المجلة الإلكترونية الشاملة متعددة التخصصات
العدد العشرون شهر(1) 2020

Detect the Authorization of the User Based on Login Process Duration by Using Virtual Keyboard

[1]Makera M Aziz
Department of Computer Science, College of Computer Science and Mathematic
University of Mosul

[2]Dina Rafaa Ahmed
Software Department ,College of Computer Science and Mathematics
University of Mosul
dina.rafaa1986@gmail.com

Abstract

This paper suggested a method that can be used to detect the authorization of user by using a method that compute the time that need for the user to complete the login process. The method used two-behavior biometrics first is the keystroke the second is mouse movement, the purpose of using two biometrics is to get better performance from the system. The system used virtual keyboards to reduce the factors that affecting typing speed that result from different keyboard design. The users asked to insert the same password and same user name to check the time that they need to finish login process for the same text.

Keywords: Detect, Authorization, User Based, Login Process Duration, Virtual Keyboard.

Introduction

The development of technology in last two decades and the huge amount of information that been shared through webs, lead the researchers to find new technology to provide a secure environment for this information to be exchange Safely through the nets (Smita S. Mudholkar , Pradnya M. Shende , Milind V. Sarode, 2012).Password is one of the methods that used to save the information from unauthorized users but this methods has some of the problems (Ankit Parekh, Ajinkya Pawar , Pratik Munot , Piyush Mantri, 2011) because the password can be lost,

copied ,share because of that the researcher used other type of biometrics like physical biometrics and behavior biometrics. These biometrics has some of the properties that solve the problem of the password, these biometrics cannot be duplicate, share or lost. This Biometric can be physical biometrics like fingerprints, face recognitions and signature. Behavior biometrics like keystroke dynamic, mouse movement dynamic and voice recognition. Authentication can be divided into three different types (N.L. Clarke, S.M. Furnell, 2007),specifically, knowledge-based, token-based and biometric- based authentication .Knowledge-based authentication verifies user identity by the information in the user memory(something-we-know), such as a password or PIN. This kind of authentication is convenient to use, but vulnerable to brute force attacks, dictionary attacks, shoulder- surfing attacks (Goucher, 2011)and smudge attack (Aviv AJ, Gibson K, Mossop E, Blaze M, Smith JM, 2010)The token-based authentication identifies uses via an object carried by the user (something we have),for instance, a SIM card or credit card. Biometric-based authentication identifies the user through the biometric characteristics of the user (something we are).

There are two types of biometrics: physical and behavioral. Physical biometrics includes palm, fingerprint, and iris recognition. On the other hand ,behavioral biometrics include the signature (Syukri AF, Okamoto E, Mambo M., 1998) and keystroke dynamics (L.C.F. Araujo , L.H.R. Sucupira , M.G. Lizarraga ,L.L. Ling ,J.B.T. Yabu-Uti, 2005) (Romain Giot , Mohamad El-Abed , Baptiste Hemery , Christophe Rosenberger, 2011) (Daniele Gunetti , Claudia Picardi, 2005) (Seong-seob Hwang , Sungzoon Cho , Sunghoon Park, 2009). Biometric features are difficult to lose, steal, or imitate due to their uniqueness. Among the biometric authentications, physical bio- metrics shows the best identification performance. Unfortunately ,it requires advanced support of devices to achieve high discriminability, such as a fingerprint or iris scanner .In contrast, keystroke dynamics can be used to provide additional protection for password authentication due to their advantages of unobtrusiveness and the ability to adopt without any other supporting devices (Chao-Liang Liu, Cheng-Jung Tsai, Ting-Yi Chang , Wang-Jui Tsaid, Po-Kai Zhong, 2015).

