DEVELOPMENT OF A PRESSURE-BASED TYPING BIOMETRICS SYSTEM FOR USER AUTHENTICATION

Oleh

Loy Chen Change

Disertasi ini dikemukakan kepada
UNIVERSITI SAINS MALAYSIA

Sebagai memenuhi sebahagian daripada syarat keperluan
untuk ijazah dengan kepujian

SARJANA MUDA KEJURUTERAAN (KEJURUTERAAN ELEKTRONIK)

Pusat Pengajian Kejuruteraan
Elektrik dan Elektronik
Universiti Sains Malaysia **Mac 2005**

DEVELOPMENT OF A PRESSURE-BASED TYPING BIOMETRICS SYSTEM FOR USER AUTHENTICATION

By

Loy Chen Change

Dissertation submitted to
UNIVERSITI SAINS MALAYSIA

In partial fulfillment of the requirements
for degree with honors

BACHELOR OF SCIENCE (ELECTRONIC ENGINEERING)

School of Electrical and
Electronic Engineering
Universiti Sains Malaysia **Mac 2005**

Nama: Loy Chen Change

Nombor Matriks: 66090

Pusat Pengajian: Pusat Pengajian Kejuruteraan Elektrik dan Elektronik.

Projek: Development of a Pressure-based Typing Biometrics System for User Authentication

ABSTRAK

Pengesahan menggunakan kata laluan adalah cara yang paling luas digunakan untuk mengenalpasti identiti individu. Namun begitu, cara ini didapati mempunyai banyak kelemahan. Kata laluan memainkan peranan seperti kunci; sesiapa yang mempunyai ia dapat masuk ke dalam sistem. Tambahan pula, kata laluan mudah dipecah masuk, diteka, dicuri, dan dikongsi bersama. Untuk meminimumkan risiko pencerobohan, biometrik penaipan boleh digunakan untuk menambahbaik system kata laluan biasa. Biometrik penaipan mengenalpasti identiti individu berdasarkan cara seseorang menaip di atas papan kekunci. Terdapat penyelidikan yang menggunakan ciri-ciri pemasaan semasa menaip untuk mengenalpasti identiti seseorang. Dalam projek ini, tekanan semasa menaip (tekanan jari di atas papan kekunci) digunakan, dan prestasi dibandingkan dengan teknik penggunaan ciri-ciri pemasaan. Projek ini juga menyelidik penggunaan kombinasi kedua-dua ciri tekanan dan ciri pemasaan. Satu papan kekunci khas yang peka terhadap tekanan telah direkabentuk untuk mengesan tekanan jari semasa menaip. Satu antaramuka pengguna digunakan untuk mengumpul data daripada 100 pengguna. Semua pengguna diminta untuk menggunakan kata laluan yang sama. Tiga cara klasifikasi telah digunakan, iaitu *Logistic Regression* (LR), *Multilayer Perceptron* (MLP), dan rangkaian neural *Fuzzy ARTMAP* (FAM). Keputusan agak menggalakkan, dengan ketepatan setinggi 93.9% didapati dengan menggunakan FAM. Keputusan yang lebih baik didapati dengan menggunakan masa di antara dua penekanan kekunci berturut-turut, berbanding dengan penggunaan tekanan semasa menaip. Tetapi jikalau kedua-dua teknik digabung bersama, keputusan yang lebih baik diperolehi, dengan 0.87% *False Acceptance Rate* (FAR) dan 4.4% *False Rejection Rate* (FRR). Keputusan eksperimen-eksperimen yang dijalankan menunjukkan penggunaan tekanan semasa menaip dapat menambah ketepatan kepada system pengesahan biometrik penaipan.

ABSTRACT

Password authentication is the most prevalently used identification system in today's cyber world. In spite of the popularity of this approach there are many inherent flaws. The password plays the role as the key to a lock; anyone who has it can gain successful access. Additionally, passwords can be easily cracked, guessed, stolen or deliberately shared. To minimize the risk of intrusion, keystroke dynamics can be used to complement this popular authentication method. As the name implies, it is an automated biometric method that analyzes the way a person types on a keyboard. There have been a lot of studies on using keystroke timing characteristics to verify the identity of a user. In this project keystroke pressure (the amount of force exerted on each key pressed) was employed, and its performance was compared with that of the conventional keystroke timings-based technique. The project also investigated the use of combined keystroke pressure and latency for the identification process. In order to measure the forces exerted during typing, a pressure-sensitive keyboard system was developed. A user interface that simulates actual login environment was used to collect data from 100 users. All users were requested to enter the same password. Three different classification methods were applied, namely Logistic Regression (LR), Multilayer Perceptron (MLP), and Fuzzy ARTMAP (FAM) neural networks. The results were very encouraging, with a maximum accuracy rate of 93.9% achieved by using FAM. Keystroke latency gave better results than keystroke pressure, but using both techniques together yielded the best results, with False Acceptance Rate (FAR) of 0.87% and False Rejection Rate (FRR) of 4.4%. The experimental results demonstrated that the proposed methods are promising, and that the keystroke pressure is a viable and practical way to add more security to conventional typing biometrics authentication system.

ACKNOWLEDGEMENT

I would like to express my gratitude to the many people who have made my undergraduate studies possible and who have made it such a rewarding experience. First and foremost, my greatest honour and appreciation go to Assoc. Prof. Lim Chee Peng, my supervisor cum lecturer for his tireless dedication and guidance. His thoughts, encouragement and suggestions especially during my hard time have greatly influence the success of this project. I am grateful to have such an experienced supervisor to guide me along the way.

Special thanks to Mr. Tang Weng Chin, for helping me unconditionally to borrow the DAQ card from Intel. Hereby, I am also indebted to Intel for lending me the DAQ card. Next, I would like to thank Mr. Ooi Woi Seng for his assistance in purchasing the BNC connector block. Besides, my sincere appreciation should be tendered to Dr. Lai Weng Kin from Mimos Bhd who lending me the pressure sensors. Thanks for his guidance during my industrial training so that I can apply the knowledge learned in this project.

I sincerely appreciate the assistance from Mr. Koay Feng Tai and Chen Kok Yeng. I would also like to acknowledge and thank to all those who willingly participated in the user trials for this project.

Last but not least, I appreciate my family for the goodwill and moral support provided by them in accompanying me until I completed the project successfully.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1

INTRODUCTION

1.1 Motivation

Computer systems are now used in almost all aspects ~~in~~ of our life. Personal Computers (PCs) have evolved from large single-user systems to multi-user networks spanning national and international territory. The increasing degree to which confidential and proprietary data are stored and transmitted electronically makes security a foremost concern in today's age of technology. The objective of information system security management is the maintenance of confidentiality (privacy), integrity, and availability of information resources for authorized organizational end users (~~Ammann~~ Jajodia et al., 1999). User authentication is a foundation procedure in the overall pursuit of these objectives.

Password mechanisms have been, and probably will remain as, the primary method of user authentication in web-based or traditional computer access terminals. Ironically, password authentication is an inexpensive, convenient and familiar paradigm that most operating systems support. Unfortunately, static identification and authentication seem to be inadequate to protect computer resources from malicious attacks and intrusions, since there are many ways in which the password authentication system can be breached. For instance, passwords can be exhaustively searched by utilizing a dictionary or brute force attack to try every possible combination of typeable letters. Moreover, if a password is transmitted from client to server or even keyboard to terminal, it is possible to intercept and record this information. Besides that, password can be easily deliberately shared, guessed and stolen without knowledge of the owner.

In order to minimize the risks, experts advise computer users to select different password for different sites and change passwords periodically. Thus, users must

Formatted: All caps

Formatted

Formatted: Underline

Formatted: All caps

Formatted: Centered, Border: Bottom: (No border)

Formatted: Font: Not Bold, No underline

Formatted: Font: 12 pt, Underline

Formatted: Font: 12 pt

remember many identities and password combinations. As a result, users tend to reuse the same password at multiple sites. Exposure of a user password at a weak site can lead to the users' accounts being used fraudulently at other sites. Experts also suggest using longer password and adding more variability in its characters to provide higher security. However, such passwords tend to be harder for end users to remember. Hence, end users select their own more easily remembered passwords which are more easily ~~to be~~ cracked. To remedy these potential security problems, more robust safeguards or strategies are needed against unauthorized access to computer resources.

