The Analysis of Emotions over Keystroke Dynamics
Su-xia CUI1*, Odinaka EKWONNAH1 and Yong-hui WANG2
1Electrical and Computer Engineering Depart Prairie View A&M University, Prairie View, TX USA
2Computer Science Department, Prairie View A&M University, Prairie View, TX USA
*Corresponding author

Keywords: Cybersecurity, User authentication, Keystroke dynamics.

Abstract. Computer is one of the fastest growing industries in the past decades. Computer network further enables the information exchange from far remote locations within an unbelievable speed. As more and more devices are connected on the Internet of Things (IoT) network, organic interface on smart devices is influencing the security requirements. The attack on mobile devices and web interfaces constitute the major source of attacks in computer networks. Password as a form of authentication based on “what you know” has become widely used in computer devices and networks because of its ease of use and limited processing requirements by the application. However, this form of authentication is susceptible to various attacks including brute force attack, shoulder surfing, memory dump and spoofing. Also this form of authentication complicates the security requirements of IoT devices. Traditional keystroke features related to timing, depression of keys, and virtual key force of users, have been considered for authentication purposes. Recently, human emotion has been studied which can add another unique feature applied to password authentication. This paper investigates the effectiveness of the keystroke dynamics with the influence of emotion.

Introduction

Now-a-days computer facilities have entered the era of high performance. Besides computational power, High Performance Computing (HPC) clusters also equipped us with massive storage capability in a form of data cloud. Through network connection, various data sets ranging from medical, financial, and research territories can be transmitted to a remote data cloud. A failure in the defense of information security will not only affect a user’s privacy, but also threatened the economic development of companies or possibly the national security of a country. According to the 2006 Computer Crime and Security Survey [1], the intrusion to computer devices is the second greatest source of financial loss. Thus to be able to verify the user at time of login is crucial. Identification is when we try to find the identity of an unknown user. This is done by checking if the unknown user matches any of the known users’ identities. User authentication is the verification of an active human-to-machine transfer of credentials required for confirmation of a user’s authenticity [2]. It begins when a user tries to access information. First, the user must prove his/her access rights. When logging into a computer, users commonly enter usernames and passwords for authentication purposes. This login combination, which must be assigned to each user, authenticates access. In order to be efficient and secure, the user must adopt a strict management of his/her credentials.

User Authentication. Usually the authentication can be classified by using either traditional or biometric methods. Traditional methods include knowledge based and object based, while biometric methods can be categorized as physical recognition and behavioral recognition. Keystroke is one example under behavioral recognition [3]. With the knowledge of biometrics, it is possible to authenticate and identify users based on who they are, not what they possess or what they know [4]. However many computer systems use the simple username/password scheme for authentication, even though it suffers from the security-usability trade-off dilemma [5]. Passwords can be guessed through different strategies such as social engineering, spyware, dictionary attack, and mere brute force attacks. These are all reasons for the user to employ extreme measures to safeguard his/her
computer by using long and complex passwords, which are unfriendly and hard to memorize. Also, most devices including IP security cameras are shipped with a default password in which the user sometimes does not change after installation. Attackers are able to gain access by using the default password of such devices. It is therefore ideal to use an alternative authentication method that can be of low-cost yet provide ease of use and transparency to the user in addition to security robustness.

**Biometric.** Biometrics, the physical traits and behavioral characteristics that make each of us unique, is a natural choice for identity verification. Unlike keys or passwords, biometrics cannot be lost, stolen, or overheard, and in the absence of physical damage, it offers a potentially foolproof way of determining someone’s identity. Physiological characteristics, such as fingerprints, are good candidates for verification because they are unique across a large section of the population [6]. The advantage of physical biometrics is that it has high accuracy compared to behavioral biometrics. In contrast, physical biometric devices need to be implemented which to some extent increase the cost of authentication. Behavioral biometrics is one of the popular methods for the continuous authentication of a person, but it produces insufficient accuracy because behavior is unstable and can change over time.

**Keystroke Dynamics.** Kevin Killourhy and Roy Maxion in [7] worked on a methodology for keystrokes biometrics [8] and presented a benchmark datasets. An application that presented stimuli to the subjects was built for recording their keystrokes; and an external reference timer for time stamping those keystrokes. The software presented the subject with the password to be typed. If the subject makes a typographical error, the application prompts the subject to retype the password. In this manner, they recorded timestamps for 50 correctly typed passwords in each session. In their methodology, the user data was used for model training, genuine user testing and imposter testing. They presented a procedure—written in the R language—to evaluate three anomaly detectors (called Euclidean, Manhattan, and Mahalanobis). Our study adopted this keystroke dynamics data collection scheme to create the baseline of database to study the influence from emotion. The use of keystrokes pattern has been considered as a form of password hardening in applications. This involves the extractions of features that can be used to build a model and saved as template in addition to the user’s authentication details. Features commonly used from keystrokes data include the duration of typed keys, latency between two consecutive keystrokes, Digraph, and Tri-graph [9].

