การพัฒนาบุคคลิกภาพส่วนบุคคลในระบบรักษาความปลอดภัยคอมพิวเตอร์

นายเปรมชัย ภูริวัฒนา

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาปริญญาวิทยาศาสตรมหาบัณฑิต
สาขาวิชาวิทยาการคอมพิวเตอร์และเทคโนโลยีสารสนเทศ ภาควิชาคณิตศาสตร์
คณะวิทยาศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2553

IMPLEMENTATION OF PERSONAL CHARACTERISTICS IN COMPUTER SECURITY

Mr. Premchai Phoorivatana

A Thesis Submitted in Partial Fulfillment of the Requirements
for the Degree of Master of Science Program in Computer Science and Information
Technology
Department of Mathematics
Faculty of Science
Chulalongkorn University
Academic Year 2010

Thesis Title	IMPLEMENTATION OF PERSONAL CHARACTERISTICS IN COMPUTER SECURITY
By	Mr. Premchai Phoorivatana
Field of Study	Computer Science and Information
Thesis Advisor	Assistant Professor Pattarasinee Bhattarakosol, Ph.D.

Accepted by the Faculty of Science, Chulalongkorn University in Partial Fulfillment of the Requirements for the Master's Degree

S. Hannongbua .... Dean of the Faculty of Science

(Professor Supot Hannongbua, Dr.rer.nat.)

THESIS COMMITTEE

Rajalida Lipikorn .... Chairman

(Assistant Professor Rajalida Lipikorn, Ph.D.)

P. Bhattarakosol .... Thesis Advisor

(Assistant Professor Pattarasinee Bhattarakosol, Ph.D.)

Panjai Tantasanawong .... External Examiner

(Assistant Professor Panjai Tantasanawong, Ph.D.)

เปรมชัย ภูริวัฒนา : การพัฒนาบุคคลิกภาพส่วนบุคคลในระบบรักษาความปลอดภัยคอมพิวเตอร์. (IMPLEMENTATION OF PERSONAL CHARACACTERISTICS IN COMPUTER SECURITY) อ. ที่ปรึกษาวิทยานิพนธ์: ผศ.ดร.ภัทรสินี ภัทรโกศล, 57 หน้า.

ปัญหาด้านความปลอดภัยจากการจารกรรมข้อมูลดิจิตอลเป็นปัญหาที่มีการดำเนินการแก้ไขมาโดยตลอด เทคนิคจำนวนมากได้ถูกพัฒนาขึ้นมาเพื่อแก้ปัญหาแต่ด้วยข้อจำกัดในการใช้งานตลอดจนการบำรุงรักษาทำให้ไม่สามารถนำไปใช้ได้ในทุกกรณี ไบโอเมทริกซ์เป็นเทคโนโลยีหนึ่งที่ได้รับความนิยมในการใช้เกี่ยวกับกลไกการรักษาความปลอดภัยส่วนบุคคล แต่คุณลักษณะบางอย่างของไบโอเมทริกซ์ก็ยังมีจุดบกพร่องเป็นผลทำให้เกิดความเสี่ยงในระบบ วิทยานิพนธ์นี้ได้เสนอ การใช้เวลาเพื่อโต้ตอบกับระบบ ซึ่งเป็นคุณลักษณะหนึ่งของ ไบโอเมทริกซ์ร่วมกับรหัสผ่าน เพื่อใช้ในการพิสูจน์ตัวตนโดยเวลาที่ใช้โต้ตอบจะตรวจสอบเมื่อทำการปลดล้อคระบบ จากการทดลองและการวิเคราะห์สรุปได้ว่า คุณลักษณะของไบโอเมทริกซ์นี้สามารถนำไปใช้จำแนกประเภทของผู้มีสิทธิ์ใช้งานในระบบกับผู้บุกรุกได้

ภาควิชา คณิตศาสตร์ ลายมือชื่อนิสิต เปรมชัย ภูริวัฒนา
สาขาวิชาวิทยาการคอมพิวเตอร์และสารสนเทศ ลายมือชื่อ อ.ที่ปรึกษาวิทยานิพนธ์หลัก P.Bhattarakosol
ปีการศึกษา 2553

5073610223 : MAJOR COMPUTER SCIENCE AND INFORMATION

KEYWORDS : BEHAVIORAL BIOMETRICS / TIME INTERVAL / COMBINED BIOMETRICS

PREMCHAI PHOORIVATANA : IMPLEMENTATION OF PERSONAL CHARACACTERISTICS IN COMPUTER SECURITY. ADVISOR : ASST.PROF. PATTARASINEE BHATTARAKOSOL, 57 pp.

Security problems of the stolen data are an unsolvable for years. Numerous techniques have been proposed but the limitations to implement and maintain are the big issues that cause problem to be unsolved until now. Since biometric is one of the most popular technology that is applied to the protection mechanisms, there are some uncompleted features that cause the system unsecured. Thus, this paper proposed the use of a biometric value, measured when the owner of the device is unlocking the system; this biometric is the time interval of the password entering. The experiment is drawn and the analysis process determines that this biometric could distinct the authorized user from unauthorized one.

Department : Mathematics .... Student's Signature เปรมชัย ภูริวัฒนา

Field of Study : Computer Science and Information Advisor's Signature P. Bhattarakosol

Academic Year : 2010 ....

ACKNOWLEDGEMENTS

I owe many thanks to many people who helped and supported me during the writing of this thesis.

My deepest thanks to my advisor, Assistant Professor Pattarasini Bhattarakosol the guide of the thesis who guiding and correcting various documents with attention and care.

I also express my thanks to the thesis committee, Assistant Professor Rajalida Lipikorn, Ph.D. and Assistant Professor Panjai Tantasanawong, Ph.D. for their constructive criticisms and invaluable advises.

Finally, my graduation would not be achieved without best wish from my parents, Mr. Suchai and Mrs. Suchitra Phoorivatana, who help me for everything and always gives me greatest love, willpower and financial support until this study completion and, the last gratefully special thanks to my relation and my friends for their help and encouragement.

CONTENTS

Page

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

This chapter states the interested problem in Section 1.1, and then the objective is described in Section 1.2. In Section 1.3, the scope and constraint of this thesis will be discussed, followed by definitions of technical terms in Section 1.4. Additionally, the benefit of thesis is elaborated in Section 1.5, and the structure of this thesis is detailed in Section 1.6.

1.1 Problem Statement

From the report of SOPHOS, a well-known vendor and developer of security software and hardware, in the year 2008, in every 5 seconds, the average number of infected web pages is more than 15,000 sites which is three times more than the year 2007 [1]. This number indicates that the security of information is very loose although the Internet is counted as the main information resources of human and various researches have proposed the security techniques to protect such information.

Currently, there are various types of devices that are developed as a gateway to the Internet access; one of those is the mobile device. Therefore, the intrusion from the Internet world will affect to the mobile device as an unavoidable issue. Thus, the mobile protection mechanism must be implemented in order to protect data in the mobile storage.

One weak point of the mobile phone is that the data can be accessed whenever a mobile holder passes the authentication process, if existed. The truth is most of the mobile holders do not have passwords to lock their mobile because of difficulty to remember. Therefore, when a mobile was stolen, all data in that mobile will be eliminated or accessed by unwanted persons. Thus, every mobile phone should be implemented with an automatic authentication technique that will not cause superfluous process to the owners.

The objective for the authentication technique is to identify something or someone. Nevertheless, traditional authentication techniques, like a password or a hardware token, have vulnerabilities. For example, the old fashion password is easily being broken, many techniques like dictionary attack or man-in-the-middle attack could be used to steal it without trouble. Therefore, the biometrics approach has been proposed to use in the authentication process. Biometrics authentication is highly reliable, because physical human characteristics are much more difficult to forge then security code, passwords, hardware keys sensors, fast processing equipment and substantial memory capacity, so the system are costly. Biometrics-based authentication applications include workstation and network access, single sign on, application logon, data protection, and remote access to resources, transaction security and web security. The promises of e-commerce and e-government can be achieved though the utilization of strong personal authentication procedures. The secure electronic banking, investing and other financial transactions, retail sales, law enforcement, and health and social services are already benefiting from these technologies. Biometrics technology is expected to play a key role in the personal authentication process for large-scale enterprise network authentication environments, point-of-sale and for the protection of all types of digital content, such as in digital right management and health care applications. Utilized alone or integrated with other technologies, such as smart cards, encryption keys and digital signatures, biometrics is anticipated to pervade nearly all aspects of the economy and our daily lives. For example, biometrics is implemented in various schools, and a school library. Examples of other current applications include verification of annual pass holders in an amusement park, speaker verification for television home shopping, Internet banking, and user's authentication in varieties of social services [50].

During the past decade, the demand of using reliable biometric systems has highly increased. However, despite of the efforts conducted in the biometrics field, there is still a possibility of successful fraud attempts. Institutes and large organizations in attempting to improve the systems false acceptance rate (FAR), depend on the concept of using more than one biometric feature to positively identify a person. This technique is referred to as the combined biometrics. With a lot of biometrics study and research, more than 90% of accuracy is claimed for the uniqueness [2].

1.2 Objective

This thesis proposes a new measurement biometric using only the response time to enter password of each person and uses this time to indicate the owner of the mobile phone in the authentication process. The objective of this thesis is to introduce a combined biometric technique with a password. In addition, it will further evaluate performance of this technique and comparing to another authentication technique.

1.3 Scope of thesis and Constraint

Since the biometrics authentication technique is widely used and trends to be applied in many fields and institutions, this thesis emphasized on improvement of biometrics with the low cost implementation and ease of use. This biometrics technique not only used for small mobile devices, such as mobile phone, PDA or handheld devices, but also adapted for many big size gadget and security.

There are various kinds of methods for measuring a performance metrics of biometrics, such as False Accept Rate (FAR), False Reject Rate (FRR), Receiver Operating Characteristics (ROC), Equal Error Rate (EER), Failure to Enroll Rate (FER or FTE), Failure to Capture Rate (FTC) and template capacity. In this thesis will use both FAR and FRR to provide and compare the introduced method and the simple password authentication technique.

1.4 Definition

Claim of Identity: A statement that a person is or is not the source of a reference in a database. Claims can be positive, in the database, or negative, outside the database or specific (specific instance in database).

Enrollment: The process of gathering a biometric sample from an end user, converting it into a biometric reference, and storing it in the biometric system's database for later comparison.

Interval time: The amount of times which a person interacts with the program or systems, starting from the first key that pressed until pushing the finishing key to stop.

Owner Group: A group of people who exercises direct control over the behavioral biometrics data which is the response time.

Emulator Group: A group of people who imposes on other behavioral biometrics data without permissions or an unauthorized group of users.

Modality: A type or class of a biometric system.

Multimodal Biometric System: A biometric system in which two or more of the modality components (biometric characteristic, sensor type or feature extraction algorithm) occurs in multiple.

1.5 Benefit

This thesis proposed an alternative biometric authentication which combines the existed techniques to enhanced the performance and solve the stated problems. Using the introduced method can obtain the low cost of implementation, commercial used and compatible with any type of devices.

Moreover, the performance of the proposed system is superior to the legacy system due to the comparison.

1.6 Structure of the Thesis

The rest of thesis is organized as follows. In Chapter 2, it provides the fundamental knowledge and the literature review for this thesis. Then, Chapter 3 describes the proposed method followed by showing the evaluation results and the comparison in Chapter 4. Finally, discussion and conclusions are drawn in Chapter 5.

CHAPTER 2

FUNDAMENTAL KNOWLEDGE AND LITERATURE REVIEW

In this chapter, it will provide fundamental knowledge and literature review for this thesis. Thus, some related works are reviewed in Section 2.1. Followed by, history of biometrics, biometrics, performance and performance mechanisms are described in Section 2.2 to Section 2.4 respectively.

2.1 Literature Review

The security issues for mobile devices are dramatically increased. Various authentication techniques were developed to solve the problem. Several systems require authenticating a person before giving access to certain resources. Biometrics has been well-known to recognize persons based on their physical and behavioral characteristics. Examples of different Biometric systems include fingerprint recognition, face recognition, iris recognition, retina recognition, hand geometry, voice recognition, signature recognition, among others. Face recognition, in particular, has received a considerable attention in recent years both from the industry and the research community. The real-life problems to be tackled here concern identifying individuals in everyday settings, such as offices or living rooms. The dynamic, noisy data involved in this type of task is very different to that used in typical computer vision research, where specific constraints are used to limit variations. Historically, such limitations have been essential in order to limit the computational resources required to process, store and analyze visual data. However, enormous improvements in terms of speed of processing and size of storage media, accompanied by progress in statistical techniques, made it possible to build such systems [3].

