Enhanced Keystroke Dynamics Authentication Utilizing Pressure Detection

Sung-Shiou Shen[2], Shen-Ho Lin[3] , Tsai-Hua Kang[4] and Wei Chien[1,]*

[1]Department of Computer Science Ningde Normal University
Ningde, Fujian Province, 352100, China.
[2]Department of Electronic Engineering De Lin Institute of Technology
Tucheng, New Taipei City, Taiwan, 23656, R.O.C.
[3]Department of Electronic Engineering De Lin Institute of Technology
Tucheng, New Taipei City, Taiwan, 23656, R.O.C.
[4]Department of Electronic Engineering De Lin Institute of Technology
Tucheng, New Taipei City, Taiwan, 23656, R.O.C.
air180@seed.net.tw, 3shubert@googlemail.com, marcular@gmail.com, shaka.kang@msa.hinet.net

Abstract

Current computer and information systems are now used in almost all aspects of our lives, especially in banking systems and network systems. Most of the times, many computer systems use the simple and common username/password or keystroke biometric scheme via a keyboard for authentication. However, those fixed secret information can be guessed easily using different methods such as network sniffer, social engineering, spyware, dictionary attack and brute force attacks, etc. Meanwhile, using the password-based solution suffers from many security flaws and usability limitations. Although the user adopts extreme measures such as changing of the password and using long and complex passwords to be efficient and secure, these are unfriendly and hard to memorize for the user. Therefore, a solution to this problem is the use of an alternative biometric authentication method called Keystroke Dynamics. It is one of the famous biometric technologies and can be yet provide ease of use and transparency to the user in addition to security robustness. Keystroke Dynamics allows to secure the authentication process by verifying the way of typing the static credentials such as typing behavior, typing period of time, etc. But the static behavior can be easy continuously monitoring the user's activities. There is always a golden opportunity for attacker who is physically close to the machine to have access to it. This paper investigates the use of keystroke dynamics that is combined user's typing pressure activities on keyboard. The proposed scheme utilizes the key press and release pressure to build random user's typing profile. The research done on Dynamic Keystroke Pressure-Based is ability to provide continual identity verification during the whole time and has a high accuracy level which was obtained under strictly controlled conditions.

Key words: Authentication, Keystroke Dynamics, Pressure-Based.

Introduction

Biometric technologies are defined as automated methods of verifying or recognizing the identity of a living person based on a physiological or behavioral characteristics [1]-[6]. Meanwhile, keystroke dynamics is considered as a strong behavioral biometric based authentication system. Keystroke dynamics secures the authentication process by verifying the person's typing pattern of credentials, and also it can be used to detect the changing of typing behaviors or patterns during the session for enhancing the security and privacy more [8]-[10]. In a word, it is depended on how you type, not what you type. The user usually types in text without any kind of extra work to be done for authentication.

Keystroke dynamics system runs in two main phases namely the enrolment phase and the verification phase that a user has to go through to be authorized. Enrolment phase has to collect data about person's identity of keystroke dynamics feature to extract the person's biometric features to create a template for each user's typing behavior namely as a user's profile that is stored in a database of a system. For each of the users, a user's biometric template profile is calculated in the training stage. A pattern that is going to be identified is matched against every known template to yielding a score for describing the similarity between the pattern and the template. Meanwhile, the system assigns the pattern to the person with the most similar biometric template. Next, verification phase is executed for identifying use without additional information besides measuring his keystroke dynamics. Second phase performs features matching with the user's pattern which was previously stored in the system database during the enrolment phase. The matching process results will take place either granting access to the user denying if biometric template and pattern are sufficiently similar or denying access to the user.

Keystroke dynamics has been first imagined in 1975 and it has been proved to work in early eighties. In general, Keystroke verification techniques can be classified as either static (Fixed-text) or dynamic (Free-text). Static verification obliges the users to use only a predefined text and at log-in time times to produce the typing samples and it is provided additional security than the traditional username/password. This approach must ask the user to type several times the same string in order to build its user's pattern. Such methodology is really appropriate to authenticate an individual by asking him to type its own password, before login to its computer session, and verifying if its way of typing matches the pattern. Static approaches provide more robust user verification than simple passwords but the detection of a user change after the login authentication is impossible because of changing the password implied to enroll again necessary.

