Project Thor

Team Members:

Name	Email
Adonay Pichardo	apichardo2019@my.fit.edu
Jared Blanco	jblanco2018@my.fit.eud
Josh Temel	jtemel2018@my.fit.edu
Luke Boneburger	lboneburger2018@my.fit.edu

Faculty Advisor:

Name	Email
Sid Bhattacharyya	sbhattacharyya@fit.edu

Client:

Name	Email
Amitabh Nag	anag@fit.edu

Date(s) of Meeting(s) with Client:

Date	Topic
September 3, 2021	● Better understanding the dataset

Goals & Motivation:

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(s)

Our overall goal for this project is to 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.

Approach:

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.

Novel Features

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.

Technical Challenges

This project is relatively simple in the sense that there is not a lot seen in the deliverables (web application and database), but it does come with a lot of technical challenges for our team to work through. Many of these challenges will be found in data analysis. However, there are also some computer science challenges that will need to be met as well. These are listed below:

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

Milestone 1 (Oct 4): itemized tasks:

A. Compare and select technical tools
   a. Website Backend Options
      i. AWS
      ii. Local server
      iii. NET

    iv. Python Django

    v. Flask

  b. Website Frontend Options

    i. Angular JS

    ii. React

  c. Database Options

    i. mySQL

    ii. PostgreSQL

    iii. MS SQL server

  d. Encryption Algorithm

    i. RSA

    ii. MD5 or MD4

    iii. AES

B. Provide demos to using chosen options to show:

  a. Importing raw data to database

  b. Display data from database to user on web browser

  c. Small presentation detailing the entropy found in the data set thus far.

C. Resolve technical challenges

  a. Create cloud based server environment for application testing

  b. Setting up backend option to add raw data to database

  c. Designing our key generator using a well known algorithm

  d. Explore the entropy of the data set.

D. Compare and select collaboration tools for software development, documents/presentations, communication, task calendar

  a. Software development: GitHub

  b. Documents/Presentations: Google Drive (docs and slides)

  c. Communication: Private Discord Server

  d. Task Calendar: GitHub Projects/Google Calendar

E. Create Requirements Document

F. Create Design Document

G. Create Test Plan

Milestone 2 (Nov 1): itemized tasks:

A. Implement, test, and demo automated data transfer from raw data

B. Implement, test, and demo user request for key

  a. Ie: show server request for secure key in backend

C. Implement, test, and demo 1 case of random number generator with lightning data implemented

D. Implement, test, and demo use of the random number in encryption

Milestone 3 (Nov 29): itemized tasks:

A. Implement, test, and demo real time data transfer from raw data stream
B. Implement, test, and demo user request for key and display secure key
C. Implement, test, and demo generating many keys
D. Implement, test, and demo use of the random key in encryption

Task Matrix for Milestone 1

Task	Adonay	Jared	Josh	Luke
Compare and select technical tools	Encryption Algo	Database	Database	Web
"Hello world" demos	Small presentation showing the entropy found thus far	Small presentation showing the entropy found thus far	Entering raw data to database	Showing connection from website to database working
Resolve technical challenges	Data Set Entropy	Data Set Entropy	Cloud based testing environment	Setting up backend
Compare and select collaboration tools	Establish Git repository	None	Establish Google Drive	Web Development IDE
Requirement document	Write 25%	Write 25%	Write 25%	Write 25%
Design document	Review & Proofread	Review & Proofread	Write 50%	Write 50%
Test plan	Write 50%	Write 50%	Review & Proofread	Review & Proofread

Approval from Faculty Advisor

"I have discussed with the team and approve this project plan. I will evaluate the progress and assign a grade for each of the three milestones."

Signature: <u>on file</u>_____ Date: _____