International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2014): 5.611

Keystroke Dynamics: Data Analysis of the Typing Features in Password Typing and Inferences

Adrian Kllogjeri[1], Qamil Kllogjeri[2]

[1]Statistician, Arval UK Ltd, Swindon, UK

[2]MSc in Applied Econometrics, Kingston University, UK

Abstract: ***This paper is about data analysis with regard to the durations and latencies and the average time used in typing different passwords by different users. To analyze all data are used different estimates, geometric representations and error tables. All the data provided by professor Patrick Bours, University of Gjovik, Norway, are time scores of typing 3 passwords "pr7q1z", "drizzle", and "jeffrey allen" by 103 participants, each typing all the three passwords at least 3 times, few typing passwords many times. There are more than 23,000 scores. There is also Timing AND Pressure information. We have presented many tables and diagrams in order to easily and clearly read, understand and interpret our data (data speak). This information processed with programs and outputted with tables and diagrams will be available to many students or specialists of Information Security, Statistics and other similar fields to use them in their study or research work or in their field of interest. The presence of several tables and diagrams, with very few comments, is purposely done in order to be available for people of interest.***

Keywords: keystroke dynamics, PIN or password security, errors analysis, cleansing of data

1. Introduction

Keystroke dynamics studies the process of typing, specially the way a user types on a keyboard (not what is typed but how is typed a text), and the problem of identifying the user based on his/her typing pattern. A person‟s typing pattern is unique depended on personal neuro-physiological factors. Keystroke dynamic can identify and authenticate the person typing on a keyboard by comparing the typing of a person against a stored template. The user stored template is created before he/she can use the system or an ATM. The user template is result of many tries of typing a password or a longer text and the average typing pattern is stored as the user template [1].

The most common features to describe a user‟s typing pattern are: the elapsed time between the release of a key and the press (or hit) of the next key (this time intervals called "**latency**"), the **duration** of each keystroke which is the time a key is held down, finger placement and its pressure on the keys, the typing speed which depends mainly on the long experience with typing [2]-[4]. Keystroke dynamics is linked with the process of determining whether a user can have access to a particular system in order to use it such as: a bank account, an important institution, a library etc. This process is named authentication and it is a critical area of security research and practice.

During this last decade, alongside with the advance of the computer science and information security is noticed a continuous increase of the number of system and particularly of ATM attackers. As a consequence the passwords and PINs need more advanced safeguards against unauthorized access to information and computer resources. The biometric recognition has been applied to identify criminals, to track the patients in medical informatics, to personalize social services and to do other things [5], [6].

The method of biometric data recording is followed by the invention of biometric tools that enable the recognition of individuals as friend or as foe.

In spite of the successes, there still remain unresolved questions about the effectiveness and management of systems for biometric recognition. The keystroke dynamics is part of biometric recognition and unresolved questions as well, and needs further intense efforts with regard to the protection and securing of the passwords and PINs.

The most common analysis about the dynamic keystroke features is the one with regard to the sums of durations and latencies during the typing of the passwords by creating templates, making calculations, constructing DET (Detection or Decision Error Trade-off) curves and drawing conclusions. **Our main concern** is to analyze all data in general using different estimates, geometric representations and error tables and do interpretation about the data in order to have them into consideration in further researches linked with the keystroke dynamic. On the other hand, we will provide some useful information, derived from the typing tests, about the keystroke dynamic. This information will be available for many other students or specialists of Information Security and of other similar fields, to use them in their study or research work or in their field of interest.

2. Definitions and Notations

The interest is about the events on the keyboard that are initiated by a user. The raw biometric data, for keystroke dynamics, is a chronologically ordered list of events. The following concepts are essential for our analysis. The **event** is generated by an action on the key which is: **press** when the key is pressed or **release** when the key is released. **Duration** is the amount of time a key is pressed. For a key the duration is computed as following:

$$duration = time\{RELEASE\} - time\{PRESS\} = Td$$

time{RELEASE} and time{PRESS} correspond to the same key.