There are many alternative systems of verification including tokens such as swipe cards as well as user biometrics. Others are researching the possibility of using graphical passwords. Of these, biometrics is the more secure option as it is difficult to forge someone else's unique physiological characteristics. Common methods of biometric identification include fingerprint scanning, iris scanning, hand geometry and etc.

Typing biometrics, also known as keystroke dynamics, is one of the most eagerly awaited of all biometric technologies in the computer security arena. As the name implies, it is an automated biometric method that analyzes the way a person types on a keyboard. The concept of typing biometrics is basically adding another protection layer to the current password or PIN system. The premise behind this protection layer is that each person exhibits a distinctive pattern and cadence of typing. Therefore unless the imposter has the ability to replicate or imitate exactly the authorized user's typing patterns, it is impossible for the imposter to gain full access to the computer resources, even if the imposter is able to guess the correct password. The advantages of keystroke dynamics in the computer environment are apparent. Neither enrolment nor verification disturbs the regular work flow significantly. From the system implementations point of view, at the present time, keystroke recognition is completely software-based solution, thus it is cost-effective.

However, there are some technical difficulties abound in making the technology work as promised. To date, though, the community has been slow in adopting keystroke dynamics verification methods because of its comparatively lower accuracy. Therefore, vendors and companies prefer other authentication systems that are more secure, such as fingerprint systems and eye scanning systems. In order to make keystroke dynamics authentication systems ~~to be~~ more reliable, ongoing research is clearly needed to increase the accuracy.

1.2 Keystroke Dynamics

Formatted: Font: 12 pt

Keystroke dynamics is an automated biometric method of examining an individual's keystrokes on a keyboard or keypad. Keystroke dynamics is also known with a few different names: keyboard dynamics, keystroke analysis, typing biometrics and typing rhythms. Studies (Refer to Section 2.8 Literature Review) have shown that a user's typing patterns can be used for identity verification. Keystroke patterns which can be measured include the latencies between successive keystrokes, keystroke durations, special typing habits and pressure exerted on the keys. These patterns are found to be more consistent on regularly typed string (e.g., password or username).

From Figure 1.1, we can observe the process of conventional password mechanism which has been hardened with keystroke dynamics. In traditional password authentication process, access to computer systems is usually controlled by user accounts with usernames and passwords. On the other hand, if the computer system is protected with typing biometrics system, users are rejected if his/her typing patterns defer from the template stored, even though they submit the correct login information.

As can be seen from Figure 1.1, when a user claims to be a particular individual and types in a login string, the test profile is compared with the reference profile for that individual. If the test profile is a reasonably close match to the reference, the user is permitted to access the system, otherwise they are rejected. If the maximum attempts to present correct typing patterns is exceeded, probably 3 to 6 attempts, the system may deny the user, notify the security administrator to lock up the system for a few minutes.

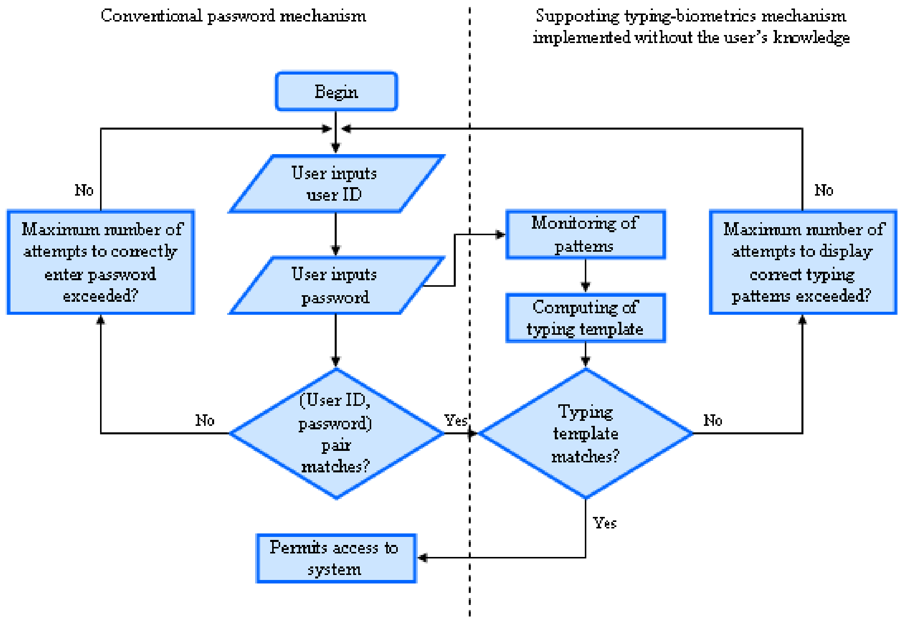

Conventional password mechanism
Supporting typing-biometrics mechanism implemented without the user's knowledge
Begin
User inputs user ID
User inputs password
No
Maximum number of attempts to correctly enter password exceeded?
(User ID, password) pair matches?
No
Yes
Permits access to system
Monitoring of patterns
Computing of typing template
Typing template matches?
No
Yes
No
Maximum number of attempts to display correct typing patterns exceeded?

Figure 1.1: Flow chart for the password authentication process which has been reinforced with keystroke dynamics (adopted from De Ru and Eloff 1997).

1.2.1 Brief History of Keystroke Dynamics

Formatted: Font: 12 pt

The origin of keystroke dynamics can be traced back to World War II. The military used to transmit messages via Morse code. Military Intelligence discovered that individuals could be identified based on the unique rhythm of keying in a message's "dashes" and "dots". This method was known as the "Fist of the Sender," and it was used to distinguish ally from enemy (BioPassword, 2005).

Formatted: Font color: Auto

Formatted: Font color: Auto

Formatted: Font color: Red

The first suggested use of keystroke characteristics for identification appeared in 1975 (Spillane, 1975). The RAND report (Gaines et al., 1980) published in 1980, funded by the National Science Foundation of America, is well known as the canonical analysis and assessment of keystroke dynamics (Refer to Section 2.8 Literature Review). In the early 1980s, a promising study was conducted by SRI International (formally known as Stanford Research Institute). Subsequently, numerous researches and studies were carried out by many others, notably Leggett and Williams (1988) and Joyce and Gupta (1990). The first patent to apply typing biometrics specifically for the purpose of identification was issued in 1989 and it is the main patent currently used in BioNet Systems' BioPassword. The title was "Method and apparatus for verifying an individual's identity" and was issued to James Young and Robert Hammon of International Bioaccess Systems Corporation of New York (Young and Hammon, 1989). In 2000, keystroke dynamics technology by BioPassword passed the Financial Services Technology Consortium (FSTC)/International Biometric Group (IBG) Comparative Testing program.

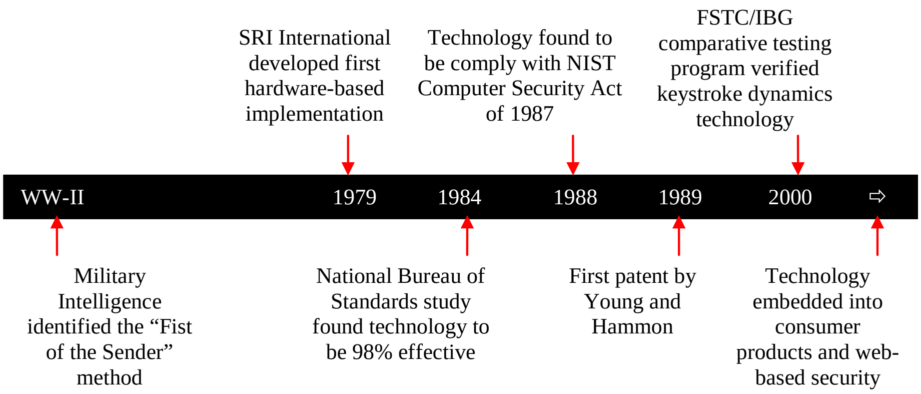

SRI International developed first hardware-based implementation
Technology found to be comply with NIST Computer Security Act of 1987
FSTC/IBG comparative testing program verified keystroke dynamics technology
WW-II
1979
1984
1988
1989
2000
⇨
Military Intelligence identified the "Fist of the Sender" method
National Bureau of Standards study found technology to be 98% effective
First patent by Young and Hammon
Technology embedded into consumer products and web-based security

Figure 1.2: Timeline for the history of keystroke dynamics.