**Emotions.** It may be useful to think of emotions as the flow and experience of feelings, for example, joy, sadness, anger, or fear. Emotions can be triggered by something external (from seeing a friend suffer or watching a movie) or internal (an upsetting memory) [10]. The cognitive approach has been attributed to Walter Cannon who suggested that emotion is experienced within the brain, independently of the sensations of the body [11]. The physical approach focuses on the physiological response (e.g. elevated heart rate) that occurs just prior or during an emotional episode; this approach has largely been attributed to William James [12]. According to [13], two generally agreed-upon aspects of emotion are: (a) Emotion is a reaction to events deemed relevant to the needs, goals, or concerns of an individual and (b) Emotion encompasses physiological, affective, behavioral, and cognitive components. When refer to emotional states in this thesis, we mean the internal dynamics (both cognitive and physiological) that are present during an emotional episode and we describe the emotional experience as what an individual perceives of their emotional state [13].

**Data Collection**

The emotions processed by users’ while typing are considered as an added feature in order to improve the level of accuracy in keystroke dynamics. There are different ways of collecting data on emotion; each has their own advantages and disadvantages. Here we discuss the most common approach in laboratory settings where moods are induced into the participant being studied in order to observe and collect data. We also discuss collecting data in a more naturalistic setting, capturing emotions as they occur naturally in participants, in a less influenced manner.
One commonly used technique in studies on emotion is the use of Mood Induction Procedure (MIP) laboratory studies [14] which is an experimental technique devised to establish a particular mood in a subject. Westermann et al. list nine different categories of MIPs from the literature, here we adopt two of these (Veltren and film/story) to obtain mood induction entails. Forty volunteers randomly selected provided the inputs through this data collection software (sample interface illustrated in Fig. 1), which built the database for our research. Each person will need to input 50 times of the fixed sentences in various emotional modes.

![Data Collection Interface Highlighting the Fixed Text Entry for Emotional States.](image)

**Data Analysis**

In total, each volunteer will provide 50 entries to the database. So multiply the total of 40 volunteers, we received 2000 rows of raw data collected during the experiment. Statistical method involves the computation of the mean and standard deviation of the features in the template. There are always statistical errors in recognition patterns, so same situation exists in any algorithm used in keystroke dynamic authentication or identification. Those error rates define the quality of the application of a keystroke dynamic system. An effective biometric system in general can distinguish people from each other. A set of metrics has been defined, in order to calculate the accuracy and the efficiency of biometric system. The set of metrics is described in Table 1. The resulting datasets is a collection of keystrokes features and a corresponding emotional state label. The features are briefly illustrated in Figure 2.

![Keystroke Extracted Features on MySQL Database Interface.](image)
Table 1. Key Features Obtained from Data Collection.

| S/N | Description                      | Meaning                                                                 |
|-----|----------------------------------|-------------------------------------------------------------------------|
| 1   | Keytyped                         | Number of keys typed                                                   |
| 2   | TimePress                        | The duration of key pressed across all keys                            |
| 3   | TimeRelease                      | The duration of key release across all keys                            |
| 4   | intervalTimePP                   | Duration from key pressed to the next key pressed across all keys      |
| 5   | intervalTimeRR                   | Duration from key release to the next key release across all keys      |
| 6   | flightTime                       | The time between "key up" and the next "key down across all keys      |
| 7   | Emotional_State                  | Emotional State when keystoke features are extracted                   |

There are several methods to analyze the data generated by this research. For example, Machine Learning (ML) can be used to train the data set and test the dependence. But it is very time consuming and computational intensive. This paper presents one of them, which uses Analysis of variance (ANOVA). ANOVA tests the hypothesis to see whether the means of two or more populations are equal. The null hypothesis states that all population means (factor level means) are equal while the alternative hypothesis states that at least one is different.

To determine whether any of the differences between the means are statistically significant, one can compare the p-value to the significance level to assess the null hypothesis. The null hypothesis states that the population means are all equal. Usually, a significance level (denoted as α or alpha) of 0.05 works well. A significance level of 0.05 indicates a 5% risk of false alarm.

- \( P\)-value \( \leq \alpha \): The differences between some of the means are statistically significant.
- \( P\)-value \( > \alpha \): The differences between the means are not statistically significant.

This test is done by using a one-way analysis of variance, as it is used to determine if there are any statistically significant differences between the means of two or more independent groups. Also, it is important to realize that the one-way ANOVA is an omnibus test statistic and cannot tell you which specific groups were statistically significantly different from each other; it only tells you that at least two groups were different. In this test, we compared the mean of the group of data collected at each emotional state (Joy, Angry, Sad, and Surprise) against the data collected at the base emotional state. The test was carried out by using python programming language running on anaconda platform.