Dynamic methodology allows authenticating individuals independently of what they are typing and don't restrict users to a particular text. Dynamic system continues to monitors the user's keystrokes through the course of the interaction even though passing the log-in session successfully. It means that the typing patterns of a person are constantly analyzed in real time for assuring the identity of the user during the full duration of sessions.

Pressure-Based Dynamics Keystroke implementation

Previous studies have identified a selection of biometric authentications. Static Keystroke authentication indeed provides robust security than the traditional username/password. But the method is not able to work with a different password. We have seen that keystroke dynamics allows securing the authentication process by verifying the way of typing the credentials. It means that such methodology can fix the flaw by motioning and analyzing the user behavior profile in real time. Even though, static and dynamic systems are quite similar in the way that they both utilize the key press and release times to build a user behavior profile, no matter directly asking the user to type some fixed-texts or indirectly monitoring their type behavior during a certain period.

When the dynamic behavior of a user could be modeled successfully, we can easy detect a changing of user to authenticate the user through a challenge during the normal login process. This literature is based on dynamic keystroke authentication and extended the dynamic and random user's behavior data capturing to the entire duration of the logged session. With such a mechanism, the real time nature of the user monitoring offers significantly more data upon authentication judgment and abnormal activities of an impostor may be detected earlier in the session than under a periodically monitored implementation. The hardware and software implementation are described in detail as followings.

Hardware subsystem Implementation

Based on the dynamic and random keystrokes and behaviors phrase, this paper proposes to monitor the continuous nature of user keystroke patterns including pressure effort, input rate and rhythm during login session for further extends the continuous or periodic monitoring. By the way, the development of the additional analysis in multiple random keystroke patterns can enhance security more. The paper proposes a new pressure-key keyboard hardware architecture shown in Figure 1.

The pressure-key keyboard is based on the pressure sensing module, counting circuits, amplifier circuits, microprocessors and control circuit combination. The combination device can simultaneously capture multiple keystroke patterns such as pressure effort, key press rate and press duration time. The design flow of hardware subsystem circuit implementation is shown in Figure 2.

Pressure sensing module is mainly responsible for sensing and calculating to output pressure signals. The pressure sensing elements with thin, light and sufficient sensitivity are first consideration because it must be installed in the limited space of the pressure-key keyboard. Meanwhile, the accuracy of verification phase in this proposed authentication scheme depends on capturing the high resolution and accuracy of the pressure and time patterns during the enrolment phase. In other words, the sticking point is on implementing the workable driving circuit of pressure sensing elements. Counting circuit is mainly responsible for calculating the key press rate and press duration time patterns which are extracting from output pressure signals. The capture operation in time bits and clock frequency in counting circuit is directly affected the accuracy of the key press rate and press duration time factors. The amplifier circuits are used for amplifying pressure signals from pressure sensing module and used to convert the signal patterns. Pressure signal before entering the microprocessor must be converted into digital patterns. This model used 14-bits Analog-to-Digital (ADC) element for increasing the accuracy.

Microprocessor is used to integrate both pressure signals output from the pressure sensing module and key press rate and press duration time signals output from the counting circuit. Meanwhile, it also cooperates with decision subsystem implementation for directing the database search, determines "matches" or "non-matches" based on the similarity measures received from the pattern matcher makes an "accept/reject" decision. Control means for receiving a control signal to the microprocessor to perform the relevant action unit.