1.2.2 Static Verification and Dynamic Identification

Formatted: Font: 12 pt

Keystroke dynamics verification techniques can be classified as either static or dynamic. Most applications of keystroke dynamics are in field of static verification. Static verification methods analyze keystroke information only at specific times, for instance, during the login section. Static approaches provide more reliable user verification than simple passwords, but do not provide continuous security. In contrast, dynamic identification monitors the user's typing behavior throughout the course of the interaction. The benefit of monitoring is to prevent an imposter from taking over a previously authenticated session. A dynamic authentication based system can lock itself down when it detect someone with a significantly different typing pattern.

1.2.3 FAR and FRR

Formatted: Font: 12 pt

In most studies on keystroke dynamics, effectiveness of an authentication system is measured by two important parameters (Woodward et al., 2003): False Acceptance Rate (FAR) – the rate that an imposter's keyboard rhythm is falsely identified as belonging to a legitimate user; and False Rejection Rate (FRR) – the rate that a keyboard rhythm is incorrectly identified as belonging to an imposter. The ideal situation is for both these parameters to be as close to zero as possible and usually it is more acceptable to have a higher FRR than FAR.

Formatted: Font: (Default) Times New Rom

Formatted: Font: (Default) Times New Rom

1.2.4 Keystroke Dynamics: Strengths and Weaknesses

Formatted: Font: 12 pt

Keystroke dynamics has several strengths. If a keystroke recognition system doesn't measure keystroke pressure, it is completely a software-based solution, thus it is very cost-effective. Since most people are accustomed to entering their authentication information during login sections, this technology is considered less invasive than some other biometrics.

However, keystroke dynamics has several weaknesses. Keystroke dynamics is designed to verify users based on the traits of their unique typing patterns. Consequently, individuals who do not type in a consistent manner may have difficulty enrolling and verifying in keystroke dynamics verification. In addition, a certain percentage of authorized users will experience rejects when a long period of time has elapsed since enrollment or since one's last verification. If significant time has elapsed since enrollment, physiological changes can complicate verification. If time has elapsed since a user's last verification, the user may have "forgotten" how he/she enrolled, and may type with different cadence and force.

Besides, many other circumstances might impede the verification accuracy. For example, a user may suffer from muscular illness; a user's hand or fingers might be injured; even the user's emotional state might influence how his/her typing patterns.

Sometimes, a user might be doing other things or using different posture (e.g., sitting or standing) whiles he/she is entering authentication information. As a result, the erratic and abnormal patterns of typing might result in a higher false rejection rate (FRR).

From the system implementations point of view, using different model of keyboards might affect keystroke dynamics tremendously. Using backspace key to correct the authentication information may also lead to rejection during verification phase. All these factors must be taken into account when designing a keystroke dynamics system.

~~1.2 Literature Review~~

~~There have been a lot of studies on using keystroke characteristics for user authentication. Most studies have used keystroke latencies as features for user verification, but some have also employed keystroke durations. The main differences between them being the information captured the sample data and the method of analysis.~~

~~In spite of different approaches, in most studies on keystroke dynamics, effectiveness of an authentication system is measured by two important parameters (Woodward et al. 2003): False Acceptance Rate (FAR) – the rate that an imposter's keyboard rhythm is falsely identified as belonging to a legitimate user; and False Rejection Rate (FRR) – the rate that a keyboard rhythm is incorrectly identified as belonging to an imposter. The ideal situation is for both these parameters to be as close to zero as possible and usually it is more acceptable to have a higher FRR than FAR.~~

~~The first studies of effectiveness of keystroke dynamics as identity verifiers appeared in 1977 and 1980 (Forsen et al. 1977) (Gaines et al. 1980). One of the earlier works in this area was undertaken by R. Gaines et al. (Gaines et al. 1980). They conducted experiments with seven secretaries in which they were asked to retype the same three paragraphs at two different times over a period of four months. Keystroke latencies were collected and analyzed for a limited number of digraphs and observations~~

~~were based on those digraph values that occurred more than ten times. These keystroke latencies were preprocessed by removing outliers and then taking the logs of the remaining values. A test of statistical independence was carried out using the *t* Test under the hypothesis that the means of the keystroke latencies at both sessions were the same, and with the assumption that the two variances were equivalent. Encouraging results were obtained and the suggested procedure claimed to have a FAR of 0% and FRR of 4%. While they proved the concept of user identification by keyboard timings as viable it is difficult to evaluate the effectiveness of their methods due to the limited scale of their experiments.~~

~~Similar experiments were undertaken by Leggett and Williams (Leggett and Williams 1985). The experiments gave results of 5.5% FRR and 5.0% FAR. In their experiments, 17 programmers provided two typing profiles, the first with about 1400 characters that served as a reference profile and the second was about 300 characters that served as the test profile. Latency was considered valid if it fell within 0.5 standard deviations of the mean reference digraph latency, and a user was accepted if more than 60 percent of the comparison between the test signature and the mean reference latencies were valid. This study proved that keystroke biometrics is a valid method for identity verification. However, the study was limited by the fact it required a large amount of input text as in the Gaines experiment.~~

~~One of the promising research efforts in applying keystroke dynamics as an authentication method was the work done by Rick Joyce and Gupta Goyal (Joyce and Gupta 1990). Their identity verifier was based on keystroke latencies obtained during the login process of 33 users. A total of 165 self login attempts and 810 imposter login attempts were recorded. In their paper, keystroke pattern was referred to "signature". A new user was required to provide eight reference signatures by typing their usernames, passwords, first and last name eight times. From the eight reference signatures, the mean reference signature was computed. During verification, the user provided a test signature which is compared with the mean reference signature to determine the magnitude of difference between two profiles. A user would login successfully if magnitude of difference is less than the threshold. Each user was given a set threshold based on a measure of the variability of his/her signatures. The authors reported that~~

~~their approach was found to have an FAR of less than 1% and FRR of 16.67%. In their paper, they also reported some results of using a technique based on comparing signature shapes for identity verification. Besides that, they also pointed out that timing accuracy was essential in the design of typing biometrics-based authentication system.~~

~~S. Bleha, Slavinski and Hussein also used keystrokes latencies as features (Bleha et al. 1990). The validity of a user was decided solely based on how he/she typed username and a fixed user-selected phrase. Thirty latest valid username entries were used as reference pattern when deciding if the user is valid. They employed two different classification approached in their experiments, i.e., minimum distance classifier and Bayesian classifier. There was a defined threshold for deciding whether the user is accepted or not. Thresholds were different for both classifiers. If the user was not accepted with the first trial the second trial was given with reduced thresholds. Both classifiers were used together to decide if the user was valid. The user was rejected only when both classifier thresholds were exceeded. In the experiments there were 10 legitimate users and 22 candidates tested the system as imposters. The imposters had a chance to observe valid users so they could try to imitate their typing rhythms. The system gave the FRR of 3.1% and the FAR of 0.5%.~~

~~M. S. Obaidat and B. Sadoun extended the basic research by examining the use of keystroke duration in addition to keystroke latencies (Obaidat and Sadoun 1997). The keystroke timing information was collected from 15 users in which each user typed his/her user ID 225 times each day for eight weeks. They carried out comprehensive study of different statistical and neural classification methods that can be used with keystroke dynamics. The authors reported that keystroke durations gave better results than latencies between keystrokes, but using both measurements together gave the best results. In their experiments, best results (zero percent of both imposter pass rate and false alarm rate) were obtained using the following neural methods: Fuzzy ARTMAP, RBFN (Radial Basis Function Network) and LVQ (Learning Vector Quantization). Best results with statistical methods were achieved with the potential function and the Bayes rule. In overall, neural methods gave better results compared to statistical methods. What is not clear from their paper is amount of training required before their system is able to perform the verification recognition that they claim. Additionally it is of concern~~

~~that both the imposter's and legitimate user's typing patterns were used for learning which is not applicable to most network situations.~~

~~In 1997 Fabian Monrose and Aviel Rubin (Monrose and Rubin 1997) conducted their experiments based on the ideas presented by Joyce and Gupta by adding some new changes: examining the use of keystroke durations in addition to keystroke latencies; exploring the long term measurement of keystroke dynamics over weeks; measuring the keystroke dynamics using the user's own computer. Their results showed that all three aspects could be achieved within a workable framework. Of particular interest is their foundation work on the design of a dynamic authentication system that authenticates a user over time using the unstructured text typed by a user in their normal work practices. A database of 42 users was constructed based on the keystroke patterns gathered. In their experiments, Euclidean distance measure and probability measure were employed as classifiers in which weighted probability measure yielded the best results.~~

