ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 10, October 2013

Keystroke Dynamics: Review Paper

Mayur Mahadev Sawant[1], Yogesh Nagargoje[2], Darshan Bora[3], Shrinivas Shelke[4], Vishal Borate[5]

Student, Department of Information Technology, MIT College of Engineering, Pune, India [1]

Student, Department of Computer, Dr. Seema Quadri Institute of Tech, Aurangabad, India[2]

Student, Department of Information Technology, MIT College of Engineering, Pune, India [3]

Student, Department of Computer, S. S. G. M. College of Engineering, Shegaon, India [4]

Student, Department of Information Technology, MIT College of Engineering, Pune, India [5]

Abstract: Today need of authentication is not limited to password and PIN. It needs a high level of security which can be achieved by Keystroke biometrics. This paper attempts to catch the imposter even if he carries login details of genuine user. The paper tries to review the keystroke methods and draw a common conclusion. Adding keystroke mechanism with existing system helps to enhance the security.

Keywords: Keystroke Biometrics, Network Security, Password Security and Password Strengthening.

I. INTRODUCTION

Nowadays developing more secure authentication methods in computer security is a biggest task. Herculean attempts have been taken to improve security of computer systems. Among them authentication is the process of differentiating between the genuine user and imposter. It is a challenging area of security research and practice. Many algorithms were discussed till date but none of them is completely secure.

User's authentication can be checked by one of these methods:

- User presents a secret (something he knows), namely password, PIN (Personal Identification Number). Password can be alphanumeric which is most commonly used and can be easily stolen by computer generated programs. Dictionary attack and brute force attack is one of the common example of such programs.
- Token such as Smart card can be used for identification. Combining password system with token based authentication is one of the good approaches. But theft and misuse of smart cards add inconvenience to the user. Remembering those password and PIN is also a tedious work.
- User presents part or structure of body as a physical attribute (something he has) to authenticate. This technique is more accurate than last one because token can be passed to anyone. This technique is more convenient and efficient than password and token.

This paper is organized as follows: section 2 focuses on the overview of biometrics. The research work of keystroke mechanism in last three decade reported in section 3.Section 4 describes the conclusion part.

II. BIOMETRICS

The term "biometrics" is derived from the Greek words 'bio' means life and 'metric' is to measure. Biometrics refers to the identification of humans by their characteristics or traits. Biometrics is used in computer science as a form of identification. Biometric identifiers are the distinctive, measurable characteristics used to label and describe individuals. Biometric broadly categorized in two parts: physiological versus behavioural characteristics.

A physiological biometric would identify by one's voice, DNA, hand print or behaviour. Behavioural biometrics is related to the behaviour of a person, including but not limited to typing rhythm, gait and voice. Researchers have mentioned the term behaviour metrics to describe the latter class of biometrics.

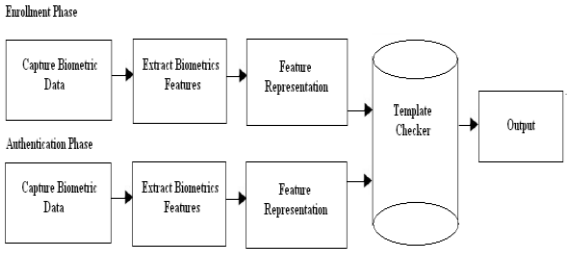

Fig. 1 Biometric System

Fig. 1 shows the biometrics system which includes enrolment and Authentication phase.

III. KEYSTROKE BIOMETRICS

All Keystroke mechanism depends upon the key press and key release duration. The time duration between key press

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 10, October 2013

and key release convert into security parameters. For two consecutive key press and key release there are six parameters associated with it. Four timestamps are associated namely first key press (P1), first key release (R1), second key press (P2) and second key release (R2).Six combinations of time differences of four timestamps, namely, d1: R1-P1, d2: P2-R1, d3:R2-P2, d4: P2-P1, d5:R2-R1, d6: R2-P1.
Every user has his unique typing style. Typing styles are the most efficient way of collecting the data between user and system. They become useful tool to obtain the level of authentication when properly sampled and analysed. The experimental results show that the use of the keystroke dynamics is simple and efficient way of authentication.