Latency is computed by getting the difference of time between two keys events. That can be **P-P (Press-Press)** latency which is the difference of time between the pressures of each key, o*r* **R-R (Release-Release)** latency which is the difference of time between the release of each key, **R-P (Release-Press)** latency which is the difference of time between the release of one key and the pressure of the next one [2]-[4]. The following notations are very important notations of our analysis:

Time: Time (in mili-seconds) when the key is pressed down or released

Duration: Time Td a key is pressed down

Latency: Time Tl or T(R-P) between release of a key and pressure of the next key:
latency = time{PRESS }−time{Release } = T(R-P);
time{RELEASE} and time{PRESS} correspond to the neighbour keys.

3. General Analysis and Information

Analyzing the three passwords “jeffrey allen”, “pr7q1z” and “drizzle” using R software we have estimated the average time each password is used by each of the 103 participants. Each one of them has typed several times the three passwords [7]. The collected data show that: “drizzle” is typed 911 times, average time 1251 and standard deviation 565. We form the triple (911, 1251, 565). “jeffrey allen” is typed 902 times, average time 2196 and standard deviation 1133. We form the triple (902, 2196, 1133). “pr7q1z” is typed 923 times, average time 2760 and standard deviation 1451. We form the triple (923, 2760, 1451).

There is not too much difference between the numbers of typing of the passwords. The maximum difference is 21. It is reasonable that the average time of “jeffrey allen” be longer than the two others because it has double of characters, but we are stunned by “pr7q1z”. This password has required more than a double of the average time used for the password “drizzle”. Their lengths change by one character only. The users face much more difficulties in typing “pr7q1z”. Based on the positions of the buttons on the keyboard related to the characters of these two passwords we think there are two reasons:

Firstly, in typing “pr7q1z” the user has to use his hands (fingers) in alternative way while in typing “drizzle” not, also there is repetition of one character. The use of the organism parts in alternative way takes longer time.

Secondly, as the experience shows the number keys are used much less than the letter keys. The experience shows that the most of the time and the most of the people type texts. From this observance we have to take into consideration what type of characters someone chooses in forming a password.

Regarding the standard deviations they are approximately half of their respective average time. This is not a good indication for the spread of the time values. The standard deviations have to be much smaller. It is so in this case because we don‟t believe that our data come from a normal population.

3.1 Analysis based on averages and variability of the typing time

The following outputs and results are generated using R program [8]. Using R, also EXCEL are generated tables, diagrams and graphs.

Password Analysis: the mean, standard deviation, written times and password lengths (table 1).

Table 1: Av. time, St. Dev. and wr. times of each password

Password	*Average Time / Password*	*St.Dev / Password*	*Written Times*	*Password Length*
drizzle	1251.45225	564.9613981	911	7
jeffrey allen	2196.474501	1132.298105	902	13
pr7q1	2760.092091	1450.516842	923	5

From the above table the Password "pr7q1" has a written time Average and Standard Deviation bigger than the other passwords. It is clear from the graph below as well, that the Password that contains numeric values takes more time to be typed, regardless the password length (Look at Fig.1).

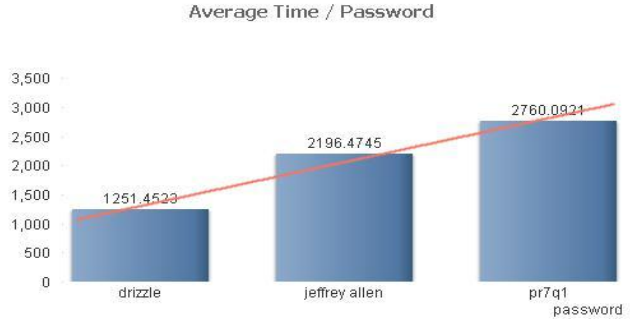

Figure 1: Diagram of Table 7(average time only)