Shoichiro Seno and et al. [4] proposed a system, which would be useful to build a network authentication system with multi-biometrics, with sufficiently small authentication processing time and wide applicability to network applications. Some researchers considered common issues with extraction of identification data from various types of biometrics, and protection of such data against conceivable attacks [5][6][7]. They aimed at facilitating reliable biometrics authentication by improving authentication preciseness and providing countermeasures against attacks to an authentication system. It is possible to strictly authenticate a person by combining multiple biometrics authentication methods while accepting some degree of authentication failures with a single biometrics. Combination of biometrics authentication [8] may be achieved by logical or statistical methods. Logical methods perform each of biometrics authentication individually and compute AND or OR of their results to reach the final answer. Statistical methods rely on a statistical function derived from matching probabilities of individual authentication methods.

In the research articles by [9], it had mentioned that the biometrics is not secret; thus, if the invader has knowledge of information in the legitimate biometric identifier, they could fraudulently inject into the biometric system to gain access. Therefore, even biometrics themselves are quite distinctive data, but lacking in the data security. In additions, they also mention that a biometric system based solely on a single biometric feature may not be able to meet the practical performance requirement in all aspects. By integrating two or more biometric features, overall verification performance may be improved.

As a consequence, an identification system combined with fingerprint and cryptography is addressed according to the vulnerabilities of using the individual biometric information. This technique was proposed by [10], the result of combining the fingerprint biometric technique with the encrypt password method can enhances the security of fingerprint reader from the fake fingerprint attacker which is the serious concern.

Additionally, [11] investigated the robustness of the gait authentication system against attackers rather than evaluating the performance of individual attackers. Furthermore, they claimed that the biometrics information is easily to attain. Thus, various types of imposters aim for this weakness point.

Another concerning in biometrics authentication technique is the measurement procedures. In the researches of brain signatures [12] [13] show that the EGG signals from the human brains can be used as alternative biometrics. Also, the authors indicated that their method has 97% accuracy. On the other hand, even their techniques provide high rate of reliability, the measurement devices and process are too complicated for handling digitizer tablets which confirmed by [14] whose proposed the online-signature verification system using probabilistic feature modeling. They stated that their method analyze human signature for authentication is appropriated for many small size devices, such as palm and mobile phone.

As the fact that biometrics is not secret and could exposed to strangers, [15] proposes a method combining standard cryptographic techniques and biometrics to provide an effective and easily deployable identity verification system. The system is privacy-aware since the information contained in the identifier is not sufficient to recover the biometric traits of users and further biometric inputs are required. Any abuses of biometric information are then prevented.

The research of [16] states the problem of a biometrics authentication process during login process verification that it is not enough. This is because a logged station or mobile is vulnerable for imposters when the user leaves her machine. Thus, verifying users continuously based on their activities is required.

The degree of fusions in a typical multimodal biometrics system can be divided into four levels: data level, feature level, match score level, and decision level. To date, many researchers have focused on matching score level fusion as it is relatively easy to access and combining the scores produced by different modalities. [17] Proposes a multimodal biometrics system that combines fingerprint and palm print features to overcome several limitations of a single modal biometrics.

Since the biometrics is widespread usage and extreme accuracy for authentication [18] emphasizes that most biometrics solutions lack of understanding of fundamental problems which are effectively and accuracy of biometrics patterns. Ensuring of measurements are not deceitful and the appropriate biometrics for each application.

Even though biometrics is dealing with the personal rights and privacy, but it also poses a substantial risk to privacy rights. [19] States the problems that once a biometric identifier is captured from an individual in the primary market, and even if it is captured only once, the biometric identifier could easily be replicated, copied, and otherwise shared among countless public and private sector databases. This sharing in a secondary market could conceivably take place without the individual's knowledge or consent. Indeed, biometric identifiers could be bought and sold in a secondary market in much the way that names and addresses on mailing lists presently are bought and sold by data merchants. Therefore, the present regulatory baseline should respect to the regulation biometrics information in order to prevent the privacy abuse situations.

[20] Introduced the idea of shadow biometrics outlined the generic processing steps for analysis, with recognition experiments on 5 subjects. The video/image processing greatly benefits from advances in two main areas: shadow detection/segmentation techniques that allow extraction of the shadow silhouette, and gait analysis techniques, which extract the information from silhouette movements. As the results, they claim that a correct classification rate (CCR) of 95.0% from 49 coefficients was obtained. A reduction of resolution to 50 % reduced the CCR from 95.0 % to 75.0 %.

Likewise, the security issues of biometrics have been concerning over years. [21] Shows the major threat of biometrics identification system which is cross-system replay attacks. This security breach occurs when a person has registered a certain biometric in many of the security authentication systems, and if one day, when an emulator successfully penetrates one of authentication systems with relatively weak security, then, the security of other authentication systems would also be uncovered. The user security system will suffer devastating blow: personal privacy, wealth, and even personal safety will be lost. Moreover, after individuals' biometrics information has been leaked, one will not be able to update his/her registration feature information, because of its uniqueness. He or she will become an individual which cannot be protected by biometric security system forever. Therefore, the idea that combines biometrics information and other authentication method will be an alternative approach to prevent the cross-system replay attack scenario, besides combining to authentication method build up stronger identification systems. In the year of 2009, [22] presents the overview of using biometrics combined with cryptography. Several algorithms are demonstrated which allow users to generate cryptographic keys and random numbers based on their unique biometric information.

Due to the fact that the biometrics authentication is not free from an error in the process of extraction of human characteristics and comparison of biometrics data, therefore single biometrics authentication technique is not sufficient to meet the satisfaction of a required reliability level. To improve the performance, the multi-biometrics is applied in order to achieve the required level, in the year 2003 [23] proposed multi-biometrics authentication over the network. According to this research, the system was built based on two network authentication system models: co-locate model and separated model. The researchers also claimed that the time required for transport of biometrics data over a network will remains valid with others type of biometrics. This is because the length of the biometrics data is usually less than 1.5 kilobytes after extraction regardless of type of biometrics. Therefore, the propose system would be useful to build a network authentication system with multi-biometrics, with sufficiently small authentication processing time and wild applicability to network applications.

Another concern of using biometrics authentication is that biometrics characteristics are immutable and hence their compromise is permanent. Whenever the biometrics database is distorted, the security bleach has been issued. The fake user could apply the distorted biometrics to track back to the original biometrics traits. To avoid this difficulty, [24] introduced the cancelable biometrics which could renewable and prevent the counterfeit to track back to the genuine. Their research proposes the techniques identification scheme based on cancelable biometrics which still keep major advantages of biometric systems: 1) the ability to identify people, 2) the capacity to work without imposing to users the need of an extra token. Moreover, exploit time-dependent templates to verify the biometrics data is used in order to have untraceable ability in the system. As a result, the ROC (Receiver Operating Characteristic) curves which represent the genuine accept rate against the FRR (False Reject Rate) for different matching threshold. The result shows that the new curve (matcher) is lower than the original.

Another idea of using cancelable biometrics to replace the biometrics trait whenever it is stolen and used to trace back for biometrics information is introduced by [25]. They combined user's tokenized random numbers with biometrics feature to generate a unique compact binary code, coined as a biophasor is highlighted; the biophasor is constructed based on the iterated mixing between the tokenized pseudo-random number (PRN) and the biometric feature. The objectives of their method are two folds: to realize cancellable biometrics in which biometric template can be reissued by replacing the token if it was compromised. Secondly, the transformation is non-invertible and thus, knowledge of the biophasor does not leak information about the actual biometrics data. The biophasor reduces intra-class and enlarge inter-class variation of biometrics features, which leads to zero equal error rate (EER) when genuine token is used. On the other hand, the biophasor is still able attain the good result when the token is stolen by an imposter and tries to verify as genuine user compare to sole biometric and formulation in the biohashing.

In the research article of emerging methods of biometrics human identifications [26], the researcher presents emerging methods which originate from real-life criminal police and forensic science practice. They also focus on perspective biometrics methods based on image analysis. Three types of biometrics: ear, lips and palm images are discussed in the research. Firstly, the ear is one of the most stable human anatomical features, as proven by [27] [28]. It does not change considerably during human life. Furthermore, the ear is one of our sensors; therefore it is usually visible, not hidden underneath anything, to enable good hearing. They used geometrical parameters of ear contours extracted from ear images. Such approach gives information about local parts of the image, which is more suitable for ear biometrics than global approach to image feature extraction. Contours corresponding to earlobes are much diversified and contain enormous amount of information allowing ear identification. Secondly, lip shape recognition has not been extensively researched so far, but some very promising results were achieved by HMM and PCA [29]. Normally, lips are detected in face images, segmented and binarized. But, the researcher calculates color statistics and moments as well as a set of standard geometrical parameters and the moments of Hu and Zernike. Finally, the palmprint feature extraction methods are mainly based on geometrical parameters, lines topology, texture features, Wavelets and Fourier transforms. In the article, they used both scanned hands dataset and hands photos dataset. Also, they calculate various palmprint texture features and Zernike Moments, in order to merge them with hand geometry features in a multimodal hand-palm biometrics system. So far they have achieved 86% Rank-1 Recognition Rate for palmprint images and 91, 33% for multimodal handpalm features.

In behavioral biometrics, the alternative technique that used to extract the biometrics data indirectly is based on HCI (Human Computer Interaction) which explores how human beings interact with computational devices. This type of interaction, relatively unique to every computer user, can be analyzed to develop a non-intrusive authentication mechanism. HCI-based biometrics are usually only briefly mentioned in surveys of biometric technology and only those which are in large part based on muscle control such as keystrokes, or mouse dynamics are well known to the biometrics community [30]. HCI-based biometrics can be divided into two different categories known as direct and indirect HCI-based biometrics. First group is made up of either those biometrics which are based on direct human interaction with input devices such as keyboard, computer mouse, and haptics which rely on supposedly innate, unique and stable muscle actions and those biometrics which are based on advanced human behavior such as strategy, knowledge or skill exhibited by users during interaction with different software. The second group consists of the indirect HCI-based biometrics which is events that can be obtained by monitoring user's HCI behavior indirectly via observable low level actions of computer software. [31] concentrates on review and analysis of indirect HCI-based biometrics frequently used in emulator detection system, those include audit logs, call-stack data, GUI interaction, network traffic, registry access, storage activity, and system calls. These events are produced unintentionally by the user during interaction with different software applications during pursuit of some high level goals. The experiments were conducted by given five different attacks. Normal behavior records were considered as an attack, thus total of six attacks were used in this experiment. In the results, the accuracy of classifying attacks is 93.2% using RBF Neural Network and 92.2% using MLP Neural Network. In most cases the Networks managed to identify an attack correctly. The false positive rate is very low in both cases, false negative rate is not high either, and the misidentified attacks rate is 5%-6%. Overall, it is possible to conclude that both neural networks were capable of identifying the attacks.

In the article of keypress biometrics for user validation in mobile consumer devices [32], the author mentioned the use of keystroke dynamics which used key rhythm, pressed and released, in the authentication process. The examination was conducted and evaluated. The evaluation of the research algorithm involved iterating with three different enrolled users. Each user undertook authentication 100 times, and more than 20 imposters attempted authentication, also 100 times. As the result, the performance shows that more than 90% accuracy. In additions, this primarily study also show an efficient low overhead statistical method to use in biometrics.

In the mouse biometrics, [33] defines four different mouse actions as follows: mouse movement, drag and drop, point and click and silence. Several different features were defined, such as the interpolation between the movement speed and the traveled distance, which estimates the average speed a user will travel for a certain distance. In addition, several histograms were used to capture different working statistics of the user such as the average traveling speed in eight direction zones or the relative occurrence of each one action. This study showed relatively good results of less than 3.29% FRR and less than 0.5% FAR, when the number of actions was greater than 2,000 and the verification session last for 13.55 minutes on average. Nevertheless it showed relatively poor results of less than 24% FRR and 4.6% FAR when the session was of a shorter duration, above 4 minutes. The period for identifying the user in this work is far beyond the reasonable time required for an attacker to take full control of a computer system; histograms may reflect different working characteristics of the user but in order for these to be accurate a relatively long time is required, during which an imposter can perform already his malicious act.

