:-:-: Keystroke Dynamics - Benchmark Data Set :-:-:

Accompaniment to "Comparing Anomaly-Detection Algorithms for Keystroke Dynamics" (DSN-2009)

by
Kevin Killourhy and Roy Maxion
(click to show email)

Contents:

This webpage is a benchmark data set for keystroke dynamics. It is a supplement to the paper "Comparing Anomaly-Detection Algorithms for Keystroke Dynamics," by Kevin Killourhy and Roy Maxion, published in the proceedings of the DSN 2009 conference [1]. The webpage is organized as follows:

Sections 1 – 4 each consist of a brief explanation of their contents, followed by a list of common questions that provide more detail about the material. Click on a question to show the answer, or display all answers by clicking on:

- *SHOW / HIDE answers to all questions below.*

1. Introduction

On this webpage, we share the data, scripts, and results of our evaluation so that other researchers can use the data, reproduce our results, and extend them; or, use the data for investigations of related topics, such as intrusion, masquerader or insider detection. We hope these resources will be useful to the research community.

Common questions:

- *Q1-1: What is keystroke dynamics (or keystroke biometrics)?*
- *Q1-2: What is your paper about? What is this webpage for?*
- *Q1-3: Where can I find a copy of the paper?*
- *Q1-4: How would I cite this webpage in a publication?*

2. The Data

The data consist of keystroke-timing information from 51 subjects (typists), each typing a password (`.tie5Roanl`) 400 times.

- `DSL-StrongPasswordData.txt` (Fixed-width format) .... MD5 hash = e5b72954c2e093a0a4ec7ca1485f9d05

- DSL-StrongPasswordData.csv (Comma-separated-value format) MD5 hash = 470235f96568f28f9ea0da62234ec857
- DSL-StrongPasswordData.xls (Excel format) .... MD5 hash = e1a69b03315664d5dcaefd52583d6ad9

Common questions:

- *Q2-1: How were the data collected?*
- *Q2-2: How do I read the data into R / Matlab / Weka / Excel / ...?*
- *Q2-3: How are the data structured? What do the column names mean? (And why aren't the subject IDs consecutive?)*

3. Evaluation Scripts

The following procedure—written in the *R* language for statistical computing (www.r-project.org)—demonstrates how to use the data to evaluate three anomaly detectors (called Euclidean, Manhattan, and Mahalanobis).

- evaluation-script.R

Note that this script depends on the R package ROCR for generating ROC curves [2].

Common questions:

- *Q3-1: What does the script really do? Can you explain the steps of the evaluation?*
- *Q3-2: How do I download R / install packages / run the script?*
- *Q3-3: Why does the script only have code for three anomaly detectors?*
- *Q3-4: What other kinds of anomaly detectors can be evaluated using these scripts?*
- *Q3-5: What if I want to do a different evaluation using the data?*

4. Table of Results

The following table ranks 14 anomaly detectors based on their average equal-error rates. The evaluation procedure described in the script above was used to obtain the equal-error rates for each anomaly detector. For example, the average equal-error rate for the scaled Manhattan detector (across all subjects) was 9.62%, and the standard deviation was 0.0694.

Detector	Average Equal-Error Rate (stddev)
Manhattan (scaled)	0.0962 (0.0694)
Nearest Neighbor (Mahalanobis)	0.0996 (0.0642)
Outlier Count (*z*-score)	0.1022 (0.0767)
SVM (one-class)	0.1025 (0.0650)
Mahalanobis	0.1101 (0.0645)
Mahalanobis (normed)	0.1101 (0.0645)
Manhattan (filter)	0.1360 (0.0828)
Manhattan	0.1529 (0.0925)
Neural Network (auto-assoc)	0.1614 (0.0797)
Euclidean	0.1706 (0.0952)
Euclidean (normed)	0.2153 (0.1187)
Fuzzy Logic	0.2213 (0.1051)
k Means	0.3722 (0.1391)

Neural Network (standard)	0.8283 (0.1483)

Note that these are results are fractional rates between 0.0 and 1.0 (not percentages between 0% and 100%).

Common questions:

- *Q4-1: How do I interpret this table of results?*
- *Q4-2: Why do you use the average equal-error rate as the sole measure of performance?*
- *Q4-3: Do you plan to update the table with new results?*

5. References

[1] Kevin S. Killourhy and Roy A. Maxion. "Comparing Anomaly Detectors for Keystroke Dynamics," in Proceedings of the 39th Annual International Conference on Dependable Systems and Networks (DSN-2009), pages 125-134, Estoril, Lisbon, Portugal, June 29-July 2, 2009. IEEE Computer Society Press, Los Alamitos, California, 2009. (pdf)

[2] T. Sing, O. Sander, N. Beerenwinkel, T. Lengauer. "ROCR: visualizing classifier performance in R," *Bioinformatics* 21(20):3940-3941 (2005). (link)

This material is based upon work supported by the National Science Foundation under grant numbers CNS-0430474 and CNS-0716677, and by the Army Research Office through grant number DAAD19-02-1-0389 to Carnegie Mellon University's CyLab. Any opinions, findings, conclusions, or recommendations expressed in this material are those of the authors, and do not necessarily reflect the views of the National Science Foundation or the Army Research Office.