Static User Authentication through Typing Behavior

Pushpanjali V. Pawar
Research Scholar
Department of Computer Science & Engineering
JJT University, Rajasthan

Abstract- In this paper we have discussed using keystroke dynamic technique we can secure our account through static or continuous observation. This technology is based on user's password typing behavior and it is hardware independent i.e. only software based technology keyboard is required for password protection. The outcome of this work is a timer based program and a deployable library for running in background for storing keystrokes.

Keywords- keystroke dynamics, security, keyboard.

I. INTRODUTION

Biometric systems are used to uniquely identify a person based on their traits or characteristics, these characteristics are unique, distinctive and measurable. In computer science, biometric system is used for access control and identification purpose. It is also used to identify a person among a group of people. Biometric system can be divided into two types: physiological and behavioral. Physiological type refers to the measurement of the physical properties i.e. fingerprint recognition, retina and iris scanning, face recognition, hand geometry, DNA testing etc. Physical properties of the person don't change rapidly. Behavioral type refers to the specific behavior of the user i.e. voice, handwritten signature and keystroke dynamics (hand typing). Both Physiological and Behavioral type has its importance. Behavioral biometrics involves verification (one-to-one) and identification (one-to-many) activities. Verification activity is done at login time by measuring the typing pattern while the user writes the username and the password and compare with the previously stored profile. Identification activity is conducted throughout the session. Here, the behavioral biometric i.e. keystroke dynamics is in consideration, for different typing habits of the user.

In keystroke dynamics, the manner and rhythm in which a user types characters on a keyboard or keypad is observed. The user's behavior of typing for lower case letters is finding. Also can find user's behavior of typing for combination of lower and upper case letters. During these cases, keystroke latencies of user's can be calculated and the use of "shift key" and "caps lock" are observed. Based on these measurements, a unique biometric template of user typing rhythm is design for future authentication. The template will be able to distinguish whether the user is fraud user or not by comparing the flight and dwell times to those set on the template.

User authentication based on keystroke dynamics will be affected by authorizing the trained and untrained users. Keystroke latencies for the "trained" and "untrained" users are observed. The typing speed is different for trained and untrained users. The trained user has taken training of typing or completed the certification course like 30WPM etc. and uses all ten fingers for typing, so that the typing speed is better. The untrained user is not certified, but having knowledge of using keyboard and not used all fingers, so that the typing speed is good.

Keystroke latencies of a user can be measured during the typing of a password. Password can be a combination of small letters, capital letters, numbers and special characters(p@s$w0rd). The use of Num Lock, special characters, shift and caps lock during password typing could be observed. There are two page-up, page-down, shift, ctrl, alter, home and end keys, because one of them may be use by user. The use of shift , ctrl and alt key is based on the habit and the combination of the keys, i.e. the user may use the left hand ctrl key for cut(ctr+x), copy(ctrl+c), paste(ctrl+v) and save(ctrl+s) operations on document or text. For using plus sign(+), curly bracs({),round bracs(()double quotes("),pipe(|) and colon(:) ,etc. in the document, user mostly uses right hand shift key. This can be observed in day to day life. Also, the number keys of nampad are used if the mathematical calculation in present document, otherwise the number keys below the functions keys are used. Hence, our analysis is not which shift key, ctrl and number keys are used. Here, just observe if the shift key, caps lock and Num lock is use or not.

User's becomes more comfortable with his/her desktop or laptop keyboard after some period of time. If the same user is switch to work with other keyboards attach to the computer system, that time the user is not comfortable to use the keyboard and do more mistakes. Also, if the user uses a keyboard after a long time span, at that time also the user hesitates to use the keyboard. These changing behaviors of different person's on different keyboard can be observed.

In keystroke dynamics, the latencies of the user can be captured continuously or at the login time also. Also the false acceptance rate(FAR) and false rejection rate(FRR) can be adjusted by changing threshold value at the individual level. The typing speed of a user may vary during a day. A user is in fresh mood at morning, but during the day, he/she may get boor, tired, angry or in hurry.

II. REVIEW OF THE RELATED LITERATURE

Daniele Gunetti et.al. (2005) Describes user identification by typing samples written in different languages like Italian and English. The Imposter Pass Rate (IPR) and False Alarm
Rates (FAR) have been calculated. Typing dynamics of free text provide useful information for user identification and authentication even when a long time has passed since typing profiles of users were formed, and even when ascertaining users are writing in a language different from the one used to form their profiles. If even when rely on dated information, and the typing samples to be analyzed are written in a language different from the one used to form users' profiles.

