Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 2, February 2015, pg.341 – 345

REVIEW ARTICLE

Keystroke and Mouse Dynamics: A Review on Behavioral Biometrics

Rohan V. Ponkshe[1], Prof. Vikrant Chole[2]

[1]M.Tech Scholar, GHRAET, Nagpur, India

[2]GHRAET, Nagpur, India

Abstract:

Today the need of authentication is not at all limited to the passwords and Personal Identification number (PIN). There is a need of higher level of security for the authenticating the genuine user. This higher level of security can be achieved by using the behavioral biometrics i.e. by using mouse movement and keystroke dynamics etc. This paper attempts to restrict the unauthorized person from gaining access to account of genuine user even if he carries the login detail i.e. username and password of the genuine user. This paper tries to review mouse movement method and keystroke dynamics method and draw a common conclusion. Adding behavioral biometrics with existing system helps to enhance the security.

Keywords: ***Keystroke biometrics, Mouse biometrics, authentication strengthening, Network Security***

I. INTRODUCTION

Identity theft is a fraud in which criminals harm users by stealing their credentials, such as details of credit card and passwords, or by exploiting logged-on computers which was remain unlocked by mistake by the user. Stolen user identities may be used to perform many of unauthorized activities such as online purchases using credit or debit card details, which come under cybercrime. Such purchases incur losses of billions of dollars to the websites as well as to their insurance companies [9]. A lot of efforts have been taken to improve the security of a computer system. Among them authentication is the process of differentiating between genuine user and imposter. It is challenging area in computer security research.

A. Genuineness of user can generally be check using one of the following methods:

- User present a secret (something he knows), namely password, PIN (Personal Identification Number). Passwords can be alphanumeric which is most commonly used and can be easily cracked by hackers using computer generated programs. Brute force attack and Dictionary attacks are some examples of such programs.
- Token such as Smart card can be used for authentication. Combining password system with token based authentication is a good idea. But theft and misuse of smart cards add risk to the user. Remembering those password and PIN is also a tedious work.
- User uses part of a body or structure as a physical attribute to authenticate i.e Biometric Authentication. This technique is more accurate than last one because token can be passed to anyone whereas biometrics can't be passed. This technique is more 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 decades reported in section 3.The research work on mouse dynamics in last three decades reported in section 4. Section 5 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 and behavioral biometric. Voices, DNA, hand print are some common examples of physiological biometrics. Behavioral biometrics is related to the behavior of a person, including typing rhythm, signature. Researchers have mentioned the term behavioral metrics to describe the latter class of biometrics.

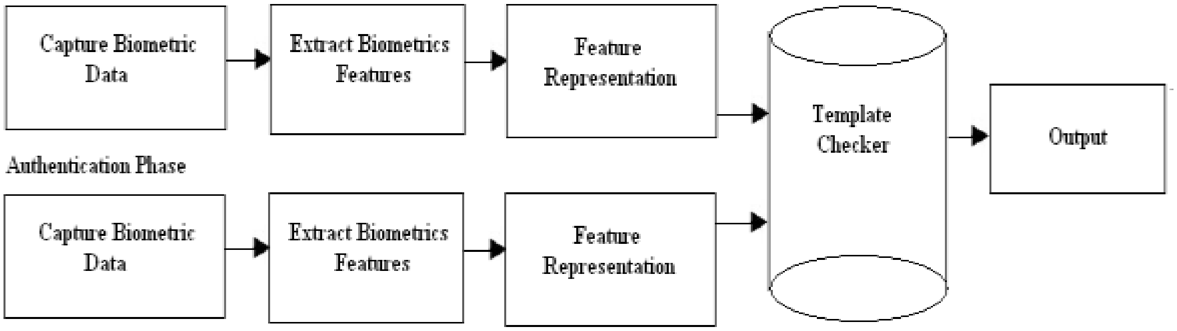

Fig. 1 Simple Biometric System.

III. KEYSTROKE BIOMETRICS

Today the username and password is the widely used for authentication of user. This data of a particular user is private and sensitive data. But as the attacking technology is becoming stronger, this method for authentication needs to be improved. This authentication method can be easily compromised. It's important to increase the level of confidentiality and security. Improvising password method, interaction of the user with the computer utilizes as a parameter to the security. One of the promising technique where user's typing style considered as an parameter for authentication is called as Keystroke biometrics.

