Proceedings of the 2009 IEEE International Conference on Systems, Man, and Cybernetics
San Antonio, TX, USA - October 2009

Keystroke-Based Authentication by Key Press Intervals as a Complementary Behavioral Biometric

Shallen Giroux, Renata Wachowiak-Smolikova, *Member, IEEE*, and Mark P. Wachowiak*, *Member, IEEE*
Department of Computer Science and Mathematics
Nipissing University
North Bay, ON Canada
*markw@nipissingu.ca

***Abstract*—Analysis of keystroke dynamics can be useful in protecting personal data because an individual is authenticated not only by password, but also by that individual's keystroke patterns. In this way, intrusion becomes more difficult because the username/password pair, as well as the typing speed and correct keystroke pattern must both be duplicated. The purpose of this paper is to present a keystroke analysis tool that can be incorporated into distributed systems and web-based services. This study also assesses the potential of keystroke analysis as a complementary authentication mechanism. Eleven individuals entered a password into specially developed keystroke analysis software twenty times over a course of four sessions. The data were statistically analyzed to determine keystroke patterns. Tests were performed to verify whether the users could be properly authenticated. Results show that authentication with mean key press timings resulted in very good false acceptance rates, while allowing access to appropriate users.**

***Keywords*—biometrics, keystroke dynamics, authentication**

I. Introduction

Biometrics is the study of employing physiological and behavioral characteristics that uniquely identify a person [1]. Physiological characteristics, including fingerprints, retina vascular patterns, hand geometry, and facial characteristics, are biologically-based characteristics that are unique and unalterable, unless they are altered by physical harm. Behavioral characteristics, such as handwritten signatures, voice patterns, and keystrokes, comprise behavior patterns that can also be considered as unique. These characteristics arise from certain physiological traits (i.e. keystroke patterns are affected by hand size and finger musculature), as well as psychological and environmental factors. Behavioral measures are dynamic, as they may change throughout life [2].

When attempting to access a computerized system, people are normally authenticated through a username and password. It has been demonstrated that this form of authentication is not completely safe because, through a series of different attacks, an intruder can determine the username and password, which would then allow unauthorized access [3, 4]. Behavioral biometrics, such as measures based on keystroke analysis, could be used as complementary metrics to defeat intrusion attempts. Keystroke measures are different from many other behavioral biometrics because of the specific human computer interaction component. Behavioral biometrics such as handwritten signatures do not directly involve the target device (i.e., the computer keyboard), whereas keystroke patterns have a direct relationship with the specific input device through which authentication takes place.

Keystroke-based authentication is a very active sub-field of computer security, and has already reached a high level of maturity [2]. Numerous studies have demonstrated the uniqueness of keystroke patterns for each individual. In systems that implement keystroke patterns as part of their authentication mechanisms, the login process requires not only the correct username and password, but also matching specific keystroke patterns that have been identified and stored for that individual. Such a mechanism could increase the difficulty of intruders being authenticated, as the unique typing pattern would be very difficult to reproduce [2, 5].

While previous approaches examined total password entry time, keystroke latency based on press and release timings, and other patterns, this paper focuses on the analysis of timing intervals between key presses, and proposes a small, portable keystroke-based authentication system that can be used in a variety of applications. The primary goal is to defeat intruders, while still maintaining an acceptable rate of acceptance; that is, false rejection is considered to be less of a problem than false acceptance. Using key press intervals, a more robust signature identifier may be established. The implementation does not require excessive computational power, and is mostly platform-independent. The primary target group is comprised of "non-casual" users who use a keyboard on a regular basis to perform everyday duties that require some degree of typing proficiency. However, such a system could also potentially be used for distributed applications over the Internet. This study, therefore, supports the conclusions of other authors delineating the efficacy of keystroke dynamics in authentication [2, 4, 5], while emphasizing the role of interval timings as a complementary measure against false acceptance.

II. Related Works

Several authors have investigated the various aspects of keystroke dynamics. In a relatively early study, keystroke profiles that can successfully identify users were generated with pattern recognition techniques [2]. Participants downloaded an executable program which they ran for data collection from their own machines. Upon data extraction and

978-1-4244-2794-9/09/$25.00 ©2009 IEEE

analysis, users were then classified according to identified patterns. Correct identification rates, varying from 83.22% to 92.14%, were reported, depending upon the classification and identification technique. It was also noted that users should enter pre-specified text instead of free text during authentication – an approach that was adopted in the current study.