Pizza diagram for relative frequency of each password

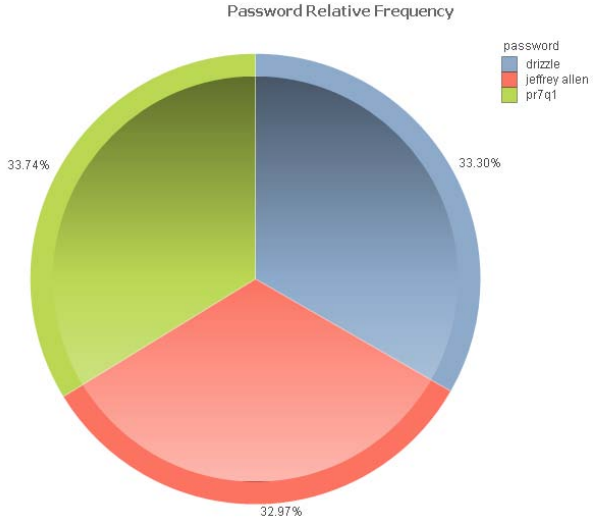

Figure 2: Diagram of relative frequencies

The diagram shows that passwords have almost the same frequency, leading to very efficient conclusions.

3.2 Normal Distribution Assumption and Inferences

If we consider that the Writing (Typing) Time follows the Normal Distribution with the Mean and Standard Deviation as shown in the table above then, using the respective Normal Distribution graphs (blue for *drizzle*, red for *jeffrey allen* and green for *pr7q1*) we are able to find the probability that a User can write the password in the Writing Time simulated as in the Table 2, below.

Table 2: Probabilities for every 100 time units

Typing Time	*drizzle*	*Jeffrey allen*	*pr7q1*
0	6.07E+00	5.37E+00	4.50E+00
100	8.85E+00	6.35E+00	5.12E+00
200	0,000124956	7.44E+00	5.79E+00
300	0,000171009	8.67E+00	6.53E-01
400	0,000226817	0,000100079	7.32E+00
500	0,000291558	0,000114684	8.17E+00
600	0,000363218	0,000130399	9.07E+00
700	0,000438535	0,000147116	0,000100318
800	0,000513139	0,000164686	0,000110375
900	0,000581913	0,000182922	0,000120864
1000	0,000639551	0,0002016	0,000131723
1100	0,000681218	0,000220458	0,000142876
1200	0,000703218	0,000239206	0,000154239
1300	0,000703538	0,000257533	0,000165716
1400	0,000682149	0,00027511	0,000177203
1500	0,000641008	0,000291603	0,000188587
1600	0,00058377	0,000306684	0,000199751
1700	0,000515244	0,000320038	0,000210574
1800	0,000440736	0,00033138	0,000220929
1900	0,000365373	0,000340457	0,000230695
2000	0,000293555	0,000347065	0,0002397517
2100	0,000228578	0,000351053	0,000247981
2200	0,000172494	0,000352328	0,000255277
2300	0,000126155	0,00035086	0,000261541
2400	8.94E+00	0,000346684	0,000266689
2500	6.14E+00	0,000339896	0,000270648
2600	4.09E+00	0,000330652	0,000273365
2700	2.64E+00	0,00031916	0,000274799
2800	1.65E+00	0,000305674	0,00027493
2900	1.00E+00	0,000290483	0,000273758
3000	5.87E-01	0,000273902	0,000271298
3100	3.34E-01	0,000256262	0,000267586
3200	1.84E-01	0,000237895	0,000262673
3300	9.86E-03	0,000219128	0,000256627
3400	5.11E-02	0,000200273	0,000249532
3500	2.57E-02	0,000181619	0,000241482
3600	1.25E-02	0,000163423	0,000232584
3700	5.89E-03	0,000145907	0,000222952
3800	2.69E-03	0,000129257	0,000212705
3900	1.19E-03	0,000113617	0,000201967
4000	5.12E-04	9.91E+00	0,000190862
4100	2.13E-04	8.58E+00	0,000179512