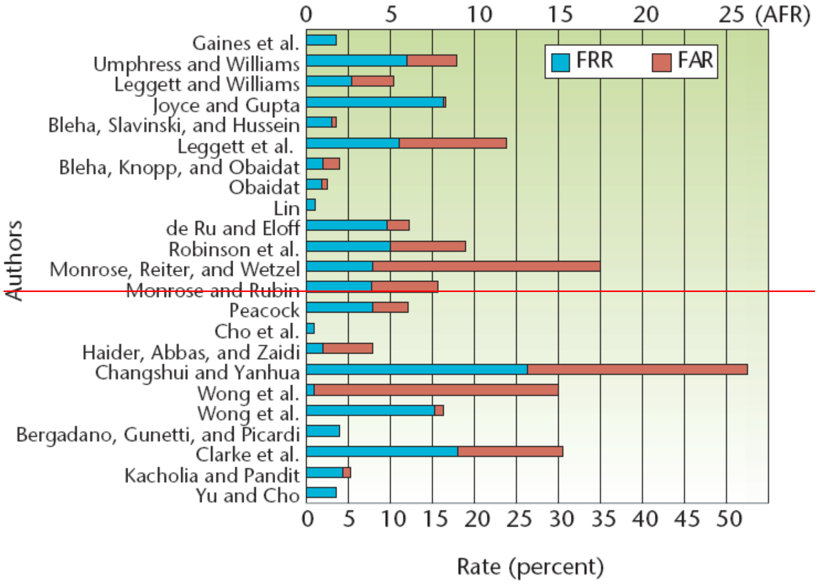
~~Willem G. de Ru and Jan H.P. Eloff attempted to reinforce password with fuzzy logic based typing biometrics (Ru and Eloff 1997). Latency and typing difficulty (a password complexity value based on the distances between keys on the keyboard) of successive keystrokes were used to categorize a user's keystroke patterns. Experimentation had shown that the typing difficulty value was less influential than the latency. They used 5 fuzzy rules in their experiments. Initially, 29 users were required to register in the experimental system. During valid access attempts, users were required to enter their usernames and passwords 25 times respectively. Next, each user typed in another user's authentication information during imposter access attempts. The experiments gave results the FRR of about 7.4% and the FAR of approximately 2.8%. The authors mentioned that simultaneously matching patterns and learning was difficult using their approach. Hence, they suggested using neural networks to overcome this shortcoming.~~

~~Enzhe Yu and Sungzoon Cho (Yu and Cho 2003) proposed to use 4-layer Auto-Associative Multilayer Perceptron (AaMLP) as well as Support Vector Machine (SVM) for keystroke dynamics identity verification. Data was collected from 21 participants with different passwords. Each participant was asked to type his password 150 to 400~~

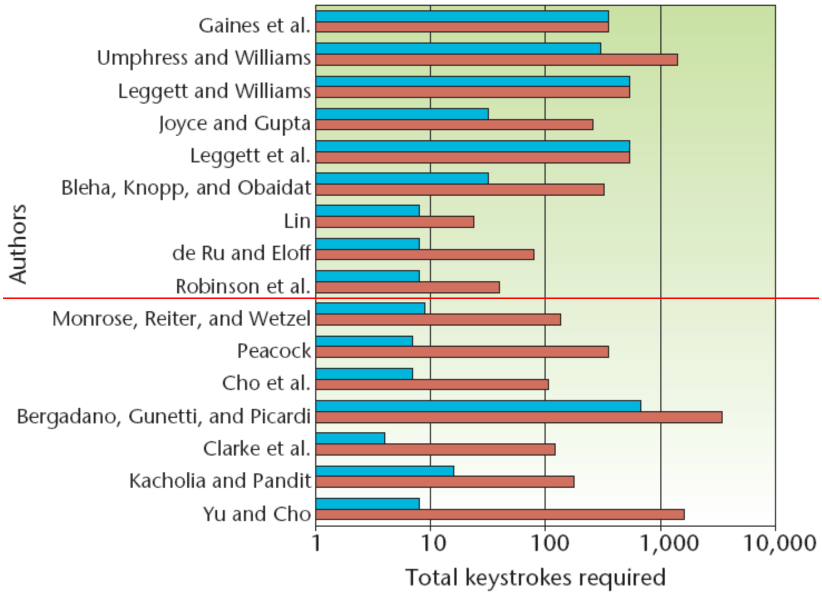
~~times, and the last 75 timing vectors were collected for testing, whereas the remaining ones were used as training patterns. 15 imposters were asked to type each of the given 21 passwords 5 times in two sessions, the first session was typing without any practice whereas the second session was typing with practice, resulting in 150 impostor timing vectors for each password. The authors reported that SVM and 4-layer AaMLP showed similar novelty detection performance. However, the computational effectiveness of SVM is much higher than AaMLP. More recently, Enzhe Yu and Sungzoon Cho (Yu and Cho 2004) proposed to perform feature subset selection using the GA-SVM wrapper approach. They found that the approach clearly improved the model performance with 3.69% of FRR and 0% of FAR.~~

~~A. Dahalan et al. attempted to build a pressure-based typing biometrics system (A. Dahalan et al. 2004) and employed neuro-fuzzy system as the classifier. A special keyboard with pressure sensors was built to capture users' keystroke pressure patterns. They also acquired keystroke duration instead of capturing pressure patterns. In their experiments, average pressure of each keystroke and keystroke durations were used as inputs to the neuro-fuzzy system. The authors reported that pressure patterns can be used to verify identity. However, due to limited participants in the experiments and there was no results of using pressure patterns alone in the classification stage, the effectiveness of using pressure patterns in identity verification is difficult to be evaluated. In addition, average pressure of each keystroke is difficult to be defined since a fast typist may press several keys at the same time.~~

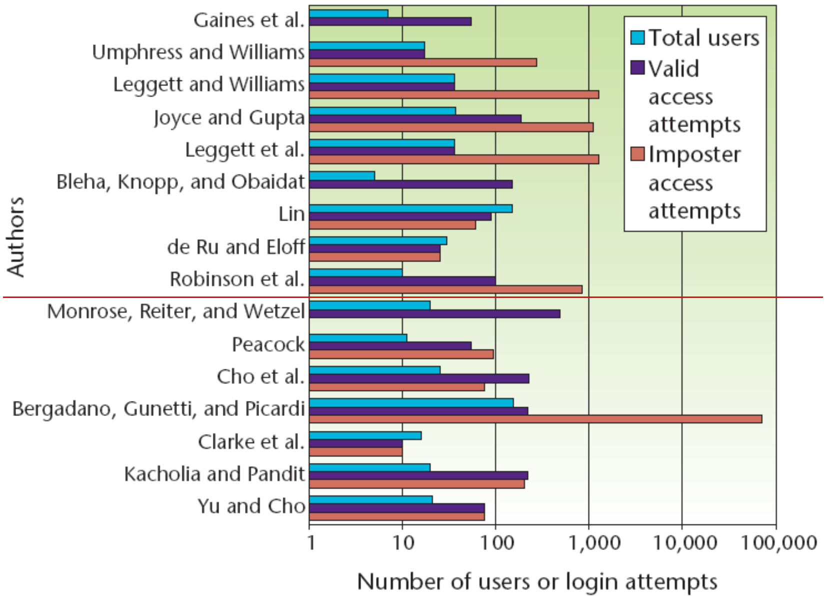
~~Figures 1.1 – 1.3 show the comparison among different studies in this domain.~~



~~**Figure 1.1:** False rejection rate (FRR), false acceptance rate (FAR), and average false rate (AFR) for several approaches. AFR is the average of FRR and FAR, and is shown by the top *y*-axis. Systems with lower FRR, FAR, and AFR are more accurate in discriminating between users, and are thus capable of being more secured (adopted from Peacock et al. 2004).~~



~~**Figure 1.2:** Comparing different keystroke approaches. The cost to a user (in keystrokes) to enroll and to authenticate for a given approach shows that systems that can enroll and authenticate with fewer keystrokes are easier to use. Blue represents the cost to a user to authenticate; red is the cost to a user to enroll (adopted from Peacock et al. 2004).~~



~~**Figure 1.3:** Confidence in test results. The involvement of more users and more valid/imposter logins lends credence to reported results, but even the largest studies in the keystroke dynamics field to date fall short of proving competence on large systems (adopted from Peacock et al. 2004).~~

1.3 Project Objectives

Formatted: Font: 12 pt

In this project, keystroke pressure is proposed to be used for the authentication purpose. In essence, there are three main parts in this project:

a) To design and develop a pressure sensitive keyboard.

b) To design and develop a user interface for the system.

c) To assess and examine the performance of using keystroke pressure for static identity verification.

