RANDOM(4) Linux Programmer's Manual RANDOM(4)

NAME

random, urandom - kernel random number source devices

DESCRIPTION

The character special files **/dev/random** and **/dev/urandom** (present since Linux 1.3.30) provide an interface to the kernel's random number generator. File **/dev/random** has major device number 1 and minor device number 8. File **/dev/urandom** has major device number 1 and minor device number 9.

The random number generator gathers environmental noise from device drivers and other sources into an entropy pool. The generator also keeps an estimate of the number of bits of noise in the entropy pool. From this entropy pool random numbers are created.

When read, the **/dev/random** device will only return random bytes within the estimated number of bits of noise in the entropy pool. **/dev/random** should be suitable for uses that need very high quality randomness such as one-time pad or key generation. When the entropy pool is empty, reads from **/dev/random** will block until additional environmental noise is gathered.

When read, **/dev/urandom** device will return as many bytes as are requested. As a result, if there is not sufficient entropy in the entropy pool, the returned values are theoretically vulnerable to a cryptographic attack on the algorithms used by the driver. Knowledge of how to do this is not available in the current non-classified literature, but it is theoretically possible that such an attack may exist. If this is a concern in your application, use **/dev/random** instead.

CONFIGURING

If your system does not have **/dev/random** and **/dev/urandom** created already, they can be created with the following commands:

```
mknod -m 644 /dev/random c 1 8
mknod -m 644 /dev/urandom c 1 9
chown root:root /dev/random /dev/urandom
```

When a Linux system starts up without much operator interaction, the entropy pool may be in a fairly predictable state. This reduces the actual amount of noise in the entropy pool below the estimate. In order to counteract this effect, it helps to carry entropy pool information across shut-downs and start-ups. To do this, add the following lines to an appropriate script which is run during the Linux system start-up sequence:

```
echo "Initializing kernel random number generator..."
# Initialize kernel random number generator with random seed
# from last shut-down (or start-up) to this start-up.  Load and
# then save 512 bytes, which is the size of the entropy pool.
if [ -f /var/random-seed ]; then
     cat /var/random-seed >/dev/urandom
fi
dd if=/dev/urandom of=/var/random-seed count=1
```

Also, add the following lines in an appropriate script which is run during the Linux system shutdown:

```
# Carry a random seed from shut-down to start-up for the random
# number generator.  Save 512 bytes, which is the size of the
# random number generator's entropy pool.
echo "Saving random seed..."
dd if=/dev/urandom of=/var/random-seed count=1
```

FILES

/dev/random
/dev/urandom

AUTHOR

The kernel's random number generator was written by Theodore Ts'o (tytso@athena.mit.edu).

SEE ALSO

mknod (1)
RFC 1750, "Randomness Recommendations for Security"

Linux 1997-08-01 RANDOM(4)