Fabian Monrose et.al. (2000) Discusses non-static biometric technique that aims to identify users based on analyzing habitual rhythm patterns in the way they type using template matching and Bayesian likelihood models. The use of digraph-specific measures of variability instead of single low-pass filters. Additionally, we argue in favor of the use of structured text instead of allowing users to type arbitrary text during the identification process.

Jarmo Ilonen Keystroke dynamics is a biometric mainly used for verification, but also identification is possible. Keystroke dynamics is a very cheap biometric verification method because there is no need for any additional hardware besides a normal keyboard. Existing words can be cracked by dictionary attacks. The short length passwords can be easily cracked. In such a cases the keystroke dynamics can be useful. Secure shell (SSH) based systems may face problem of password cracking. SSH is designed to provide a secure channel between two hosts. As the mechanism of sending IP packets immediately after the key is press, the keystroke timing information of the users typing is reveled at the other end. The timing differences detected by the eavesdropper can cause serious problem of security, even by knowing root password. The statistical study is done and Hidden Markov model and key sequence prediction algorithm developed in this work. The SSH system is monitored and collection of the timing information is done. The application to the general class protocols for encrypting interactive traffic is done. The suggestions to develop the new protocol by considering the timing attacks are given in this work.

K. Senathipathi et.al. (2012) Discusses the VKF for the authentication in addition to the time related features. VKF is calculated based on the typing speed and behavior of the user on the key board. In this paper the authentication system consists of three steps: Feature Extraction, Preprocessing, Feature Subset Selection (Genetic Algorithm). From the reduced set of genes obtained in the previous pre-processing stage, third stage uses a wrapper approach that combines a GA and a SVM to accomplish the feature subset selection. After applying GA(Genetic Algorithm) & SVM(Support Vector Machines) good data set is found. From that data set the author find Feature reduction rate and error authentication rate by using the MATLAB. In this method author used efficient Genetic Algorithm for the feature reduction.

Koichiro Niinuma et.al.(2007) Systems need continuous user authentication methods from usability, security and cost, that continuously monitor and authenticate users based on some biometric trait(s) using webcam that watch user's face and color of clothing. Our method can authenticate users regardless of their posture in front of the workstation (laptop or PC). Previous methods for continuous user authentication cannot authenticate users without biometric observation. Color information of users' clothing as an enrollment template in addition to their face information. The system cannot pre-register the clothing color information because this information is not permanent. The system automatically registers this information every time the user logs in and then fuses it with the conventional, password identification system.

Lívia C. F. Araújo et.at. (2005) Describes the inputs of the key down and up times and the key ASCII codes captured while the user is typing a string. This paper innovates using four features to authenticate users. Four features i.e. key code, two keystroke latencies, and key duration were analyzed and seven experiments were performed combining these features. The results of the experiments were evaluated with three types of user: the legitimate, the impostor and the observer impostor users. Claimed obtaining a false rejection rate of 1.45% and a false acceptance rate of 1.89%. This approach can be used to improve the usual login-password authentication when the password is no more a secret. [6].

Manoj Devare(2013) Measured user's keystroke latencies for free hand typing with use of combination of "shift key" and "caps lock" . The thread based program is used for that analysis/observation which is run in background. Sampling data is collected through the developed software and that data is stored is flat file. The software has a data entry screen for typing mixed data i.e. small and capital characters to find the use of "shift key" and "caps lock".

Romain Giot et.al. (2010) Shows multimodal biometric system combining keystroke dynamics and 2D face recognition. Different fusion methods like min, max, mul, svm, weighted sum configured with genetic algorithms, and, genetic programming on the scores of three keystroke dynamics algorithms and two 2D face recognition. This multimodal biometric system improves the recognition rate in comparison with each individual method. On a chimeric database composed of 100 individuals, the best keystroke dynamics method obtains an EER of 8.77%, the best face recognition one has an EER of 6.38%, while the best proposed fusion system provides an EER of 2.22%.