This Keystroke dynamics is a behavioral biometrics based on the hypothesis that different people type in uniquely different typing rhythm. It is an intelligent data processing technique that analyzes the way user's type at terminals by monitoring the keyboard inputs in attempt to identify the users based on their habitual typing patterns (Ramu Thanganayagam, Arivoli Thangadurai, 2015). Keystroke is one of the behavioral biometrics that difference from person to person it can be used for authorization detection it is different from person to person and each person has its own pattern that use when he/she type. Recognition of the pattern typing can be used for authorization detection (Daniele Gunetti, Claudia Picardi, 2005). The typing speed measures the time that need by the user to go from one key to another key in keyboard also can be used to measure the typing speed one touch screen devices. Mouse movement is the other type of behavior biometrics that use to check the authorization of users. It is also different from person to another (Bassam Sayed, Issa Traor, Isaac Woungang, 2013). The login process is need both biometrics keystroke with mouse movement. That mean the users have different time to finish the login process even they have the same password and id. This study will measure the time that need by each user to login to system when they are using the same used name and password.

Related Works

(Chang, 2012) proposed system that combine the keystroke biometric and neural network and used the key stroke to generate the private key that can use as long-lived key rather than statistical key that saved in computer storage and that dynamic generation of key help to make password revealed if storage unit is damage generation of private key goes through four phases (a) application phase (b) training phase (c) key generation phase (d) cryptographic function phase. (N. Harun , W. L. Woo , S.S. Dlay, 2010)this paper studied the time that needs to transfer from one key to another to type difference characters by using multilayer Neural Network for training and valeting BP learning algorithm has been used. (Mohammad S. Obaidat, David T. Macchiarolo, 1993)This paper focused on the typing technics that follow by each user. Artificial neural network used to identify the users. The author studied the time that need by each user to inter the character. The results showed that 97.8% could be recognized successfully.

This system can be used to improve the computer system security. (Nathan D'Lima m, Jayashri Mittal, 2015) proposed new method that obtain information about users by using multiple sensor, and used neural network to recognize the user's typing pattern. (Fabian Monrose, Aviel D. Rubin, 2000) the author used fix length text instate of free long text. The technics that used to classify was Enclidance distance and Bayesian alike classer. (AAlsultan, K. Warwick, 2013) a text of 380 characters is used to enroll a user and a 75 characters string is used in testing.

To keep the test user friendly, only one sample per user was taken. Only 15 users were used in the experiment. This method takes into account the layout of the keyboard and stores keystroke latencies for each key and pair of keys. Euclidean distance is used to find the level of similarity between the login data and the user's stored template. This method gives an FAR of 21 % and FRR of 17% which is because of the less number of training samples. (D. Hosseinzadeh, S. Krishnan, A. Khademi, 2006) introduced Gaussian Mixture Models (GMM) in keystroke identification. A total of 8 subjects were enrolled into their system by typing their full name ten times. This is logical as lower number of characters has lower complexity pattern and thus can be easily replicated. The Expectation Maximization algorithm was used to train the GMMs separately using the two extracted keystroke features. Log-likelihood test was performed on the test vector to obtain a probability on how close it was as compared to the user template. The experiment produced result of FRR of 2.4% and FAR of 2.1 %. However, due to the small number of subjects tested, the result obtained was not decisive.

In (Y. Sang, H. Shen, P. Fan, 2004) authors have tested the efficiency of SVM in the keystroke dynamics. They have tested one-class SVM and two-class SVM (in this case, impostors' data simulating the second class are generated). The performance trade-off and time consumption were better and faster than with neuronal networks, but the experiment was done with only 10 individuals. Joyce and Gupta (Rick Joyce, Gopal Gupta, 1990) were used keystroke latencies from strings of first name, last name, username, and password. It is used absolute distances for authentication and using only absolute distances they achieved a false acceptance rate (FAR) of 0.25% and a false reject rate (FRR) of 16.67%.