A. Features related to Keystroke Dynamics

1) Dwell time: It's the time between Key press and key release.
2) Flight time: It's the time between Key press and key press, key release and key release [4].

The combining of keystroke authentication with the password based system adds a layer of security which takes care of the shortcomings of the passwords. The legitimate user's password as well as the typing style in terms of the timing (dwell time and flight time) are input to the system which makes hard to crack the password as well as the keystroke timings. This promising technique is yet to be accepted by the users. All Keystroke mechanism depends upon the key press and key release duration. The timing is converted into security parameters. For two consecutive key press and key release there are six combinations associated with it. There are Four timestamps associated namely 1.first key press (P1), 2**.**first key release (R1), 3**.**second key press (P2) 4.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 analyzed. The experimental results show that the use of the keystroke Dynamics is simple and efficient way of authentication.

B. Advantages of Keystroke Biometrics:

1. No extra hardware needed other than keyboard.
2. Keyboard biometric technique is cheapest as compared to other biometric techniques used for authentication.
3. No specialized training is needed for keystroke as it is a daily activity.
4. Keyboard biometric acts as a promising system even if intruder knows the username and password of the genuine user.

C. Disadvantage of Keystroke Biometrics:

There is no consistency in Keystroke mechanism like other biometrics. Keystroke biometrics can lead inconsistency in the typing style due to,

1. Casual typing

2. Using one hand for entering the password. Keyboard layout also plays an important role typing style. Keystroke biometrics irritates the user since he/she has to enter the same string repeatedly.

D. 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 corporate companies like Psylock and ID Control are using keystroke mechanism on Microsoft Windows login, to web login, to Citrix and VPN integration.

E. Related Work To Keystroke Dynamics:

Most of the researchers used neural networks and statistical methods for keystroke based authentication mechanism.

[3] Author proposed a Monte Carlo approach for data collection and parallel decision tree (DT) for identifying the genuine user. Data collection included six basic parameters, which are formed by comparing key press and key release of successive keys. A vector was 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 decision tree (DT) classifiers were trained for every user. Almost 19 times training data generated at the training level. Eight decision trees were formed on the basis of raw data. User gets authenticated as the genuine user 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. Addition of a new user without changing the entire system was a tough task.

[5]Author suggested that keystroke mechanism can be used to identify the intruder when he gets hold of the secret Personal Identification Number (PIN) and password. In this paper two approaches 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 only, user successfully logs on the system. The FRR was almost zero and FAR ranged between 0.12% and 0.28% using this method.

[7]Author suggested a different technique for strengthening the password system by combining with keystroke biometrics technique. In this paper author proposed combination 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%. Retraining process is also discussed in this paper which helps in updating the template data.

IV. MOUSE DYNAMICS

Mouse dynamics is a part of behavioral biometrics which can be used to authenticate the user with the lesser cost. Mouse handling is a parameter to the security in mouse dynamics. Mouse dynamics focuses on the activities regarding to mouse while handling the system. Mouse dynamics is divided into two parts, static authentication and dynamic authentication. Mouse features are easy to handle even without user's consent. The mouse authentication can be divided into 2 parts, registration phase and login phase. The captured mouse features by assigning a mouse related task helps to build a template at the time of registration. The same template is compared with login details which are captured by the mouse task. In case of laptop, touchpad helps to extract the mouse features. The sensitivity of the mouse is also an important factor while performing the mouse activities. The mouse dynamics not only focuses on basic data but also on advanced features. Single clicks and double clicks [6] are used to gather the clicks related data. Data is stored and the other details of distance coverage also helpful to separate the legitimate user from hacker. Directional features and angular movement tries to find the rotation and angle of mouse movement to complete the task. The angular movement can be positive or negative. The focus of Directional code is on the 8 basic directions. When two movements show same directional code, then angle of movement come into the picture and differentiate between the two different motions of mouse. The combination of above features adds the variability and uniqueness to the research in mouse dynamics technique. The next section covers the description of mouse related features.