The feasibility of validation through digraphs and trigraphs was also investigated [6]. In this context, a digraph is defined as the time difference between the key press event of the first key and the release event of the second key, while a trigraph is the time difference between the key press event of the first key and the release event of the third key. The study tested users who logged in as themselves, and also as someone else to simulate impersonation attempts. The false rejection rate was between 0% and 55%, and the false acceptance rate was 0% for 80% of those acting as intruders, which was considered to be a satisfactory result.

The effectiveness of fixed strings within free text of English and non-English words (such as "ttyl" – "talk to you later") as a tool for authentication was also investigated [7]. This is a form of continuous authentication that proceeds during keyboard entry. From data collected from several individuals and from over 9.5 million keystroke events, it was found that non-English words were more effective for identification than English words.

In a different approach to keystroke analysis, research was conducted to test the effectiveness of adding pauses and cues to a password [8]. A pause is a specific place within a password where entry is delayed for a pre-determined amount of time. If cues are used within a password, sounds were presented to indicate when to pause and when to continue typing. It was concluded that the use of pauses and cues are more effective than employing keystroke dynamics alone.

Although the previous studies generally focused on the standard QWERTY terminal-style keyboard, a recent investigation attempted to determine whether keystroke-based authentication could be applied to mobile devices, such as cell phones [9]. Eleven digit telephone numbers and specific text messages were entered. It was found that this system is inadequate because of the extra computational power required to perform this type of authentication, which is not suitable for those who do not use mobile devices on a regular basis.

This brief survey underscores the attention devoted to keystroke dynamics, and underscores its potential as a complementary authentication measure. With the exception for mobile devices, which are greatly dependent upon the specific interface, results to date have been very encouraging, and suggest that keystroke-based authentication techniques will continue to develop and to improve.

III. Methods

In the current study, key press intervals were employed as the authentication measurement. Specifically, a key press interval is defined as the elapsed time between two consecutive key presses. For authentication to be successful, key press interval timings during password entry must reproduce, within a specified tolerance, those that were recorded during an earlier data collection process, known as registration. Determination of these tolerances is explained below. It is proposed that this type of keystroke analysis will result in a low false rejection rate (FRR) and, more importantly, a low false acceptance rate (FAR), where the FRR is defined as the rate at which a user is rejected when they should be accepted, and the FAR is the rate at which a user is accepted when they should be rejected.

Eleven volunteers, all intermediate to upper-level undergraduate students, participated in this study. Although this is a small sample size, the range of typing abilities varied enough that they approximately represent people who would be affected by keystroke analysis on a regular basis. None of the users were trained typists, but they all perform work daily that requires a keyboard.

Each participant was assigned a username derived from their own name, as well as a unique password representing a course code for the Computer Science Department at Nipissing University (for example, cosc1557). As course codes are frequently typed by students, it was expected that this choice of passwords would reflect each individual's specific keystroke dynamics, and that these codes would be entered consistently. Having all participants use a similar template also facilitates the study of inter- and intra-user variability. The passwords also contain a combination of letters and numbers, which, in real applications, typically increases password security [2].

The keystroke application software was written in Visual C# under the Microsoft® Visual Studio .NET 2003 framework. Visual C# is a fully object-oriented language, and this paradigm facilitated the development of the programs required for the system. For example, information could be passed to a main class, which is then used during the processing of registration information. Visual C# also has built-in networking and database connection capabilities, enhancing utility for web based services. Networking capabilities are also helpful where the login information is stored on a single password server. Finally, Visual C# has encryption capabilities that allow password and keystroke information to be encrypted en route to the server. However, the keystroke system could be implemented in any appropriate language.

The data collection, as well as all login attempts, was performed on the same laptop PC using a standard QWERTY keyboard that did not include a number pad. The data were stored in an MS Access database, which were queried through SQL invocations. In the experiments, the participants entered their user name and password twenty times over the course of four sessions. During each session, the users entered their information five consecutive times. The system stored the timings of the keystroke intervals, from which a profile was generated.