Advantages of Keystroke Biometrics:

Biometrics based on typing of the user which doesn't require any extra hardware other than keyboard. Keystroke biometric is cheaper to implement, more distributed and more unobtrusive than other biometrics. Collection of data needs keyboard and simple software using Java's swing and awt package. It is relatively cheap investment than other biometrics like fingerprint and retinal scan. It's very easy to replicate the collected data if hardware is not available. Keystroke biometrics doesn't depend upon the location of the user as we can collect the data from anywhere using Internet. Keystroke collection software can be distributed via client-server methodology. No specialized training is needed for keystroke as it's a daily activity. It is relatively unobtrusive method as compared to retinal scan where we have to put some part of the body in front of the machinery. Keystroke biometrics can be considered as secure system even if user knows the username and password.

Disadvantage of Keystroke Biometrics:
No consistency in Keystroke mechanism like other biometrics which last fairly long period of time. Keystroke biometrics can lead inconsistency in the typing style due to

1. Casual typing
2. Using single hand for entering the password,
3. Sweaty hand after a long session

Keyboard layout also adds some difference in typing style. The posture can lead to change in the keystroke as it's easy to enter the password by sitting rather than standing. Keystroke biometrics can be a irritate approach as user has to enter the same string repeatedly. No login transfer can be done even in urgent situation.

Applications:
Keystroke mechanism can be used as Authentication method. Keystroke can be used to identify password sharing system and to ensure that no software licenses are being shared. Many companies like Psylock and ID Control are using keystroke mechanism on MS Windows login, to web login, to Citrix and VPN integration.

Types:
No specific type of keystroke mechanism is present, but different types of keyboards can be used. Keyboard is of different types which include Virtual Keyboards, Gaming Keyboards, Standard Keyboard Ergonomic Keyboards, Wireless Keyboards, Compact Keyboards and Internet Keyboards.

IV. RELATED WORK

Most of the papers used statistical methods and neural networks for keystroke based authentication.[3] proposed a Monte Carlo approach for data collection and parallel decision tree (DT) for identifying the genuine user. Data collection included six basic parameters by comparing key press and key release of successive keys. A vector formed on the basis of raw data. Wavelet analysis was performed on four 16-element sub vectors by splitting the keystroke feature vectors and eight DT classifiers were trained for every user. Almost 19 times training data generated at the training level and eight decision trees were formed on the basis of raw data. User gets an entry to the system if and only if user matches any of the three decision trees. The average FRR (False rejection rate) was 9.62% and FAR (false acceptance rate) was 0.88%. Complexity of the algorithm depends upon the number of characters in the string. Adding a new user without disturbing the entire system was tedious task.

[5]Author suggested that keystroke mechanism can be used to identify the imposter when he gets hold of the secret PIN and password. In this paper two algorithms were proposed to implement the keystroke efficiently. The resulted mean, standard deviation and weight formula used to calculate the weight in first step. In second step, the login time keystroke data is compared with the registered mean± standard deviation which resulted into match count. If both conditions are satisfied with 50% and 75% respectively then, user successfully logs on the system. This paper produced FRR which was almost zero and FAR ranged between 0.12% and 0.28%.

[14]Author suggested a different technique to strengthen the password system by combining with keystroke biometrics. In this paper author proposed fusion of two algorithms named as Gaussian probability density function and direction similarity measure. The fusion of two algorithms is done by different methods and among them AND rule showed the best result. This paper showed FRR and FAR as 1%.Calculated EER reported as 1.401% which helps the security concern. Retraining process is also discussed in this paper which helps in updating the template.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 10, October 2013

V. CONCLUSION

The above paper discussed the different methods of keystroke dynamics. The problem with keystroke dynamics is improper dataset. No one has used the common dataset. The need of multi-modal biometrics can be helpful to the keystroke to achieve the less False Accept Rate (FAR) and False Reject Ratio (FRR).

The different methods used and authenticated by the user are discussed. Amongst them Statistical and Neural network have been widely used methods. The advantages, disadvantages and future work also reviewed. Future works includes Mobile, PDA and ATM machines. The fusion of keystroke with the other biometrics can be another new idea. The web-based enablement of keystroke and adding more feasibility can be part of future works. The size of keystroke data and the reduction in the number of attempts at the time of registration should be part of future works. FAR, FRR and EER should be low down to zero to achieve higher security.

ACKNOWLEDGMENT

Author would like to thank all the references.