[34] Attempted to uniquely partition users according to their mouse movement behavior. They calculated the mean, standard deviation and the third moment of the distance, angle and speed between different two adjacent points, when a defined window of data points is considered. A decision tree classifier was trained to differentiate among users activity. [35] [36] consider features such as the angle, curvature, horizontal, vertical and combined velocity; acceleration and jerk obtained from a vector of data points that were intercepted between two mouse clicks in a web memory game. The authors evaluated the use of two statistical models with the use of the extracted features to verify the identity of an individual.

2.2 History of Biometrics

The word biometrics is originated from the Greek words, bio means life and metrics refers to measure. Automated biometric systems have only become available over the last few decades, due to major advances in the field of computer processing. Many of these new automated techniques, however, are based on ideas that were originally conceived hundreds, even thousands of years ago. One of the oldest and most basic examples of a characteristic that is used for recognition by humans is the face. Since the foundation of civilization, humans have used faces to identify known and unknown individuals. This simple process became more challenging as populations increased and as more convenient methods of travel introduced many new individuals into once small communities. The concept of recognize the person is also seen in behavioral-predominant biometrics such as voice and gait recognition. Individuals use these characteristics instinctively to recognize known individuals. Other characteristics have also been used throughout the history of civilization as a more formal means of recognition. Some examples are:

In a cave estimated to be at least 31,000 years old, the walls are adorned with paintings believed to be created by prehistoric men who lived there. Surrounding these paintings are numerous handprints that are felt to "have…acted as an un-forgeable signature" of its originator [37].

There is also evidence that fingerprints were used as a person's mark as early as 500 B.C. "Babylonian business transactions are recorded in clay tablets that include fingerprints" [38].

Joao de Barros, a Spanish explorer and writer, wrote that early Chinese merchants used fingerprints to settle business transactions. Chinese parents also used fingerprints and footprints to differentiate children from one another [39].

In early Egyptian history, traders were identified by their physical descriptors to differentiate between trusted traders of known reputation and previous successful transactions, and those new to the market [40].

In the mid of 18th century, with the rapid growth of cities due to the industrial revolution and more productive farming, there was a officially standard need to identify people. Merchants and authorities were faced with increasingly larger and more mobile populations and could no longer rely solely on their own experiences and local knowledge. Influenced by the writings of Jeremy Betham and other Utilitarian thinkers [51], the courts of this period began to codify concepts of justice that endure with us to this day. Most remarkably, justice systems sought to treat first time offenders more leniently and repeat offenders more harshly. The formal system that recorded offenses along with measured identity templates of the offender is needed. The first approach was the Bertillon system of measuring various body dimensions, which originated in France. These measurements were written on cards that could be sorted by height, arm length or any other parameter. This field was called anthropometrics. The other approach was the formal use of fingerprints by police departments. This process emerged in South America, Asia, and Europe. By the late 1800s a method was developed to index fingerprints that provided the ability to retrieve records as Bertillon's method did but that was based on a more individualized metric, fingerprint patterns and ridges. The first such robust system for indexing fingerprints was developed in India by Azizul Haque for Edward Henry, Inspector General of Police, and Bengal, India. This system, called the Henry System, and variations on it are still in use for classifying fingerprints [41]. True biometric systems began to emerge in the late of twentieth century, coinciding with the emergence of computer systems. The growing field experienced an enormous of activity in the 1990s and began to surface in everyday applications around year 2000.

2.3 Biometrics

Biometrics is a common term used to describe a characteristic or a process.

As a characteristic:

- A measurable biological, anatomical and physiological, and behavioral characteristic that can be used for automated recognition.

As a process:

- Automated methods of recognizing an individual based on measurable biological (anatomical and physiological) and behavioral characteristics [51].

Biometric systems have been researched and tested for a few decades, but have only recently entered into the public consciousness because of high profile applications, usage in entertainment media (though often not realistically) and increased usage by the public in day-to-day activities. Example deployments within the United States Government include the FBI's Integrated Automated Fingerprint Identification System (IAFIS), the US-VISIT program, the Transportation Workers Identification Credentials (TWIC) program, and the Registered Traveler (RT) program. Many companies are also implementing biometric technologies to secure areas, maintain time records, and enhance user convenience. For example, for many years Disney World has employed biometric devices for season ticket holders to expedite and simplify the process of entering its parks, while ensuring that the ticket is used only by the individual to whom it was issued.

A typical biometric system is comprised of five integrated components: a sensor is used to collect the data and convert the information to a digital format. Signal processing algorithms perform quality control activities and develop the biometric template. A data storage component keeps information to which new biometric templates will be compared. A matching algorithm compares the new biometric template to one or more templates kept in the data storage. Finally, a decision process, either automated or human-assisted, uses the results from the matching component to make a system-level decision.

Commonly implementing or studying biometric modalities include fingerprint, face, iris, voice, signature and hand geometry. Many other modalities are in various stages of development and assessment. There is not one biometric modality that is best for all implementations. Many factors must be taken into account when implementing a biometric device; these include expected number of users, user circumstances and existing data, location, security risks, and task (identification or verification). It is also important to note that biometric modalities are in varying stages of maturity. Table 1 shows the comparison among biometric characteristics under various types of considered factors [42].

Table 1. The comparison among different types of biometric characteristics

Biometrics characteristics	Universality	Unicity	Persistence	Collectability	Performance	Aceptabilty	Circumvention
Face	high	Low	medium	High	Low	high	low
Fingerprint	medium	High	high		High		high
Hand Geometry	medium	Medium	medium	High	Medium	medium	medium
Iris	high	High	high	Medium	High	low	high
Retinal Scan	high	High	medium	Low	High	low	high
Signature	Low	Low	low	High	Low	high	low
Voice	medium	Low	low	Medium	Low	high	low
Thermogram	high	High	low	High	Medium	high	high

Research and development in the past decades have suggested a wide variety of different modalities to be used for biometric user authentication. Today, a large number of products are available on the market, based on different recognition techniques. Looking at the nature of the underlying modalities, two basic categories can be identified: behavioral and physiological features [52].

- Physiological Biometrics

Physiological biometrics measures the distinct traits that people have, usually, but not always or entirely, dictated by their genetics. Examples of physiological biometrics include advanced techniques like DNA, retinal scans, and, facial geometry, but also well-known methods like fingerprinting and photography. In the early days, chemicals were used to record the photons of light that bounced off a human face, reproducing eye and hair color, facial shape, unique features, and so on. Modern photography records reflected photons digitally, as pixels on a fine grid. Either way, the relatively well understood technology of photography is a physiological biometric that need not be as daunting as those big words suggest.

- Behavioral Biometrics

The second category of biometrics is behavioral. Behavioral biometrics measures the distinct actions that human's action, which are generally difficult to be copied from one person to another. Examples of behavioral biometrics include voice printing and gait analysis, which use computers to analyze the sound created by the human voice box or the movement of a person walking. Another common behavioral biometric is the handwritten signature, daily used by people to formally or informally indicate their authorship of a document or assent to an agreement. The name behavioral biometric may be intimidating, but the signature is entirely familiar to the average consumer.

2.3.1 Physiological Vs Behavioral Biometrics

Acquisition of behavioral biometric information need users to be active, to capture activities in front of the detector, whereas data acquisition in biometric systems of the physiological biometrics, a human body part is taken from subjects, which does not necessarily require an action by the user. From the user's point-of-view, it can be stated that in the behavioral biometrics some co-operation is required, whereas biometrics of the physiological biometrics can be acquired even without explicit consent of subjects. With respect to potential applications, the differentiation between behavioral and physiological biometrics can be of great importance for many reasons. Among this variety, three aspects shall be mentioned to demonstrate the differences in suitability of single biometric modalities.

- *Declaration of Intention*

In scenarios, where user authentication is linked to an explicit consent to the authentication process, behavioral schemes appear more adequate than physiological. For example signature verification constitutes a socially well-accepted and widely used process and has been in application for many centuries. Besides the possibility for a user authentication based on the visible and physical traces of the writing process, signatures also serve for at least two additional goals: declaration of intention and warning functions. The first aspect of authentication can be confirmed due to the fact that the result of the signature process represents individual properties of the writing style, intrinsic to the writer. For the second aspect, declaration of intention, it can be assumed that if the signature is linked to a particular document, the signer has produced the signature in an agreeable attitude. The third function, warning, assumes that subjects are aware that signing documents can have severe consequences and thus should be well considered. Apparently, behavioral biometrics, particularly signature verification as sub-discipline of handwriting biometrics, is more adequate to reproduce these functions than physiological modalities. This particularly is the case in environments, which are not continuously observed by trusted persons, where no witnesses of voluntaries exist, however that behavioral methods have the tendency towards higher error rates as compared to physiological biometrics.

- *Identification*

Biometric authentication can be achieved in two different modes: verification and identification. Applications, where the automated identification of persons is intended have quite different demands. While behavioral features can easily be repudiated by disguise of a particular writing style, this is not the case for physiological features. For example in crime prevention, biometric recognition and automated search of suspects can support observation of public areas. Obviously in this scenario, disguise of biometric features is undesired and consequently, physiological traits such as face recognition appear more practical.

- *Ascertainability*

Another important criterion for the use of particular biometric modalities is ascertainability, the question, if the biometric information can be acquired under different operational, environmental and geographical conditions in sufficient quality and quantities. For example, it appears difficult to implement speaker recognition in scenarios such as factory halls, where noisy machinery is in use. On the other hand, signature verification used for access control to buildings appears infeasible, when biometrics is to be verified frequently and at numerous locations to and inside a building. Further, the later modalities are not appropriate, if it can be foreseen that subjects will not be able to use their hands while transiting access control gates.

Another distinction between behavioral and physiological biometrics is the possibility of including semantic information in behavior. A speaker, for example, can articulate a specific message in her or his biometric trait as well as a writer in a handwriting trace. This characteristic implies some advantages of behavioral biometrics, when combining them with knowledge and possession-based authentication schemes.

2.4 Performance

To determine the best biometric system for a specific operational environment and how to set up that system for optimal performance requires an understanding of the evaluation methodologies and statistics used in the biometrics community. The following section provides a baseline testing and statistics review, thus enabling appropriate analysis of available thesis.

2.4.1 Performance Mechanisms

Performance evaluations of biometric identification technology are divided into three overlapping categories with increasing complexity in uncontrolled variables: technology, scenario, and operational [43]. A thorough evaluation of a system for a specific purpose starts with a Technology Evaluation, followed by a Scenario Evaluation, and finally an Operational Evaluation. The primary goal of Technology Evaluations is to measure the performance of biometric systems, typically only the recognition algorithm component. They are repeatable and usually short in duration. Technology Evaluations are usually performed using standard datasets collected previous to testing. In general, results from a Technology Evaluation show specific areas that require future research and development (R&D) and provide performance data that is useful when selecting algorithms for scenario evaluations. An example of a Technology Evaluation is the Face Recognition Vendor Test [44]. The primary aim of scenario evaluations is to measure performance of a biometric system operating in a particular application. For example, testing biometrics for access control purposes at a mock doorway in a laboratory, each tested system normally would have its own acquisition sensor and would receive and produce slightly different data. For this reasons, scenario evaluations are not always completely repeatable. Scenario evaluations usually take a few weeks to complete because multiple trials must be completed to ensure adequate habituation of the end users and to achieve a statistically relevant number of samples. Results from a typical scenario evaluation show areas that require additional system integration and provide performance data on systems for the application tested [45].

At first glance, an Operational Evaluation appears very similar to a Scenario Evaluation, except that the test is conducted at the actual site using actual end users, a subset of the end users, or a representative set of subjects. Rather than testing for performance, operational evaluations typically aim to determine the workflow impact caused by the addition of a biometric system. Operational evaluations are typically not repeatable. Operational evaluations can last from several weeks to several months because the evaluation team must first examine workflow performance prior use of the technology and again after users are familiar with the technology. An accurate analysis of the benefit of the new technology requires a comparison of the workflow performance before and after use of the technology. In an ideal three-step evaluation process, technology evaluations are first performed on all applicable technologies that could conceivably meet requirements. The technical community then uses the results to plan future R&D activities, while potential users use the results to select promising systems for application specific scenario evaluations. Results from the scenario evaluations will enable users to determine the best system for their specific application and to have a good understanding of how it will operate at the proposed location. This performance data, combined with workflow impact data from subsequent operational evaluations, will enable decision makers to develop a solid business case for potential installations. So for those analyzing evaluation reports, it is important to determine which type of evaluation occurred and its relevance to an intended application. Generally, technology evaluation reports contain information relevant to most intended applications of a given biometric, while operational evaluation reports are generally only useful if the intended application is very closely related to what was tested.