For each key press interval, the data were observed in order to determine the timing that best represents each individual's normal key press patterns. For example, if a key press interval had registered times that fell between 90 and 200 msec, but most of the times were approximately 150 msec, then a timing of 150 msec best represents the normal key press time for that key press interval. Fig. 1 shows the mean results for a specific user that were obtained by this method. The bars in this figure represent the mean time of each key press interval, and the error bars denote the standard deviations. As seen from this example, the standard deviations for the key press intervals "c-o", "o-s" and "s-c" are very small, indicating that the "cosc" portion of the password was entered in a consistent manner. The standard deviation for "c-x" represents the transition from typing characters to numbers. The standard deviation in this case is relatively large, indicating that this portion of the password was typed inconsistently. Additionally, for key press intervals in the numeric part of the password, the standard deviations are much larger than those of the intervals containing only characters, indicating that for this individual, the interval timings for the numbers in the password are less consistent than for the characters.

Initially, it would seem that tolerance bounds should be set according to the standard deviation of interval timings obtained during registration. However, the variability in the timings during entry of the numeric portion would allow intruders to have easier access. As a result, for this study, the standard deviations were used as the basis to empirically tighten – and, in a few cases, loosen – the bounds, with the goal of eliminating or greatly reducing false acceptance. However, such an adjustment was based on the timing variability as observed from analysis of the experimental data, resulting in tolerances that are unique to each user. In the sample population, most of the timings had high standard deviations, especially during the transition from entering alphabetic to numeric characters, and during numeric entry. For these participants, the tolerance bounds were tightened. For those individuals who exhibited consistent timing intervals, the bounds were slightly loosened.

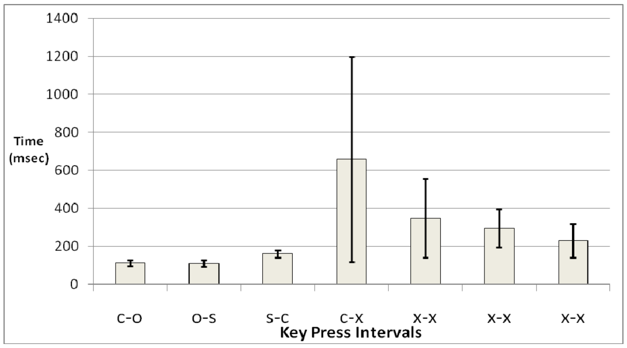

Figure 1. Key press means at registration, Participant 1.

It was also empirically determined that the timings for key press intervals should fall within the specified tolerance for five of the seven intervals (for an eight-character password), as the same interval timings will not be registered every time passwords are entered. For instance, typing patterns may be affected by injuries, psychological factors (e.g. moods, stress, hurriedness), along with many environmental factors. These factors can also potentially affect other keystroke metrics.

After registration and setting tolerances, the system was tested with each participant attempting to log in five consecutive times. The false rejection rates were recorded. To check robustness with respect to intrusion, three of the eleven users attempted impersonate users different from themselves during authentication. The person that they were impersonating was selected based on the similarities within the two individuals key press times. For example, if two people type "c-o" within 110 milliseconds, "o-s" within 90 milliseconds, and "s-c" within 124 milliseconds, then the typing patterns were considered to be similar. Testing against individuals with similar keystroke patterns was considered useful because a successful system must prevent intruders from being authenticated as users who have similar keystroke dynamics.

IV. Results

The primary goal of authentication with keystroke interval timings is to defeat intruders. In other words, the requirement for such a biometric is a low FAR. After adjustment of each participant's tolerances, the FAR, as measured by successful intrusion attempts, was zero (0%). Over all the testing trials, 36% of the participants were able to successfully login more than 50% of the time; 27% were able to login between 20% and 40% of all attempts, and 36% could not be authenticated.

Users who were either unable to login, or who had a low acceptance rate, were found to have the most inconsistent keystroke patterns, and therefore the bounds for these individuals could not be properly determined. The false rejection rates of each user are found in Table I.

