Project Thor

Team Members:
Adonay Pichardo
Jared Blanco
Josh Temel
Luke Boneburger

Faculty Advisor:
Dr. Sid Bhattacharyya

Client:
Dr. Amitabh Nag

FLORIDA TECH

Motivation

Today's society has grown more and more dependent on the use of computers and this trend doesn't seem to be slowing down anytime soon. Along with this increased use of computers comes an increased importance for the data being transmitted and stored by these computers to be secure. Designing the methods used by computers to create encryption keys that are practically immune to attacks has proven to be a very complicated (if not impossible) challenge that computer scientists still struggle with today and random numbers lie at the root of the problem.

Computers primarily use pseudo-random numbers which are created using a mathematical formula that produces a deterministic, periodic sequence of numbers, which is completely dependent on the initial state or seed. However, today's computing systems are powerful enough to predict the random numbers being generated by PRNGs within a reasonable amount of time. This has placed an increased emphasis on finding a truly non-deterministic process which we believe may be found in the use of natural phenomena to inject true randomness.

Goal

- Develop a web application that allows users to generate encryption keys with high-entropy, truly random data that is gathered from the study of lightning strikes.

Key Features

Feature 1: Automated Data Transfer

The original data set will be provided to us via ASCII text files. Much of the data within this file is unusable due to its predictable nature. Only a few data types will be potentially useful for this project. Therefore, to make them more easily accessed and usable, the web application will automatically parse the relevant data from the ASCII files and add it into our working database from which the web application will be able to generate random numbers.

Feature 2: Random Number Generator

The web application, using the random data gathered in the database, will be able to algorithmically generate random numbers. These random numbers will be theoretically less predictable than those produced by pseudo-random number generators currently being used as the seed data being pulled from the database is considered to be random by nature.

Feature 3: Create Encryption Keys

Users will be able to use our web application to create cryptographic keys. These keys will be generated using the random number generator mentioned above and should be very secure due to the fact that they were developed using numbers and data sets that have a higher degree of entropy (randomness) than those typically employed by other modern cryptographic algorithms.

Technical Challenges

1. Automating raw data entry into the database.
2. Measuring entropy.
3. Creating a random number generator using multiple parameters drawn from the data set.
4. Integrating a strong encryption algorithm that uses our random number generator.
5. Learning how to use chosen website backend option.
6. Learning about integrating backend to database.

Novel Features

Novel Feature 1: Collected Data

The original data set that will be collected, sorted, and transferred into our database is a novel feature to our project as it will have a degree of randomness inherent to it due to it being based directly from lightning. A natural phenomena that is highly abundant yet very unpredictable.

Milestone 1 - Oct 4

- Find tools and options for
  - Frontend
  - Backend
  - Database
  - Encryption algorithm
- Demo
  - Automating raw data entry into the database.
  - Creating a random number generator using multiple parameters drawn from the data set.
  - Integrating a strong encryption algorithm that uses our random number generator
  - Learning how to use chosen website backend option
  - Learning about integrating backend to database

Milestone 2 - Nov 1

- Implement, test, and demo:
  - automated data transfer from raw data
  - user request for key
    - Ie: show server request for secure key in backend
  - 1 case of random number generator with lightning data implemented
  - use of the random number in encryption

Milestone 3 - Nov 29

- Implement, test, and demo:
  - real time data transfer from raw data stream
  - user request for key and display secure key
  - generating many keys
  - use of the random key in encryption