2.4.2 Evaluation Terms

Biometric terms such as recognition, verification and identification are sometimes used interchangeably. This is not only confusing but incorrect as each term has a different meaning.

Verification occurs when the biometric system attempts to confirm an individual's claimed identity by comparing a submitted sample to one or more previously enrolled templates.

Identification occurs when the biometric system attempts to determine the identity of an individual. A biometric is collected and compared to all the templates in a database. Identification is "closed-set" if the person is assumed to exist in the database. In "open-set" identification, the person is not guaranteed to exist in the database. The system must determine if he person is in the database. A "watchlist" task is an example of "open-set" identification.

Recognition is a generic term and does not necessarily imply either verification or identification. All biometric systems perform "recognition" to "again know" a person who has been previously enrolled

• *Other Performance Statistics*

Other statistics are sometimes used to show performance of biometric systems. These, listed below, are the most commonly used.

- **Crossover Error Rate (CER) or Equal Error Rate (EER)** is the rate at which both accept and reject errors are equal. The value of the EER can be easily obtained from the ROC curve. The EER is a quick way to compare the accuracy of devices with different ROC curves. In general, the device with the lowest EER is most accurate. Obtained from the ROC plot by taking the point where FAR and FRR have the same value. The lower the EER, the more accurate the system is considered to be.

- **Detection Error Trade-off (DET)** is a graphical plot of error rates for binary classification systems, plotting false reject rate versus false accept rate. The x- and y-axes are scaled non-linearly by their Normal Deviates, yielding tradeoff curves that are more linear than ROC curves, and spend most of the image area highlighting the differences of importance in the critical operating region.
- **Difference Score** is the value returned by a biometric engine that indicates the degree of difference found between a reference biometric sample or the data in the database and the data being obtained for comparison.

- **Failure to Enroll Rate (FTE/FER)** is the probability that an individual is unable to enroll. Good reporting practices should describe the main causes that produced such failures. These might include user injuries, image quality problems or positioning problem. Failure to enroll rates for most systems is normally quite low. Enrollment problems for large populations tend to result from logistical and programmatic issues more than from isolated technical difficulties.
- **False Match Rate (FMR) or False Accept Rate (FAR)** is a statistic used to measure biometric performance when operating in the verification task. The percentage of times a system produces a false accept, which occurs when an individual is incorrectly matched to another individual's existing biometric. For example, Frank claims to be John and the system verifies the claim.
- **False Non-Match Rate (FNMR) or False Reject Rate (FRR)** is a statistic used to measure biometric performance when operating in the verification task. The percentage of times the system produces a false reject. A false reject occurs when an individual is not matched to his/her own existing biometric template. For example, John claims to be John, but the system incorrectly denies the claim.

- **Hamming Distance** is the number of non-corresponding digits in a string of binary digits; used to measure dissimilarity. Hamming distances are used in many Daugman iris recognition algorithms.
- **Throughput Rate** is the number of biometric transactions that a biometric system processes within a stated time interval.
- **True Accept Rate (TAR) or True Match Rate (TMR)** this measure represents the degree that the biometric system is able to correctly match the biometric information from the same person. Developers of biometric systems attempt to maximize this measure.

- **True Reject Rate (TRR) or True Non-Match Rate (TNMR)** his measure represents the frequency of cases when biometric information from one person is correctly not matched to any records in a database because, in fact, that person is not in the database. Developers attempt to maximize this measure.
- **Type I Error** is an error that occurs in a statistical test when a true claim is incorrectly rejected, also known as the FRR or false reject rate.
- **Type II Error** is an error that occurs in a statistical test when a false claim is incorrectly not rejected, also known as the FAR or false accept rate.

• *Other Types of Testing*

Not all biometrics tests are accuracy-based. A summary of the more common of these tests is described as follow.

- **Acceptance Testing:** "The process of determining whether an implementation satisfies acceptance criteria and enables the user to determine whether or not to accept the implementation. This includes the planning and execution of several kinds of tests (e.g., functionality, quality, and speed performance testing) that demonstrate that the implementation satisfies the user requirements."[46]
- **Conformity:** "Fulfillment by a product, process or service of specified requirements."[47]
- **Conformity Evaluation:** "Systematic examination of the extent to which a product, process or service fulfils specified requirements."[47]
- **Conformance Testing (or Conformity Testing):** "Conformity evaluation by means of testing." [47]
- **Interoperability Testing:** "The testing of one implementation (product, system) with another to establish that they can work together properly"[48]
- **Performance Testing:** "Measures the performance characteristics of an Implementation Under Test (IUT) such as its throughput, responsiveness, etc., under various conditions."[49]
- **Robustness Testing:** "The process of determining how well an implementation processes data which contains errors."[49]

2.4.3 Comparison Biometric Systems

When discussing the accuracy of a biometric system, it is often beneficial to talk about the equal-error rate or at least to consider the false-acceptance rate and false-rejection rate. On the other hands, if two biometric systems need to be compared, specifying a single value for the FAR or FRR alone is clearly insufficient. In the case that FAR is given, it is possible that the system with the lower FAR has got an unacceptable high FRR. Thus, the systems should provide the corresponding FRR in order to make the accurately comparison. But also when the values for FAR and FRR are given, there still exists the problem that those values are threshold depending. Assuming that the threshold of the systems is adjustable, there is no reasonable way to decide if a system with a higher FAR and a lower FRR performs better than a system with a lower FAR and a higher FRR value. The EER of a system can be used to give a threshold independent performance measure. The lower the EER is, the better is the system's performance, as the total error rate which is the sum of the FAR and the FRR at the point of the EER decreases.

In theoretical, it works fine, if the EER of the system is calculated using an infinite and representative test set, which of course is not possible under real world conditions. To get comparable results it is therefore necessary that the EER that are compared are calculated on the same test data using the same test protocol.

CHAPTER 3

METHODOLOGY

This chapter describes the proposed method by combining simple password authentication technique with, behavioral biometrics, responded times. Moreover, the result that shows how the proposed method is superior to other techniques is demonstrated. Therefore, in Section 3.1 describes the proposed method. Then, Section 3.2 the evaluation process that consists of two parts: data gathering, extracting features.

3.1 Proposed Method

In this thesis, a new method using combination of simple password technique with the responded time (interval time) is introduced. The method is based on two distinctive features: a password and an interval time. Even password authentication technique is ease of use and low cost of implementation, but it lacks of identified capability and easy to break. Also, it provides low security performance level after comparing to other techniques. An interval time, itself, doesn't provide much useful information in the authentication process. When combining the two features together, the result produces a new method that provided a high performance for authentication process with low cost and ease of use features.

The main idea for the authentication technique is the time interval when a password or a phase is entered by the owner must be different from the time interval measured when emulators enter the password or the phase of others. For example, if A is a owner of the mobile phone X, then time interval when A enters password to unlock X will be *T*(A). Then, when an emulator, B, enters A's password to unlock X, the time interval for this entering will be *T*(B). The assumption for this authentication process is that *T*(A) will always be different from *T*(B). Since people uses their devices several times, the time interval that is used to identify the owner is the average time interval measured in a time limit from time to time. The strength of this technique is that people normally do not change the rhythm of their movement, especially their fingers and thought. Thus, the time interval of an authenticated person will not be changed and cannot be emulated effortlessly [50].

3.2 Evaluation Process

Base on behavioral biometrics authentication process, many techniques were developed to compete not only for providing high rate of accuracy, but also for ease of uses and ideal for applying in a specific situation. For the proposed method, the ease of uses and the ideal for applying in a specific purposed were described in earlier section, hence the process of proving this method is provided in this section to confirm that the proposed method is efficient.

In order to provide the proof of the proposed method, the Time Interval Testing System (TINTS) is implemented and used as a tool. The evaluation process is conducted which dividing into three parts: data gathering, extracting features, and analyzing features. Figure 3.1 illustrates the use case of the system. Each of activity will be described in details in the following section. Furthermore, the class diagram of the whole system is presented in Figure 3.2.

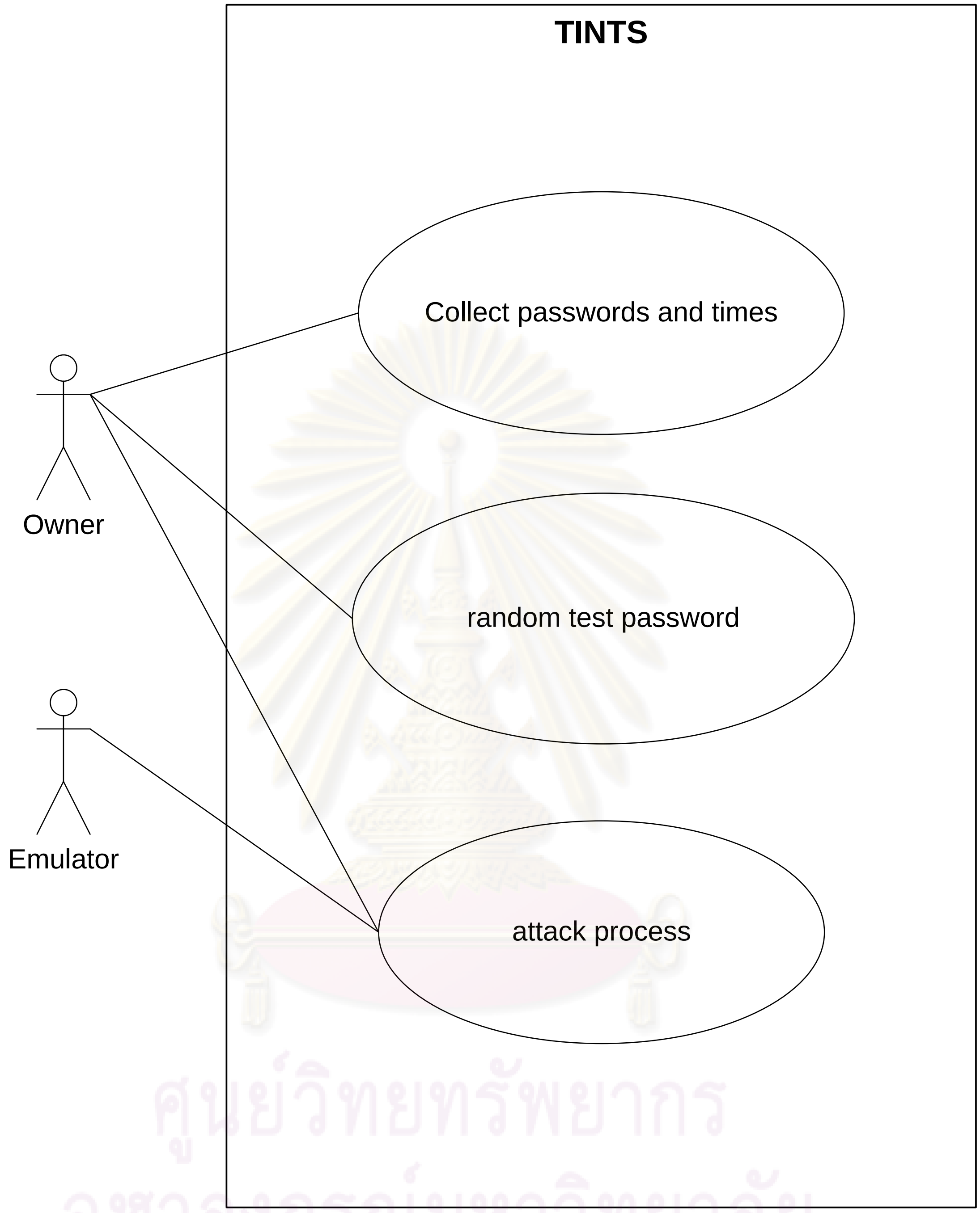


Figure 3.1 Use case diagram of the TINTS system

Use case diagram: Template

- Use case name: TINTS
- Participant actors:
    - Invoked by Owner,
    - Communicates with Emulator

- Entry condition:
    - Owner participates in the TINTS.
- Flow of events
    - The TINTS requests Owners to create their profile.
    - The Owner starts creating their own template, passwords and time interval.
    - The owner calls random testing password function to test for time intervals, then recorded via The TINTS.
    - The TINTS randomly sends test case to emulators.
    - The Emulator trial for the time intervals via the test case.
    - The test case checks correctness of the emulator's time interval and the number of attempt.
    - All test cases are recorded and stored back to the TINTS.
- Exit conditions
    - All of emulators complete all test cases
- Special requirements
    - A user must not act as an emulator to test more than one time per test case.