TABLE I. False rejection rates at login

User	False Rejection Rates (%)
1	0
2	20
3	100
4	40
5	80
6	40
7	100
8	60
9	80
10	100
11	100

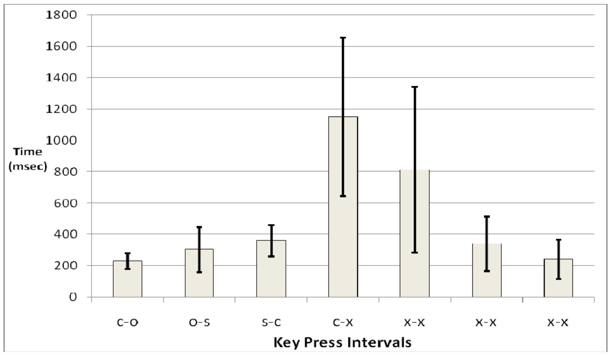

Figure 2. Mean key press times at registration, Participant 10.

An example of an inconsistent user's key press times is seen in Fig. 2. This figure shows the means of the key press times that were found for each interval at registration, and the error bars represent the standard deviations. For this individual, there is only one key press interval ("c-o") which was typed with low variability. That is, only one interval could be used to determine an accurate tolerance. Generally, the intervals of the password containing numbers have larger standard deviations than the character intervals of the password for all participants. Therefore, Fig. 2 is an example pattern from an unusually inconsistent typist, who may represent "casual" users that could not be authenticated through keystroke analysis, because the normal keystroke patterns for these individuals could not be determined. Further relaxing the tolerances (for true acceptance) would likely result in a higher FAR. Higher FARs allow easier access for intruders, which is what the system is specifically designed to avoid. Therefore, authentication of this user through keystroke-based metrics would pose difficulties.

As mentioned previously, during registration, it was observed that participants typed the alphabetic portion of the password with much less variability than the numeric portion, resulting in difficulties during authentication. In a false rejection, the key press times were generally not within the correct range for the numeric portion of the password. To illustrate this point, consider timing information for two additional participants, as shown in Fig. 3 and Fig. 4. Comparing the timings in these two figures, it is observed that the mean times at login have decreased for most of the numerical key press intervals. The mean timings for the character key press intervals remain stable, indicating that the user was not reproducing the correct key press times for four of the seven key press intervals, which explains why this individual was not properly authenticated.

Fig. 5 shows the differences between a participant's mean interval timings, one of that person's successful login attempts, and an intruder's attempt to impersonate that user's keystroke patterns. The two lines that represent each of the login attempts have a similar shape, indicating the similarity in typing patterns between the true user and the intruder.

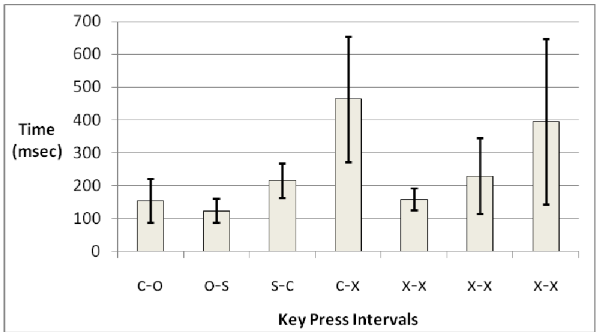

Figure 3. Mean key press times at registration, Participant 5.

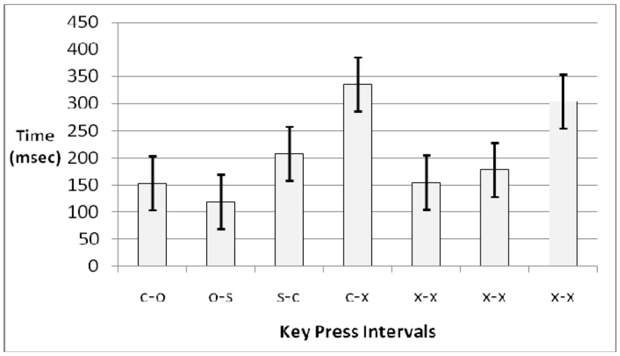

Figure 4. Mean key press times at login, Participant 5.

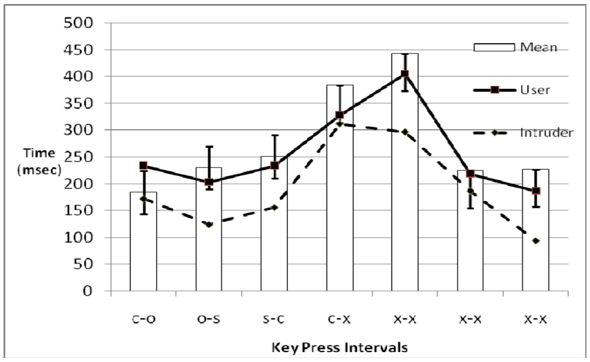

Figure 5. Intruder login attempts vs. valid key press timings.

