 生成指定范围随机数与随机字符串 1.使用系统的 $RANDOM 变量 fdipzone@ubuntu:~$ echo $RANDOM 17617 $RANDOM 的范围是 [...

fdipzone 2014-04-22 22:17:25 阅读数：76016

linux系统产生随机数的6中方法

linux系统产生随机数的6种方法 1、通过系统环境变量($RANDOM)实现 [root@i-1pbhgm8j ~]# echo $RANDOM | md5sum | cut -c 5-11 3ed...

m0_37814112 2017-10-09 15:46:56 阅读数：516

Linux中的随机数文件 /dev/random /dev/urandom

Linux中的随机数可以从两个特殊的文件中产生，一个是/dev/urandom.另外一个是/dev/random。他们产生随机数的原理是利用当前系统的熵池来计算出一定数量的随机比特，然后将这些比特作为...

redheavenliu 2017-03-10 10:16:31 阅读数：151

linux下的c语言的随机数算法代码

在linux下取随机数，当然可以简单的用rand函数，不过要注意的是一定要设置好种子，否则伪随机数就会变成非常伪的随机数。设置种子，一般就用time函数返回当前时间即可。一般来讲，这样的做法基本上就...

lchunli 2009-11-07 16:02:00 阅读数：2476

linux_shell 中，产生随机数的方法

如何在linux中用命令产生一个范围内的随机数？ 在shell中有一个环境变量RANDOM,它的范围是0--32767如果我们想要产生0-25范围内的数，如何做呢？如下：$RANDOM%26 用这个...

baludejia 2010-07-14 20:43:00 阅读数：3473

个人资料

鱼翅1013 关注

原创	粉丝	喜欢	评论
172	191	4	147

等级： 博客 6 访问： 75万+

积分： 7067 排名： 4156

最新文章

gdb小结

个人分类

归档

热门文章

最新评论

tiramisu_L：没有运行结果吗？把运行结果分享一下？