Capstone Project-II

Academic Year- 2021-22

SRS

Password Entry Profiling

Group Members

1. Vidyam Sreevathsav Sharma BT18GCS077
2. Siddhartha Adapa BT18GCS071
3. Raghunath V BT18GCS208
4. Malla Vimal Sanathan BT18GCS205
5. K Harshitha BT18GCS087

Contents:

Introduction

Purpose:

This is the Software Requirements Specification(SRS) for password entry profiling, a concept where we authenticate a user by their way of typing The time it takes between keystrokes in milliseconds, and the time spent on pressing the keys and the start. The purpose of this document is to convey information about the application's requirements to the reader both functional and non-functional. This document provides detailed information about the application and its working environment.

Document Convention:

- Users: The users of the project. This includes people who are trying to authenticate.
- Python: Python is an interpreted high-level general-purpose programming language
- Pandas: pandas is a software library written for the Python programming language for data manipulation and analysis.
- Keystroke Dynamics: Keystroke dynamics is the study of the typing patterns of people to distinguish them from one another, based on these patterns.
- Hold time – time between press and release of a key.
- Keydown-Keydown time – time between the pressing of consecutive keys.
- Keyup-Keydown time – time between the release of one key and the press of the next key.

Intended Audience and Reading Suggestions:

This document is intended for Software Engineers and Developers. One will be able to get a detailed insight into the system that is to be developed and its purpose. We suggest you read this document using the standard top-to-bottom approach. If you have a good understanding of how SRS documents are done, please feel free to pick any topic from the contents section and start reading.

Project Scope:

- We use password authentication for different websites but what if other users know your password there is a chance of the user taking over your account. So we solve this authentication problem by using a concept called Keystroke Dynamics.

- The way one user enters the password is different from the way another user enters the password. An authentic user profile can be created for every password change. The time it takes between keystrokes in milliseconds, and the time spent on pressing the keys and the start and completion of the password can be used to create a profile that can be compared with another user's password entry . If there is a doubt another factor of verification can be used.

Overall Description

Product Perspective:

The product is an Authenticator made use in Authenticating a User to a website safely. This Authentication method most depends on the concept of keystroke Dynamics. It is the study of the typing patterns of people to distinguish them from one another, based on these patterns. Every user has a certain way of typing that separates him from other users; for example, for how long does a user press the keys, how much time between consecutive key presses, etc.No additional hardware is required to collect keystrokes; only a keyboard. Keystroke dynamics, together with security measures already in place (eg, password) can hence serve as a convenient 2-factor authentication.

Product Functions:

The function of the Product developed is to verify the identity of users on the basis of their keystroke information. A model will be first trained by providing it with the typing patterns of the users to be enrolled, multiple patterns per user. The model is then provided with test patterns from the user as well as others posing as that user. The model should be able to reject the imposters while accepting the genuine user based on the test pattern's similarity to the trained model for the user. We will test various detectors which provide different ways of measuring this similarity.

Operating Environment:

This Product can be used on any website which has passwords for authentication.

Tools and Technology:

For Developing this Authenticator The following Tools and Technology would be required-

- No additional hardware is required to collect keystrokes; only a keyboard,Keystroke dynamics, together with security measures already in place (eg, password) can hence serve as a convenient 2-factor authentication.
- Keystroke dynamics, keystroke biometrics, typing dynamics and lately typing biometrics, refer to the detailed timing information which describes exactly when each key was pressed and when it was released as a person is typing at a computer keyboard.
- Programming Language: Python
- Libraries: Panda, Numpy,etc..

Functional requirements

- SRS001 Login

Users will be able to login using their User ID and Password.

- SRS002 Password Profiling

Profiling the Users by the concept of Keystroke Dynamics.

- SRS003 Register

Registering new users.

System Design