2006-287: BIOMETRIC AUTHENTICATION TOOL FOR USER IDENTIFICATION

Mario Garcia, Texas A&M University-Corpus Christi

Biometric Authentication Tool for User Identification Based on Keystroke Dynamics

Abstract

Biometric access methods for computer systems are gaining popularity because of governmental and corporate businesses' increased focus to secure sensitive data on computer systems and networks. Biometrics is the science of measuring a unique physical characteristic about an individual as an identification mechanism. Keystroke Biometrics is a relatively new method of biometric identification and provides a comparatively inexpensive and unobtrusive method of hardening the normal login and password process. This Project aims at investigating the validity of using typing dynamics to strengthen security in a computer system. A Keystroke Dynamics Analysis tool is developed that uses statistical analysis of a user's typing patterns to perform identity verification.

Introduction

The increasing need for securing access to computer systems and networks from intruders is growing rapidly as the type of data and capabilities of these systems is becoming significantly sensitive. To provide access to these systems while preventing illegitimate access is the key requirement of modern day computing. Since biometric systems do not identify a person by what he or she knows (a code) or possesses (a card), but by a unique characteristic that is difficult for a different individual to reproduce, the possibility of forgery is greatly reduced [4]

Biometric Authentication

Biometrics is the science of measuring a unique physical characteristic about an individual as an identification mechanism. A number of widely used biometric technologies and techniques exist. Some of the common methods include fingerprints, voice characteristics, eyes, facial features. Newer techniques like iris recognition and keystroke dynamics are now becoming more popular as they measure stronger and reliable biometric traits of human beings. Researches have shown that these techniques have virtually no FAR (False Acceptance Rates) and extremely low 0.2% FRR (False Rejection Rates).

Keystroke Biometrics

Keystroke Recognition is completely a software-based solution. It involves two processes:

1. Enrollment Process: This process will enroll the user and generate a template for him/her. To start with, the individual must type in a specific word or a phrase or a set of alphanumeric characters. This is usually a username and password.
2. Verification Process: This process will verify an enrolled individual to confirm the identification of the person. It will match the current template with an existing one for authentication purposes [7]

This research aims at using the inexpensive and unobtrusive method of keystroke biometrics to build a user authentication system. The motivation to use this technology for this work comes

from the fact that this is would be complete software based solution for building an efficient user identification tool. The tool designed has the following characteristics:

1. No additional or specialized hardware is needed to implement, as it would use the existing computer keyboard.
2. No additional costs are involved for training individuals using the system.
3. Easy to use with minimal set up time and can be readily installed on a system or network.
4. Data will be stored in the form of templates.

Project Description

The system asks the user to enter three types of strings, which would be a username, a password and a phrase, which can be alphanumeric. The input phrase field is a constant phrase, added to the system to harden the security policy where the system can compare the typing dynamics of multiple users for the same phrase. The login screen layout is presented in figure 1. If it is a new user, the enrollment process starts and the system prompts the user to choose a login screen name, password and phrase of choice. This information is stored in a configuration file. To enter the system, the user is now required to use the same data to fill in the login form several times. This form is shown in figure 2

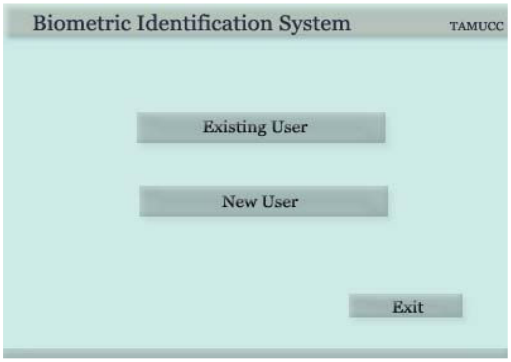

Figure1. Entry/Start up Screen for access into system

Figure 2. Login Screen

The login process is the verification process where the user's keystroke dynamics is matched with the stored biometric profile to ensure accurate identification. If a valid match is produced, the tool prompts the user with a successful login note providing access to the computer or network. The overall steps in the proposed system can be represented as shown in Figure 3.

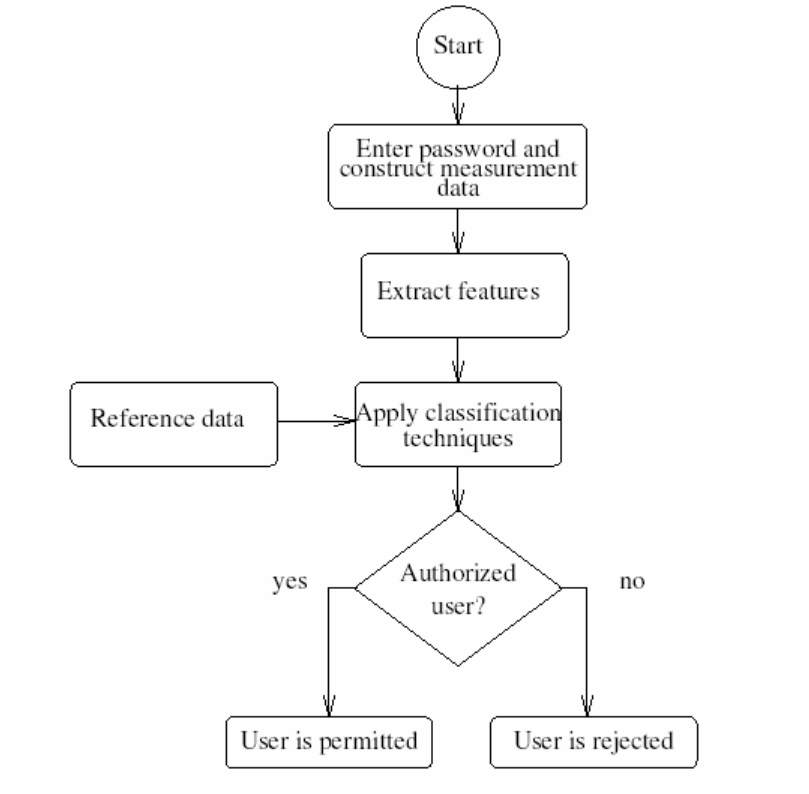

Figure 3. Flowchart of the overall steps involved [5]

