Random Number Generators

Alec Parten

COSC 462 Project

Fall 2017

Introduction

- Random numbers
- Used for
  - Cryptography
  - Simulations
  - Procedural Generation

Randomness

- Unpredictable
- Difficult to generate actual randomness
  - Easy to generate pseudo-randomness
- Can be “gathered” from the environment

Pseudo-random number generators

- Actual random data is hard to produce efficiently
- Pseudo-Random Number Generators (PRNGs)
  - Seeded with a value
  - Apparently random sequence
  - Actually deterministic
  - Can be seeded with actual randomness for secure usage

True random number generators

- Non-deterministic
- Gather randomness from the environment
  - Atmospheric noise
  - Radioactive decay
  - Basic computer inputs
  - Others
- Slow

Operating System APIs

- /dev/random on UNIX and Linux
  - random blocks, urandom does not
- Linux uses a custom RNG for both /dev/urandom and /dev/random
  - Cryptographically Secure Pseudo Random Number Generator (CSPRNG)
  - Seeded and reseeded from entropy pool
  - /dev/random blocks when estimated entropy is low

References & Links

- Dr. Mads Haahr, Introduction to Randomness and Random Numbers
  - https://www.random.org/randomness/
- Thomas Hühn, “Myths about /dev/urandom”
  - https://www.2uo.de/myths-about-urandom/