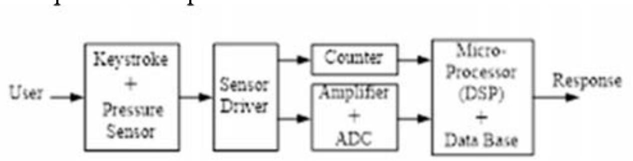
User
Keystroke + Pressure Sensor
Sensor Driver
Counter
Amplifier + ADC
Micro-Processor (DSP) + Data Base
Response

Figure 1. The keyboard hardware architecture

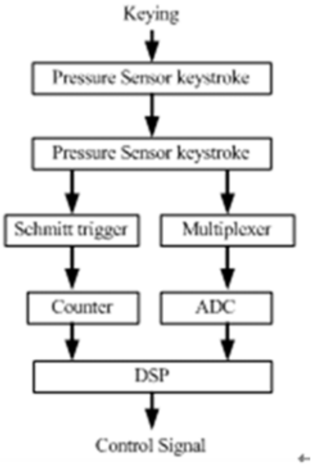

Figure 2. The design flow of hardware subsystem circuit

Software subsystem Implementation

The capture phase is considered as an important issue within the proposed authentication process. The software subsystem in the proposed authentication scheme both implements the enrollment phase and the verification phase which are included data collection, signal processing, decision and data storage. Figure 3 shows the design flow of software subsystem implementation.

It is necessary to collect several samples of the user in order to build its model during data collection phase. The manner is quite different from static keystroke systems that a user is normally monitored for real time. This software is interested by a chronologically ordered list of events on the keyboard initiated by its user. Those events are included starts empty, press occurs when the key is pressed and release occurs when the key is released. Data collection phase can capture two important raw data called key code and timestamp. The key code can gives some information on the frequency of the key on the keyboard and differentiate different keys giving the same user profile. Timestamp feature extraction are basically calculated using the press and release times of every key the user types and then processed to store in the user's profile. When all the typing data collected, the profile creation of the system infers the typing pattern that the user typically follows which will be then stored as the user profile.

The signal processing phase is designed for having acquired and matching possible biometric characteristic with other like measures. It divides into segmentation, feature extraction, quality control, and pattern matching tasks designed with the goal of differentiating small distances between profile models in the database and user templates. Meanwhile, the later user templates are from the same individual and large distances between profile models and templates and samples of different individuals.

After data collection, signal processing and data storage in enrolment phase, the users' typing features has been extracting and profiles has been creating and storing. Next, the decision phase implements system verification process by directly searching the database, determines "matches" or "non-matches" based on the similarity measures received from the pattern matcher. The verification method compares the query the biometric data captured during the authentication to the model. Based on the result of this comparison, the decision module ultimately makes either accept or reject decision to the user.

Performance

This article presents the implementation result by the self-development software interface shown in Figure 4. The figure clearly shows that the proposed hardware and software subsystem accurately captures the user key code (key rhythm and key pressure) and timestamps. Meanwhile, as the data phase collects the user query templates more, the signal processing phase must process more to build more accurate user profiles.

It is good for the subsequent decision phase to enhance the successful possibility of the verification process and security more. In any case, in the testing of biometric dynamic keystroke devices, it is necessary to decouple the performance of the data collection, signal processing subsystem from the policies implemented by the decision subsystem.

Conclusion

Current computer or mobile communication systems depend greatly on using username/password authentication method to protect the system data. Ultimately, the classical authentication methodology suffers from many security flaws and usability limitations. Today a fascinating biometrics authentication with human physiology and psychology technology is currently suitable for automatic identification mechanism. Dynamics Keystroke is one of the famous biometric technologies. This paper extends the dynamics keystroke concepts and proposes pressure-based dynamics keystroke methodology as a more security and useable dynamics keystroke authentication alternative. Capturing and analyzing additional user key code (key rhythm and key pressure) and timestamps during the enrollment phase in real time enhances the successful possibility of the verification process and security more. Furthermore, the hardware and software subsystem prototype implementation also shows the feasibility and usability of the proposed authentication scheme in this literature.

