Journal of Multidisciplinary Engineering Science and Technology (JMEST)
ISSN: 2458-9403
Vol. 3 Issue 6, June - 2016

Securing Password Through Keystroke Forensic

Brijesh Jajal
IT Department
Higher College of Technology
Muscat, Sultanate of Oman
jajalbr@yahoo.com

Kunal Gupta
IT Department
Higher College of Technology
Muscat, Sultanate of Oman
guptas.kunal@gmail.com

***Abstract*— Our Research work revolves around the idea of providing Secure Authentication Services without the usage of any special devices. We have been witnessing the widespread usage of biometric systems, such as retina scans, fingerprint or face detection, etc., which requires the biological uniqueness of a person to establish his/her identity. Our research work utilizes the same principle, but does not involve the usage of any special hardware.**

The Study works towards proving that each and every individual have different keystroke values and that the same can be established by the means of Minimum and Maximum Delay positions, Overall Curve Shape and Area, and Standard Deviation, based on the set password that have been duly assigned to individuals. The study involves the sample size of ten people entering the same password and also records their attempts of same individual with ten instances. The results show that 88.8% of the times, our study logic is able to detect the uniqueness of keystrokes for the person despite of usage of the same password.

***Keywords*— Password; Keystroke; Forensic; Secure Authentication**

I. INTRODUCTION

In the current era of technology, information is the key to everything. It is of essence to identify who gets to access what data, and whether to give access to a person at all. Authentication Services proved to be the first milestone in providing such a security. And much work has been done in the area to protect authentication breach, by providing biometrics mechanism which ensures that the biological uniqueness of the person provides an additional layer of security for a person to prove his identity to the system. But such system cannot be deployed everywhere, due to their physical limitations and cost factors. And the hackers take advantage of such a limitation. If someone is able to acquire the username or password of a person, he can easily bypass the authentication mechanism and access the system to meet his own goals. We have created a study in an effort to provide additional security to the authentication mechanism, which does not involve expensive hardware, but does rely on the biological attribute of the person [1] to prove their identity to the system respectively. The idea for the research work comes from the motivation of protecting user account even if a hacker has acquired the user name and password of a person.

II. METHOD

The current study is attempted to focus on the uniqueness of the keystroke values [2], which are recorded in form of time taken, in seconds, for each character, to enter the given password. In this study, these keystroke timings are recorded for each individual for ten different instances, assuming that the same person may have minor variation with maximum 14%, while entering or typing the password. There are ten different individuals, taken as a sample space for the study, who enter the same password, to check the performance of the algorithm suggested here.

The following algorithm is devised in order to record the key stroke timings [4],[5] for the 6 character password entered by the user.

A. Algorithm used to implement the Keystorke forensic.

Step 1. For Users = 1 to 10, repeat step2 through step 4

Step 2. For Chars =1 to 6, repeat step 3

Step 3. $T_i = T_i + r$

$T_c = T_c + d$

$S_d = T_{iMax} - T_{iMin}$

Step 4. Save T_i, T_c, S_d

In an Algorithm described above, the value of T_i represents the Total time taken by each individual to enter the 6 characters password; T_c represents the Total Curve area, which is calculated as the sum of differences for timing of each character with its preceding character; S_d represents the self deviation, which is difference between the character with maximum time taken to type, and the character with minimum time, for the same user.

III. RESULT AND CONCLUSION

The result of implementation of the above algorithm, with values of Ti, Tc, Sd and Standard Deviation can be visualized in the Figures Fig.1 to Fig. 5, with the corresponding Column no. 9, 10, 11 and Column 12 respectively.

TABLE I. DEVIATION OF INDIVIDUAL USER

User	Factors	
	Total Curve Area T_i	***Self deviation S_d***
A	249.2	32
B	298.6	42
C	403.5	68
D	368.3	46
E	389.3	83
F	394.7	57
G	440.6	37
H	555.4	97
I	261.4	19
J	321.8	49

We can conclude from the results shown in Table 1 that the maximum deviation found with an individual, considering it as 14% of the other attempts or keystroke values, the user is found to match only with 1 user, out of total 9 other users, i.e., the deviation between User F and H, which is the only deviation less than 14%. This indicates that the suggested logic is successful in 88.8% of the cases.

However, in order to further add the success rate, the below mentioned criterion may be helpful:

a) Comparison of minimum duration keystroke, and maximum duration keystroke, along with the key position.

b) The curve design or pattern formed for individual user's keystroke timing [6].

c) Finding and analyzing the correlation factors and trapezoidal integration.

The above result supports our theory that the keystroke values can prove to be a vital instrument for providing security to the authentication mechanism.

The above algorithm can easily deployed and can act as a secure layer for the authentication services for any desktop or mobile [3] application. The future enhancement will involve a learning curve being embedded to provide with more accurate results.

ACKNOWLEDGMENT

We would like to thank Dr. Prakash, Dr. Vinesh and Dr. Manisha, from Mathematics department, to guide us in right direction, and IT members for providing us the sample inputs for analysis. We sincerely express our gratitude to Head of Sections - Dr. Khalfan and Mr. Taalib, and Head of Dept. of IT - Dr. Fatma al Abri for their constant motivation for research.

REFERENCES

[1] F. Monrose and A.D. Rubin, "Keystroke dynamics as a biometric for authentication," in Future Generation Computer Systems, vol. 16, issue 4, pp. 351-359, February 2000.

[2] A. Guven and I. Sogukpinar, "Understanding users' keystroke patterns for computer access security," in Computers & Security, vol. 22, issue 8, pp. 695-706, December 2003.

[3] N.L. Clarke and S.M. Furnell, "Authenticating mobile phone users using keystroke analysis," in Internation ournal of Information Security, vol. 6, pp. 1-14, 2007.

[4] M. Karnan, M. Akila and N. Krihnaraj, "Biometric personal authentication using keystroke dynamics: A review," in Applied Soft computing, vol. 11, issue 2, pp. 1565-1573, March 2011.

[5] P. Bours, "Continuous keystroke dynamics: A different perspective towards biometric evaluation," in Information Security Technical Report, vol. 17, issue 1-2, pp. 36-43, February 2012.

[6] P.S. Dowland, S.M. Furneell and M. Papadaki, "Keystroke analysis as a method of advanced user authentication and response,", in Security in the Information Soceity, vol. 86, pp. 215-226, 2002.