In order to collect the keystroke patterns for experiments, a special keyboard is first built and a user interface is designed. The user interface is mainly used for capturing users’ keystroke pressure patterns, transforming the pressure patterns into amplitude spectral, extracting features, and classifying the pressure features. A series of experiments have been conducted to evaluate the performance of the system in a systematic way. In contrast to keystroke pressure patterns, some experiments have been carried out using keystroke latency patterns. A comparison between keystroke pressure and keystroke latency is made to determine which approach is better. Besides that, this project also investigates the possibility of combining both keystroke pressure and keystroke latency to form a single user profile in order to achieve a higher accuracy rate. In summary, this project is geared towards achieving the following objectives:

a) To develop hardware and software for the pressure-based typing biometrics system.

b) To examine the use of keystroke pressure in addition to keystroke latency.

c) To examine the features extraction approach in which features are extracted from the amplitude spectral of the keystroke patterns.

d) To compare and evaluate different classification methods using the data set collected.

Formatted: Indent: Left: 0"

1.4 Dissertation Outline

Formatted: Font: 12 pt

This dissertation is organized into 6 chapters. In Chapter 2, a general overview of biometrics is presented. The overview covers the definition, history, benefits of biometrics and an explanation of how biometrics works. In addition, a number of conventional biometrics technologies are described briefly. These include fingerprint, hand geometry, as well as facial recognition. Then the applications of keystroke dynamics are~~is~~ ~~introduce~~described. A review of typing biometrics systems and researches revealing different approaches and methodologies is presented. ~~In particular~~Besides, two selected commercial products based on keystroke dynamics are reviewed, they are BioPassword™ and bioChec™.

Underlying theories and algorithms used in this project are covered in Chapter 3. Fast Fourier Transform is performed on the acquired pressure waveform in order to get their amplitude spectral. Hence, an explanation of Fast Fourier Transform is first provided. Subsequently, pattern classification and modeling techniques are elaborated. Particularly, Logistic Regression (LR), Multilayer Perceptron (MLP), and Fuzzy

ARTMAP (FAM) are studied. Next, Principal Components Analysis (PCA) is explained, and cross validation is covered at the end of the chapter.

The work in Chapter 4 concentrates on system design and development. Basically, this chapter is subdivided into two sections, i.e. hardware design and development is discussed in the first section whereas software development is presented in the second section. In the first section, the method and procedures involved in building the pressure sensitive keyboard is presented. Each hardware component is discussed. Several experiments have been carried out to ensure the pressure sensors are within the specifications. In the next section, the software design and development process is discussed. Requirements and specifications of the software are first listed out. Subsequently, a general introduction of LabVIEW is provided. After that, a graphical user interface of the system is explained. Apart from that, the main modules of the software such as data capture module, feature extractor, and classifier are also explained in detail.

To investigate the capability and effectiveness of the authentication system, various experiments have been conducted. The results and analyses are reported in Chapter 5. The chapter commences by providing the explanation of procedures for setting up the experiments. In this section, data collection, feature extraction, feature selection and data preprocessing are explained. In the next section, PCA visualization of the keystroke patterns is presented. The results obtained from experiments of keystroke pattern classification are analysed. For comparison, three different classification methods have been used, i.e. Logistic Regression (LR), Multilayer Perceptron (MLP), and Fuzzy ARTMAP (FAM). Experiments have also been conducted to examine the effects on network performance by reducing the dimension of feature vectors using PCA. Eventually, plurality of features is discussed at the end of the chapter.

Finally, conclusions are drawn in Chapter 6. Some problems and limitations of the system are highlighted, and some solutions to the problems are suggested. A number of areas to be pursued as further work are suggested at the end of the dissertation.

CHAPTER 2

BIOMETRICS AND KEYSTROKE DYNAMICS

2.1 Introduction

Authentication is the process of verifying a claimed identity. In our daily lives, we often need to verify our identities or someone else's identity. For examples, we have to type in our usernames and passwords when logging onto computer or email accounts; we have to provide our PIN codes together with the smart cards when we want to use automated teller machine (ATM). These authentication processes bring greater security to out daily activities and public safety. Typically, there are three credentials in authentication mechanisms. Going from the lowest to the highest levels of security these include (Woodward et al., 2003):

- Something you have - card, token, key.
- Something you know- PIN, password.
- Something you are - biometrics.

Any combination of these elements further heightens security of an application. Requiring all three for an application provides the highest form of security.

The next section presents a background to biometrics. A review of typing biometrics systems and researches revealing different approaches and methodologies is presented. In particular, two commercial typing biometrics products are reviewed. A summary is included at the end of this chapter.

2.2 Definition of Biometrics

Because biometrics can be used in such a variety of applications, it is very difficult to establish an all-encompassing definition. A general, concise definition of biometrics is

“The automated use of physiological or behavioral characteristics to determine or verify identity.” (International Biometric Group, 2005)

2.3 Identification and Verification

Biometrics can be used for both *identification* and *verification.* The terms differ significantly. With *identification*, the biometric system asks and attempts to answer the question, “Who is X?” In an identification application, a larger amount of biometrics data is collected, and the user of the computer is identified based on previously collected information of profiles of all users. This type of comparison is called a “one-to-many” search. Depending on how the system is designed, it can make a “best” match, or it can score possible matches, and rank them in order of likelihood. Identification applications are common when the goal is to identify criminals, terrorists, or other “wolves in a sheep’s clothing,” particularly through surveillance.

Verification occurs when the biometric system asks and attempts to answer the question, “Is this X?” after the user claims to be X. In a verification application, the biometric system requires input from the user, at which time the user claims his identity via a password, token, or user name (or any combination of the three). This user input points the system to a template in the database. The system also requires a biometric sample from the user. It then compares the sample to or against the user-defined template. This is called a “one-to-one” search. The system will either find or fail to find a match between the two. Verification is commonly used for physical or computer access.

2.4 Brief History of Biometrics

The term *biometrics* is derived from the Greek words *bio* (life) and *metric* (to measure). Biometrics dates back to the ancient Egyptians, who measured people to identify them. Among the first known examples of practiced biometrics was a form of memberprinting used in China in the fourteenth century, as reported by the Portuguese historian Joao de

Barros (Woodward et al., 2003). The Chinese merchants were stamping children's palm and footprints on paper with ink to distinguish the babies from one another.

In the 1890s, an anthropologist and police desk clerk in Paris named Alphonse Bertillon sought to fix the problem of identifying convicted criminals and turned biometrics into a distinct field of study (Woodward et al., 2003). He developed a method of multiple body measurements that was named after him (the Bertillonage technique - measuring body lengths). Police throughout the world used this system until it proved to be exceedingly prone to error as many people shared the same measurements. After this failure, the police started using fingerprinting - developed by Richard Edward Henry of Scotland Yard (Woodward et al., 2003).

2.5 Types of Biometrics

Biometric measurements can be classified as physiological and behavioral. Physiological biometrics is based on measurements of biological aspects of the human body. Physiological traits are stable physical characteristics and hence tend to offer greater accuracy and security. Fingerprint, iris-scan, retina-scan, hand geometry, and facial recognition are famous biometrics. Behavioral biometrics, in turn, is based on measurements of controllable actions, and indirectly measure characteristics of the human body. Behavioral biometrics such as one's signature, voice, or keystroke dynamics is leading biometric technologies. Behavior-based biometrics can be less expensive and less intrusive to users. Various famous biometric technologies are introduced below:

- **Iris Scan**

Iris can be defined as "the round pigmented membrane surrounding the pupil of the eye" (Woodward et al., 2003). The iris is layered beneath the cornea and has patterns that are intricate, richly textured, and composed of many furrows and ridges. Iris scanning measures these patterns to identify a person. Iris patterns are formed randomly. As a result, the iris patterns in a person's left and right eyes are different, and so are the iris patterns of identical twins. Iris scanning can be used quickly for both identification and verification applications because the iris is highly distinctive and robust.