The authors built a mean reference signature for eight sets of users' keystroke patterns. They then computed the norm of the test keystroke pattern to the mean reference signature, which was used to determine if a user was legitimate based on a predefined threshold. Rodrigues (Ricardo N. Rodrigues , Glauco F. G. Yared , Carlos R. do N. Costa , João B. T. Yabu-Uti , Fábio Violaro , Lee Luan Ling, 2006) implemented Hidden Markov Models as classifier and limited their investigation over numerical passwords of length eight. Twenty people were invited to contribute to this experiment. Each individual was instructed to type their passwords ten times in four different sessions, yielding a total of 800 samples. An EER of 3.6% was obtained.

Methods and Materials

- **Design a virtual keyboard**

The keyboard type and brand is one of the important factor that affecting. The keystroke speed of user because of the different design. The different keyboards has different key size and different distance between the key , all of these affecting the type speed of the person and change the time that need to transfer from one key to another key in key board. (Anna Pereira, David L. Lee, Harini Sadeeshkumar, Charles Laroche, Dan Odell, David Rempel, 2013) (Placeholder1).The device also is affect the time that need to type one text. For example, the time that need to type one text is different if you are using desktop, laptop and mobile, to avoid these various and reduce the factors that affecting the behavior biometric, we will use virtual keyboard that showed in figure 1 that will same for all the users and this and this keyboard will appear on login and registration windows. The user has to use this keyboard to insert the ID password and one line text to text to increase the range of the time that need to complete login process.

Mouse movement it is the one of the behavior biometric that different from person to person using virtual keyboard need to use mouse to type the characters. That mean the system will use two behaviors biometric to detect the authorization. And this will increase the performance of the system.

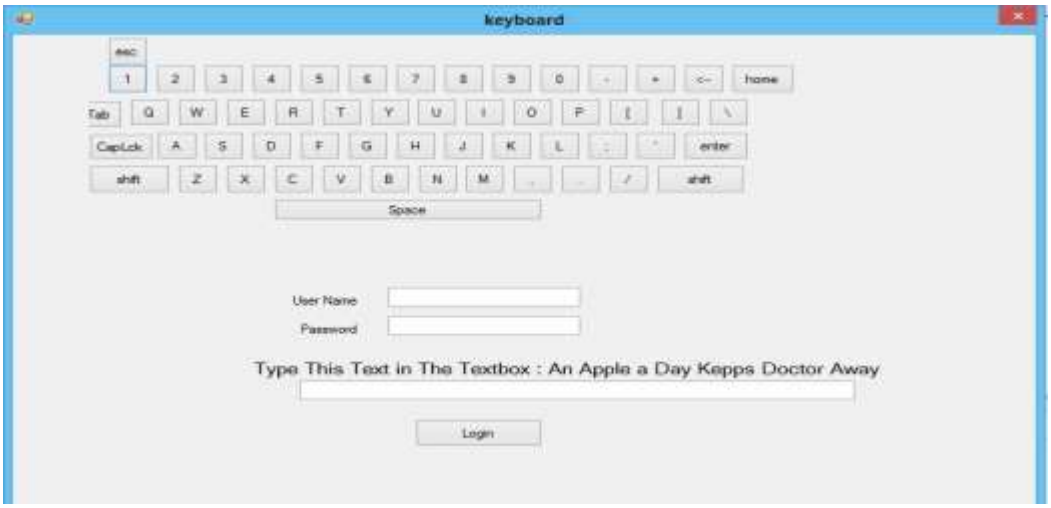

Figure 1: The virtual Keyboard That Use for login process

- **User Registration Process**

The user of the system will register as new user and insert his and insert his / her information by using the virtual keyboard, after that user will login to the system five time to check the time that need for login process that mean the login will repeat five time and if the time that need for each login is the same (± 2 second is allow) the time will be save for each user. When the user login to the system the authorization process will be check the user name, password and login process duration.

- **Data Collection**

The data that use for this system has been collected from ten users. The users asked to type the same user name and password and one-line text to compute the time that they need for each user to type the same characters with same sequences to finish the login process. Typing the same words by using same keyboard will reduce the factors that affecting the typing speed and the system will depend only on typing behavior.

