SEED Security Labs : Cryptography
Pseudo Random Number Generator Lab

Matthew Chin

August 2025

0 Introduction

This project is a guided lab by *SEED Security Labs*, exploring pseudo-random number generation, and when/how it is appropriate for certain situations such as encryption keys and secret generation.
Random number generation is fundamental in modern computing and is necessary in various situations like simulations, statistical modeling, and secure/private communications. This is a lab focused on increasing security, because in encryption we desire not just any sequence of random numbers (which may be adequate for situations like the Monte Carlo Simulation), we want some control over that sequence to actually be able to use it. Developers should know how to generate *secure* random numbers, avoiding mistakes like weak or predictable randomness in well-known products like *Netscape* and *Kerberos*.
This lab and project explores the differences between catch-all-type random number generation and cryptographically safe, secure random number generation. By exploring common mistakes and failed algorithms for random number generation, attempting key-recovery attacks, and analyzing entropy sources within a Linux OS (Ubuntu 20.4 VM), this entire process investigates the challenges of achieving **true randomness** in software. Experiments are also conducted using `/dev/random` and `/dev/urandom` to provide some insight into how certain operating systems manage entropy, the pros and cons of blocking or not blocking random sources, and their effects on security.
The objective of the lab is to build an understanding of how pseudo-random numbers are generated within software, why the insecure methods are inadequate, and how to properly use system-level randomness to strengthen cryptographic systems through hands-on experiments within a controlled Linux OS.

1 Pseudo-Random