- **Retinal Scan**

Retina biometrics distinguishes individuals by using the patterns of veins occurring in the back of the eye. The device involves a low intensity infrared light source shined into the eye of a user. The user must be standing very still within inches of the device and must ensure proper alignment because the retina is a protected internal organ. At present, the market for retinal scanning is mainly for door access control. It is not widely used because it is being one of the more expensive technologies. Another factor that affects its popularity is misconception that retina scans for identification purposes also reveal personal medical information, which this technology is more prone to privacy abuse.

- **Facial Recognition**

Facial recognition records the spatial geometry of distinguishing features of the face. Different vendors use different methods of facial recognition, however, all focus on measures of key features of the face. Because a person’s face can be captured by a camera from some distance away, facial recognition has a clandestine or covert capability (i.e. the subject does not necessarily know he has been observed). For this reason, facial recognition has been used in projects to identify card counters or other undesirables in casinos, shoplifters in stores, criminals and terrorists in urban areas. And as facial recognition and other technology improves, it is possible that future applications will increasingly make use of facial recognition in cell phones, videoconferencing application, robots, interactive games, and smart home appliances.

- **Speaker /Voice Recognition**

Voice verification or speaker recognition is a biometric with both physiological and behavioral components. From physiological perspective, it uses vocal characteristics to identify individuals using a pass-phrase. The motion, manner, and pronunciation of words form the basis for the behavioral aspects of voice biometrics. It is comparatively cheaper and easily deployable technology because a telephone or microphone can serve as a sensor. However, voice recognition can be adversely affected by environmental factors such as background noise or degraded communication channels. Normally, it is used in conjunction with PIN authentication.

- **Fingerprint**

Fingerprints are the oldest and most widely recognized biometric markers. They are the impressions of the papillary or friction ridges, endings, and bifurcations on the surfaces of the hand. From the old ink and paper method used for more than a century for identification, fingerprint biometric has changed to automated comparison of fingerprints. The biometric device involves users placing their finger on a platen for the print to be electronically read. Fingerprint biometrics currently has three main application arenas: large-scale Automated Finger Imaging Systems (AFIS) generally used for law enforcement purposes, fraud prevention in entitlement programs, and physical and computer access.

- **Hand/Finger Geometry**

Hand or finger geometry is an automated measurement of many dimensions of the hand and fingers, such as length, width, thickness, and the surface area of the hand and four fingers. Spatial geometry is examined as the user puts his hand on the sensor's surface and uses guiding poles between the fingers to properly place the hand and initiate the reading. Hand geometry is a widely used and well-developed technology that has been thoroughly field-tested and is easily accepted by users. Because hand and finger geometry have a low degree of distinctiveness, the technology is not well-suited for identification applications but distinctive enough to permit verification of a claimed identity.

- **Signature Verification**

Signature verification is an automated method of measuring an individual's signature. It can be used anywhere conventional signature are used. This technology examines features of the signature itself (static product) and details on how the signature is produced (dynamic process). Forgers were able to duplicate the static signature but difficult to duplicate the manner in which it was produced. The additional dynamic information that makes forgery very difficult are stroke direction, speed, pen up and pen down events.

Table 2.1 shows a general comparison of biometric technologies in terms of primary usage, robustness, distinctiveness, perceived intrusiveness, and cost.

Table 2.1: Comparison of biometric technologies.

Biometric	Usage	Robustness	Distinctiveness	Intrusiveness	Cost
Iris	Identification/ Verification	High	High	3 – 7 inches	High
Retinal	Identification/ Verification	High	High	2 – 3 inches	High
Facial	Identification/ Verification	Moderate	Moderate	12+ inches	Moderate
Voice	Verification	Moderate	Low	Remote	Low
Fingerprint	Identification/ Verification	Moderate	High	Touching	Moderate
Hand	Verification	Moderate	Low	Touching	Moderate
Signature	Verification	Low	Moderate	Touching	Moderate
Keystroke	Verification	Low	Low	Touching	Low

The *robustness* of a biometric refers to the extent to which the characteristic or trait is subject to significant changes over time. These changes can occur as a result of age, injury, illness, occupational use, or chemical exposure. A highly robust biometric does not change significantly over time while a less robust biometric will change. For example, the iris, which changes very little over a person’s lifetime, is more robust than one’s voice (Woodward et al., 2003).

Distinctiveness is a measure of the variations or differences in the biometric pattern among the general population. The higher the degree of distinctiveness, the more individual is the identifier. A low degree of distinctiveness indicates a biometric pattern found frequently in the general population. The iris and the retina have higher degrees of distinctiveness than hand or finger geometry (Woodward et al., 2003).

Intrusiveness refers to the manner in which biometric systems capture biometric information from users during enrollment and authentication phase. If a system causes uncomfortable or inconvenient to users, then the system is said to be intrusive. For example, eye scanning biometrics may cause unpleasant feeling because the systems involve lights shooting into eyes. Moreover, the scanning process requires close focal distance and good alignment of an eye into the lens.

Figure 2.1 shows the market share of biometric technologies in 2003 exclusive of Automated Fingerprint Identification System (AFIS) revenue, used by the FBI and other law enforcement agencies. As one can see, fingerprint biometrics is by far the largest chunk of the market, as measured by International Biometric Group.

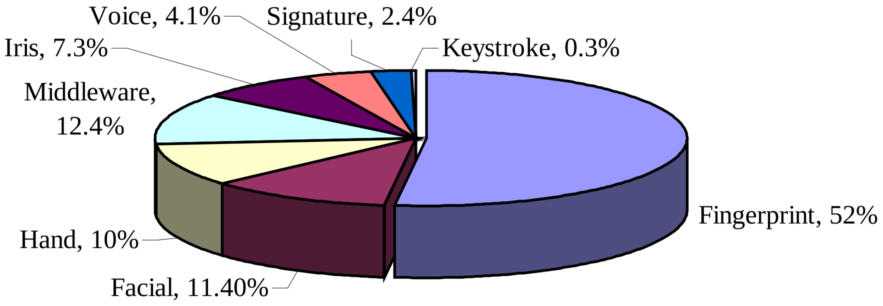


Figure 2.1: 2003 Comparative market share by technology (does not include AFIS revenue) (adopted from International Biometric Group, 2005).

2.6 Benefits of Biometrics

There are several key benefits that make biometrics is becoming increasingly popular.

- **Increased security**

Password and PINs can be stolen, guessed, and cracked easily. Biometrics offers a greater protection against unauthorized access. With biometrics, confidential files can be stored securely. Besides that, online purchases are safer when enabled by biometric. Account access much more secure than via password.

- **Reduced costs**

Improvement in hardware and software technologies has brought down the costs of biometric authentication to be affordable at the commercial market level. Form employers' point of view, biometrics is a stronger way to detect and deter benefits fraud. They can reduce cost by cutting down the password maintenance cost and replacing buddy punching by biometrics system.

- **Convenient authentication**

The convenience of quick-and-easy authentication makes a smoother system of identity assurance than using keys, tokens, cards or PINs. With biometric technology, there is nothing to lose or forget since the characteristics or traits of the person serve as the identifiers. In addition, biometrics helps to eliminate the need to replace badges or reset password.

2.7 Applications of Keystroke Dynamics

There is a slow adoption of keystroke dynamics technology since it was introduced. The reasons might be the technology is new and there may be a resistance and lack of trust towards such an innovation. Nevertheless, keystroke dynamics has already found its way into some areas in the past two years.

The emerging typing biometrics based authentication technology is applicable to many areas. For corporations, this technology has found uses in network security as well as asset identification. In the consumer market, e-commerce developers are exploring the use of typing biometrics to more accurately verify a trading party’s identity. Besides, the technology can be integrated to desktop computers, laptops, PDAs, and tablet PCs.

Keystroke dynamics have also been studied and tested for use with numeric keypads. If such system is effective, adoption for this technology will be seen in the banking security especially in automated teller machine (ATM) security. In addition, the ability of third generation telephones to store sensitive information, such as financial records, digital certificates and company records, makes them desirable targets for impostors. Hence, keystroke dynamics could have an enormous application area for phone systems.

2.8 Literature Review

There have been a lot of studies on using keystroke characteristics for user authentication. Most studies have used keystroke latencies as features for user verification, but some have also employed keystroke durations. The main differences between them being the information captured the sample data and the method of analysis.