The intruder was generally able to type within the bounds for two of the key press intervals, but this is not sufficient for proper authentication.

As presented earlier, each participant who attempted to impersonate another user had a 0% false acceptance rate. These results suggest that keystroke interval authentication is capable of defeating intrusion based on similar keystroke interval timings. Although the false rejection rate was found to be higher than would be acceptable in most applications, there are many circumstances in which keeping intruders out is a preferable outcome, at the cost of occasionally rejecting legitimate users. High security applications, where users are authenticated on specific keyboards, constitute a large class of these situations. Further study will be done to determine how to decrease false rejections, while maintaining very strict false acceptance rates.

V. Discussion

The extremely low false acceptance rate observed in this study demonstrates the efficacy of keystroke interval timings in defeating intrusion attempts. However, the false rejection rate, which was unacceptably high in some cases, strongly suggests that keystroke intervals should be employed only in specialized applications, where at least a moderate degree of typing proficiency can be expected. The results also suggest that, at present, adjustment of acceptance/rejection tolerances, even with empirical methods, is necessary.

As with behavioral biometrics in general, authentication based on keystroke dynamics has drawbacks. For example, typing patterns and entry speed are very dependent upon emotional factors [1]. If, during the registration phase, an individual's emotions affect typing patterns, statistical analysis will produce bounds for authentication that may not properly represent the person's normal typing patterns. The same holds true during normal password entry after registration.

Furthermore, personal behavioral characteristics, including keystroke dynamics, are likely to change over time [2, 4, 11, 12]. Consequently, a keystroke-based authentication system requires maintenance on a regular basis. Determining the regularity of system updates could prove to be difficult. Behaviors of some individuals may change more rapidly than others, and if the data for those people are not frequently updated, system integrity could be compromised.

Current systems that authenticate through username and password make allowances for human error, as mistakes can be corrected. However, with keystroke-based authentication, a mistake generally means that authentication needs to be restarted – or at least the error must be removed from the keystroke pattern before analysis. Non-authentication based on "incorrect" keystroke patters could lead to frustration, which may further affect typing patterns, resulting in an individual being constantly denied access.

A secondary form of authentication may be needed for those who have sustained an injury and are incapable of typing properly. Such measures, a security question, for instance, are common practice when users forget their passwords. However, it may be relatively easy for intruders to obtain the proper information required for authentication. Other behavior biometrics not based on human-computer interaction may then be used to complement authentication.

VI. Conclusions And Future Work

The investigation presented in this paper focuses on a specific group of computer users: those who use a keyboard on a regular basis. This is an important issue, because people naturally type differently on different keyboards. Becoming familiar with unknown keyboards requires time. As a result, keystroke interval timings are most appropriate for computer users with typing efficiency, who are entering their passwords on a familiar keyboard.

Due to the inconsistencies in registration information of specific individuals (see, for example Fig. 2), this type of authentication would be less practical for casual users (i.e. those that require authentication when using email). Keystroke interval timings may however, prove to be beneficial for those who are working in high security facilities, or for those who access sensitive information. For instance, keystroke dynamics add an extra security measure for online banking. An interesting question is whether individuals who are aware that their keystrokes are being analyzed would be more conscientious of their typing during registration, as well as when they are attempting to log in.

Keystroke-based authentication systems decrease the possibility of password attacks by intruders (e.g. dictionary attacks), because, even with login and password information, it is extremely difficult for an intruder to reproduce keystroke patterns. Attacks on behavioral biometrics are difficult because, as has been previously stated, behavioral biometrics are unique to each person: a fact that has been employed for years in signature verification. Keystroke patterns are difficult to reproduce, even with much practice. As biometrics measures, these patterns vary from person to person, even among those who have undergone the same typing training, just as students learning cursive writing from the same teacher still have different writing styles after training. Furthermore, behavioral biometrics change over time. They can even change between consecutive entries, making forgery very difficult for intruders [2, 4, 11, 12]. For these reasons, keystroke-based dynamics comprise a good complementary security tool.