- **Calculate the login duration**

For each user the system will calculate the duration that need to complete login process this method start from the user insert the first letter of his/her user name till click on login button.

Login Duration = Insert the user name + insert the password + insert the text + click login button

The system will calculate the time for each user for five time and take the average of time. The system will accept the duration for user ± 2 second of average.

Results

After collecting the data from 10 users, the time that need for login has been compute for each user of the system. The result showed that the user needs different duration to complete the login process. Figure number 2 shows the time that need for each user to complete the login process.

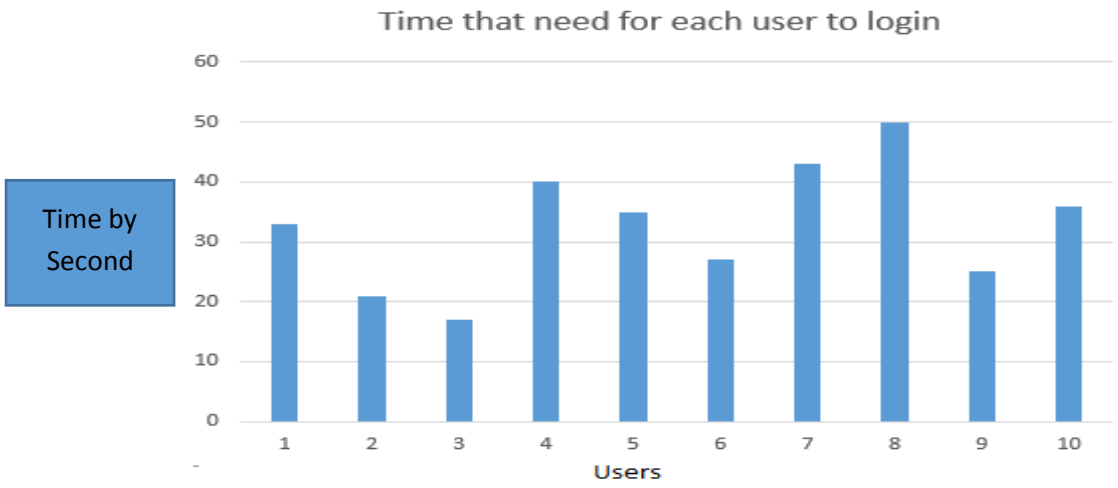

Figure 2: Time that need to finish login process

The time that need for the same user to finish the login process is showed in figure 3 and table 1 and they showed that the time that need for the same user to finish login process is very near to each other.

Table 1: The time that need for each user to finish the login in three different login trial

USER	FIRST LOGIN	SECOND LOGIN	THIRD LOGIN	MEAN	SDANDARD DIVIATION
1	33	33	31	32.33	1.15
2	21	19	19	19.67	1.15
3	17	18	17	17.33	0.58
4	40	42	42	41.33	1.15
5	35	35	35	35.00	0.00
6	27	27	27	27.00	0.00
7	43	42	42	42.33	0.58
8	49	48	48	48.33	0.58
9	25	25	25	25.00	0.00
10	36	37	36	36.33	0.58