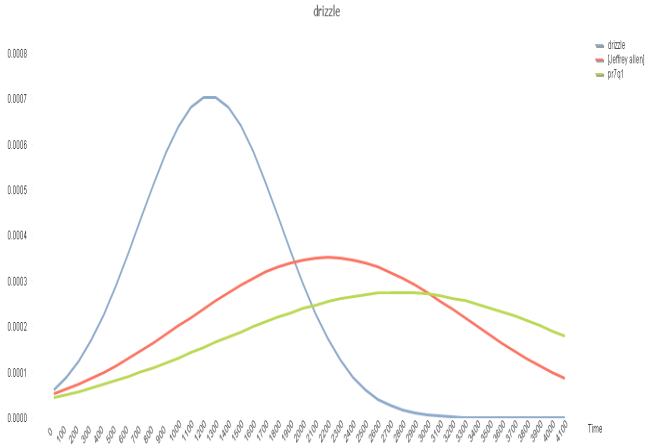

Figure 3: Normal curves of the three passwords

The normal distribution curves (Fig. 3) are generated by the program. So, the normal curve (blue) corresponds to the password “drizzle” with mean 1251.5 and standard deviation 565. From the data about the written time of the three passwords, got from the mean time population and generated by the tests of 103 users, the maximum time length of typing a password is 4100 time units. In the table above (Table 2) are generated probabilities for every 100 time units.

Inference: From the Probability Graph we can conclude that the Users can type password "drizzle" faster while not differing in Time. For password "jeffrey allen" is very clear that Time deviation from the Mean is bigger than what we had in password "drizzle. This is due to the length of the Password, which makes a big sample with size 902 Users, number which varies in Time.

3.3 Analysis of Errors

Are observed two types of errors: I. Done during typing or errors of Switching between the buttons, II. Errors with regard to the starting and the stopping time.

I. Errors of Switching between the buttons
In Table 3 are shown the switches done by the users during the typing of the three passwords, the average numbers of switches performed and their respective standard deviations.

Inferences: From this table we can see that the data contain some errors, as none of the passwords has a letter "n" followed by a "p", an "e" followed by a "d" and an "z" followed by a "p". But the table shows such switches that are shown in red at the bottom of the table such as n-p, e-d, z-p??!!! The user has typed wrongly. Maybe there are other wrong switches in the main data.

These letters have been wrongly typed because of the typing speed or careless or the finger has simultaneously pressed two keys as in the case e-d where the keys are neighbors.

Table 3: Errors during typing

Switching Buttons	*Average*	*Standard Deviation*
f-f	113,6219512	53,28398657
z-z	114,6546053	77,03948694
d-r	120,1480263	90,60441646
a-l	64,49445676	92,99876166
e-n	55,28381375	95,76283681
j-e	97,07095344	115,8266504
r-e	21,87361419	115,9381729
l-e	86,27673649	123,3250162
l-l	118,2605322	125,3806005
z-l	107,3684211	160,1297711
Space-a	97,25277162	167,1269874
e-f	151,2605322	176,6932222
i-z	225,0142544	190,9521777
e-y	107,4068736	194,5960547
f-r	211,3292683	201,6542001
p-r	214,3275676	239,4910498
y-Space	134,6219512	245,5976472
1-z	425,0389189	270,7265249
r-i	112,5888158	293,8654658
q-1	334,3081081	361,7169752
7-q	672,8421622	577,8896045
r-7	683,5362162	640,5986479
n-p	16936	-
e-d	-106	-
z-p	415	-

Table 4: Time of switch between the buttons after cleansing

Switching Buttons	*Average*	*Standart Deviation*
p-r	214,3275676	239,4910498
r-7	683,5362162	640,5986479
7-q	672,8421622	577,8896045
q-1	334,3081081	361,7169752
1-z	425,0389189	270,7265249
j-e	97,07095344	115,8266504
e-f	151,2605322	176,6932222
f-f	113,6219512	53,28398657
f-r	211,3292683	201,6542001
r-e	21,87361419	115,9381729
e-y	107,4068736	194,5960547
y-Space	134,6219512	245,5976472
Space-a	97,25277162	167,1269874
a-l	64,49445676	92,99876166
l-l	118,2605322	125,3806005
l-e	86,27673649	123,3250162
e-n	55,28381375	95,76283681
d-r	120,1480263	90,60441646
r-i	112,5888158	293,8654658
i-z	224,9374314	191,0429657
z-z	114,6546053	77,03948694
z-l	107,3684211	160,1297711

Cleansing the Data

It is necessary to clean the data from these errors in order to avoid bias to the estimates. After cleansing the Data, we can make a Summary for the Time needed to switch between the buttons as is shown in Table 4 and the respective diagram: Fig. 4.