Use case diagram: Scenarios

- Scenario Name: TINTS
- Participating actor instances:
    - Alice: Owner
    - Bob: Emulator
- Flow of events
    - The TINTS requests Alice to create his/her profile.
    - Alice starts creating her own template, passwords and time intervals.
    - Alice calls random testing password function to test for time intervals, then recorded via The TINTS.
    - The TINTS randomly sends test case to Bob.
    - Bob trials for the time intervals via the test case.
    - The test case checks correctness of the Bob's time interval and the number of attempt.
    - Bob's test case is recorded and stored back to the TINTS.

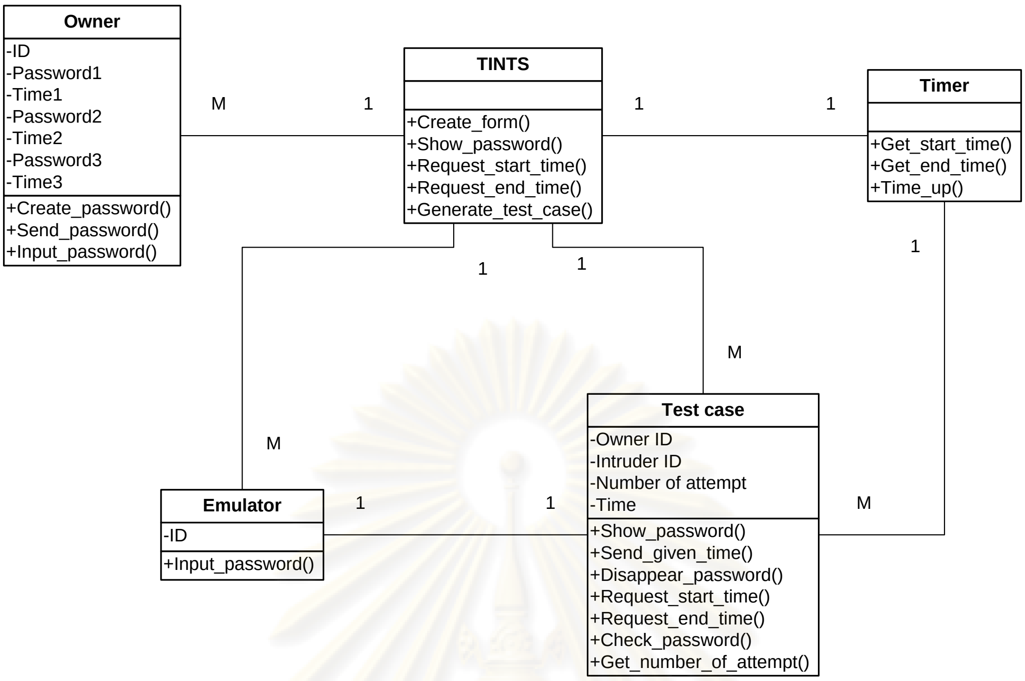


Figure 3.2 Class diagram of the TINTS

3.2.1 Data Gathering

Authorized user

In this component, the owner's time intervals are gathered through the TINTS. 45 people are randomly selected as owners from various groups of people: sex, ages, and careers Figure 3.3 demonstrates the sequence diagram of the owner's template creation.

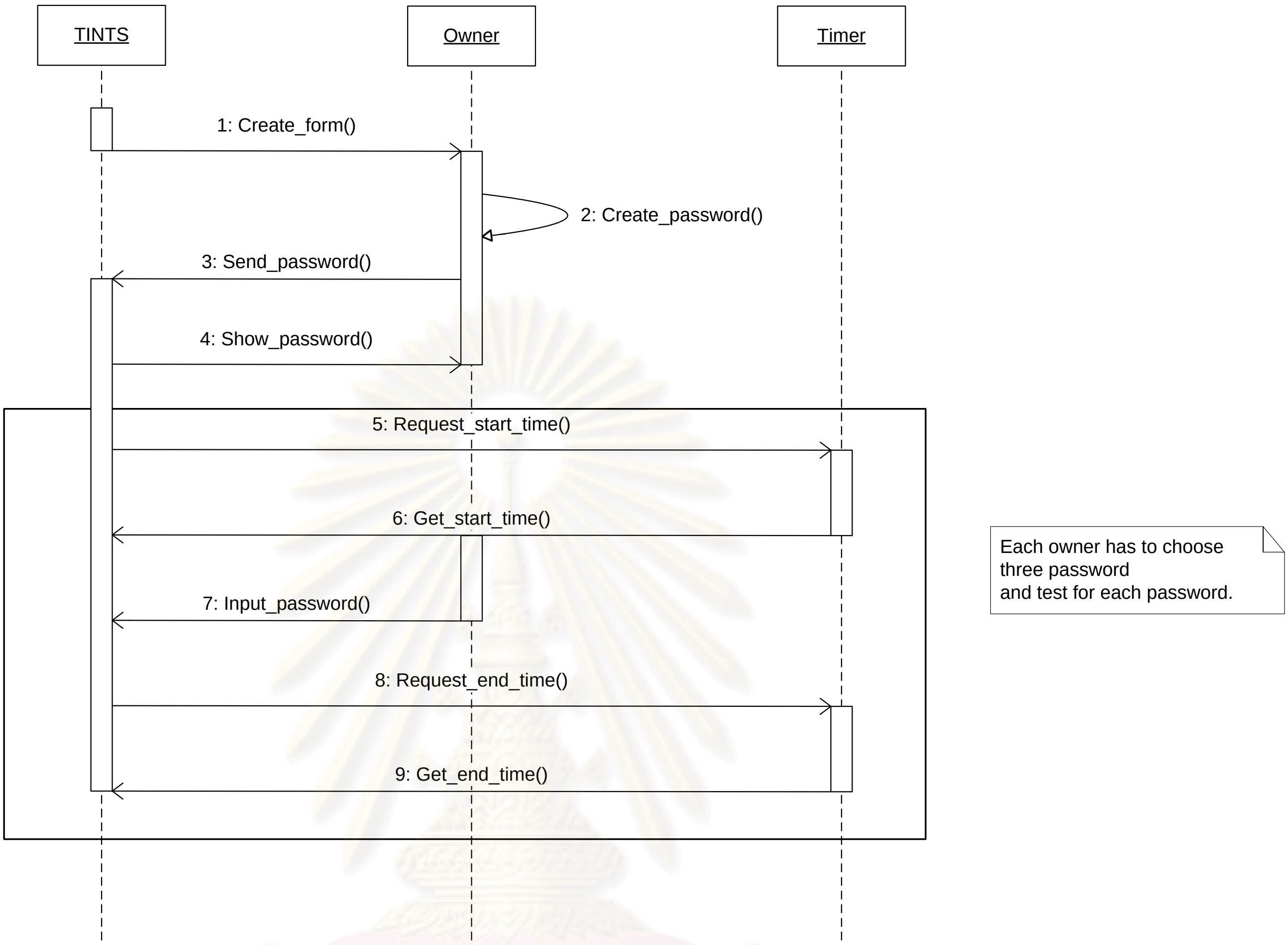


Figure 3.3 Sequence diagram of the owner’s template creation

From Figure 3.3, the process of the owner’s template creation can be describes as follow.

(1) The TINTS creates forms which is based on VBA scripts in MS excel and distributes it to each owner.

(2) An owner user freely creates passwords which have no limit on length and no boundary on languages.

(3) The owner sends their own passwords back to the TINTS. Each owner has to create three passwords.

(4) The TINTS shows random password to the owner.

(5) The TINTS requests the start time to the timer, right after the password text appears on the screen.

(6) The TINTS captures the start time value from the timer.

(7) The owner types in the presented password from the screen.

(8) When the owner finishes typing, the TINTS requests the end time from the timer.

(9) The TINTS obtains the end time value from the timer.

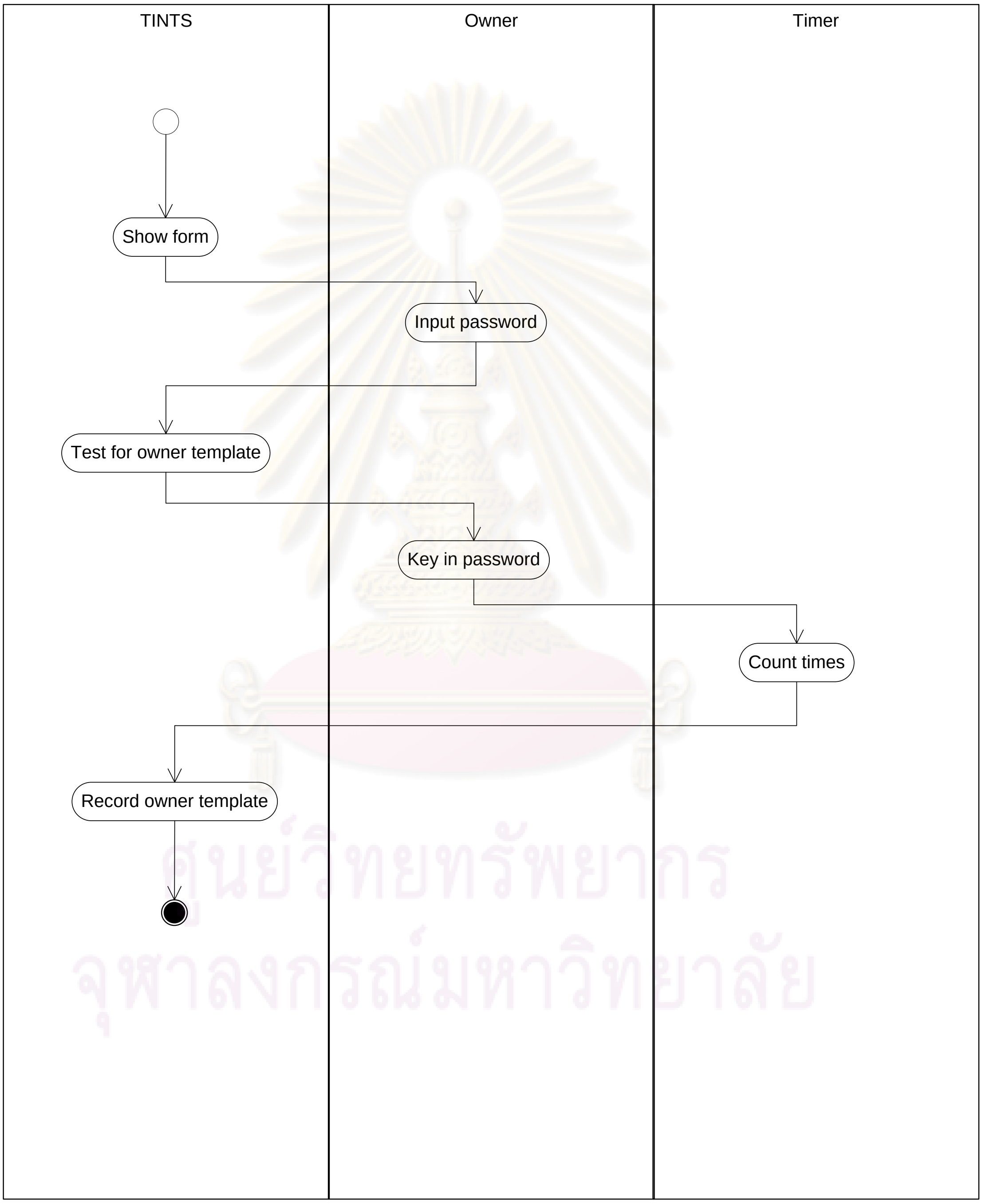
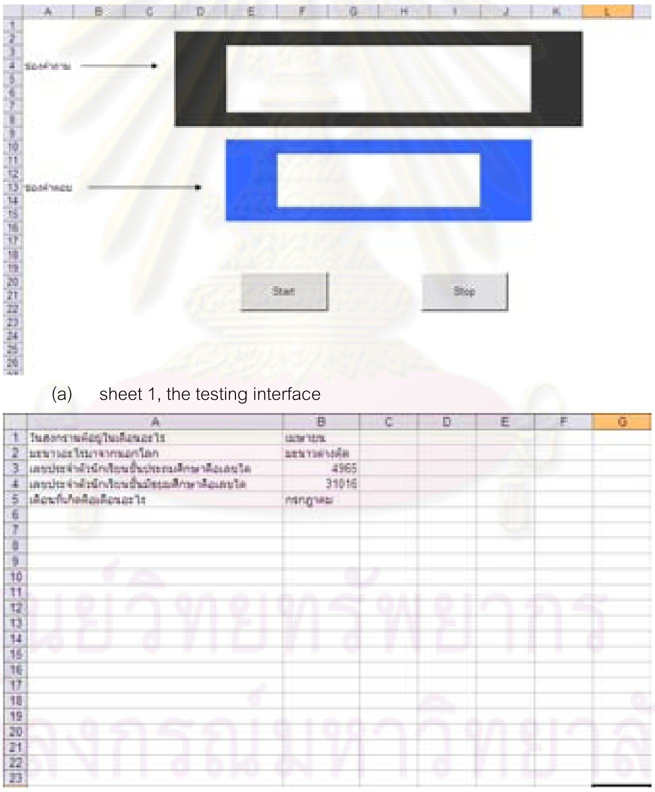


Figure 3.4 Activity diagram of the owner's template creation

According to the activity diagram in Figure 3.4, the first step is that the TINTS creates and shows form to owners. Later on, owners build their own passwords and send back to the TINTS to prepare ownership test. Then, the TINTS passes the test case to the owner to fill in the password, captures the owner time interval, while the timer starts capturing the time interval right after the beginning of the test. When the owner completes the ownership test, all of the owner data, both password and the related time interval, will be record and stored in the TINTS as the owner template.