The first studies of effectiveness of keystroke dynamics as identity verifiers appeared in 1977 and 1980 (Forsen et al., 1977) (Gaines et al., 1980). One of the earlier works in this area was undertaken by R. Gaines et al. (Gaines et al., 1980). They conducted experiments with seven secretaries in which they were asked to retype the same three paragraphs at two different times over a period of four months. Keystroke latencies were collected and analyzed for a limited number of digraphs and observations were based on those digraph values that occurred more than ten times. These keystroke latencies were preprocessed by removing outliers and then taking the logs of the remaining values. A test of statistical independence was carried out using the *t*-Test under the hypothesis that the means of the keystroke latencies at both sessions were the same, and with the assumption that the two variances were equivalent. Encouraging results were obtained and the suggested procedure claimed to have a FAR of 0% and FRR of 4%. While they proved the concept of user identification by keyboard timings as viable it is difficult to evaluate the effectiveness of their methods due to the limited scale of their experiments.

Similar experiments were undertaken by Leggett and Williams (Leggett and Williams, 1988). The experiments gave results of 5.5% FRR and 5.0% FAR. In their experiments, 17 programmers provided two typing profiles, the first with about 1400 characters that served as a reference profile and the second was about 300 characters that served as the test profile. Latency was considered valid if it fell within 0.5 standard deviations of the mean reference digraph latency, and a user was accepted if more than 60 percent of the comparison between the test signature and the mean reference latencies were valid. This study proved that keystroke biometrics is a valid method for identity verification. However, the study was limited by the fact it required a large amount of input text as in the Gaines experiment.

One of the promising research efforts in applying keystroke dynamics as an authentication method was the work done by Rick Joyce and Gupta Goyal (Joyce and Gupta, 1990). Their identity verifier was based on keystroke latencies obtained during the login process of 33 users. A total of 165 self login attempts and 810 imposter login attempts were recorded. In their paper, keystroke pattern was referred to "signature". A new user was required to provide eight reference signatures by typing their usernames, passwords, first and last name eight times. From the eight reference signatures, the mean reference signature was computed. During verification, the user provided a test signature which is compared with the mean reference signature to determine the magnitude of difference between two profiles. A user would login successfully if magnitude of difference is less than the threshold. Each user was given a set threshold based on a measure of the variability of his/her signatures. The authors reported that their approach was found to have an FAR of less than 1% and FRR of 16.67%. In their paper, they also reported some results of using a technique based on comparing signature shapes for identity verification. Besides that, they also pointed out that timing accuracy was essential in the design of typing biometrics-based authentication system.

S. Bleha, Slivinski and Hussein also used keystrokes latencies as features (Bleha et al., 1990). The validity of a user was decided solely based on how he/she typed username and a fixed user-selected phrase. Thirty latest valid username entries were used as reference pattern when deciding if the user is valid. They employed two different classification approached in their experiments, i.e., minimum distance classifier and Bayesian classifier. There was a defined threshold for deciding whether the user is accepted or not. Thresholds were different for both classifiers. If the user was not accepted with the first trial the second trial was given with reduced thresholds. Both classifiers were used together to decide if the user was valid. The user was rejected only when both classifier thresholds were exceeded. In the experiments there were 10 legitimate users and 22 candidates tested the system as imposters. The imposters had a chance to observe valid users so they could try to imitate their typing rhythms. The system gave the FRR of 3.1% and the FAR of 0.5%.

M. S. Obaidat and B. Sadoun extended the basic research by examining the use of keystroke duration in addition to keystroke latencies (Obaidat and Sadoun, 1997). The keystroke timing information was collected from 15 users in which each user typed his/her user ID 225 times each day for eight weeks. They carried out comprehensive study of different statistical and neural classification methods that can be used with keystroke dynamics. The authors reported that keystroke durations gave better results than latencies between keystrokes, but using both measurements together gave the best results. In their experiments, best results (zero percent of both False Acceptance Rate and False Rejection Rate) were obtained using the following neural methods: Fuzzy ARTMAP, RBFN (Radial Basis Function Network) and LVQ (Learning Vector Quantization). Best results with statistical methods were achieved with the potential function and the Bayes rule. In overall, neural methods gave better results compared to statistical methods. What is not clear from their paper is amount of training required before their system is able to perform the verification recognition that they claim. Additionally it is of concern that both the imposter's and legitimate user's typing patterns were used for learning which is not applicable to most network situations.

In 1997 Fabian Monrose and Aviel Rubin (Monrose and Rubin, 1997) conducted their experiments based on the ideas presented by Joyce and Gupta by adding some new changes: examining the use of keystroke durations in addition to keystroke latencies; exploring the long term measurement of keystroke dynamics over weeks; measuring the keystroke dynamics using the user's own computer. Their results showed that all three aspects could be achieved within a workable framework. Of particular interest is their foundation work on the design of a dynamic authentication system that authenticates a user over time using the unstructured text typed by a user in their normal work practices. A database of 42 users was constructed based on the keystroke patterns gathered. In their experiments, Euclidean distance measure and probability measure were employed as classifiers in which weighted probability measure yielded the best results.

Willem G. de Ru and Jan H.P. Eloff attempted to reinforce password with fuzzy logic based typing biometrics (de Ru and Eloff, 1997). Latency and typing difficulty (a password complexity value based on the distances between keys on the keyboard) of successive keystrokes were used to categorize a user's keystroke patterns.

Experimentation had shown that the typing difficulty value was less influential than the latency. They used 5 fuzzy rules in their experiments. Initially, 29 users were required to register in the experimental system. During valid access attempts, users were required to enter their usernames and passwords 25 times respectively. Next, each user typed in another user's authentication information during imposter access attempts. The experiments gave results the FRR of about 7.4% and the FAR of approximately 2.8%. The authors mentioned that simultaneously matching patterns and learning was difficult using their approach. Hence, they suggested using neural networks to overcome this shortcoming.

Enzhe Yu and Sungzoon Cho (Yu and Cho, 2003a) proposed to use 4-layer Auto-Associative Multilayer Perceptron (AaMLP) as well as Support Vector Machine (SVM) for keystroke dynamics identity verification. Data was collected from 21 participants with different passwords. Each participant was asked to type his password 150 to 400 times, and the last 75 timing vectors were collected for testing, whereas the remaining ones were used as training patterns. 15 imposters were asked to type each of the given 21 passwords 5 times in two sessions, the first session was typing without any practice whereas the second session was typing with practice, resulting in 150 impostor timing vectors for each password. The authors reported that SVM and 4-layer AaMLP showed similar novelty detection performance. However, the computational effectiveness of SVM is much higher than AaMLP. More recently, Enzhe Yu and Sungzoon Cho (Yu and Cho, 2003b) proposed to perform feature subset selection using the GA-SVM wrapper approach. They found that the approach clearly improved the model performance with 3.69% of FRR and 0% of FAR.

A. Dahalan et al. attempted to build a pressure-based typing biometrics system (Dahalan et al., 2004) and employed neuro-fuzzy system as the classifier. A special keyboard with pressure sensors was built to capture users' keystroke pressure patterns. They also acquired keystroke duration instead of capturing pressure patterns. In their experiments, average pressure of each keystroke and keystroke durations were used as inputs to the neuro-fuzzy system. The authors reported that pressure patterns can be used to verify identity. However, due to limited participants in the experiments and there was no results of using pressure patterns alone in the classification stage, the effectiveness of using pressure patterns in identity verification is difficult to be evaluated. In addition, average pressure of each keystroke is difficult to be defined since a fast typist may press several keys at the same time.

Figures 2.2 – 2.4 show the comparison among different studies in this domain.