II. Errors with regard to the starting and the stopping time (Table 5)

In the table below are shown the starting and the stopping time for the characters of the passwords. From all the data with starting and stopping time, here in this table, are set apart those cases when the starting time of the password does not relate to the stopping time of the previous password typed. These cases are shown in red color. Having a granular look at the data shown in the table below, we can see that the starting time that the User with the ID = "1268930220" writes the password "pr7q1z" has been given wrongly, that is why it is in red. We have to consider the observations relating with this user ID, as outliers. The same thing can be said about the other two users shown in this table who type wrongly.

Table 5: outliers in observed data

entry_id	*Start*	*stop*	*key_char*
1268930220	19137	19249	p
1268930220	19488	19600	r
1268930220	19756	19826	7
1268930220	21512	21617	q
1268930220	22068	22233	1
1268930220	23124	23250	z
1268934158	1163	1219	d
1268934158	1388	1430	r
1268934158	1571	1613	i
1268934158	1908	1936	z
1268934158	2035	2077	z
1268934158	2148	2204	1
1268934158	2318	2362	e
1268927242	2618	2693	p
1268927242	3834	3918	r
1268927242	4241	4311	7
1268927242	5608	5781	Q
1268927242	5751	5842	1
1268927242	6112	6187	Z

Inferences: the outliers cause biasing to the estimates.

We have to remove these outliers [3], otherwise we commit biasing our estimates. From Table 5, we can see that the starting time of the password "pr7q1z" is not related with the stopping time of the previous password. These three cases are considered as outliers and will be removed from the data in order to have more precise estimates of data.

3.4 Analysis of the switching time between letters and between letters and numbers

The program generated the following summary table (Table 6) regarding the average time of switching from letters to numbers and vice versa and from letters to letters. We can see that the average time to type the numbers is bigger than typing letters.

Table 6: The percentage of switching average time

Switching to Numbers	528,9313514
Switching between Letters	119,5987957
Difference in %	0,773885977

Conclusion

We can conclude that the average time of switching from numbers to letters, and from letters to numbers is approximately 77% (Table 6) bigger than the average time of switching from letters to letters.

Problems with huge time differences between the buttons

In the following table (Table 7) are set aside those cases when there are huge differences in time between the stopping time of a button kept pressed and the starting time of the next key pressed. There are two cases, shown in red, that must be considered.

Table 7: Huge time differences between the keys

entry_id	*start*	*Stop*	*key_char*
1268544897	0	56	d
1268544897	196	252	r
1268544897	8150	8210	i
1268544897	8540	8585	z
1268544897	8690	8765	z
1268544897	8855	8930	l
1268544897	8975	9065	e
1268926710	0	135	p
1268926710	315	435	r
1268926710	871	983	7
1268926710	3020	3188	q
1268926710	3732	3882	l
1268926710	4617	4752	z

Having a closer look, anyone can spot at the biggest differences between the keys. We cannot explain why is that.