Sam Hyland(2004) The comparison of typing samples of free text used to verify personal identity. The technique tested with a wide set of experiments on more than two hundred individuals, obtaining a False Alarm Rate(FAR) of less than 5% and an Impostor Pass Rate of less than 0.005%. The samples have been collected in different working sessions. As the use of the keystroke dynamics is absolutely suitable for different application areas of e-commerce like Amazon.com. It can direct or indirect control the access to company resources and verifying the billing of a customer.

Swarna Bajaj et.al. (2013) System is based on to calculate the pressing time, dwell time and total time of password. There statistical method is used to measure the mean time and average time by using Net Beans IDEdeveloped in JAVA. When a user starts the application, a login activity is launched where a registered user submits his 4 character password and for new user entry is made first and then check.

Yvonne J. et.al. (2013) Describes that access to a resource may be denied or granted in response to a score value of threshold. This score value is calculated on timing information of key-press and key-release events. To denied or accept a user, template is created and prompt a user to inter password. At the time of entering a password, timing information of key-press & key-release events is calculated for biometric authentication. Timing information score value is below threshold value, access is denied to user and ask user to be want more attempt and repeat cycle if answer is yes, otherwise apply secondary authentication method. If score value is above the threshold value, then access is directly grated and incorporate that timing information into keystroke dynamic template. Finally end the session/authentication method.

III. PROPOSED WORK & RESULTS

The proposed method is based on to calculate the pressing time, releasing time, overall delay, SHIFTKEY and CAPSLOCK of password. The data is collected in simple file which is run in background and noted down all observations. The sampling is collected through the laptop and desktop keyboard from office faculties with the help of program written in VB 6.0.

When a user starts the application, the user interface screen for registered user is open to submit their mixed password and unregistered user can register through New User button. After entering password and clicking on login button, if the password and overall time is not found in database an error message is displayed.

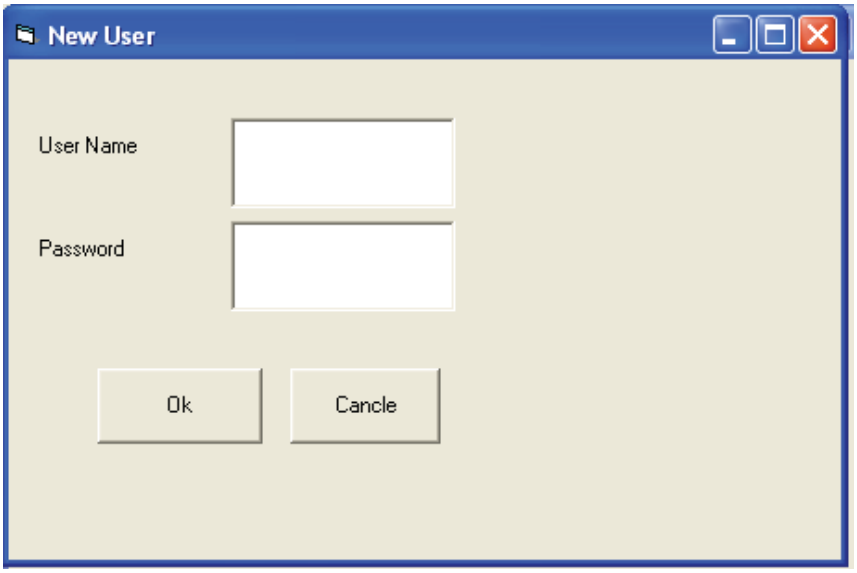

Fig.1 New User registration Screen

Table 1: Flight time & hold time of password “girl” & user name “save” entered by 10 users

User	f1	f2	f3	h1	h2	h3h	h4	Total Time
1	11	14	22	8	7	6	6	73
2	29	17	13	11	9	11	8	98
3	7	6	7	9	7	9	6	52
4	9	9	10	11	10	10	9	67
5	14	14	15	8	8	8	7	74
6	15	18	9	7	6	8	6	69
7	15	10	12	9	8	8	6	68
8	9	7	7	10	9	9	8	59
9	14	17	15	9	9	9	8	82
10	11	11	15	10	8	9	7	70

IV. CONCLUSION

As shown in Table 1, flight time is the time between two consecutive keystroke, hold time is the how long user hold key and total time is the time on last key press minus the time elapsed on first key press. This is measured on screen shown in figure 1.