Behavioral Characteristics Measured by the Tool

The distinctive, behavioral characteristics measured by the system include:

- The cumulative typing speed.
- The time that elapses between consecutive keystrokes.
- The time that each key is held down.
- The frequency of the individual in using other keys on the keyboard, such as the number pad or function keys.
- The sequence utilized by the individual when attempting to type a capital letter-for example, does the individual release the shift key or the letter key first?

These behavioral characteristics are then created into statistical profiles, which then essentially become the enrollment and verification templates. These templates also store the actual username and password [2]

Development of an Authentication Algorithm

The algorithm develops a signature profile for each of the three input strings entered by the user. The algorithm uses two variables, a test signature "T" which will be acquired at the login time

and a mean reference signature "M" where M = {$M_{username}$, $M_{password}$, M_{phrase} }[6]. Verification is performed by comparing the test signature T with M and determining the magnitude of difference between the two profiles [3]. Given M = {m1, m2, …….m_n} and T = { t1,t2, …….t_n} where n is the total number of latencies in the signature, the algorithm will compute the magnitude of the difference and positive identification is declared when the difference is within the threshold variability of the reference signature. When more than 80% of all the possible latencies passed this test then input for that string would be considered valid.

System Design and Development of the Tool

A graphical user interface is designed for the authentication system. The interface consists of a Login module and a Verification module. For new users, the login module precedes an enrollment module. The system design is using the Microsoft Developer tools of Visual Studio .Net. To the user, the verification and login processes appear the same on the front end as two similar forms. Figure 4 shows a sample login for a user. If the user is verified after several logins, the verification screen prompts the user to continue with a successful login message as shown in Figure 5.

Figure 4. Sample login of user John Smith

Figure 5. Login verification screen

The first stage in the verification process is to timestamp all key press and release events. Then from the stored profile files the standard deviation for each latency is determined. For an approval for a login string to occur only 50% of latencies must fit within one standard deviation away from the mean of the reference profile.

Effectiveness of Keystroke Dynamics

False Acceptance Rate (FAR): This determines how often an intruder can successfully bypass the biometric authentication. A lower rate is more secure.

False Rejection Rate (FRR): This signifies how often a real user will not be verified successfully. A high rate translates into more user retries; hence usability suffers.

Crossover: Crossover is where the FAR and FRR would be equal. The best technologies have the lowest crossover rate. Figure 6 below shows where Keystroke Dynamics falls with respect to physical biometrics.

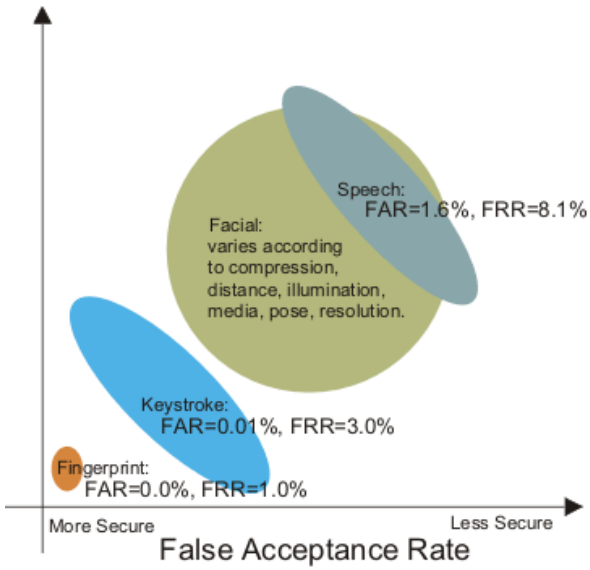

Figure 6. Effectiveness of Keystroke Dynamics via FAR [1]

Conclusion

Keystroke biometrics provides an economic and successful arena to develop authentication methods which would allow logging of data and generating biometric profiles for identification. The tool designed in this project is not complicated or fancy, yet it is simple and efficient. There is a problem of false reject rate discovered while testing, and this will be looked into as future modifications. However False Acceptance rate is 0% which does not allow intruders to compromise the system. Overall, the project is successful in showing that typing dynamics can be used to build a system for user authentication.

References

[1] Checco, J., Keystroke Dynamics and Corporate Security, WTSA Publications acquired from http://www.wsta.org/publications/articles/1003_article06.html
[2] Das, R., An Application of biometric Technology: Keystroke Recognition, Article Published by HTG Systems.
[3] Joyce, R. and G. Gupta, "Identity Authentication Based on keystroke Latencies," Communications of ACM, Volume 33, Issue 2, (February 1990). Retrieved on 8th March 2005.
[4] Kung, S., Biometric Authentication: A Machine Learning Approach, First Edition , Published by Prentice Hall, PTR.
[5] Obaidat, S. and B. Sadoun, Verification of Computer users using Keystroke Dynamics," *IEEE, Volume 27, Issue 2,* (April 1997). Retrieved from IEEE on 16th February 2005.
[6] Peacock, A., Learning User Keystroke Latency Patterns, acquired from http://pel.cs.byu.edu/~alen/personal/CourseWork/cs572/KeystrokePaper/index.html
[7] Umphress, D., and G. Williams, Identity Verification Through keyboard Characteristics," International Journal Man-Machine Studies, Volume 23, Academic Press, 1985.