Problem Statement

The most widely used means of granting access to a computing system is through passwords. The issue of “guessing” passwords has been addressed through password standards. However, once compromised it is impossible to tell if the computer system is being accessed by an unauthorized individual.

The purpose of Dynamic Keystroke Authentication is to strengthen the password by employing the biometric characteristics of keyboard usage. Those characteristics are: key press duration and key transition time. The hypothesis is that the biometric characteristics are sufficiently different between individuals that they can act as an additional, real time, authentication mechanism.

Experimental Design

The typical biometric design requires that:

- An enrollment process is created that captures and extracts the relevant features that are to be used as the baseline or template of authentication.

- An operational process is created that employs the biometric in which the “test” data is captured, features extracted and compared to the enrolled templates. The case here is a 1 to 1 match.

Enrollment Design

The password to be used for enrollment is created by each individual. The password will be at least 6 characters and less than 15. The enrollment model will be that of n consecutive passes of entry of the password by the individual. Extracted from each pass will be the time to depress the key, time of transition to the next key and the total duration of entry.

- Key(d) = Duration of the ith character in the password
- KeyTrans(i) = Transition of time from the ith character in the password to the ith +1 character in the password
- Time = Total time of entry of the entire password
The feature vector will then be:

\[
\text{Feature} = f(\text{Key}(d)) \text{ where } d = 1 \text{ to } n \) (\text{KeyTrans}(i) \text{ where } i = 1 \text{ to } n-1) .
\]

It is anticipated the total time will be used to normalize transition and key press times.

**Operational Design**

On entry of the password, the same features will be captured for that specific password which had been previously enrolled. The feature vector will be compared to the enrolled base. Mismatches will be recorded. The authentication match is done against the password now associated with the feature template for the associated individual.

**Further Areas of Research**

Should the method outlined, which is highly constrained, prove viable the possibility exists of broadening the role of Dynamic Keystroke Authentication. By either additional enrollment or learning from usage authentication of an individual during actual usage can be attempted. This will address the more subtle issue of usage of an idle but not logged of system.