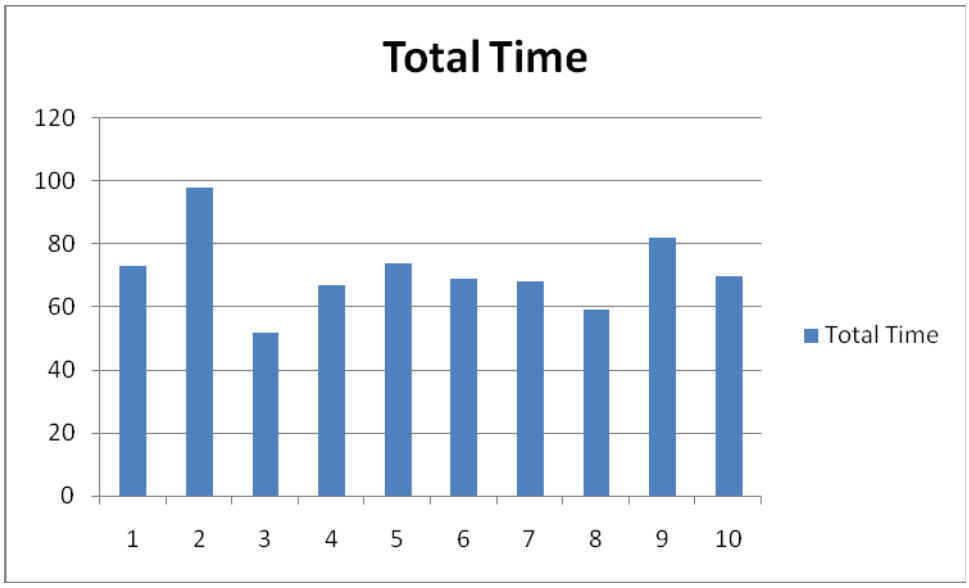

Fig 2. Total time calculated for password "girl" entered by 10 users

In this paper, user authentication through keystroke is done only static i.e. user typing pattern is observed only at login time not throughout the session i.e. continuously.

Keystroke Dynamics is a two factor biometric security, hence, for a successful login, firstly password should be known and secondly, typing rhythm should be match . In another method of biometrics we require hardware but human behavior method we generate a secure key to protect our password. This key Static User Authentication through Typing Behavior is generating according to human behavior.

REFERENCES

[1] Daniele Gunetti, Claudia Picardi, and Giancarlo Ruffo , "Keystroke Analysis of Different Languages: A Case Study", IDA, LNCS 3646, pp. 133–144,2005
[2] Fabian Monrose, Aviel Rubin,"Keystroke dynamics as a biometric for authentication", Future Generation Computer Systems, Vol. 16, pp. 351-359,2000
[3] Jarmo Ilonen, "Keystroke dynamics", Lappeenranta University, Finland, Vol. 2.
[4] K. Senathipathi, Krishnan Batri, "Keystroke Dynamics Based on Human Authentication System using Genetic Algorithm", European Journal of Scientific Research,Vol. 82,No.3 pp. 446-459, 2012.
[5] Koichiro Niinuma, Anil K. Jain , "Continuous User Authentication Using Temporal Information", Fujitsu Laboratories, Vol. 7, pp. 243-256,2007.
[6] Lívia C. F. Araújo, Luiz H. R. Sucupira Jr., Miguel G. Lizárraga, Lee L. Ling, Andjoão B. T. Yabu-Uti, "User Authentication Through Typing Biometrics Features" , IEEE Transactions On Signal Processing, Vol. 53, No-2, pp. 851-855,2005.
[7] Manoj Devare, "Mixing and Matching Human Traits using Hand typing", International Journal of Computer Application,Vol. 73, No.18,2013.
[8] Romain Giot, Baptiste Hemery, Christophe Rosenberger, "Low Cost and Usable Multimodal Biometric System Based on Keystroke Dynamics and 2D Face Recognition",IEEE Computer Society, International Conference on Pattern Recognition, pp. 1128-113, 2010.
[9] Sam Hyland , "An Analysis of Keystroke Dynamics Use in User Authentication",Software engineering report,2004.
[10] Swarna Bajaj, Sumeet kaur (2013), "Typing Speed Analysis of Human for Password Protection (Based on Keystroke Dynamics)", International Journal of Innovative Technology and Exploring Engineering (IJITEE), Vol. 3, pp. 88-91,2013.
[11] Yvonne J., Stark,Mechthild R. Kellas-Dicks, "Incorporating False Reject Data IntoTemplates for User Authentication", US Patent,2013.