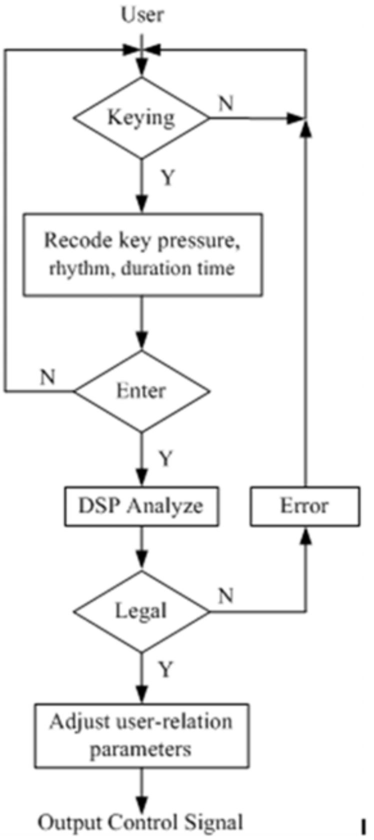
User
Keying
N
Y
Recode key pressure, rhythm, duration time
N
Enter
Y
DSP Analyze
Error
Legal
N
Y
Adjust user-relation parameters
Output Control Signal

Figure 3. The design flow of software subsystem

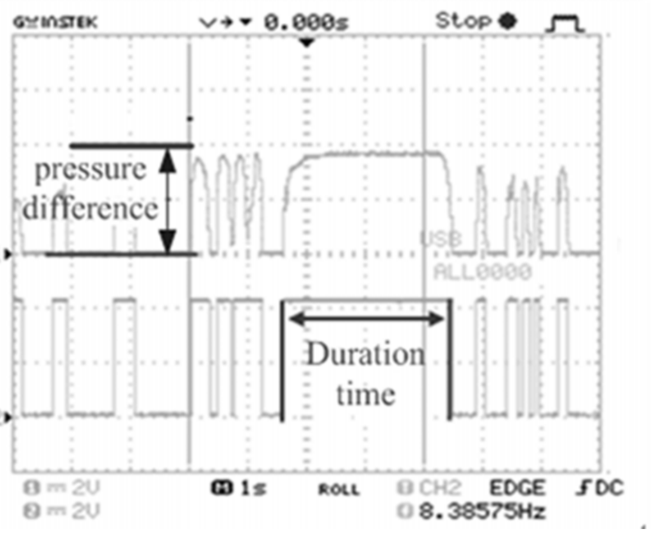

Figure 4. Systerm Performance

References

[1]Y. Wang, T. Tan and A. K. Jain, "Combining Face and Iris Biometrics for Identity Verification," National Science Foundation(NSF) IUC .

[2] S. Prabhakar and A. K. Jain, "Decision-level fusion in fingerprint verification," Pattern Recognition 35, pp. 861–874, Feb., 2002.

[3] Wayman, A. Jain, D. Maltoni and D. Maio , "An Introduction to Biometric Authentication Systems," Biometric Systems, Springer London, pp 1-20, 2005.

[4] A. K. Jain, A. Ross and S. Prabhakar, "An Introduction to Biometric Recognition," IEEE Trans. On Circuits and System for

Video Technology, Vol. 14, No. 1, Jan., 2004.

[5] W. Yan, "Biomechanical Simulation of the Human Hand and Forearm," A I I E Transactions, Vol. 7, Issue 1, 1975.

[6] A. Ross and A. Jain, "Information fusion in biometrics," Pattern Recognition Letters 24, 2115–2125, 2003.

[7] A. Maria, "INTRODUCTION TO MODELING AND SIMULATION," Proceedings of the Winter Simulation Conference, pp.7-13, 1997.

[8] R. Janakiraman and T. Sim, " Keystroke Dynamics in a General Setting," Advances in Biometrics Lecture Notes in Computer Science, Vol. 4642, pp 584-593, 2007.

[9] D. Shanmugapriya and G. Padmavathi , " A Survey of Biometric keystroke Dynamics: Approaches, Security and Challenges," International Journal of Computer Science and Information Security (IJCSIS), Vol. 5, No. 1, pp.115-119, 2009.

[10] S. P. Banerjee and D. L. Woodard , " Biometric Authentication and Identification using Keystroke Dynamics: A Survey," Journal of Pattern Recognition Research 7, pp. 116-139, July,2012.

Acknowledgments: This research is supported by the Fujian Provincial Department of Science & Technology under Contract no. 2016I0011.