ECE 471 Lab 3

MD5 Collision Attack Lab

Mitchell Dzurick

3/9/2020

Github with all documentation - `https://www.github.com/mitchdz/ECE471`

Contents

Secret Key Encryption Lab

1 Overview

Generating random numbers is a quite common task in security software. In many cases, encryption keys are not provided by users, but are instead generated inside the software. Their randomness is extremely important; otherwise, attackers can predict the encryption key, and thus defeat the purpose of encryption. Many developers know how to generate random numbers (e.g. for Monte Carlo simulation) from their prior experiences, so they use the similar methods to generate the random numbers for security purpose. Unfortunately, a sequence of random numbers may be good for Monte Carlo simulation, but they may be bad for encryption keys. Developers need to know how to generate secure random numbers, or they will make mistakes. Similar mistakes have been made in some well-known products, including Netscape and Kerberos.

In this lab, students will learn why the typical random number generation method is not appropriate for generating secrets, such as encryption keys. They will further learn a standard way to generate pseudo random numbers that are good for security purposes. This lab covers the following topics:

- Pseudo random number generation
- Mistakes in random number generation
- Generating encryption key
- The /dev/random and /dev/urandom device files

Lab Environment. This lab has been tested on our pre-built Ubuntu 12.04 VM and Ubuntu 16.04 VM, both of which can be downloaded from the SEED website.

2 Lab Tasks