Besides, the example of the TINTS collecting interfaces illustrate in Figure 3.5. The interface is created using MS excel as a tool to develop and consists of two sheets. The first sheet is an interface which used for interact with users; additionally, there are instructions on this sheet to help completing the process. On the second sheet, it is used as the database of the passwords that are filled in by the owner users.



(a) sheet 1, the testing interface

	A	B	C	D	E	F	G
1	[illegible]	[illegible]					
2	[illegible]	[illegible]					
3	[illegible]	4965					
4	[illegible]	31016					
5	[illegible]	กรกฎาคม					

(b) sheet 2, owner group's profile

Figure 3.5 The interface formed by MS excel

Unauthorized user

In this section, the invasion process of an emulator will be simulated, and then the time interval factor of emulators will be obtained through the process and used for comparing and analyzing with the owner template. Figure 3.6 presents the sequence diagram of the extracting features from emulators.

From the sequence diagram of extracting features from emulators, Figure 3.6, the details of the diagram are explained as follow.

(1) The TINTS generates test case for emulators. The total numbers of test cases are 405 test cases.

(2) The test case shows a password to the emulator. The emulator tries to remember the password from the screen.

(3) The test case sends the given time to the timer to trigger it.

(4) The test case obtains the start time after the timer starts triggered.

(5) The time limit is reached.

(6) The password on the screen disappears; the cursor prompts on the answer box at the middle of the screen.

(7) When an emulator presses the first character on the keyboard, it will activate the next method.

(8) The test case requests the start time value from the timer.

(9) The test case obtains the start time value.

(10) The emulator presses the "enter" key to finish the key-in process.

(11) The test case requests the end time value from the timer.

(12) The test case retrieves the start time value.

(13) The test case performs password validation process. If the validation fails, it will loop back to step (7).

(14) The test case retrieves number of attempt.

(15) The TINTS gathers all test cases back and stored all data in the system.

Additionally, if emulators take times to input the passwords exceed one minute, the test case will count as failure attempt and loop back to step (7). Consequently, all outlier values will be removed.

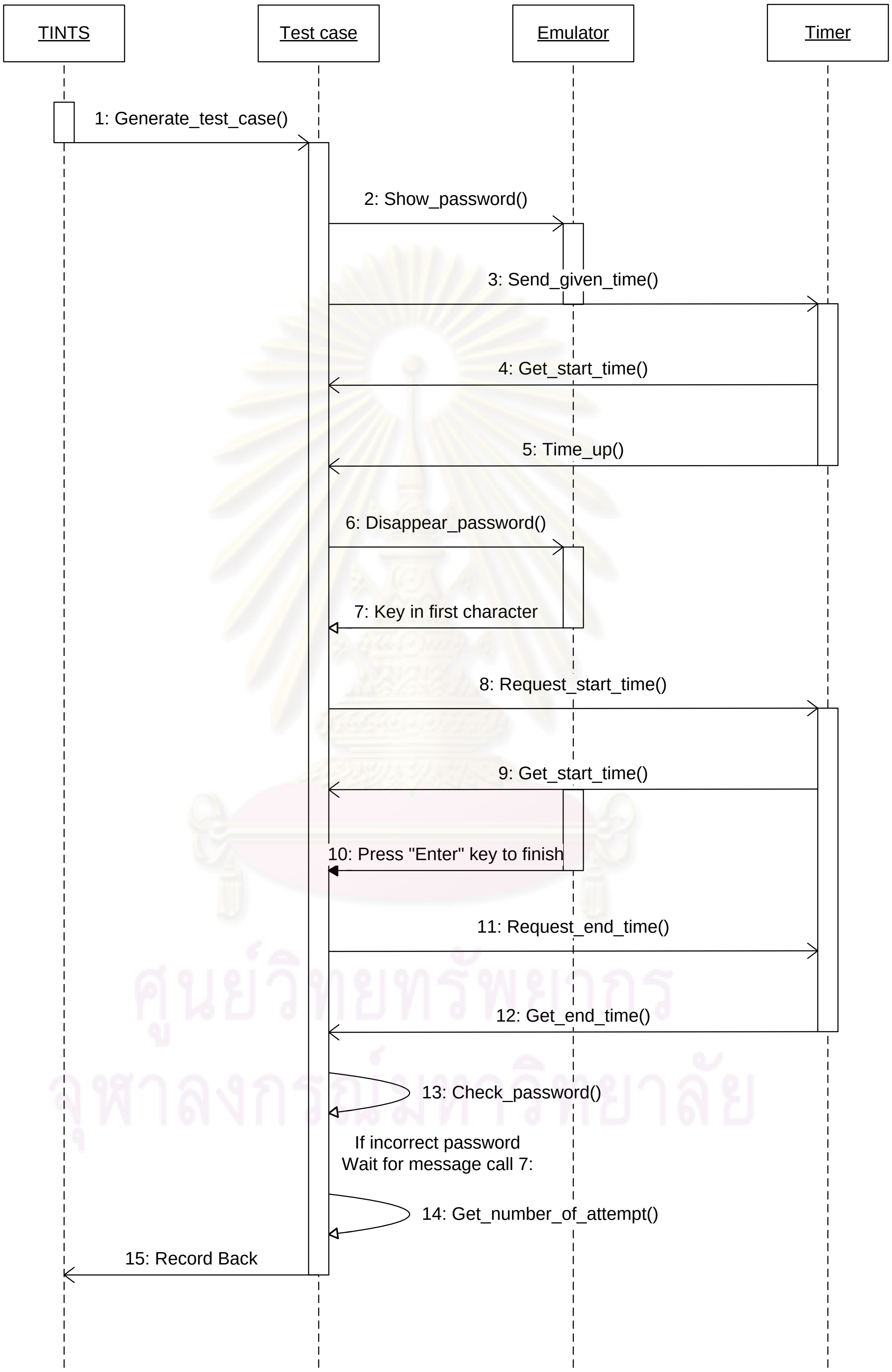


Figure 3.6 Sequence diagram of extracting features from emulators

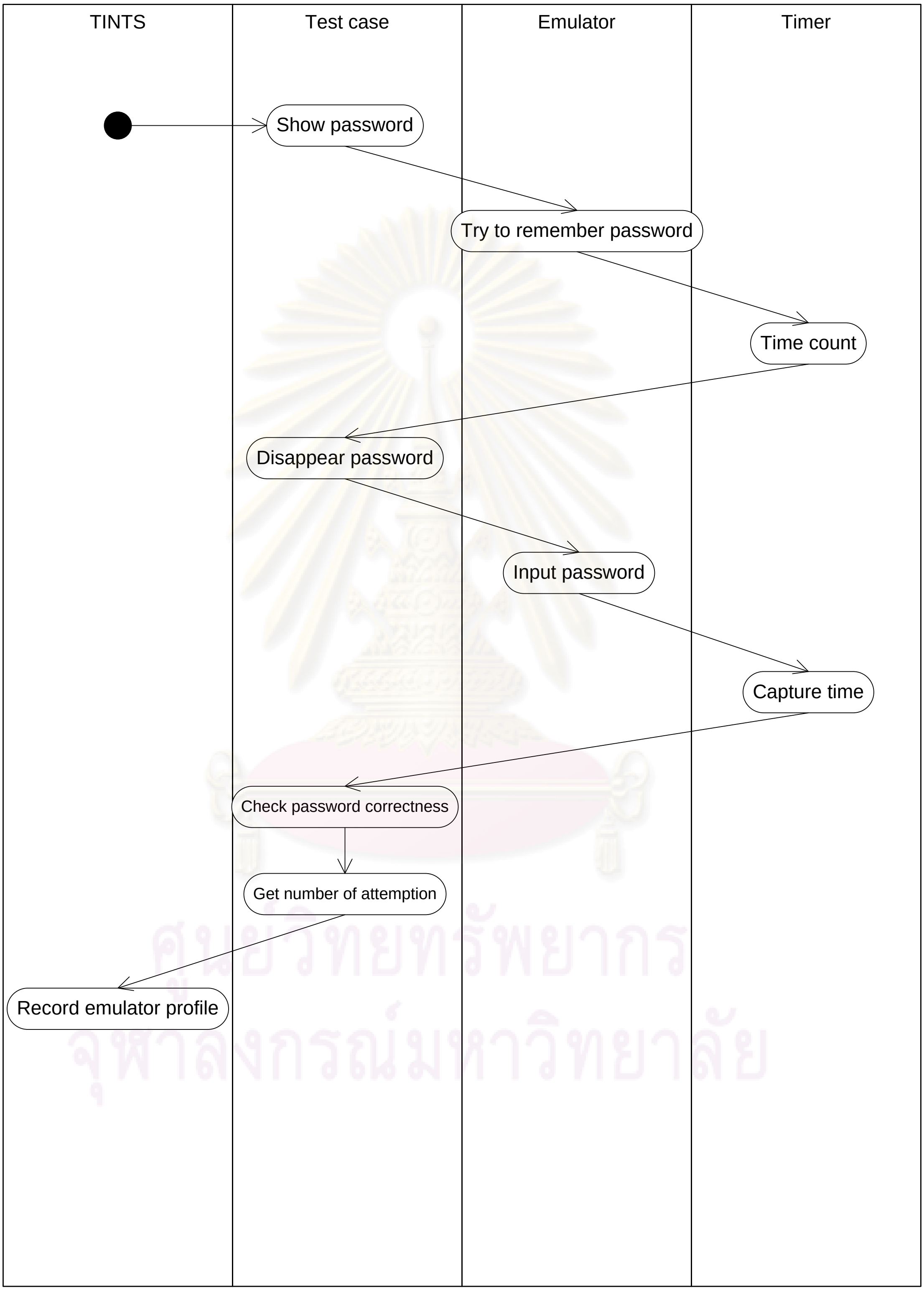


Figure 3.7 Activity diagram of extracting features from emulators

According to activity diagram of extracting features from emulators, Figure 3.7, it begins with the test case show the password to the emulator. Next, the emulator has to try to remember password which appears on the screen until a certain amount of time. The password will disappear instantly when the time is up. Then, the emulator types the password that he or she remembered and the interval time of the emulator is collected during this phase. Later, the test case performs a password validation and obtains the number of attempt. Lastly, all data from test case will be recorded back to the TINTS.

During the collecting procedure, the time intervals of the unauthorized persons are extracting. This time interval is based on assumption that each individual spend on different time to unlock the system. The time interval starts from the moment that the password disappeared from the screen and the user press on the first character on the keyboard until the user press "Enter" key to finish it. This could signify the behavior of the persons during the authentication process. Thus, the behavioral biometrics data of the unauthorized person are obtained through the procedure which will be used for analyzing along with the owner templates gathered from the data gathering section. This biometrics features will play as the main key in this experiment.