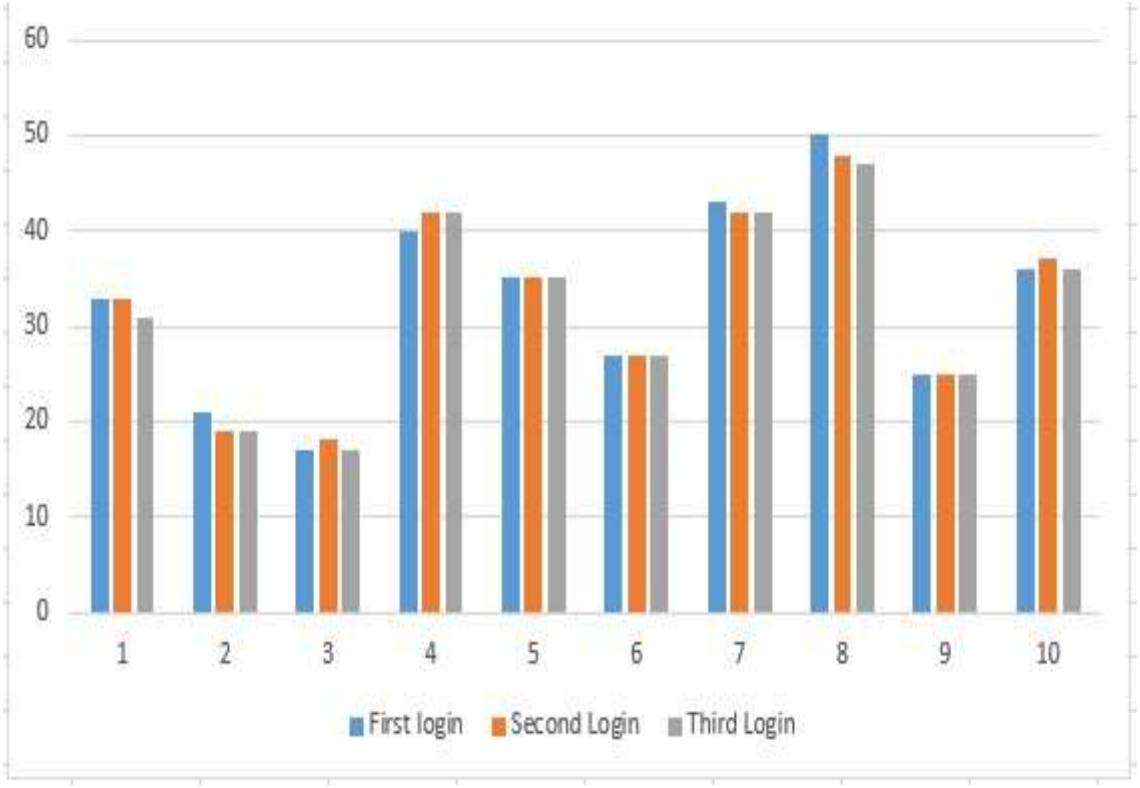

Figure 3 : Time that need for the same user to finish the login process

Conclusion

The result showed that each user need different time from the other to finish the login time and he/she need the same time when repeat the login process with ±2 second. That mean the keystroke behavior can be used as authorization detector. Using virtual keyboard and asking the users to type the same user name and password by using the virtual keyboard reducing the factors that affect the time the needed to type the text.

References

AAlsultan , K. Warwick. (2013). User-Friendly Free-text Keystroke Dynamics Authentication for Practical Applications. *International Conference on Systems, Man, and Cybernetics.* IEEE.

Ankit Parekh, Ajinkya Pawar , Pratik Munot , Piyush Mantri. (2011). Secure Authentication using Anti-Screenshot Virtual Keyboard. *International Journal of Computer Science Issues, 5*(2), 534-537.

Anna Pereira, David L. Lee, Harini Sadeeshkumar, Charles Laroche, Dan Odell, David Rempel. (2013). The Effect of Keyboard Key Spacing on Typing Speed, Error, Usability, and Biomechanics: Part 1. *HUMAN FACTORS, 55*(3), 557-566.

Aviv AJ, Gibson K, Mossop E, Blaze M, Smith JM. (2010). Smudge attacks on smartphone touch screens. *Proceedings of the 4th USENIX conference on offensive technologies* (pp. 1-7). Washington: USENIX Association.

Bassam Sayed , Issa Traor , Isaac Woungang. (2013). Biometric Authentication Using Mouse Gesture Dynamics. *IEEE Systems Journal, 7*(2), 262 - 274.

Chang, T.-Y. (2012). Dynamically generate a long-lived private key based on password. *Information Sciences, 211*, 35-47.