Among all the compared pairs, most of them show no or boundary difference. Only the angry mode experience significant difference as shown in Figure 3 (Base vs. Sad) has a significant difference with the \( P\)-value of DT (Dwell Time) and ITPR (Interval Time of Press-Release) being less than or equal to 0.05.

![Figure 3. Base vs. Sad.](image)
Conclusions
The current study aimed to test the hypotheses that keystroke dynamics may be influenced by emotions. Based on the experimental setup, traditional statistical methods could be used to examine the variance and reveal the relationship, without the use of sophisticated ML algorithms. It was hypothesized that difference in keystroke dynamics due to different emotional states would appear as a factor to influence the biometric identification result. The research question between emotions and keystroke dynamics are answered by using simple statistical methods instead of using ML algorithms. The evidence found supports the hypotheses that the effect of emotion plays a role in keystroke dynamics exists in certain mode. However, the size of the emotional effect is small, compare to the individual variability. And the data collecting environment can be modified to add a close loop to prove the emotion states. Future studies can be extended to conducting the experiment over a longer period of time or giving the participants more incentives (or other forms of encouragement) to keep submitting data throughout the study’s duration. Due to these ethical considerations, care must be taken in the application of this research in real-world applications.

Acknowledgement
This research was financially supported by the National Science Foundation HBCU-UP TIP project (Award #1332566), HBCU-UP RIA (Award #1411260), and MRI project (Award #1229744).

References
[1] S. Bleha, C. Slivinsky, et al, Computer-Access Security Systems Using Keystroke Dynamics, IEEE Trans. on Pattern Anal, vol. 12, issue 12 (1990), pp. 1217-1222.
[2] D. Gunetti, and C. Picardi, Keystroke Analysis of free text. ACM Trans. Inf. Syst. Security, Vol. 8, issue 3 (2005), pp. 312-347.
[3] A. Reham, G. Tarek, et al., Biometric and Traditional Mobile Authentication Techniques: Overviews and Open Issues, Bio-inspiring Cyber Security and Cloud Services: Trend and Innovations, Springer, DOI 10.1007/978-3-662-43616-5_16, Feb. 2014.
[4] A.K. Jain, A. Ross, and S. Prabhakar, An Introduction to Biometric Recognition, IEEE Transactions on Circuits and Systems for Video Technology, vol. 14, issue 1, Jan. 2004.
[5] D. Feth, User-centric Security: Optimization of the security-usability Trade-off, Proceedings of the 2015 19th Joint Meeting on Foundations of Software Engineering, pp. 1034-1037.
[6] F. Monrose, and A. D. Robin, Keystroke Dynamics as a Biometric for Authentication, Future Generation Computer Systems, vol. 16, 2000, pp. 351-359.
[7] K. Killourhy, and R. Maxion, Comparing Anomaly-Detection Algorithms for Keystroke Dynamics, Proceedings on the 47th IEEE/IFIP International Conference on Dependable Systems & Networks (DSN), pp. 125-134, Estoril, Lisbon, Portugal, June 29-July 2, 2009.
[8] Wikipedia, Keystroke Dynamics, in Wikipedidia [Online]. Available: http://en.wikipedia.org/wiki/Keystroke_dynamics. [Accessed January 2018].
[9] J. Leggett, G. Williams, et al, Dynamic Identity Verification via Keystroke Characteristics, International Journal of Man-Machine Study vol. 28, pp. 67-76, 1988.
[10] K. Lawson, What are Thoughts & Emotions? https://www.takingcharge.csh.umn.edu/what-are-thoughts-emotions. [Accessed Sept. 2018].
[11] W. B. Cannon, The James-Lange Theory of Emotions: A Critical Examination and an Alternative Theory, The American Journal of Psychology, vol. 39, pp. 106-124, 1927.
[12] J. Barbalet, William James’ Theory of Emotions: Filling in the Picture, Journal for the Theory of Social Behavior, Dec. 2001, vol. 29, no. 3, pp. 251-266.

[13] S. Brave, and C. Nass, Emotion in human-computer interaction, in the human-computer interaction handbook, vol. 1, pp. 81-96, Sept. 2002.

[14] D. Kučera, and J. Havigerb, Using Mood Induction Procedures in Psychological Research, in Proceedings of Social and Behavioral Sciences, vol. 69, pp. 31-40, Dec 2012.

[15] M. Villani, C. Tappert, and et al, Keystroke Biometric Recognition Studies on Long- Text Input under Ideal and Application-Oriented Conditions, in Proceedings of the 2006 Conference on Computer Vision and Pattern Recognition Workshop, vol. 39, 2006.