A. Features related to Mouse Dynamics [2]

1. Interval between consecutive mouse single click: It's the time duration between two consecutive single clicks of mouse. Single click generated by the user are captured and the time difference between them adds as security parameter. The interval is comparatively very small. The duration differentiates the action of single click from the rest of the user.
M1 = SC2 (Single click 2) - SC1 (Single Click 1)

2. Relative Interval between consecutive mouse single clicks: It's the time interval between two nonconsecutive single clicks is called as Relative interval. The relative time difference adds the additional check for the timing of single clicks.
M2 = SC3 (Single click 2) - SC1 (Single Click 1)

3. Interval between consecutive mouse Double click: It's the time duration interval between two consecutive double clicks. Double click done by the user are captured and the time difference between them adds as security parameter. The interval is comparatively small. The duration differentiates the action of double click from the rest of the user.
M4 = DC2 (Double click 2) - DC1 (Double Click 1)

4. Relative Interval between consecutive mouse double clicks : It's the time duration between two nonconsecutive double clicks is called as Relative interval. The relative time difference adds the additional check for the timing of double clicks.
M5 = DC3 (Double click 3) - DC1 (Double Click 1)

B. Related Work To Mouse Dynamics

[8]Author has proposed two phase authentication system with numbers of dots placed on the screen. 10 dots were clicked by the 20 times for the training purpose by each user. Mouse features were calculated which includes angular movement, speed, deviation from a straight line, angle. Standard deviation, minimum, maximum and average of 4 parameters made it sixteen parameters. The verification of the legitimate done by the standard deviation. The results showed error rate of 20% and it was decreased by average and standard deviation for the 15 users. Author also focused on passive authentication by observing the mouse pattern for 15 minutes.

[9]Author focused on the preexisting ideas and found out the limitations of them. Author classified into three parts, Impractical Verification Time, Uncontrolled Environmental Variables and remote Access scenario. Author used MDA techniques and tested the system for 18 users. Results showed different results with existing system. The author pointed out the reasons as controlled environment or difference among the test subjects. The author concluded that mouse authentication was not a good choice for user authentication because of fluctuations.

[10]Author described a new behavioral biometric system based on the pointing devices. Using statistical pattern recognition system, author developed classifier based on user interaction which accepts the user if he satisfies the threshold value. Parson density

estimation and a unimodal distribution were used as statistical model. Author used memory game to collect the pointing device features and testing showed that mouse can be used for authentication purpose effectively.

V. CONCLUSION

The above paper discussed the different methods authentication techniques that may be added to the existing system to make existing system more secure. One of the problems associated with the keyboard dynamics is improper 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). Future works includes Mobile, PDA and ATM machines. The fusion of keystroke with the other biometrics like mouse dynamics can be new idea. The fusion of keyboard dynamics with mouse dynamics will help to bring FAR, FRR AND EER value to near zero and hence can achieve higher security.

ACKNOWLEDGEMENT

Author would like to thank all the references.

References

[1] A. K. Jain, P. Flynn and A. A. Ross, Handbook of Biometrics, Springer, 2008.

[2] Vanaja Roselin.E. Chirchi, L.M.Waghmare and E.R.Chirchi, “Iris Biometric Recognition for Person Identification in Security Systems”, International Journal of Computer Applications (0985 –8888), Volume 24–No.9, June 2011

[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] F. Monrose, A. Rubin, Authentication via Keystroke Dynamics ACM Conference on Computer and Communications Security (1997)48-56.

[5] A. Peacock: Learning User Keystroke Latency Patterns (Preliminary Report)

[6] Patrick Bours, "Continuous keystroke dynamics: A different perspective towards biometric evaluation", Information Security Technical Report Volume 17, Issues 1–2, pp. 36–43, February 2012.

[7] F. Monrose, A. Rubin, Authentication via Keystroke Dynamics ACM Conference on Computer and Communications Security (1997)48-56.

[8] Shivani Hashiaa, Chris Pollettb, Mark Stamp, “On Using Mouse Movements As A Biometric”, International Conference on User Science and Engineering (i-USEr), pp. 206 – 211, Dec 2011

[9] Zach Jorgensen and Ting Yu, “On Mouse Dynamics as a Behavioral Biometric for Authentication”, Systems Journal, IEEE (Volume: 8, Issue: 2), pp. 262 – 284, June 2013.

[10] Hugo Gamboa, Ana Fred, “A behavioral biometric system based on human-computer interaction”, Proc. SPIE 5404, Biometric Technology for Human Identification, 381, August 25, 2004.

[11] P. S. Teh, A. B. J. Teoh, T. S. Ong and C. Tee, "Keystroke dynamics in password authentication enhancement," Expert Systems with Applications 37 (2010) 8618–8627, Elsevier,2010.