3.2.2 Extracting Features

According to the data gathering process, the feature that extracted from the procedures is the average time interval of individuals which has been calculated from the authentication process. Based on the data observation, the individual time values within the owner group are quite different from the time values of the emulator group. Thus, there is a probability that the average time interval of the owner group is different from the average time interval of the emulator group; each group has their own characteristics. However, there is no indicator that the time interval of which group will be higher or lower than another when typing the selected password. Nevertheless, the difference among these two groups can indicate that emulators cannot emulate the typing speed of the owner although they know the significant keywords and have typing experience. Therefore, the average time interval can be counted as a biometric for distinguishing between owners and emulators. In order to ensure this assumption, the results from the experiment are presented in Chapter 4.

CHAPTER 4

EXPERIMENTAL RESULTS

This chapter will show experimental results from the proposed method and provide the comparison with other behavioral biometrics factors that effect on authentication process. The analyzed features will be described in Section 4.1 and the hypothesis test and the details of the result will be demonstrated in Section 4.2. Section 4.3 summarize to the final conclusion.

4.1 Analyzing Features

4.1.1 Setting Assumptions

In the analysis process, based on the fact that the proposed method could classify between authorized and non-authorized persons using the mean time interval combining with simple password for each individual. The hypothesis for this is that:

H_{01}: The mean time intervals of the owners and emulators have no significant difference.

H_{11}: The mean time intervals of the owners and emulators have significant difference.

Moreover, the significant factor on the length of the passwords towards the time interval of the owners is considered. Thus, the hypothesis for this measurement is as follow.

H_{02}: There is no significant difference of mean time interval between owner and emulator groups when the lengths of the passwords are different.

H_{12}: There is significant difference of mean time interval between owner and emulator groups when the lengths of the passwords are different.

In addition, since passwords have various lengths, then this research also focuses on the time length that emulators see the password in which they can emulate the time interval of the owners. Therefore, the third hypothesis that must be proven is shown below.

H_{03}: There is no significant difference of mean time interval between owner and emulator groups when the time appearance of the password is different.

H_{13}: There is significant difference of mean time interval between owner and emulator groups when the time appearance of the password is different.

4.1.2 Testing Parametric Conditions

In this research, the parametric test is applied. However, there are three assumptions needed to be proved. The first condition to be proved is that the data must be random and independent. Since all samples are collected by volunteers and each sample has freedom in entering and selecting their passwords. Therefore, the randomize condition is satisfied.

The second criterion is that the distribution of data must be normal. In order to ensure this characteristic, the normality test must be performed. Using SPSS, with confident level 95%, the result shows that the distribution of the time interval of owners is normal with p-value$_{(ower)}$= 0.607(> α=0.05) which similar to the distribution of the emulators (p-value$_{(emulator)}$ = 0.153 > α=0.05). Thus, the second condition is satisfied.

Lastly, the variances of the both groups are homogeneous characteristics. This condition can be tested using Homogeneity of Variances, running Levene test with confident level 95%. The hypothesis for this test is as follow.

$H_{0\delta}$: There is no significant difference between variances of the time intervals obtained from the owners and the emulators.

$H_{1\delta}$: There is significant difference between variances of the time intervals obtained from the owners and the emulators.

The result from SPSS shows that with significant level 0.05, the variances of the time intervals obtained from the owners and the emulators are not significantly different, p-value = 0.801.

4.2 Testing Hypothesis

In this section there are three tests to be performed.

1. The test to identify authorized persons using mean time interval, H_{01}.
2. The test to identify the impact of length of the password against the values of mean time interval, H_{02}.
3. The test to identify the impact of password appearance against the values of mean time interval, H_{03}.

Details of each test are described as follows.

4.2.1 The test to identify authorized persons using mean time interval:

In order to prove that there is a significant different between mean time interval of the authorized and non-authorized persons, *t*-test with equal variance is applied.

Using SPSS, the result of the Levene-test for homogeneity of variances confirms that the variances between the time interval of the authorized and non-authorized groups are equal with p-value=0.642 > α=0.05. Moreover, the t_{cal} = -12.892 (df=538), p-value = 0.00 < α=0.05. Thus, the alternative hypothesis is accepted, or the null hypothesis is rejected. Therefore, the combination of time interval and the password can be applied to identify authorized person.

4.2.2 The Test to Identify The Impact of Length of The Password

Another hypothesis that needed to be proven is that there is significant different of mean time interval between owners and emulators when the length of passwords are varied. The result of the Levene-test indicates that the variances of the time interval between owners and emulators when the length of passwords are varied is equal with p-value = 0.666 > α=0.05. The result also shows that using various lengths of passwords of mean time interval has no significant different with $\text{p-value}_{(\text{CharInterv})}$ = 0.557 > α=0.05. Hence, the null hypothesis, H_{02} is accepted, the lengths of passwords have no impact to the mean time interval. Therefore, in the authentication process, there is no impact from the length of the entering password.

4.2.3 The Test to Identify The Impact of Password Appearance

The last hypothesis is to test the differences between the values of mean time interval of owners and emulators when the time-appearances of the passwords is different. This test is based on the assumption that the equivalence of the mean time interval obtained from owners and emulators can be exist according to the appearance of the password.

The ANOVA with multiple comparisons is applied for this test. Checking on the Levene-test, the p-value= 0.049 < α=0.05. Thus, the variances between owners and emulators with different time-appearances of passwords are significant difference. Therefore, the non-parametric, Kruskal-Wallis test is computed. The result of the computation shows that the p-value is 0.00 < α=0.05. Therefore, H_{13} is rejected; this means there is at least one mean time interval that has its value different from other mean time intervals when the time-appearance of the password is different. Therefore, the time-appearances of the passwords have impact on some of the mean time interval.

In order to identify the difference among two groups with different time-appearances, the Mann-Whitney *U*-Test is applied. The hypothesis of the test is drawn as follow.

H_{04}: The mean time interval of the *k* time-appearance is equal to the mean time interval of the *l* time-appearance.

H_{14}: The mean time interval of the *k* time-appearance is not equal to the mean time interval of the *l* time-appearance.

When *k*, and *l* are running from 0, 30, 45 and 60.

According to the test of SPSS, the results are shown in Table 4.1

Table 4.1 Mann-Whitney *U*-Test with 95% confident level

Time-appearance	0 sec	30 sec	45 sec	60 sec

30 sec	z=-12.108
	p=0.00
		-	z=-9.176
			p=0.00
				z=-8.143
				p=0.00

45 sec	z=-7.356
	p=0.00
		z=-9.176
		p=0.00
			-	z=-1.699
				p=0.089

60 sec	z=-8.143	z=-8.814	z=-1.699	-

	p=0.00	p=0.00	p=0.089	

Referring to the results in Table 4.1, the emulators cannot emulate the owners' behavior when they have a chance to see the password within 60 seconds.

4.3 Final conclusion

Password is the basic protection of every system, and it is very easy to be hacked. However, this research has proposed a mechanism to increase the strength of the password implementation by combining the time-interval when keying the password of the owner as an access key to the authentication system. In this research, three aspects have been tested. The first test is to confirm that the time-interval of the authorized person always be different from the emulators; the test result is confirmed as expected. The second test is to ensure that the length of the keyword has no impact to the time differences; the result has been confirmed as needed. The last test is to classify that the time length of visibility of the keyword may have impact for emulator's emulation. This test can classify that no matter the visible time length is, the emulators cannot emulate the time interval for keyword entering of owners. Therefore, this result backs up the result obtained from the first test.

Based on the results of all tests, the use of time interval combining with the keyword in the authentication system can be applied to fulfill the strength of the keyword mechanism. Additionally, the condition of setting up the length of the keyword is not the first priority to be concerned since it has neither impact on the correctness of authentication system, nor the emulation of the emulators.

CHAPTER 5

DISCUSSION AND CONCLUSIONS

In this chapter, the discussion will be discussed in Section 5.1, and conclusions will be drawn in Section 5.2, followed by the future work for this thesis in Section 5.3.

5.1 Discussion

In the real world, mobile devices are easily stolen and the data stored in it will be in a risk mode. Therefore, various techniques have been proposed and implemented to protect the unauthorized usages from unwanted persons. One popular technology is to apply the biometric value to be the identifier, or applied as a protector of the system. However, this biometric is very uncertainty when used, according to the change of biological value based on uncontrolled situations. Thus, choosing the right biometric will lead to a flexible and qualified protection system.

In order to obtain a required protection system as mentioned above, the combination of biometric values, called as multi-biometrics, is considered [23][24]. These researches confirmed that applying of the multi-biometrics provides the higher accuracy rate in the detection mode. Additionally, this combination also reduces the risk from external emulators since many copies of biometrics data must be obtained before attack. Consequently, the computation time of hacking mechanisms will be increase.

Although there are various biometrics have been applied in the real-world applications, those metrics can be changed according to time such as fingerprint, voice, retina, etc. Therefore, this research is looking for a biometric that hardly changes by time or cannot be affected by the age change. One biometric that has been considered and studied in this research is the typing time interval of user's password, since the use of password is common to all systems and the typing time interval has never been studied. Moreover, the implementing of the typing time interval protection mechanism into the password protection procedure is simple and practical in the every application.

Using the typing time interval of a person in the authentication mechanism may have some small risk to be considered such as the typing time when people is exhausted might be different from the normal condition. Thus, the use of time in the authentication procedure is the mean time interval which obtained from the average time value when people entering the password. Even though the test in this research has indicated that there is a significant different between mean time intervals of the authorized person and unauthorized persons, this test is performed on 95% confident level. Therefore, if the confident level is changed to be 99.5% then the result of the test might be different. However, using 95% confident level is reasonable since 99% may cause type-II error (accepts a person while that person is the emulator) for the detection mechanism, and using 90% is too sensitive until it can cause the type-I error for the test, rejects a person when that person has the right to access the system.

The strength of the proposed method is based on the fact that the biometric value, mean time interval, will not be changed according to the age change or the situation of person is changed. However, this method also has weakness in that the detection mechanism cannot be performed correctly when the user is under illness condition such as Parkinson, or Alzheimer's disease, or under the unfortunate situation to become physical disability. Nevertheless, in some unfortunate event, the old mean time interval can be reset with the new mean time value under the new physical condition by recalculating and replacement.

5.2 Conclusions

It is the fact that bio information is unique values for each person. Therefore, these data are applied in the authentication system, as called the biometric security system. Thus, this system can offer a high degree of security. Nevertheless, there is no system that has no defect.

Since the bio data is unchangeable, therefore, when an unexpected event occurs to unexpectedly change the biometric value of the owner, such as arm amputated (for fingerprint detection), or eye damaged (for retina detection), the detection mechanism cannot be performed. In such case, the use of only one biometric may not be a proper protection method. Thus, combination between biometrics or between a biometric and another indicator is applied to avoid such unexpected situation and leave some solution for users.

The proposed solution in this research is the combination among the mean time interval for password entering and the value of the password. Since the mean time interval is a biometric value that is obtained from the average value of password entering system. The results of this studied have shown that the use of the mean-time interval can used as the biometrics features to indicate authenticated person and emulators. Moreover, this method has been proved that it is the length-independent from passwords. In addition, the proof on the appearance of the password against the emulation times of the emulators has been performed. The result of this proof also indicates that the mean time interval of the authorized person is significantly different from the unauthorized one.

As mentioned previously that the defect of using a single value of biometric is the unusable biodetection when the physical condition of the owner has been unconditionally changed with respected to the biometric data. However, the proposed mechanism provides an alternative solution to the protection system in such a case that the mean time interval can be reset as same as the password can be reset by the owner. Therefore, using the mean time interval with the password in the authentication process is an effective and flexible method when comparing to other biometric values.

5.3 Future work

This thesis performed the preliminary study of the method using behavioral biometrics features combining with a simple password technique. Thus, the mechanism to identify the authenticated person must be developed and tested. In addition, the real implementation in the commercial area to the digital devices should be studied for cost-effectiveness, including the acceptability under users' expectations.