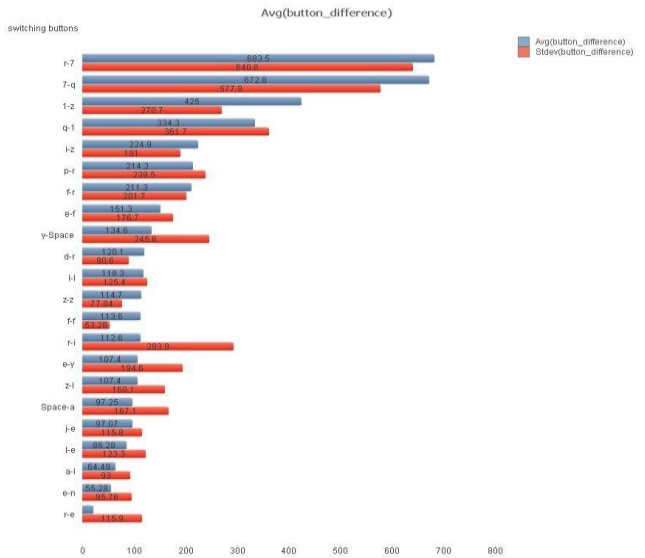

Figure 4: Diagram of average time differences between the keys

Suggestion for solution: The best suggestion is resetting the starting time to zero. Than the differences between the keys with regard to time will be the same, even we reset to zero the starting time.

Analysis of the average time differences between the keys

In the Table 4, above, are shown the average time differences for all the switches between the keys, also their respective standard deviations. Anyone can easily interpret their meanings. For example, the average time of switching from r to 7 is 683.5 and its standard deviation is 640.6 (these are the highest values). We can say that this is not a usual and normal thing to be accepted because the standard deviation is so close to the average value of switching time. The cases with considerable differences are logically acceptable.

3.5 Key Analysis

In the following table (Table 8) are shown the average, minimum and maximum time for each key corresponding to the characters of the passwords. For easier grasp look at the respective diagram: Fig. 5. It is clearly and easily readable.

Table 8: Average, minimum and maximum duration time

Key	*Average Time*	*Minimum Time*	*Maximum Time*
1	67,83891892	14	182
7	64,54378378	14	154
A	83,21286031	28	168
D	72,64473684	14	168
E	80,71614151	14	210
F	52,63747228	14	126
I	65,36951754	19	155
J	66,50997783	15	180
L	59,21023564	14	180
N	64,59866962	14	271
P	66,81837838	15	165
Q	78,81189189	14	224
R	76,95910916	14	210
Y	69,65742794	14	168
Z	70,72135322	14	210
Space	77,70731707	15	182

In Figure 4 is displayed the diagram of average time differences between the keys, showing the average of durations for each key, or the average time that a key is kept pressed down during the typing. From the diagram we understand and conclude that the keys "F" and "L" are the keys that are pressed and released more quickly. The results are shown in Table 9 where is calculated the average time for the two keys "F" and "L" and the average time for the rest.

Table 9: "F" and "L" keys and the rest

Keys	*Average Time*
F & L	55,92385396
The Rest of the keys	71,865006
Time Ratio	0,285051028

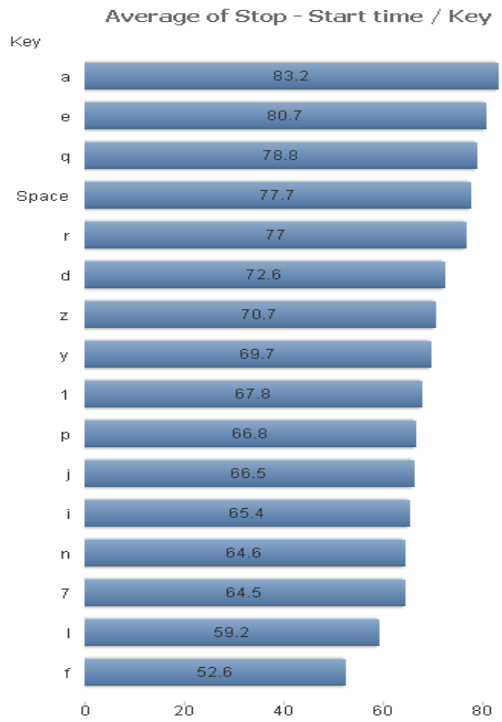

Figure 5: Diagram of average, minimum and maximum duration time

The conclusion: Keys "F" and "L" can be released 28.5% faster than the rest of the buttons. Maybe this is due to the fact that in the passwords there are two "F" that are neighbors alone, while "L" is by the end of the two respective passwords.