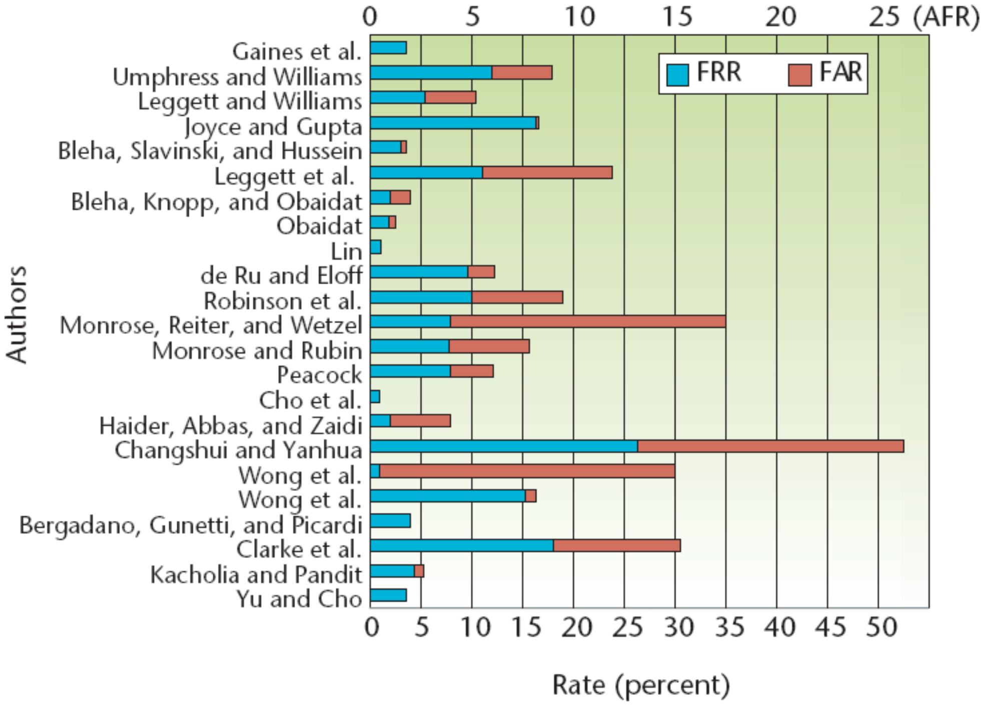


Figure 2.2: False rejection rate (FRR), false acceptance rate (FAR), and average false rate (AFR) for several approaches. AFR is the average of FRR and FAR, and is shown by the top *y*-axis. Systems with lower FRR, FAR, and AFR are more accurate in discriminating between users, and are thus capable of being more secured (adopted from Peacock et al., 2004).

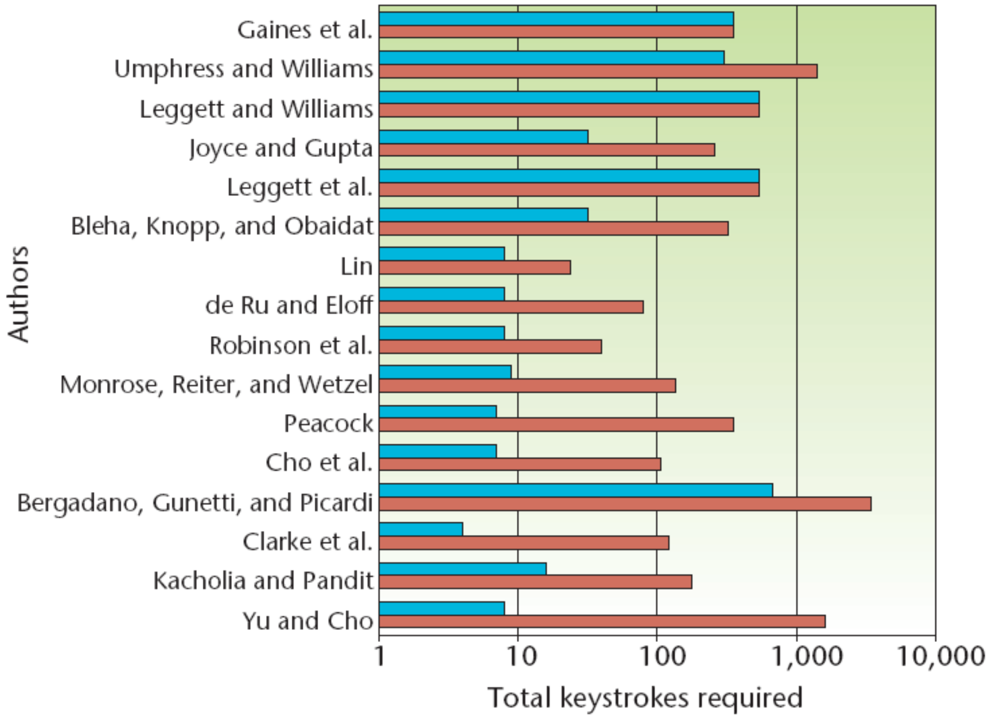


Figure 2.3: Comparing different keystroke approaches. The cost to a user (in keystrokes) to enroll and to authenticate for a given approach shows that systems that can enroll and authenticate with fewer keystrokes are easier to use. Blue represents the cost to a user to authenticate; red is the cost to a user to enroll (adopted from Peacock et al., 2004).

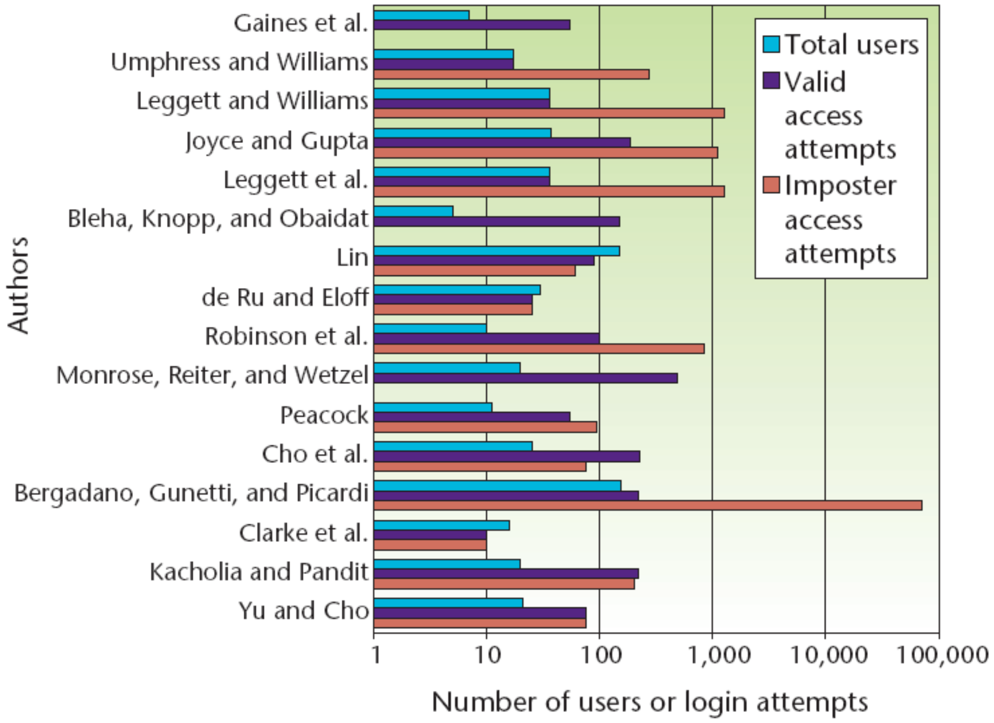


Figure 2.4: Confidence in test results. The involvement of more users and more valid/imposter logins lends credence to reported results, but even the largest studies in the keystroke dynamics field to date fall short of proving competence on large systems (adopted from Peacock et al., 2004).

2.9 Review of Commercial Products

2.9.1 BioPassword™

BioPassword with model number BP-127 is manufactured by BioNet Systems (BioPassword, 2005). The company is better known for its internet filtering and monitoring system, NetNanny™. The BioPassword technology was originally developed by SRI International between 1979 and 1985. It was qualified as a valid biometric solution by IBG in 2000.

BioPassword is specially designed to protect Windows NT and Window 2000 server platforms from intruders. Before installation, the user must have administrative rights to the local computer. The username and password of his/her account must contain at least 8 characters. During this process, the user will be asked to answer two challenge and response questions. This is a backdoor method to grant access to a local administrator in case the user is unable to type with a natural rhythm as recorded (e.g. because of a hand injury). The administrator can adjust the threshold for each user with the security setting. The security setting ranges from 1 to 10 (default is 3). The higher the number, the more accurate a user's typing rhythm must be.

In general, BioPassword works as follows:

a) Individual users enroll by typing 15 training (by default) samples of their password.
b) The keystroke template is stored in the server.
c) In order to grant access to the server, the user must key in the right user name and password, furthermore, the keystroke rhythm must match the template stored.

BioPassword is reviewed in Altman (2002) from a functional point of view. The reviewers tested whether they could access each others accounts when they knew the username and the password. The imposter had a chance to observe valid user so they could try to imitate each other typing styles. The reviewers reported that they were locked out of one other's accounts with the default security setting. However, they