Chao-Liang Liu, Cheng-Jung Tsai, Ting-Yi Chang , Wang-Jui Tsaid, Po-Kai Zhong. (2015). Implementing multiple biometric features for a recall-based graphical keystroke dynamics authentication system on a smart phone. *Journal of Network and Computer Applications, 53*, 128-139.

D. Hosseinzadeh, S. Krishnan , A. Khademi. (2006). Keystroke identification based on Gaussian Mixture Models. *Conference on Acoustics, Speech and Signal Processing* (pp. 1144-1147). IEEE.

Daniele Gunetti , Claudia Picardi. (2005). Keystroke analysis of free text. *ACM Transactions on Information and System Security (TISSEC), 8*(3), 312-347 .

Fabian Monrose , Aviel D. Rubin. (2000). Keystroke dynamics as a biometric for authentication. *Future Generation Computer Systems*, 351-359.

Goucher, W. (2011). Look behind you: the dangers of shoulder surfing. *Computer Fraud & Security, 2011*(11), 17-20.

L.C.F. Araujo , L.H.R. Sucupira , M.G. Lizarraga ,L.L. Ling ,J.B.T. Yabu-Uti. (2005). User authentication through typing biometrics features. *IEEE Transactions on Signal Processing, 53*(2), 851 - 855.

Mohammad S. Obaidat , David T. Macchiarolo. (1993). An On-Line Neural Network System for Computer Access Security. *TRANSACTIONS ON INDUSTRIAL ELECTRONICS.* IEEE.

N. Harun , W. L. Woo , S.S. Dlay. (2010). Performance of Keystroke Biometrics Authentication System Using Artificial Neural Network (ANN) and Distance Classifier Method. *International Conference on Computer and Communication Engineering.* Kuala Lumpur: IEEE.

N.L. Clarke, S.M. Furnell. (2007). Advanced user authentication for mobile devices. *Computers & Security, 26*(2), 109-119.

Nathan D'Lima m ,Jayashri Mittal. (2015). Password Authentication using Keystroke Biometrics. *International Conference on Communication, Information & Computing Technology.* Mumbai: IEEE.

Ramu Thanganayagam , Arivoli Thangadurai. (2015). Fusion Approach on Keystroke Dynamics to Enhance the Performance of Password Authentication. *International Conference on Electrical, Computer and Communication Technologies (ICECCT).* Coimbatore, India: IEEE.

Ricardo N. Rodrigues , Glauco F. G. Yared , Carlos R. do N. Costa , João B. T. Yabu-Uti , Fábio Violaro , Lee Luan Ling. (2006). Biometric access control through numerical keyboards based on keystroke dynamics. *ICB'06 Proceedings of the 2006 international conference on Advances in Biometrics*, (pp. 640-646). Hong Kong.

Rick Joyce , Gopal Gupta. (1990). Identity Authentication Based on Keystroke Latencies. *Communications of the ACM, 33*(2), 168-176.

Romain Giot , Mohamad El-Abed , Baptiste Hemery , Christophe Rosenberger. (2011). Unconstrained keystroke dynamics authentication with shared secret. *Computers & Security, 30*(6-7), 427 -445.

Seong-seob Hwang , Sungzoon Cho , Sunghoon Park. (2009). Keystroke dynamics-based authentication for mobile devices. *Computers & Security, 28*(1-2), 85-93.

Smita S. Mudholkar , Pradnya M. Shende , Milind V. Sarode. (2012). BIOMETRICS AUTHENTICATION TECHNIQUE FOR INTRUSION DETECTION SYSTEMS USING FINGERPRINT RECOGNITION. *International Journal of Computer Science, Engineering and Information Technology, 2*(1), 57-65.

Syukri AF, Okamoto E, Mambo M. (1998). A user identification system using signature written with mouse. *Information security and privacy. Springer*, 403- 414.

Y. Sang, H. Shen , P. Fan. (2004). Novel impostors detection in keystroke dynamics by support vector machine. *Parallel and Distributed Computing: Applications and Technologies*, 666-669.