Random Number Generation on Linux Systems

How does it work ?

Technical Terminology

- Entropy
- Special files on Linux distributions
- Pseudorandom number generation (PRNG)
- Seed (in a random number generator context)

What is the entropy ?

The entropy means a measurable physical property that is particularly associated with a state of ***disorder***, ***randomness***, ***uncertainty*** *or even* ***chaos***.

Example in computer science

String 1 : `aiK!l0bUMud5?2`

String 2 : `aaaAbkkKmmB99b`

Example in computer science

String 1 : `aiK!l0bUMud5?2` ← Better entropy

String 2 : `aaaAbkkKmmB99b`

What are the special files on Linux distributions ?

*A **device file** or **special file** is an interface to a **device driver** that appears in a file system as if it were an ordinary file.*

Block devices

```
/dev/sda
/dev/nvme
/dev/vda
/dev/cdrom
```

Characters devices

```
/dev/random
/dev/urandom
/dev/zero
/dev/ttyX # where X is a number
```

Why we talk about "*pseudo-random*" generation ?

Pseudo-random number generation creates a sequence of numbers that approximates the properties of perfect random numbers as closely as possible. It's based on ***mathematical algorithms****.*

What is a seed in pseudo-random number generation ?

*The seed is the **entry point** of the pseudo-random generation algorithm. This value is defined explicitly by the user or directly with a default value like the system timestamp for example. The purpose of the seed is to allow the user to **lock** the pseudo-random number generator, to **prevent replicable analysis**.*

/dev/random vs /dev/urandom

The most common special files to generate random numbers

/dev/random

- High entropy quality
  → Blocks the reading process if the entropy isn't enough
- Can rely on hardware peripherals

Used to generate SSH keys, for LUKS encryption...

/dev/urandom

- Lower entropy quality
  → Doesn't block the reading process no matter how much entropy
- Better to use for long processes

Used to wipe disks (shred command for example)

Other random data source devices

Not implemented on every Linux distributions

- **/dev/arandom** : Generates high-quality pseudo-random output data (based on RC4)
- **/dev/prandom** : Simple pseudo-random generator
- **/dev/srandom** : This device returns reliable random data even if sufficient entropy is not currently available (based on MD5)

Any questions ?