The results of this study also suggest future research directions. Initially, the passwords consisted of characters and numbers, because of the added security over and above passwords that containing only characters [3]. In future work, keystroke analysis will be tested on passwords that contain only characters, as well as on those including both numbers and special characters. The experimental results indicate that people type a string of characters at a more consistent rate than they type numbers, and the passwords containing only characters may result in lower false rejection rates. The disadvantage of (theoretically) less secure passwords would need to be assessed against the potential added password strength provided by keystroke-based biometrics.

Additional experiments will be done with the same and with different forms of password, entered on a keyboard containing a number pad. In the current experiment, participants found that typing the numbers was more difficult without a number pad. It can therefore be hypothesized that having a number pad would produce more consistent registration results, allowing for a better determination of normal typing patterns, while decreasing the FRR.

Future experiments will also include larger sample sizes. Although the sample in the current study was felt to approximately representative of the user group to whom keystroke-based authentication was target, larger sample sizes would aid in the determination of threshold tolerances, which, in the current work, were empirically determined. Larger sample sizes and more extensive trials will allow statistical techniques and methods from computational intelligence [2] to be applied to computing tolerances. In particular, neural network approaches [2, 13] and fuzzy logic techniques [14] have been successfully used in pattern recognition, and will be employed in future work to classify individuals using key press intervals. Furthermore, users' entry of their username, in addition to their password, will also be analyzed for keystroke characteristics.

In this paper, a keystroke-based behavioral biometrics measure employing key press interval timings was discussed. It was demonstrated that this metric could be useful for authenticating users with some degree of typing ability, although this approach may not be suitable for casual users who exhibit wide variability in their keystroke patterns. However, keystroke intervals, when used in conjunction with other keystroke-based measures and behavioral biometrics, may complement the traditional username/password paradigm to provide added protection and security.

ACKNOWLEDGMENT

The authors thank all the volunteers who participated in this study.

REFERENCES

[1] W. S. Coates, A. Bagdasarian, T. J. Houle, and T. Lam, The Practitioner's Guide to Biometrics, American Bar Association, 2007.

[2] F. Monrose and A. Rubin, "Keystroke dynamics as a biometric for authentication," Future Generation Computer Systems, vol. 16(4), 2000, pp. 351-359.

[3] D. Gollman, Computer Security, 2nd ed., Wiley, 2005.

[4] A. Peacock, X. Ke, and M. Wilkerson, "Typing patterns: A key to user identification," IEEE Security and Privacy, vol. 2(5), 2004, pp. 40-47.

[5] K. Omoty and E. Okamoto, "User identification systems based on biometrics for keystrokes," LNCS 1726, 2004, pp. 216-229.

[6] M. Choras and P. Mroczkowski, "Keystroke dynamics for biometrics identification," LNCS 4432, 2007, pp. 424-431.

[7] R. Janakiraman and T. Sim, "Keystroke dynamics in a general setting," LNCS 4642, 2007, pp. 584-593.

[8] S. Hwang, H. Lee, and S. Cho, "Improving authentication accuracy of unfamiliar passwords with pauses and cues for keystroke dynamics-based authentication," LNCS 3917, 2006, pp. 73-78.

[9] N.L. Clarke and S.M Furnell, "Authenticating mobile phone users using keystroke analysis," International Journal of Information Security, vol. 6(1), 2007, pp. 1-14.

[10] K. Revett, S. Tenreiro de MagalHaes, and H.M.D. Santos, "Enhancing login security through the use of keystroke input dynamics," LNCS 3832, 2005, pp. 661-667.

[11] L.Ballard, D. Lopresti, and F. Monrose, "Forgery quality and its implications for behavioural biometrics security," IEEE Systems, Man and Cybernetics, vol. 31(5), 2007, pp. 1107-1118.

[12] F. Bergandano, D. Gunetti, and C. Picardi, "User authentication through keystroke dynamics," ACM Transactions on Information and Systems Security, vol. 5(4), 2002, pp. 367-397.

[13] L. Fausett, Fundamentals of Neural Networks. Upper Saddle River, NJ: Prentice Hall, 1993.

[14] T. J. Ross, Fuzzy Logic With Engineering Applications, 2nd Ed. West Sussex, UK: John Wiley and Sons Ltd., 2008.