REFERENCES

[1] R. Gaines, W. Lisowski, S. Press, N. Shapiro, Authentication by keystroke timing some preliminary results, Rand Report R-2526-NSF, Rand Corporation,1980.
[2] A. K. Jain, R. bolle, S.Pankanti, Biometrics personal identification in networked society, in: M. Obaidat, B. Sadoun, Keystroke dynamics based authentication, kluwer academic publishers, USA, 1999, pp. 213-229
[3] S. Cho, C.Han, D. Han, H. Kim, Web based keystroke dynamics identity verification using neural network, Journal of organizational computing and electronic commerce, 10 (4)(2000) 295-307
[4] J. Ilonen, Keystroke dynamics, Lappeenranta University of Technology, Finland,http://www2.it.lut.fi/kurssit/03-04/010970000/seminars/Ilonen.pdf
[5] A. Peacock: Learning User Keystroke Latency Patterns (Preliminary Report),
[6] Enzhe Yu, Sungzoon Cho, Keystroke dynamics identity verification and its problems and practical solutions, Computers & Security - COMPSEC,23 (5)(2004) 428-440
[7] R. Joyce, G. Gupta, Identity Authorization Based on Keystroke Latencies, ACM 33(2) (1990) 168-176
[8] S. Furnell, Continuous user identity verification using keystrokes analysis, Proceedings of International Conference on Multimedia Communications, Southampton, (1995)189-193
[9] F. Bergando, D. Gunetti, C. Picardi, User Authentication through keystroke Dynamics, ACM Transactions on Information and System Security,5(4) (2002) 367–397
[10] D. Shanmugapriya, G. Padmavathi, A Survey of Biometric keystroke Dynamics: Approaches, Security and Challenges, International Journal of Computer Science and Information Security- IJCSIS, 5(1) (2009) 115-119
[11] P. S. Teh, A. B. Teoh, T. S. Ong, H. F. Neo, Statistical Fusion Approach on Keystroke Dynamics, Third International IEEE Conference on Signal-Image Technologies and Internet-Based System –SITIS, (2007) 918-923.
[12] D. Gunetti, D. Picardi, Keystroke analysis of free text, ACM Transactions on Information and System Security, (2005) 8(3) 312–347.
[13] V. Kacholia , S. Pandit, Biometric Authentication using Random Distributions (BioART), 2003
[14] F. Monrose, A. Rubin, Authentication via Keystroke Dynamics ACM Conference on Computer and Communications Security (1997)48-56.
[15] I. Sogukpinar, L. Yalcin, User Identification at Logon via Keystroke Dynamics, Journal of Electrical & Electronics Engineering, 4(1) (2004) 995-1005.
[16] F. Monrose, A. Rubin,Keystroke Dynamics as a Biometric for Authentication, Future Generation Computer Systems 16 (2000) 351–359.
[17] Sally Dafaallah Abualgasim,IzzeldinOsman,An Application of the Keystroke Dynamics Biometric for Securing PINs and Passwords, World of Computer Science and Information Technology Journal (WCSIT)(2011), ISSN: 2221-0741,Vol. 1, No. 9, 398-404
[18] Yong Sheng, Vir V. Phoha, Steven M. Rovnyak, A Parallel Decision Tree-Based Method For User Authentication Based on Keystroke Pattern,IEEE Transactions on System, Man, and Cybernetics—Part B: Cybernetics, Vol. 35, No. 4, August 2005

BIOGRAPHIES

Mayur Mahadev Sawant received his B.E. degree in Information Technology from Mumbai University. Currently he is doing Master Of Engineering from MIT College Of Engineering, Pune University. His research area includes Database Partitioning, Keystroke Biometrics and Mouse Dynamics. He published a review paper on 'Database Partitioning' in International Journal of Innovative Technology and Exploring Engineering (IJITEE).

Yogesh Nagargoje received his B.E. degree in Computer Engineering from Mumbai University. Currently he is doing Master Of Engineering from Dr. Seema Quadri Institute of Tech, Aurangabad, India. His research area includes Keystroke Biometrics and Mouse Dynamics.

Darshan Bora received his B.E. degree in Computer Engineering from Pune University. Currently he is doing Master Of Engineering from MIT College Of Engineering, Pune University. His research area includes cloud computing.

Shrinivas Shelke received his B.E. degree in Information Technology from Mumbai University. Currently he is doing Master Of Engineering from S. S. G. M. C. O. E Shegaon, India. His research area includes Keystroke Biometrics and Mouse Dynamics.

Vishal Borate received his B.E. degree in Computer Engineering from Pune University. Currently he is doing Master Of Engineering from MIT College Of Engineering, Pune University. His research area includes Database Partitioning, Keystroke Biometrics and Mouse Dynamics.