3.6 Overlapping Issues

The experiment: Using the program are randomly chosen 6 passwords "jeffrey allen" from the set of all these passwords. Also, using the program is plotted the following graph (Fig.6) The horizontal axis represents the characters of the password whereas, the vertical axis represents the time of releasing a button and pressing the next one. Each distinguishable point on the graph has as second coordinate the time of pressing a button calculated from the moment when the previous button was released. The meaning of the case when the time is negative is that a button is pressed down before the previous button is fully released. So, -50 shows that button „e" is pressed down before the button j" is fully released. The same with buttons r and e . When happens such a thing during the typing we say that there are overlappings. The positive values show that a button is pressed down after the previous button is fully released. In this case we have normal performance during the typing.

The reason: such events are present because of the personal features [9] of the user and of the high speed during the typing.
Cases when the new button pressing time overlaps with the releasing time of the previous button are: 1449 Overlaps.

Overlapping Ratio:
There exist more than 6.12% probability that a button be pressed before the previous one is released.
Especially with the buttons that are placed close to each other. For instance, (D-R-E)

4. Forecasting

In this section we will find the expected average and standard deviation of the typing time based on the length of the password.
From the above analysis, we can deem that the passwords that contain numeric values are trending to delay in typing, even if the length of the password is smaller than the length of a password containing only letters.
For this reason, we can exclude the password "pr7q1" to draw more efficient conclusions.

Password "jeffrey allen" analysis.
(Picked Randomly)

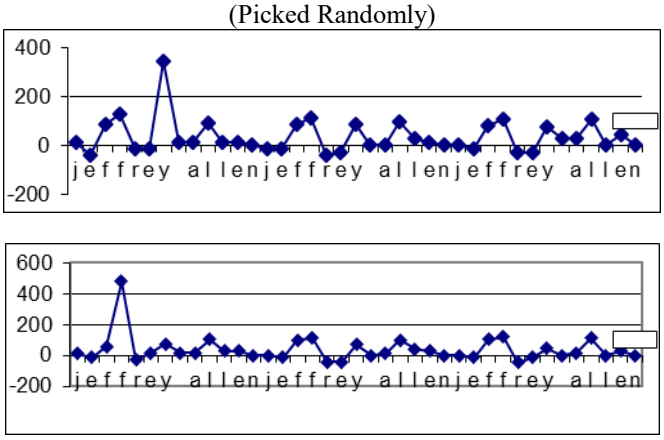

Figure 6: Password "jeffrey allen" analysis

Let us consider only the two other passwords as in the following table (Table 10):

Table 10: Av. time, St. Dev. and wr. times of two passwords

Password	*Length*	*Average Time / Password*	*StDev / Password*
drizzle	7	1251,45225	564,9613981
jeffrey allen	13	2196,474501	1132,298105

Based on these two Passwords, the Regression equations are:

Average Time = 1251.4 x(times) The Password Length + 2196.5
Standard Deviation = 564.9 x(times) The Password Length +1132.3

Their graphs are in Figure 7

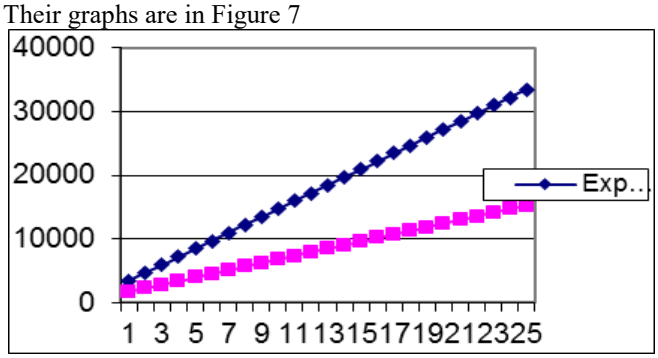

Figure 7: Regression graphs for the Average Time and its Standard Deviation

Using this Regression Equation [8] and [11]-[12], we can find the Expectations for the Average Time and its Standard Deviation, depended on the password length. Look at the following table -Table 11.