REFERENCES

[1] SOPHOS: security threat report //Q1 08

URL: http://www.sophos.com

[2] Rodwel PM, Furnel SM, Reynolds PL. “A Non-Intrusive Biometric Authentication Mechanism Utilising Physiological Characteristics of the Human Head”, Computers & Security (2007), doi: 10.1016/j.cose.2007.10.001

[3] Deriche, M.; , "Trends and Challenges in Mono and Multi Biometrics," Image Processing Theory, Tools and Applications, 2008. IPTA 2008. First Workshops on , vol., no., pp.1-9, 23-26 Nov. 2008

URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4743801&isnumber=4743728

[4] Seno, S.; Sadakane, T.; Baba, Y.; Shikama, T.; Koui, Y.; Nakaya, N.; , "A network authentication system with multi-biometrics," Communications, 2003. APCC 2003. The 9th Asia-Pacific Conference on , vol.3, no., pp. 914- 918 Vol.3, 21-24 Sept. 2003

URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1274231&isnumber=28516

[5] A. K. Jain, L. Hong, and S. Pankanti, "Biometrics Identification," Communications of the ACM, Vo1.43, No.2, pp.91-98, February 2000.

[6] B. Schneier, "Inside Risks: The Uses and Abuses of Biometrics," Communications ofthe ACM, Vo1.42, No.8, pp.136-, August 1999.

[7] N. K. Ratha, J. H. Connell, and R. M. Bok, "Enhancing Security and Privacy in Biometrics-based Authentication Systems", IBM Systems Joumal, Vo1.40, No.3, pp.614-634,2001.

[8] L. Hong, A. K. Jain, and S. Pankanti, "Can Multibiometrics Improve Performance?," Proc. AutoID '99, pp.59-64, October 1999.

[9] Jain, A.K.; Pankanti, S.; Prabhakar, S.; Lin Hong; Ross, A., "Biometrics: a grand challenge," Pattern Recognition, 2004. ICPR 2004. Proceedings of the 17th International Conference on , vol.2, no., pp. 935-942 Vol.2, 23-26 Aug. 2004.

[10] Hao Li; Peishun Liu, "An Identification System Combined with Fingerprint and Cryptography," Computer and Computational Sciences, 2006. IMSCCS '06. First International Multi-Symposiums on , vol.2, no., pp.105-108, 20-24 June 2006

[11] Gafurov, D.; Snekkenes, E.; Bours, P., "Spoof Attacks on Gait Authentication System," Information Forensics and Security, IEEE Transactions on , vol.2, no.3, pp.491-502, Sept. 2007

[12] Hema, C.R.; Paulraj, M.P.; Kaur, H., "Brain signatures: A modality for biometric authentication," Electronic Design, 2008. ICED 2008. International Conference on , vol., no., pp.1-4, 1-3 Dec. 2008

[13] Dogaru, R.; Dogaru, I., "Biometric authentication based on perceptual resonance between CNN emergent patterns and humans," Cellular Neural Networks and Their Applications, 2002. (CNNA 2002). Proceedings of the 2002 7th IEEE International Workshop on , vol., no., pp. 267-274, 22-24 Jul 2002

[14] Kiran, G.V.; Kunte, R.S.R.; Samuel, S., "On-line signature verification system using probabilistic feature modelling," Signal Processing and its Applications, Sixth International, Symposium on. 2001 , vol.1, no., pp.355-358 vol.1, 2001

[15] Cimato, S.; Gamassi, M.; Piuri, V.; Sassi, R.; Scotti, F., "Privacy-Aware Biometrics: Design and Implementation of a Multimodal Verification System," *Computer Security Applications Conference, 2008. ACSAC 2008. Annual* , vol., no., pp.130-139, 8-12 Dec. 2008
URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=4721551&isnumber=4721526

[16] Moskovitch, R.; Feher, C.; Messerman, A.; Kirschnick, N.; Mustafic, T.; Camtepe, A.; Lohlein, B.; Heister, U.; Moller, S.; Rokach, L.; Elovici, Y., "Identity theft, computers and behavioral biometrics," *Intelligence and Security Informatics, 2009. ISI '09. IEEE International Conference on* , vol., no., pp.155-160, 8-11 June 2009
URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=5137288&isnumber=5137253

[17] Yong Jian Chin; Thian Song Ong; Goh, M.K.O.; Bee Yan Hiew, "Integrating Palmprint and Fingerprint for Identity Verification," *Network and System Security, 2009. NSS '09. Third International Conference on* , vol., no., pp.437-442, 19-21 Oct. 2009
URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=5319331&isnumber=5318887

[18] Jain, A.K.; Pankanti, S.; Prabhakar, S.; Lin Hong; Ross, A., "Biometrics: a grand challenge," *Pattern Recognition, 2004. ICPR 2004. Proceedings of the 17th International Conference on* , vol.2, no., pp. 935-942 Vol.2, 23-26 Aug. 2004
URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=1334413&isnumber=29386

[19] Woodward, J.D., "Biometrics: privacy's foe or privacy's friend?," *Proceedings of the IEEE* , vol.85, no.9, pp.1480-1492, Sep 1997
URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=628723&isnumber=13673

[20] Iwashita, Y.; Stoica, A., "Gait Recognition Using Shadow Analysis," *Bio-inspired Learning and Intelligent Systems for Security, 2009. BLISS '09. Symposium on* , vol., no., pp.26-31, 20-21 Aug. 2009
URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=5376864&isnumber=5376766

[21] Shan Ao; Weiyin Ren; Shoulian Tang, "Analysis and Reflection on the Security of Biometrics System," *Wireless Communications, Networking and Mobile Computing, 2008. WiCOM '08. 4th International Conference on* , vol., no., pp.1-5, 12-14 Oct. 2008
URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=4681014&isnumber=4677909

[22] Venkatachalam, S.P.; Kannan, P.M.; Palanisamy, V., "Combining cryptography with biometrics for enhanced security," *Control, Automation, Communication and Energy Conservation, 2009. INCACEC 2009. 2009 International Conference on* , vol., no., pp.1-6, 4-6 June 2009
URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=5204448&isnumber=5204362

[23] Seno, S.; Sadakane, T.; Baba, Y.; Shikama, T.; Koui, Y.; Nakaya, N.; , "A network authentication system with multi-biometrics," Communications, 2003. APCC 2003. The 9th Asia-Pacific Conference on , vol.3, no., pp. 914- 918 Vol.3, 21-24 Sept. 2003
URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1274231&isnumber=28516

[24] Bringer, J.; Chabanne, H.; Kindarji, B.; , "Anonymous identification with cancelable biometrics," Image and Signal Processing and Analysis, 2009. ISPA 2009. Proceedings of 6th International Symposium on , vol., no., pp.494-499, 16-18 Sept. 2009
URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5297678&isnumber=5297612

[25] Teoh, A.B.J.; Ngo, D.C.L.; , "Biophasor: Token Supplemented Cancellable Biometrics," Control, Automation, Robotics and Vision, 2006. ICARCV '06. 9th International Conference on , vol., no., pp.1-5, 5-8 Dec. 2006
URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4150370&isnumber=4126184

[26] Choras, M.; , "Emerging Methods of Biometrics Human Identification," Innovative Computing, Information and Control, 2007. ICICIC '07. Second International Conference on , vol., no., pp.365, 5-7 Sept. 2007
URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4428007&isnumber=4427647

[27] J. Kasprzak, *Forensic Otoscopy (in Polish)*, University of Warmia and Mazury Press, 2003.

[28] A. Iannarelli, *Ear Identification*, Forensic IdentificationSeries, Paramont Publishing Company, 1989.

[29] Gomez E., Travieso C.M., Briceno J.C., Ferrer M.A., "Biometric Identification System by Lip Shape," Proc. of Carnahan Conference on Security Technology, 39- 42, 2002.

[30] R. V. Yampolskiy, "Human Computer Interaction Based Intrusion Detection," presented at 4th International Conference on Information Technology: New Generations (ITNG 2007), Las Vegas, Nevada, USA, April 2-4, 2007.

[31] Yampolskiy, R.V.; , "Indirect Human Computer Interaction-Based Biometrics for Intrusion Detection Systems," Security Technology, 2007 41st Annual IEEE International Carnahan Conference on , vol., no., pp.138-145, 8-11 Oct. 2007
URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4373481&isnumber=4373447

[32] McLoughlin, I.V.; Naidu, N.; , "Keypress biometrics for user validation in mobile consumer devices," Consumer Electronics, 2009. ISCE '09. IEEE 13th International Symposium on , vol., no., pp.280-284, 25-28 May 2009
URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5156933&isnumber=5156791

[33] A.A.E. Ahmed, I. Traore, A New Biometric Technology Based on Mouse Dynamics, IEEE Transactions on Dependable and Secure Computing, Vol. 4, No. 3, July-September 2007, pp 165-179.

[34] M. Pusara and C.E. Brodley, User Re-Authentication via Mouse Movements VizSEC/DMSEC'04: Proceedings of the 2004 ACM workshop on Visualization and data mining for computer security, ACM Press, Washington DC, USA, 2004, pp. 1-8.

[35] H. Gamboa and A. Fred, An Identity authentication system based on human computer interaction behaviour, Proc. Of the 3rd IntL. Workshop on Pattern Recognition in Information Systems. ICEIS PRESS, 2003, pp. 46-55.

[36] H. Gamboa and V. A. Fred., A Behavioral Biometric System Based on Human Computer Interaction, In Proceedings of SPIE, 2004.

[37] Asha, S.; Chellappan, C., "Authentication of e-learners using multimodal biometric technology," *Biometrics and Security Technologies, 2008. ISBAST 2008. International Symposium on* , vol., no., pp.1-6, 23-24 April 2008
URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=4547640&isnumber=4547627

[38] Janeen Renaghan, “Etched in Stone,” Zoogoer, August 1997, (Smithsonian National Zoological Park, 26 January 2005).

[39] “Dermatoglyphics,” Hand Analysis, International Institute of Hand Analysis, 24 January 2005.

[40] Z. McMahon, Biometrics: History, Indiana University, Indiana University Computer Science Department, 24 January 2005 <http://www.cs.indiana.edu/~zmcmahon/biometrics-history.htm>.

[41] J. L. Wayman, “Biometrics – Now and Then: The development of biometrics over the last 40 years,” H. Daum (ed.) Biometrics in the Reflection of Requirements: Second BSI Symposium on Biometrics 2004. SecuMedia, Bonn, 2004.

[42] URL: http://www.griaulebiometrics.com/page/en-us/book/understanding-biometrics/introduction/types/comparison-of-biometrics

[43] P. Philips, A. Martin, C. L. Wilson, and M. Przybocki, “An Introduction to Evaluating Biometric Systems” (2000).
URL :http://www.frvt.org/DLs/FERET7.pdf.

[44] “Face Recognition Vendor Test,” FRVT.org
URL: http://www.frvt.org

[45] Tony Mansfield, Gavin Kelly, David Chandler, and Jan Kane, “Biometric Product Testing Final Report” 19 March 2001, CESG/BWG Biometric Test Programme.
URL: http://www.cesg.gov.uk/site/ast/biometrics/media/BiometricTestReportpt1.pdf

[46] P.J. Phillips, P. Grother, R.J Micheals, D.M. Blackburn, E Tabassi,
and J.M. Bone, “Face Recognition Vendor Test 2002” FRVT.org
URL: http://www.frvt.org/DLs/FRVT_2002_Evaluation_Report.pdf

[47] International Organization for Standardization, “Information technology -- JPEG 2000 image coding system: Conformance testing” ISO/IEC 15444-4:2004
URL:
http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=39079&ICS1=35&ICS2=40&ICS3=&scopelist=

[48] International Organization for Standardization, “Standardization and related activities -- General vocabulary” ISO/IEC Guide 2:2004
URL: http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=39976

[49] National Institute of Standards and Technology, “Metrology for Information Technology (IT)” NISTIR 6025

URL: http://www.itl.nist.gov/lab/nistirs/ir6025.htm

[50] P. Phoorivatana and P. Bhattarakosol, A High Qualification Biometric for Mobile Intruder Detection: presented at 8th International Conference on e-Business (iNCEB2009), Bangkok, Thailand, 28-30 October, 2009

[51] “History of Biometrics”, Biometric.gov

URL:www.biometrics.gov/documents/biofoundationdocs.pdf

[52] Eric Jukes, (2008)”Encyclopedia of Multimedia: (2nd ed.)", Reference Reviews, Vol. 24 Iss: 1, pp.50 – 51

VITAE

In 2000, Mister Premchai Phoorivatana graduated in Business Information Technology from Chulalongkorn University, Bangkok, Thailand

Publication

Phoorivatana, P., and Bhattarakosol, P., “A High Qualification Biometric for Mobile Intruder Detection” Proceedings of 8th International Conference on e-Business (iNCEB2009), October 28th-30th, 2009