Table 11: Expectations for the Average Time and its Standard Deviation

Password Length	*Expected Average Time*	*Standard Deviation*
1	217,0742249	55,78354719
2	389,4705624	140,6465223
3	561,8669	225,5094975
4	734,2632376	310,3724726
5	906,6595751	395,2354478
6	1079,055913	480,0984229
7	1251,45225	564,9613981
8	1423,848588	649,8243732
9	1596,244925	734,6873484
10	1768,641263	819,5503235
11	1941,037601	904,4132986
12	2113,433938	989,2762738
13	2285,830276	1074,139249
14	2458,226613	1159,002224
15	2630,622951	1243,865199
16	2803,019288	1328,728174
17	2975,415626	1413,59115
18	3147,811964	1498,454125
19	3320,208301	1583,3171
20	3492,604639	1668,180075
21	3665,000976	1753,04305
22	3837,397314	1837,906025
23	4009,793651	1922,769
24	4182,189989	2007,631976
25	4354,586327	2092,494951

5. Conclusions

1) Tables, diagrams and graphs generated by sophisticated software are the best representations that help to understand and interpret data.
2) During the passwords typing are observed errors of different natures linked with the type of the person and with the structure and the content of the password.
3) In order to do accurate interpretations about given data is necessary to clean them from outliers.

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), Estoril, Lisbon, Portugal, June 29-July 2, 2009. IEEE Computer Society Press, Los Alamitos, California, pp. 125-134, 2009.
[2] Patrick Bours, Authentication Course 2012/2013, slides (Keystroke Authentication), IMT4721.
[3] Patrick Bours, Authentication Course, Reader (1.0.3.pdf), 2012/2013, IMT4721, Gjøvik University College, NISlab, chapter 8, 2008.
[4] Jucheng Yang (editor), Biometrics, Published by InTech, Janeza Trdine 9, 51000 Rijeka, Croatia, InTech, Printed in Croatia, ISBN 978-953-307-618-8, pp. 157-182, Copyright © 2011.
[5] Joseph N. Pato and Lynette I. Millett, Biometric Recognition: Challenges and Opportunities, Copyright 2010 by the National Academy of Sciences, Printed in the United States of America (http://www.nap.edu/catalog.php?record_id=12720), Introduction and Fundamental Concepts(pp. 15-35)
[6] Fred Erlend N. Rundhaug, Keystroke dynamics: Can attackers learn someone‟s typing characteristics?, Master‟s Thesis, Master of Science in Information Security, Department of Computer Science and Media Technology, Gjøvik University College, pp. 3-7, 2007
[7] Kevin S. Killourhy, A Scientific Understanding of Keystroke Dynamics, School of Computer Science, Carnegie Mellon University, Pittsbirgh, USA, pp 76-78
[8] Dryden, Ian; Shapes: Statistical shape analysis, R package version 1.0-8, 2004.
[9] Monrose and Rubin, “Keystroke dynamics as biometrics for authentication”, Future Generation Computer Systems 16, pp. 351-359, 2000.
[10] Richard Lowry, Concepts & Applications of Inferential Statistics, Spearman Rank-Order Correlation Coefficient, chapter 3/b.
[11] M. Plonsky, Ph.D, An Online Hypertext,. University of Wisconsin - Stevens Point , Copyright © 1997-2012.

Authors Profile

Adrian Kllogjeri has received **a)** the MSc. in Statistics, University of Kent, UK (Sep. 2010 – Nov. 2011). Subjects: Experimental Design, Linear Modeling, Discrete Data, Probability and Inference, Multivariate Analysis, Time Series, Stochastic Processes etc.; **b)** MSc in Applied Econometrics, Kingston University, London (Sep.2013-Nov. 2014). He worked as *Actuarial Programmer* with AIG EMEA Headquarters, London (Dec. 2011-Sep. 2013) and now is working as *Statistician* with Arval UK Ltd, Swindon, UK (Aug. 2014-ongoing).

Qamil Kllogjeri is a student for MSc in Applied Econometrics, Kingston University, London, UK (started in Sep. 2014). Also, he is continuing the master studies (Part-Time) in Information Security, University of Gjovik, Norway.